Wireless Controller and Service Platform

WiNG 5.9.5 System Reference Guide

9036314-00 Rev AA

Published June 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..6
Text Conventions..6
Platform-Dependent Conventions..6
Providing Feedback to Us..7
Getting Help..7
Documentation and Training..8

Chapter 1: About this Guide..9
Notational Conventions..9

Chapter 2: Overview..10
About the WiNG Software..10

Chapter 3: Web UI Features..13
Accessing the Web UI..13
Glossary of Icons Used..14

Chapter 4: Dashboard..20
Summary..20
System Screen..22
RF Domain Screen..25
Controller Screen..30
Access Point Screen..34
Network View..38
Debug Wireless Clients..40
Debug Captive Portal Clients..42
Packet Capture..44

Chapter 5: Device Configuration..46
Device Configuration..47
Auto-Provisioning Policies..315
Managing an Event Policy..323
Managing MINT Policies..325
Password Encryption..325

Chapter 6: Wireless Configuration..328
Wireless LAN Policies..329
WLAN QoS Policies..378
Radio QoS Policies..392
Association ACL..403
Smart RF Policies..406
MeshConnex Policies..421
Mesh QoS Policy..428
Passpoint Policy..435
Sensor Policy..446
Location Policy..449

Chapter 7: Network Configuration..453
Policy Based Routing (PBR)..454
L2TP V3 Configuration..458

Crypto CMP Policy....................462
AAA Policy....................465
AAA TACACS Policy....................476
IPv6 Router Advertisment Policy....................481
Border Gateway Protocol (BGP)....................485
Alias....................498
Application Policy....................506
Application....................509
Application Group....................511
Schedule Policy....................513
URL Filtering....................514
Web Filtering....................518
Configuring EX3500 QoS Class....................519
Configuring EX3500 QoS Policy Map....................523
Network Deployment Considerations....................527

Chapter 8: Manage Profiles....................528
General Profile Configuration....................531
Profile Cluster Configuration (Controllers Only)....................533
Profile Adoption Configuration (Access Points Only)....................535
Profile Adoption Configuration (Controllers Only)....................537
Access Point Radio Power Overrides (AP7161 Only)....................539
Profile 802.1x Configuration....................540
Profile Interface Configuration....................541
Profile Network Configuration....................607
Profile Security Configuration....................676
VRRP Configuration....................712
Critical Resources Configuration....................716
Profile Services Configuration....................719
Profile Management Configuration....................723
Profile Mesh Point Configuration....................729
Environmental Sensor Configuration (AP8132 Only)....................736
Advanced Profile Configuration....................737

Chapter 9: RF Domains....................747
Managing RF Domains....................748

Chapter 10: Security Configuration....................771
Wireless Firewall....................771
Configuring IP Firewall Rules....................789
Wireless Client Roles....................803
Device Fingerprinting....................811
Intrusion Prevention....................816
EX3500 Time Range....................830

Chapter 11: Services Configuration....................834
Captive Portal Policies....................834
Setting the Guest Management Configuration....................848
Setting the DHCP Configuration....................858
Setting the Bonjour Gateway Configuration....................874
Setting the DHCPv6 Server Policy....................878
Setting the RADIUS Configuration....................884

Setting the URL List....899
Setting the Imagotag Policy....900

Chapter 12: Management Access.... 904
Viewing Management Access Policies....904
Adding or Editing a Management Access Policy.... 906
EX3500 Management Policies....924
Configuring a Hierarchical Tree....938
Management Access Deployment Considerations.... 942

Chapter 13: Diagnostics.... 943
Fault Management....943
Crash Files....947
Advanced.... 948

Chapter 14: Operations.... 952
Device Operations....952
Certificates....973
Smart RF.... 991

Chapter 15: Statistics....995
System Statistics....996
RF Domain Statistics.... 1009
Controller Statistics....1060
EX3500 Interface Extended IF....1211
Access Point Statistics.... 1211
Wireless Client Statistics....1334
Guest Access Statistics....1346

Chapter 16: WiNG Events.... 1357
WiNG Event Messages....1357

Glossary.... 1374

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

Notational Conventions

This manual supports the following access points, wireless controllers and service platforms:

- Access Points — AP7502, AP7522, AP7532, AP7562, AP7602, AP7612, AP7622, AP7632, AP7662, AP8163, AP8432, AP8533
- Wireless Controllers — RFS4010
- Service Platforms — NX5500, NX7500, NX9500, NX9510, NX9600, VX9000,

Note

In this document:

- NX9500 and NX9510 are collectively referred to as NX9500.
- AP7502, AP7522, AP7532 and AP7562 are collectively referred to as AP75XX.
- AP7602, AP7612, AP7622, AP7632 and AP7662 are collectively referred to as AP76XX.

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 Overview

About the WiNG Software

About the WiNG Software

Extreme Networks' WiNG 5 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 5 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.

WiNG 5 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 5 advances the following technology:

Comprehensive Wi-Fi support - WiNG supports all Wi-Fi protocols, including 802.11a/b/g/n/ac, 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 5 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 *network operating center* (NOC) 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 DPI *(Deep Packet Inspection)* 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 (a separate target starting with WiNG 5.9.3). 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 5 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

WiNG 5 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 5 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-andspoke architecture can't stop threats until they reach the controller inside your network, WiNG 5 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

WiNG 5 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* (TCO). 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

WiNG's comprehensive end-to-end management capabilities cover 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 WiNG software contains a Web UI allowing network administrators to manage and view access point, controller and service platform settings, configuration data and status. This *Graphical User Interface* (GUI) allows full control of all administration features.

Access points, controllers and service platforms also share a *Command Line Interface* (CLI) for managing and viewing settings, configuration and status. For more information on the command line interface and a full list of available commands, refer to the Wireless Services CLI Reference Guide available at www.extremenetworks.com/support.

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

- Accessing the Web UI on page 13.
- Glossary of Icons Used on page 14.

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), wireless controller or service platform's Web UI for the first time:

1. Connect one end of an Ethernet cable to a LAN port on the front of the controller or service platform 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.
3. Once the computer has an IP address, point the browser to: https://192.168.0.1/ and the following login screen will display.

   The Web UI login dialog displays:

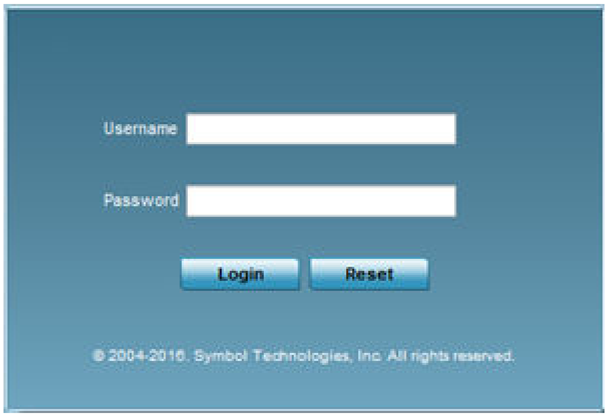


Figure 1: Web UI Login Screen

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.

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	*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	*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 Dashboard

Summary
System Screen
RF Domain Screen
Controller Screen
Access Point Screen
Network View
Debug Wireless Clients
Debug Captive Portal Clients
Packet Capture

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.

The dashboard provides the following tools and diagnostics:

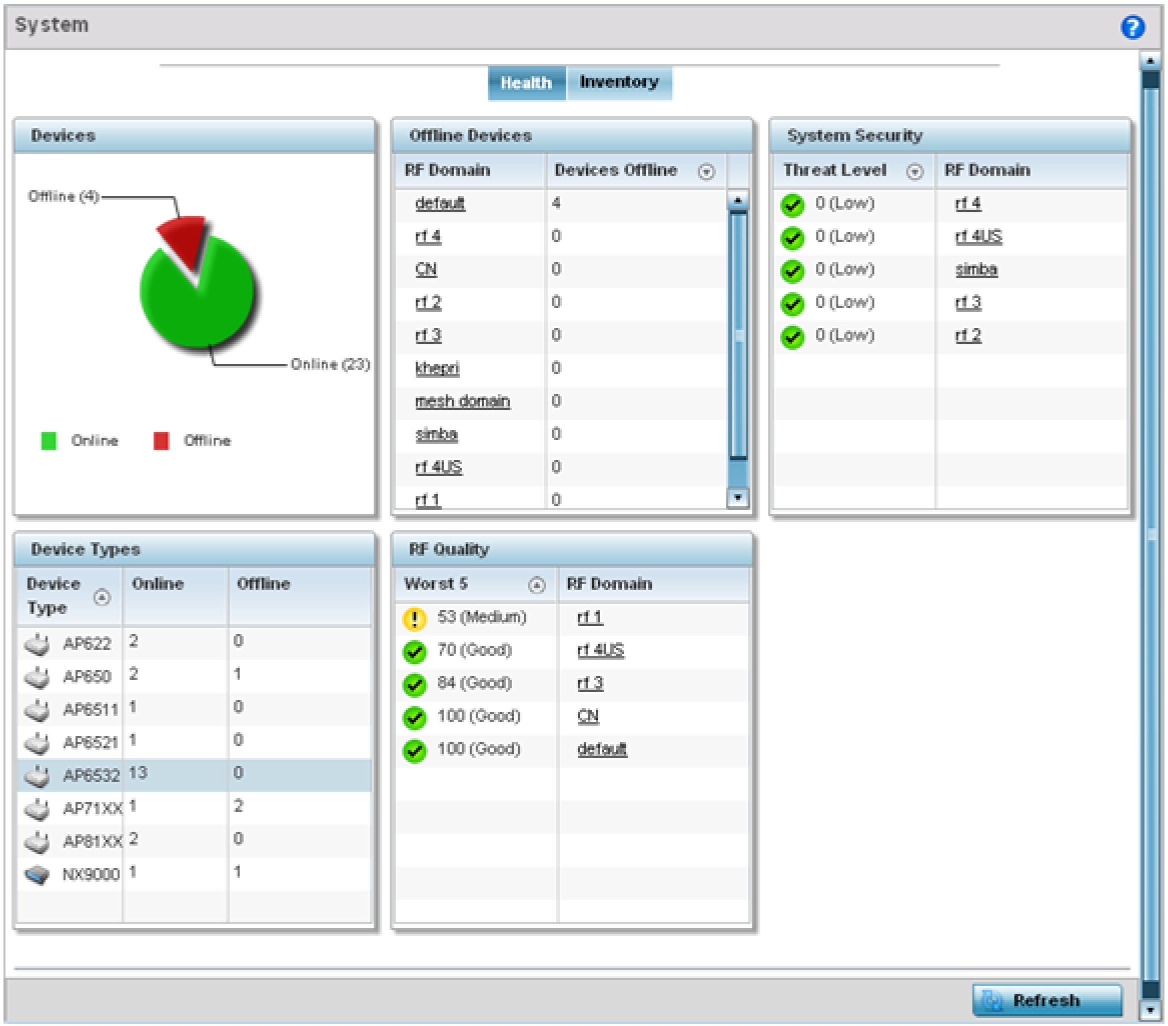
- Summary on page 20
- System Screen on page 22
- RF Domain Screen on page 25
- Controller Screen on page 30
- Access Point Screen on page 34
- Network View on page 38
- Debug Wireless Clients on page 40
- Debug Captive Portal Clients on page 42
- Packet Capture on page 44

Summary

The Dashboard displays information organized by device association and inter-connectivity between connected access points and wireless clients.

1 To review dashboard information, select **Dashboard**.

The **Summary** → **System** → **Health** tab is displayed by default.



Offline Devices

RF Domain	Devices Offline
default	4
rf 4	0
CN	0
rf 2	0
rf 3	0
khepri	0
mesh domain	0
simba	0
rf 4US	0
rf 1	0

System Security

Threat Level	RF Domain
✓ 0 (Low)	rf 4
✓ 0 (Low)	rf 4US
✓ 0 (Low)	simba
✓ 0 (Low)	rf 3
✓ 0 (Low)	rf 2

Device Types

Device Type	Online	Offline
AP622	2	0
AP650	2	1
AP6511	1	0
AP6521	1	0
AP6532	13	0
AP71XX	1	2
AP81XX	2	0
NX9000	1	1

RF Quality

Worst 5	RF Domain
! 53 (Medium)	rf 1
✓ 70 (Good)	rf 4US
✓ 84 (Good)	rf 3
✓ 100 (Good)	CN
✓ 100 (Good)	default

Figure 2: Dashboard Screen - Health Tab

Device Listing

The device menu displays information as a hierarchical tree, where each node is a RF Domain. Each RF Domain is populated by the specific model access points or controllers.

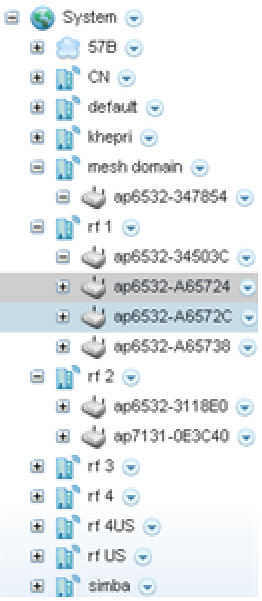


Figure 3: Dashboard Menu Tree

The **Search** option, at the bottom of the screen, enables administrators to filter (search among) RF Domains.

System Screen

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

- Health – The Health tab displays information about the state of the WiNG device managed wireless network.
- Inventory– The Inventory tab displays information on the physical devices managed within the WiNG wireless network.

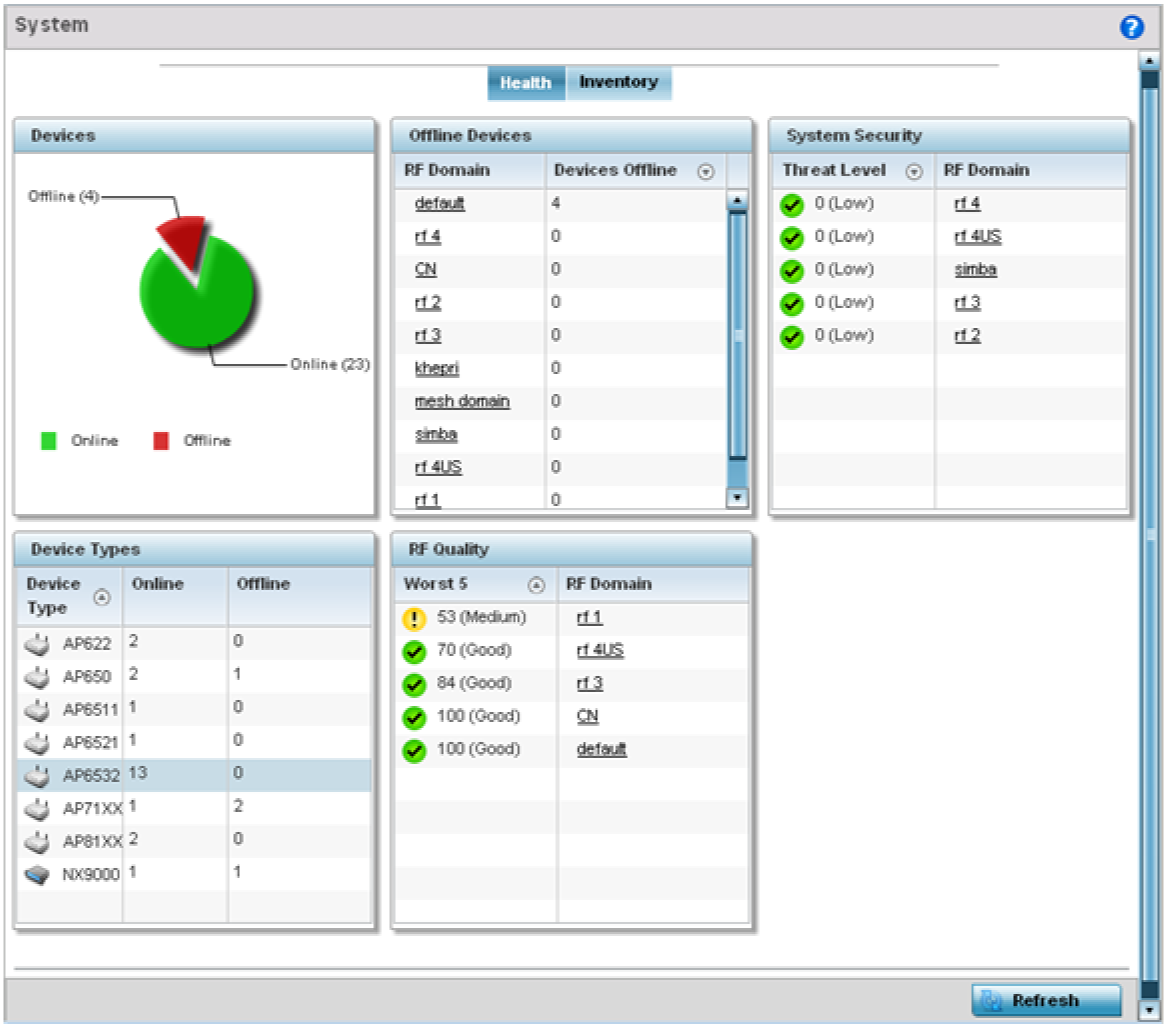
System Health

The System screen's 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.



Offline Devices

RF Domain	Devices Offline
default	4
rf 4	0
CN	0
rf 2	0
rf 3	0
khepri	0
mesh domain	0
simba	0
rf 4US	0
rf 1	0

System Security

Threat Level	RF Domain
✓ 0 (Low)	rf 4
✓ 0 (Low)	rf 4US
✓ 0 (Low)	simba
✓ 0 (Low)	rf 3
✓ 0 (Low)	rf 2

Device Types

Device Type	Online	Offline
AP622	2	0
AP650	2	1
AP6511	1	0
AP6521	1	0
AP6532	13	0
AP71XX	1	2
AP81XX	2	0
NX9000	1	1

RF Quality

Worst 5	RF Domain
! 53 (Medium)	rf 1
✓ 70 (Good)	rf 4US
✓ 84 (Good)	rf 3
✓ 100 (Good)	CN
✓ 100 (Good)	default

Figure 4: Dashboard Screen - Health Tab

The Health screen is partitioned into the following fields:

- 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.

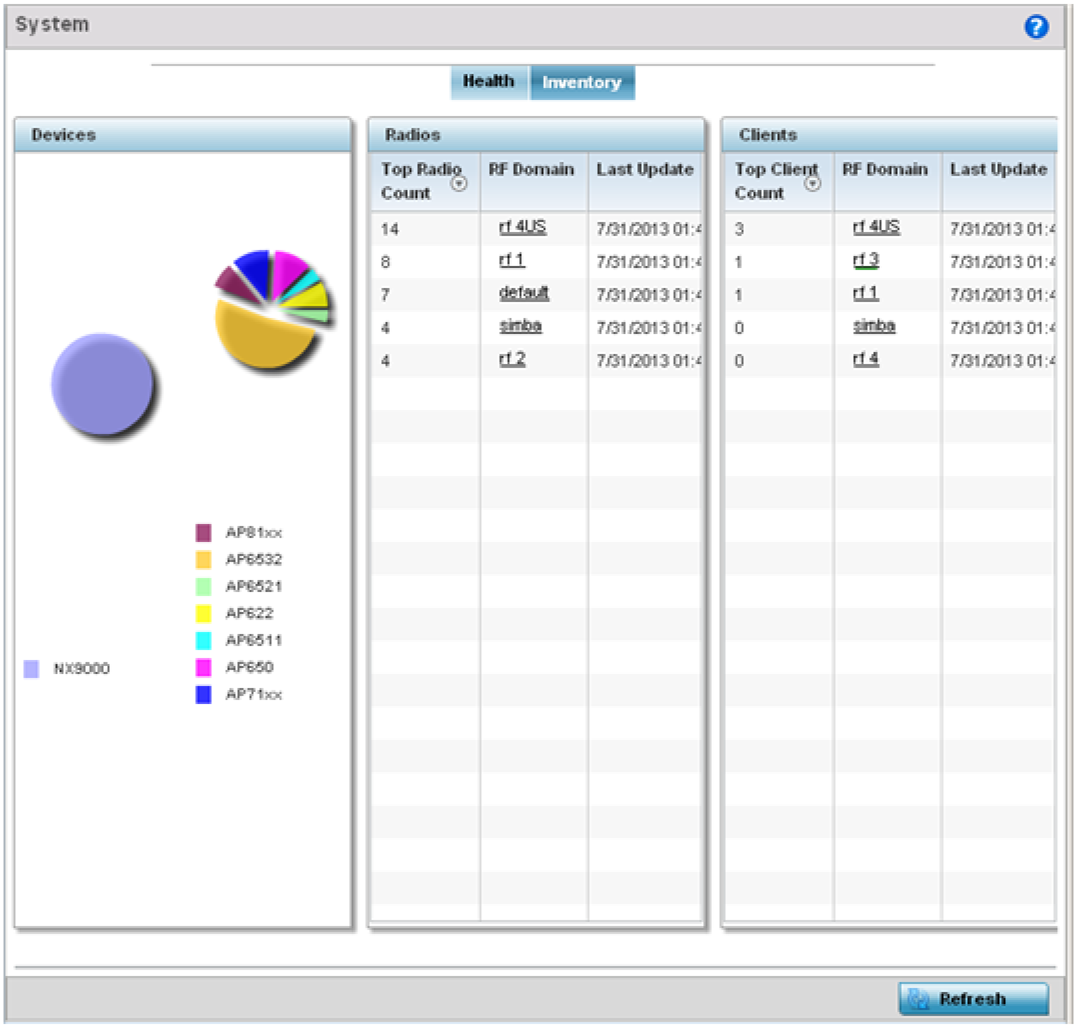
The quality is measured as:
  - 0-20 - Very poor quality
  - 20-40 - Poor quality
  - 40-60 - Average quality
  - 60-100 - Good quality
- The System Security field displays RF intrusion prevention stats and their associated threat level. The greater the number of unauthorized devices, the greater the 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.

To assess the system inventory:

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



Radios

Top Radio Count	RF Domain	Last Update
14	rf 4US	7/31/2013 01:4
8	rf 1	7/31/2013 01:4
7	default	7/31/2013 01:4
4	simba	7/31/2013 01:4
4	rf 2	7/31/2013 01:4

Clients

Top Client Count	RF Domain	Last Update
3	rf 4US	7/31/2013 01:4
1	rf 3	7/31/2013 01:4
1	rf 1	7/31/2013 01:4
0	simba	7/31/2013 01:4
0	rf 4	7/31/2013 01:4

Figure 5: System Screen - Inventory Tab

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 Screen

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:

Default RF domain	Automatically assigned to each controller or service platform and associated access point by default.
User Defined RF domains	Created by administrators and manually assigned to individual controller or service platforms, but can be automatically assigned to access points using adoption policies.

Each controller and service platform is assigned to only one RF domain at a time. However, a user defined RF domain can be assigned to multiple controllers or service platforms as required. User defined RF domains can be manually assigned or automatically assigned to access points using an AP provisioning policy.

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

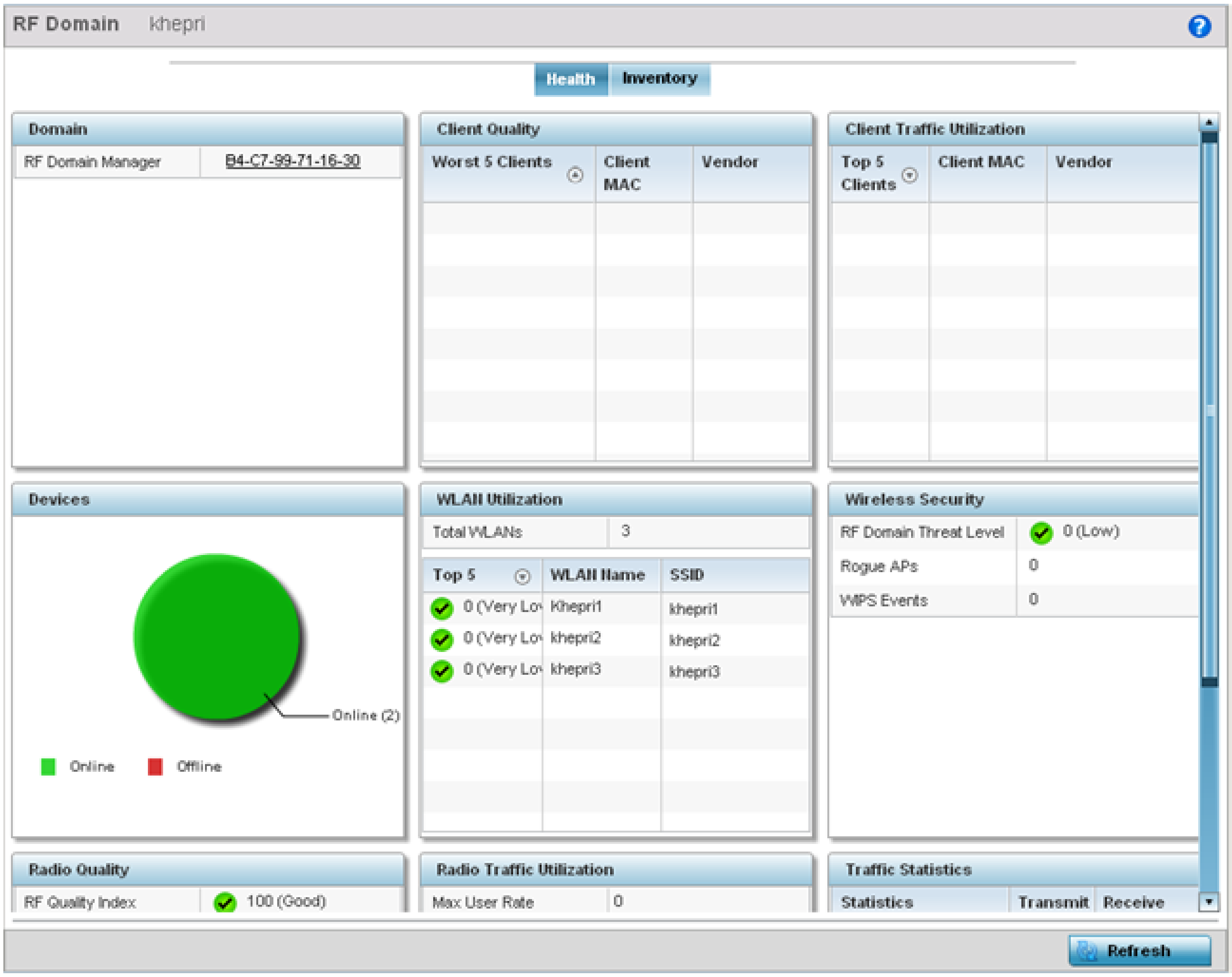
- RF Domain Health – The **Health** tab displays information about the state of the RF domain and network performance as tallied from its collective device members.
- RF Domain Inventory – The **Inventory** tab displays information on the physical devices comprising the RF domain.

RF Domain Health

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



Domain

RF Domain Manager	B4-C7-99-71-16-30

Client Quality

Worst 5 Clients	Client MAC	Vendor

Client Traffic Utilization

Top 5 Clients	Client MAC	Vendor

Devices

WLAN Utilization

Total WLANs	3

Top 5	WLAN Name	SSID
✓ 0 (Very Lo	Khepri1	khepri1
✓ 0 (Very Lo	khepri2	khepri2
✓ 0 (Very Lo	khepri3	khepri3

Wireless Security

RF Domain Threat Level	✓ 0 (Low)
Rogue APs	0
WIPS Events	0

Radio Quality

RF Quality Index	✓ 100 (Good)

Radio Traffic Utilization

Max User Rate	0

Traffic Statistics

Statistics	Transmit	Receive

Figure 6: RF Domain Screen - Health Tab

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.
- 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.

- The **Client Quality** table 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.

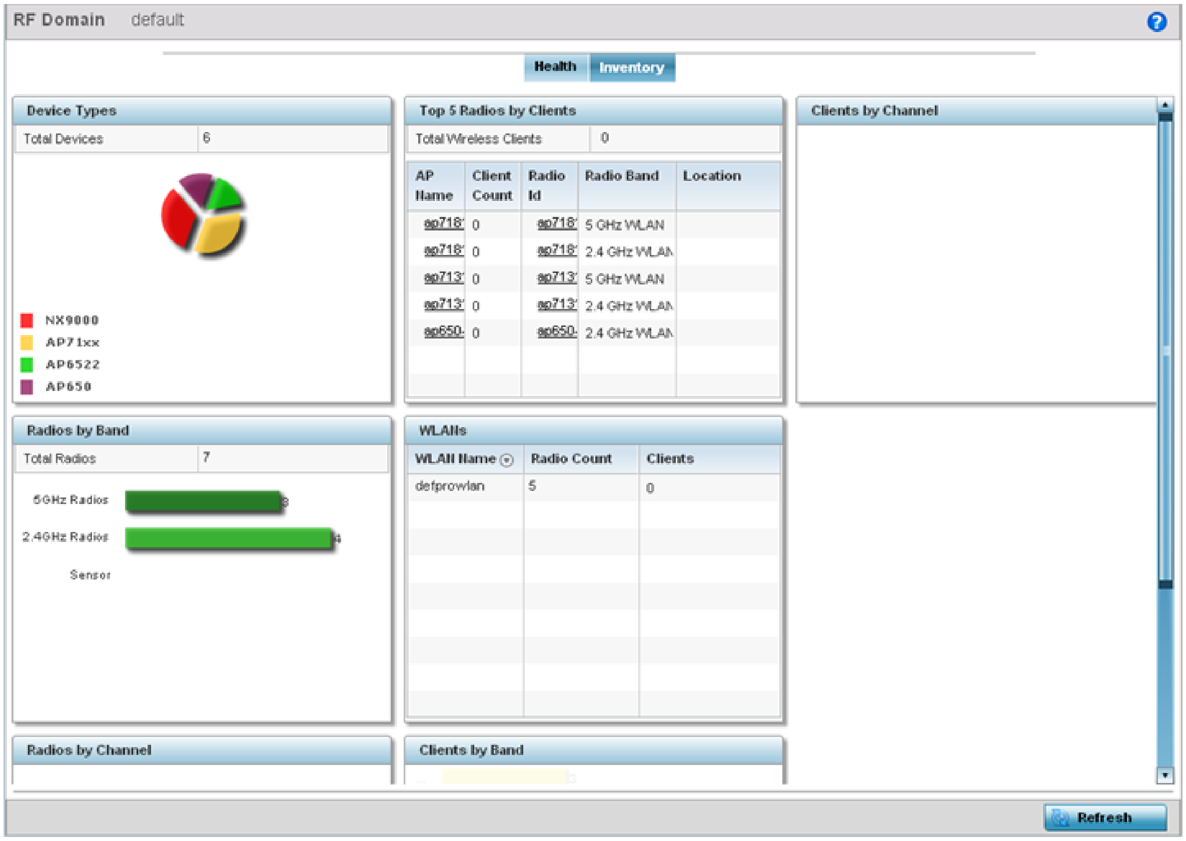
- **WLAN Utilization** displays how efficiently the WLANs are used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the WLAN. The total number of WLANs is displayed above the table. The table displays a list of the top five WLANs in terms of overall traffic utilization. It displays the utilization level names, WLAN name and SSIDs for each of the top five WLANs.
- **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.
- **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.
- **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.
- **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 **Dashboard** → **Summary**.
2. Expand the **System** node to display RF domains.
3. Select an RF domain. The Health tab displays by default
4. Select the **Inventory** tab.



Total Devices	6

Total Wireless Clients	0

AP Name	Client Count	Radio Id	Radio Band	Location
ap718	0	ap718	5 GHz WLAN	
ap718	0	ap718	2.4 GHz WLAN	
ap713	0	ap713	5 GHz WLAN	
ap713	0	ap713	2.4 GHz WLAN	
ap650-	0	ap650-	2.4 GHz WLAN	

Total Radios	7

WLAN Name	Radio Count	Clients
defprowlan	5	0

Figure 7: RF Domain Screen - Inventory Tab

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.

Controller Screen

The Wireless Controller screen displays system collected network status for controllers and service platforms. The screen is partitioned into two tabs:

- Wireless Controller Health– The Health tab displays information about the state of the controller or service platform managed wireless network.
- Wireless Controller Inventory– The Inventory tab displays information on the physical devices managed by the controller or service platform.

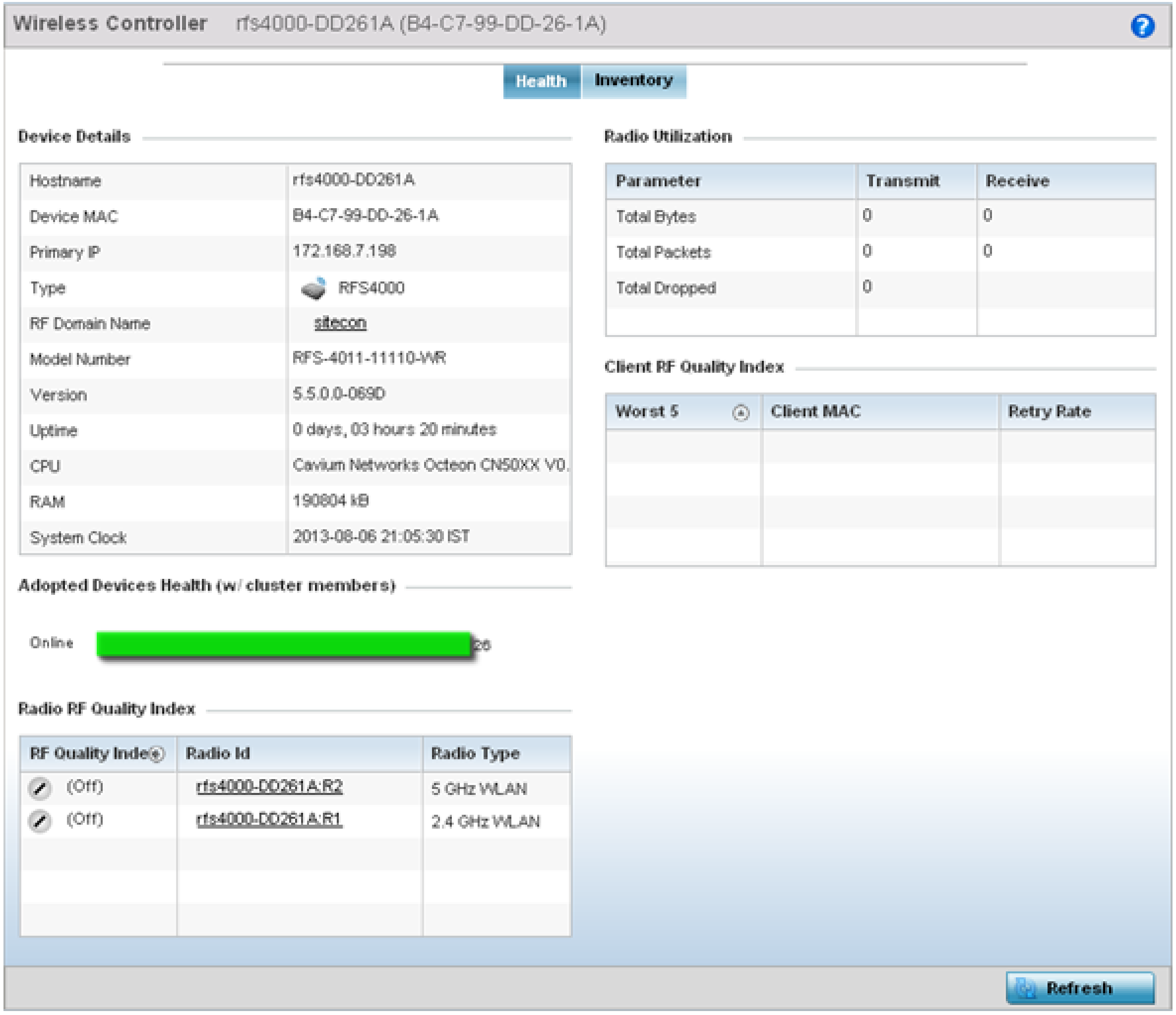
Note

T5 controller can also be selected from the dashboard's controller level to display a set of unique T5 dashboard screens. A T5 controller uses a different operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. For information on enabling controller adoption of external devices (for T5 support specifically) refer to Controller Adoption Overrides (Controllers Only) on page 93.

Controller Health

To assess the controller or service platform's network health:

1. Select **Dashboard** → **Summary**.
2. Expand the **System** node to display RF domains.
3. Select and expand an RF domain to expose its member controllers or service platforms.
4. Select a controller or service platform. The Health tab displays by default.



Wireless Controller rfs4000-DD261A (B4-C7-99-DD-26-1A)

Device Details

Hostname	rfs4000-DD261A
Device MAC	B4-C7-99-DD-26-1A
Primary IP	172.168.7.198
Type	RFS4000
RF Domain Name	sitecon
Model Number	RFS-4011-11110-WR
Version	5.5.0.0-069D
Uptime	0 days, 03 hours 20 minutes
CPU	Cavium Networks Octeon CN50XX V0.
RAM	190804 kB
System Clock	2013-08-06 21:05:30 IST

Adopted Devices Health (w/ cluster members)

Online 26

Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type
(Off)	rfs4000-DD261A:R2	5 GHz WLAN
(Off)	rfs4000-DD261A:R1	2.4 GHz WLAN

Radio Utilization

Parameter	Transmit	Receive
Total Bytes	0	0
Total Packets	0	0
Total Dropped	0	

Client RF Quality Index

Worst 5	Client MAC	Retry Rate

Figure 8: Wireless Controller Screen - Health Tab

Refer to the following to assess the overall health of the controller and its adopted devices:

- The Device Details table provides the following information:
  - Hostname - Lists the administrator assigned name of the controller or service platform.
  - Device MAC - Lists the factory encoded MAC address of the controller or service platform.
  - Type - Indicates the type of controller or service platform. An icon representing the RFS controller or NX service platform device type is displayed along with the model number.
  - RF Domain Name - Lists the RF domain to which the controller or service platform belongs. The RF Domain displays as a link that's selectable to display RF Domain data in greater detail.
  - Model Number - Lists the model number and hardware SKU information of the selected controller or service platform to refine its intended deployment region.
  - Version - Lists the firmware version currently running on the controller or service platform. Compare this version against the version currently on the support site to ensure the controller or service platform has the latest feature set available.
  - Uptime - Displays the duration the controller or service platform has been running since it was last restarted.
  - CPU - Displays the CPU installed on this controller or service platform.

  - RAM - Displays the amount of RAM available for use in this system.
  - System Clock - Displays the current time set on the controller or service platform.
- The Adopted Devices Health (w/ cluster members) field displays a graph of access points in the system with the available access points in green and unavailable access points in red.
- The Radio RF Quality Index table provides 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 connect rate in both directions, the retry rate and the error rate. The screen displays the average quality index within the access point single radio. The table lists the bottom five (5) of the RF quality values by access point radio. 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 statistics in greater detail.
- The Radio Utilization table displays how efficiently the RF medium is used. Radio utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the radio. Use this table to assess access point radios in terms of the number of associated wireless clients and the percentage of utilization. It also displays a table of packets types transmitted and received.
- The Client RF Quality Index table displays a table of RF quality on a per client basis. 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. This area of the screen displays the average quality index for a client. The table lists the bottom five (5) of the RF quality values by a client. 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 MAC** to view all the statistics for the selected client in greater detail.

Controller Inventory

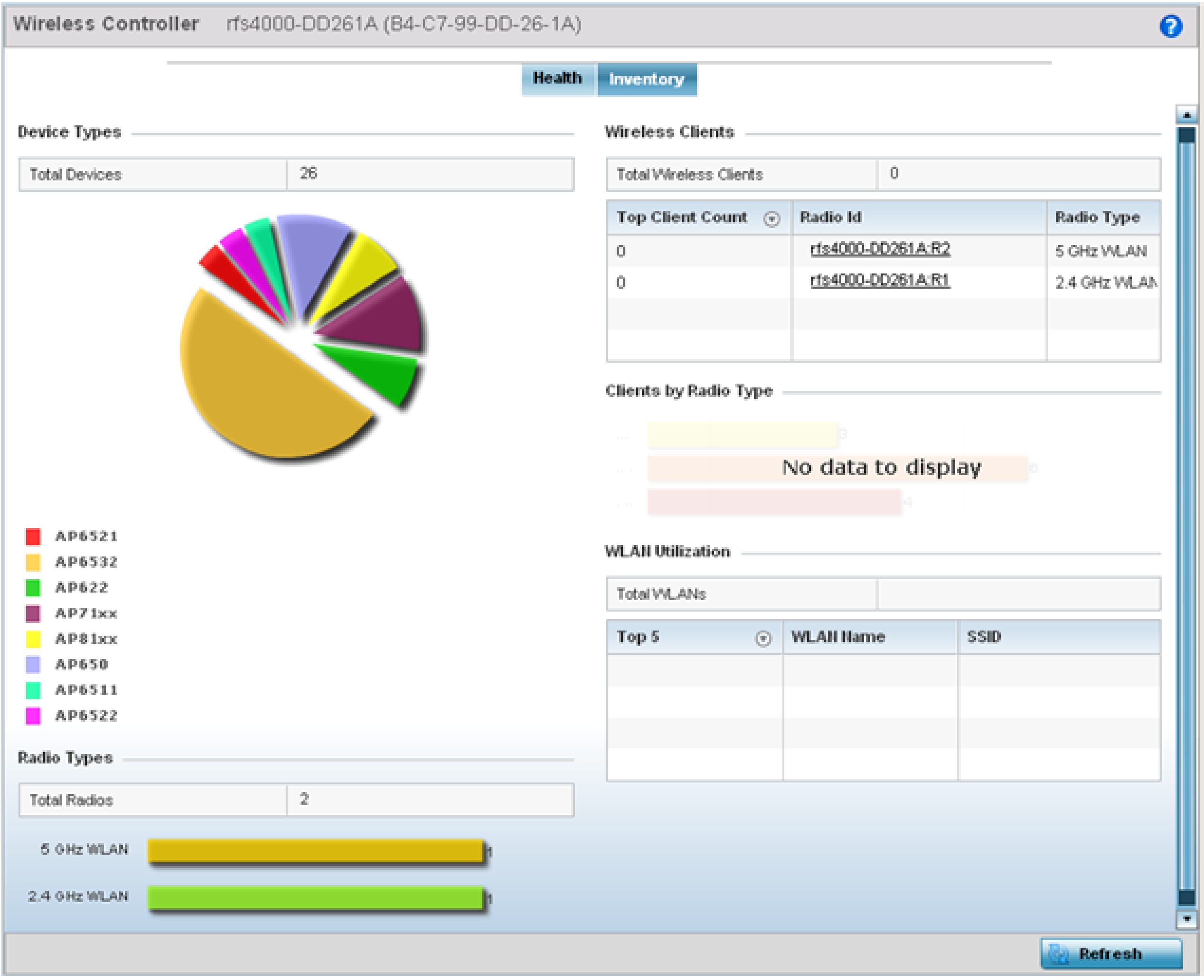
The Inventory tab displays information for the devices managed by the system. This screen enables a system administrator to have a complete overview of the number and state of managed devices. Information is displayed in easy to read tables and graphs. The Inventory screen also provides links for the system administrator to get detailed information.

To assess the controller or service platform inventory:

1. Select **Dashboard** → **Summary**.
2. Expand the **System** node to display RF domains.
3. Select and expand an RF domain to expose its member controllers or service platforms.

4 Select a controller or service platform. The Health tab displays by default.

5 Select the **Inventory** tab.



Total Devices	26

Total Radios	2

Total Wireless Clients	0

Top Client Count	Radio Id	Radio Type
0	rfs4000-DD261A:R2	5 GHz WLAN
0	rfs4000-DD261A:R1	2.4 GHz WLAN

Total WLANs	

Top 5	WLAN Name	SSID

Figure 9: Wireless Controller Screen - Inventory Tab

Refer to the following Inventory data:

- The Device Types field displays a ratio of devices managed by this controller or service platform in pie chart format. The Device Type area displays an exploded pie chart that displays the type of device and their numbers in the current system.
- The Radios Type field displays the total number of radios managed by this controller or service platform. The graph lists the number of radios in both the 2.4 GHz and 5 GHz radio bands.
- The Wireless Clients table lists clients managed by this controller or service platform by connected client count. Information is presented in two (2) tables and a graph. The first table lists the total number of clients managed by the listed controller or service platform. 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.
- The WLAN Utilization table displays utilization statistics for controller or service platform WLAN configurations. Information displays in two tables. 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 the name and network identifying SSID.

Access Point Screen

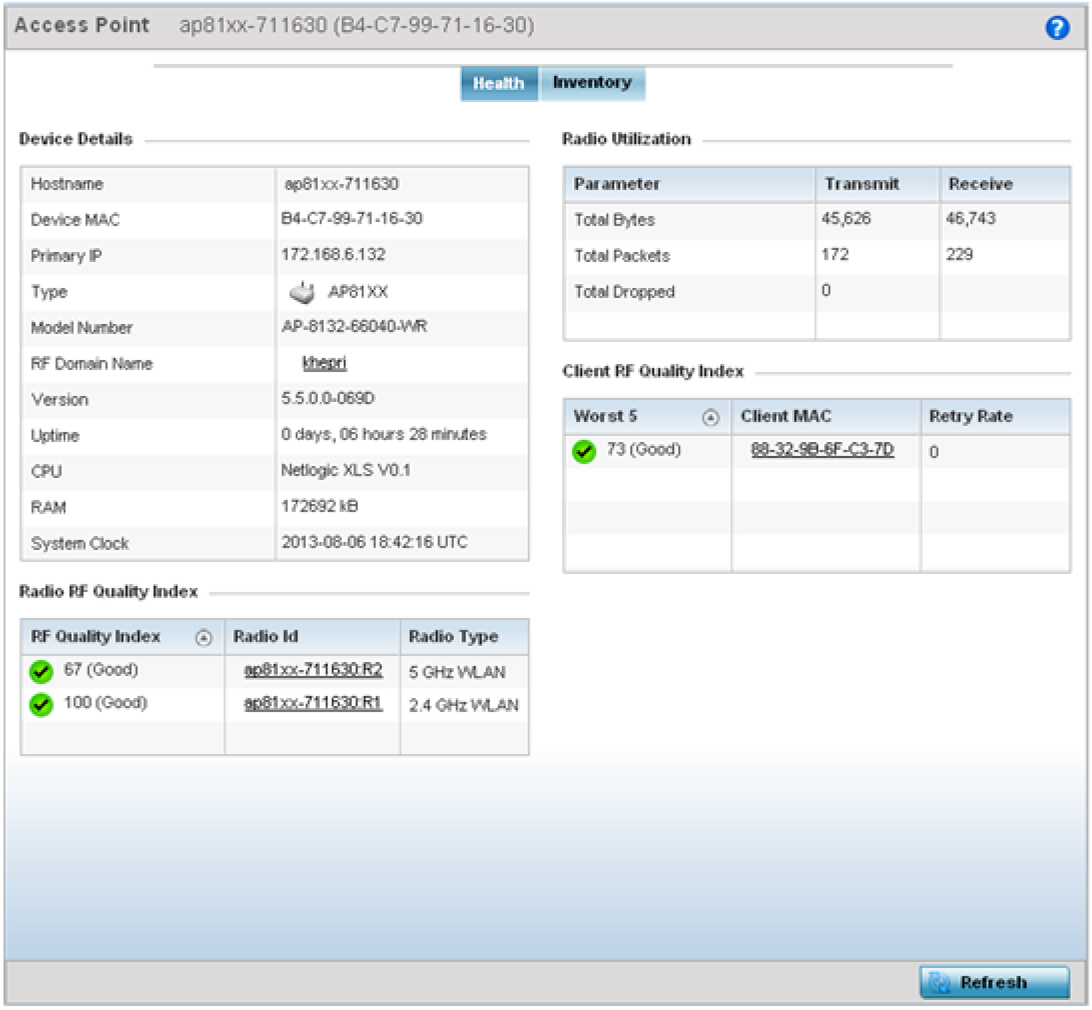
The Access Point screen displays system-wide network status for standalone or controller-connected access points. The screen is partitioned into the following tabs:

- Access Point Health – The Health tab displays information about the state of the access point managed network.
- Access Point Inventory – 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. Select and expand an RF domain to expose its member controllers or service platforms.
4. Select a controller or service platform and expand the menu item to display connected access points.
5. Select an access point. The Health tab displays by default.



ap81xx-711630 (B4-C7-99-71-16-30)

Device Details

Hostname	ap81xx-711630
Device MAC	B4-C7-99-71-16-30
Primary IP	172.168.6.132
Type	AP81XX
Model Number	AP-8132-66040-WR
RF Domain Name	khepri
Version	5.5.0.0-069D
Uptime	0 days, 06 hours 28 minutes
CPU	Netlogic XLS V0.1
RAM	172692 kB
System Clock	2013-08-06 18:42:16 UTC

Radio Utilization

Parameter	Transmit	Receive
Total Bytes	45,626	46,743
Total Packets	172	229
Total Dropped	0	

Client RF Quality Index

Worst 5	Client MAC	Retry Rate
✓ 73 (Good)	88-32-9B-6F-C3-7D	0

Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type
✓ 67 (Good)	ap81xx-711630:R2	5 GHz WLAN
✓ 100 (Good)	ap81xx-711630:R1	2.4 GHz WLAN

Figure 10: Access Point Screen - Health Tab

The access point Health screen displays 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

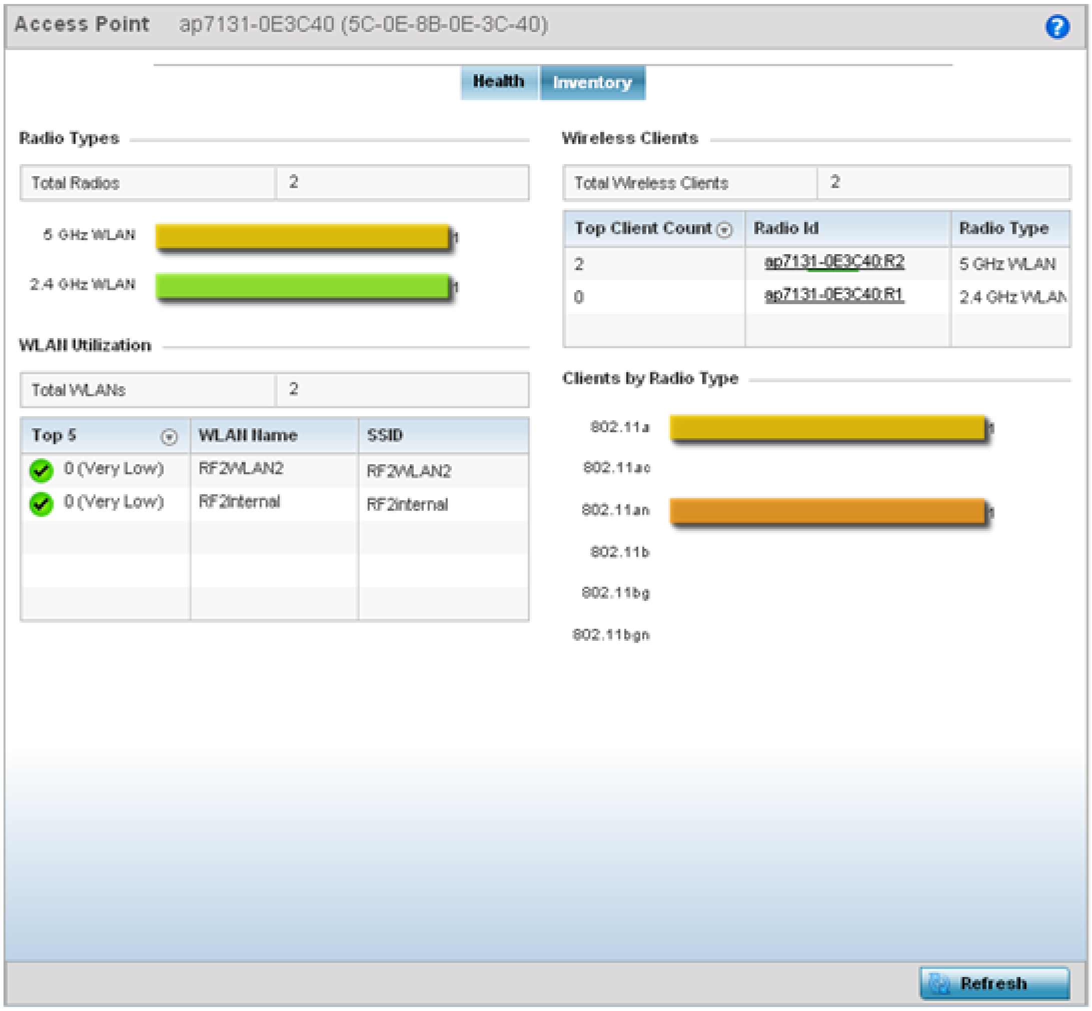
  Periodically select **Refresh** (at the bottom of the screen) to update client RF quality.

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 **Dashboard** → **Summary**.
2 Expand the **System** node to display RF domains.
3 Select and expand an RF domain to expose its member controllers or service platforms.
4 Select a controller or service platform and expand the menu item to display connected access points.
5 Select an access point. The Health tab displays by default.
6 Select the **Inventory** tab.



Access Point ap7131-0E3C40 (5C-0E-8B-0E-3C-40)

Radio Types

Total Radios	2

WLAN Utilization

Total WLANs	2

Top 5	WLAN Name	SSID
✓ 0 (Very Low)	RF2WLAN2	RF2WLAN2
✓ 0 (Very Low)	RF2Internal	RF2internal

Wireless Clients

Total Wireless Clients	2

Top Client Count	Radio Id	Radio Type
2	ap7131-0E3C40:R2	5 GHz WLAN
0	ap7131-0E3C40:R1	2.4 GHz WLAN

Clients by Radio Type

Figure 11: Access Point Screen - Inventory Tab

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

- 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

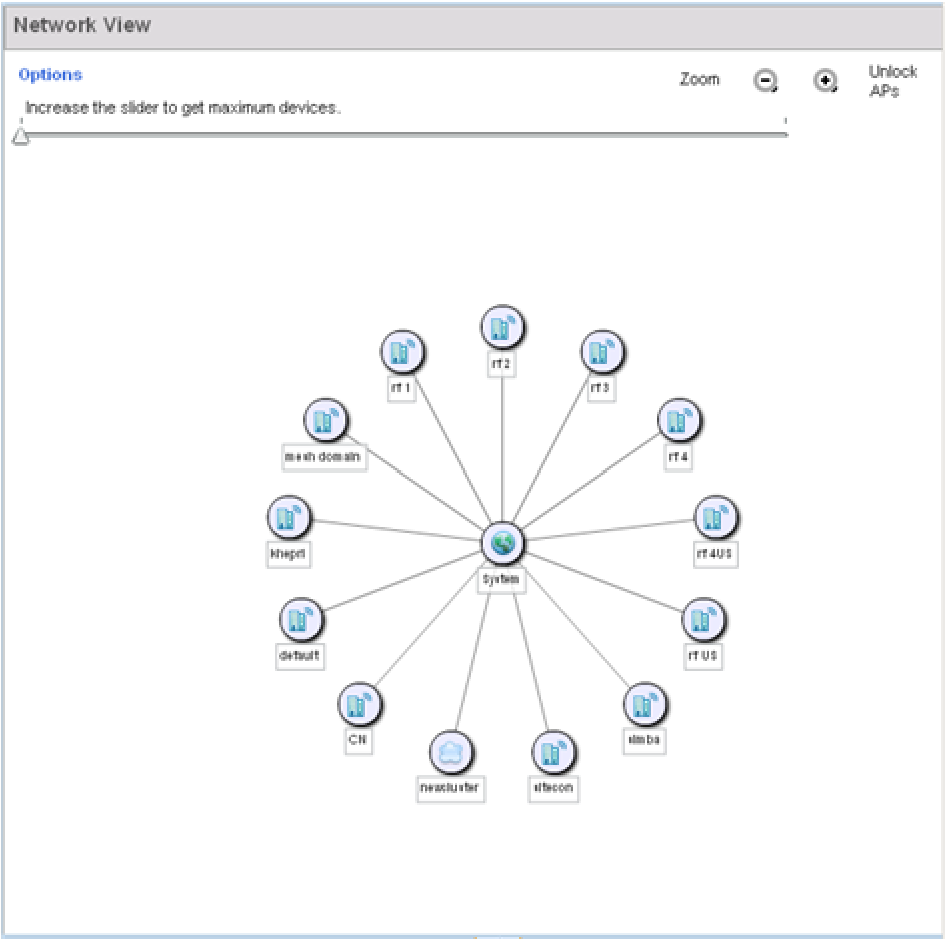
Periodically select **Refresh** (at the bottom of the screen) to update WLAN utilization information.

- 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 association connectivity among wireless controllers, service platforms, access points, and wireless clients. This association is represented by a number of different graphs. Use this view to assess whether controllers and access point radios are properly deployed in areas where high volumes of client traffic are anticipated.

To review the Network Topology, select **Dashboard** → **Network View**.



Increase the slider to get maximum devices.

Figure 12: Network View Topology

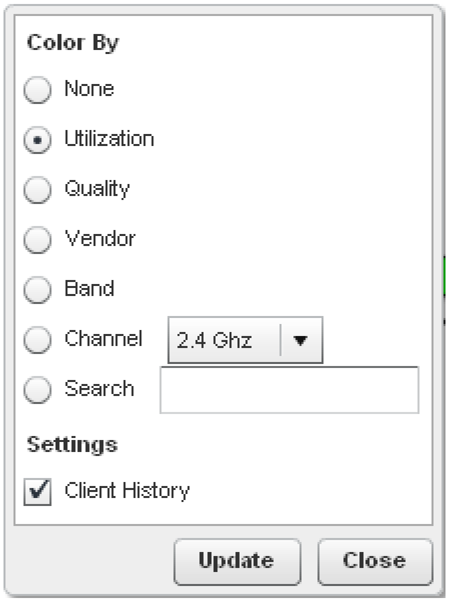
The screen displays icons for the different views available to the system. Apart from device specific icons, the following three icons are available:

- *default* – Displays information about the default RF Domain.
- *system* – Displays information about the current system.
- *cluster* – Displays information about clusters managed by this system.

Use these icons to navigate quickly within top level groupings.

The middle field displays a Network View, or graphical representation of the network. Nodes display whether or not they are members of a cluster or mesh domain. Use this information to assess whether the topology of the network has changed in such a manner that devices need to be added or moved. This field changes to display a graphical network map.

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



Color By

○ None

● Utilization

○ Quality

○ Vendor

○ Band

○ Channel 2.4 Ghz

○ Search

Settings

☑ Client History

Figure 13: Network View - Display Options

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.

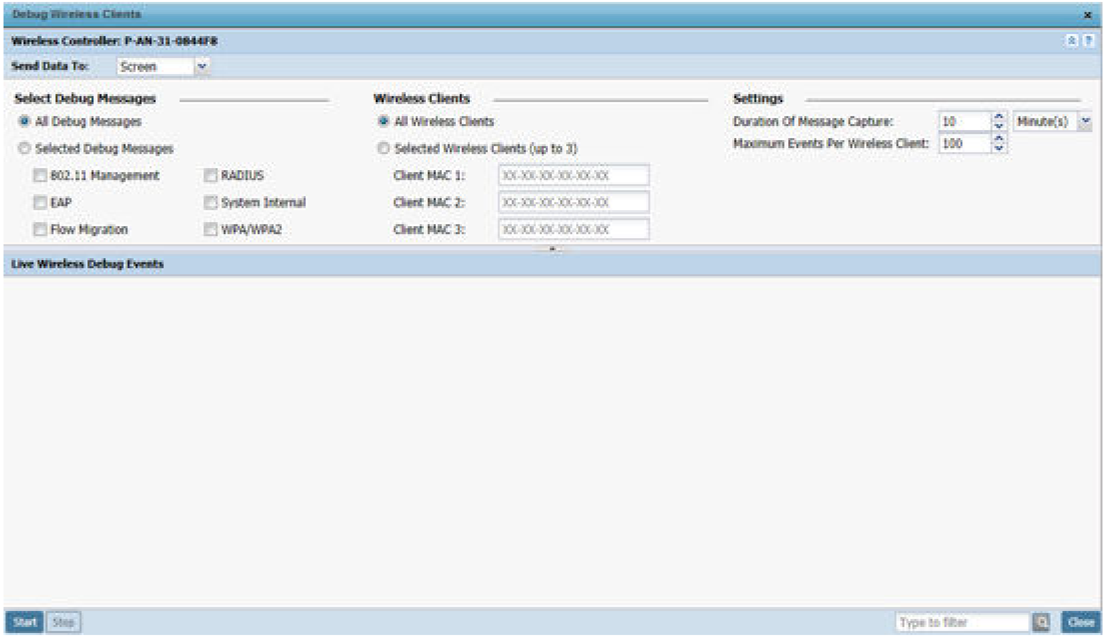
Use the **Lock / Unlock** icon in the upper right of the screen to prevent users from moving APs around within the specified area.

Debug Wireless Clients

An administrator has the ability to select an RF domain and capture connected client debug messages at an administrator assigned interval and location. Client debug information can either be collected historically or in realtime.

To troubleshoot issues with wireless client connectivity within a controller, service platform or access point managed RF domain:

1 Go to **Dashboard** → **System** to display managed RF domains.
2 Select and expand an RF domain and click on the down arrow to the right of the RF domain's name.
3 Select **Troubleshooting**.
4 Select **Debug Wireless Clients**.



Wireless Controller: P-AN-31-0844F8
Send Data To: Screen
● All Debug Messages
○ Selected Debug Messages
● All Wireless Clients
○ Selected Wireless Clients (up to 3)
Client MAC 1: XX-XX-XX-XX-XX-XX
Client MAC 2: XX-XX-XX-XX-XX-XX
Client MAC 3: XX-XX-XX-XX-XX-XX
Duration Of Message Capture: 10 Minute(s)
Maximum Events Per Wireless Client: 100

Figure 14: Debug Wireless Clients Screen

5 Refer to the following remote debug information for RF domain member connected wireless clients:

RF Domain	Displays the administrator assigned name of the selected RF domain used for wireless client debugging. 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.
Send Data To	Use the **Send Data To** drop-down menu to select where wireless client debug messages are collected. If `Screen` is selected, the wireless client debug information is sent to the Live Wireless Debug Events window at the bottom of the dialog window. If `File` is selected, the file location must be specified in the File Location section of the window.
Select Debug Messages	Select **All Debug Messages** to display all wireless client debug information for the selected wireless clients on the current RF domain. Choose **Selected Debug Messages** to specify which types of wireless client debug messages to display. If the **Selected Debug Messages** radio button is selected, you can display information for any combination of the following: • 802.11 Management • EAP • Flow Migration • RADIUS • System Internal • WPA/WPA2

Wireless Clients	Select **All Wireless Clients** to display debug information for all wireless clients currently associated to the current RF domain. Choose **Selected Wireless Clients** to display information only for specific wireless clients (between 1 and 3). If **Selected Wireless Clients** is selected, enter the MAC address for up to three wireless clients. The information displayed or logged to the file will only be from the specified wireless clients.
Duration of Message Capture	Use the spinner controls to select how long to capture wireless client debug information. This can range between 1 second and 24 hours, with the default value being 1 minute.
Maximum Events Per Wireless Client	Use the spinner controls to select the maximum number of debug messages displayed per wireless client. Set the number of messages from 1 - 9999 events with the default value being 100 events.
File Location	When the Send Data To field is set to **File**, the **File Location** configuration displays below the configuration section. If **Basic** is selected, enter the URL in the following format:

```
URL Syntax:
tftp://<hostname|IP>[:port]/path/file
ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file

IPv6 URL Syntax:
tftp://<hostname|[IPv6]>[:port]/path/file
ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file
```

	If **Advanced** is selected, configure the *Target*, *Port*, *Host/IP*, *User*, *Password* and optionally the path for the wireless client debug log file you want to create.
Live Wireless Debug Events	When the **Send Data To** field is set to **Screen**, this area displays live debug information for connected wireless clients in the selected RF domain.

6 When all configuration fields are complete, select **Start** to start the wireless client debug capture.

If information is being sent to the screen, it displays in the Live Wireless Debug Events section. If the data is being sent to a file, that file populates with remote debug information. If you have set a long message capture duration and want to end the capture early, select **Stop**.

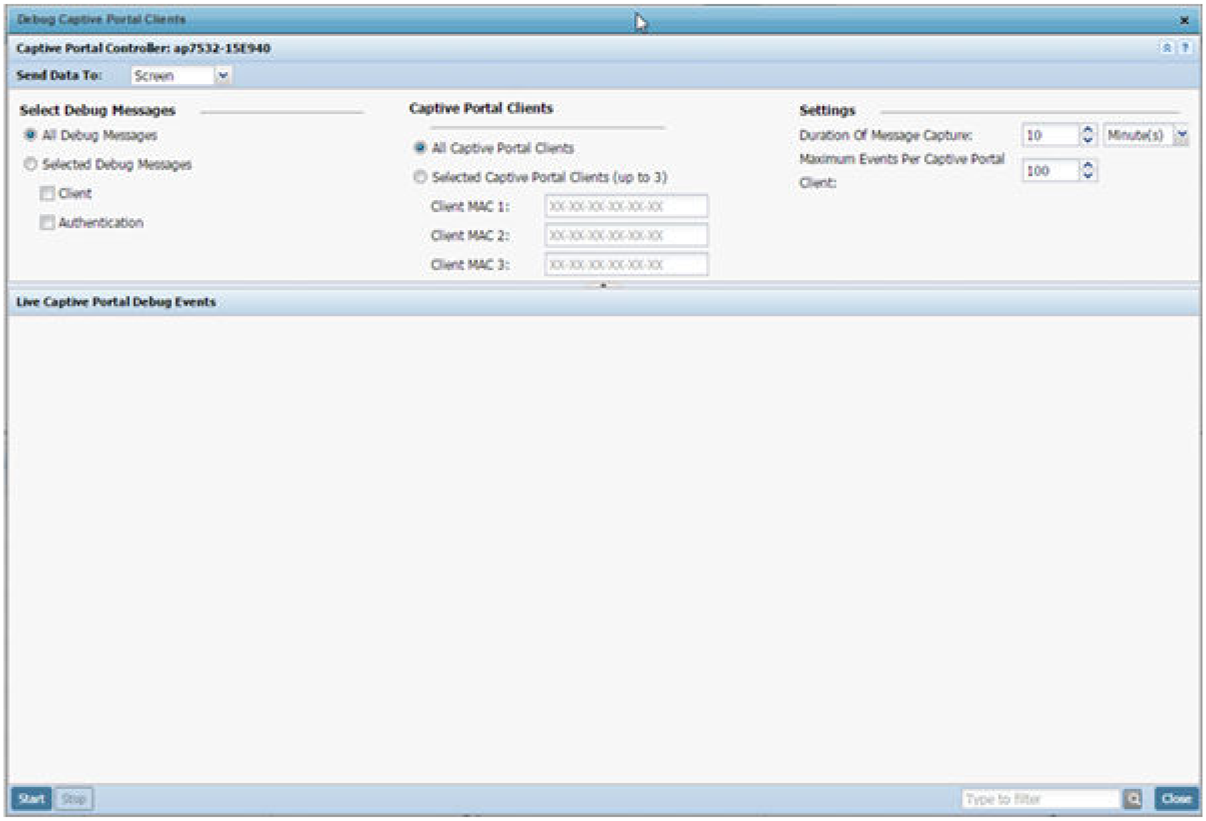
Debug Captive Portal Clients

An administrator can select an RF domain and capture captive portal client and authentication debug messages at an administrator assigned interval and location. Captive portal debug information can either be collected historically or in real-time.

To troubleshoot captive portal client debug messages:

1. Select **Dashboard**.
2. Expand the **System** node to display managed RF domains.
3. Select and expand an RF domain and click on the down arrow to the right of the RF domain's name.
4. Select **Troubleshooting**.

5 Select **Debug Captive Portal Clients**.



Debug Captive Portal Clients

Captive Portal Controller: ap7532-15E940

Send Data To: Screen

Select Debug Messages

● All Debug Messages

○ Selected Debug Messages

☐ Client

☐ Authentication

Captive Portal Clients

● All Captive Portal Clients

○ Selected Captive Portal Clients (up to 3)

Client MAC 1: XX-XX-XX-XX-XX-XX

Client MAC 2: XX-XX-XX-XX-XX-XX

Client MAC 3: XX-XX-XX-XX-XX-XX

Settings

Duration Of Message Capture: 10 Minute(s)

Maximum Events Per Captive Portal Client: 100

Live Captive Portal Debug Events

Figure 15: Debug Captive Portal Clients Screen

6 Use the **Send Data To** drop-down menu to select where captive portal debug messages are collected.

If **Screen** is selected, information is sent to the Live Wireless Debug Events window at the bottom of the screen. If **File** is selected, the file location must be specified in the **File Location** field.

7 In the Select Debug Messages area, refine how captive portal client debug messages are trended:

All Debug Messages	Select this option to capture all captive portal client and captive portal authentication request events collectively without filtering by type.
Select Debug Messages	Select this option to specify the type of captive portal event messages to display. Options include captive portal client events and events specific to captive portal authentication requests.

8 Set **Captive Portal Clients** filter options to refine which clients are included in the debug messages.

All Captive Portal Clients	Select this option to display debug information for each client utilizing a captive portal for network access within the selected RF domain.
Select Captive Portal Clients (up to 3)	Optionally display captive portal debug messages for specific clients (1 - 3). Enter the MAC address for up to three wireless clients. The information displayed or logged to the file is only from the specified wireless clients. Change the client MAC addresses as needed when clients are no longer utilizing the RF domain's captive portal resources.

9 Define the following captive portal client **Settings** to determine how messages are trended:

Duration of Message Capture	Use the spinner controls to set the message capture interval for captive portal debug information. This can range between 1 second and 24 hours.
Maximum Events Per Captive Portal Client:	Use the spinner controls to select the maximum number of captive portal event messages displayed per RF domain member client. Set the number of messages from 1 - 9999 events with the default value being 100 events.

10 When all configuration fields are complete, select **Start** to start the captive portal client debug message capture.

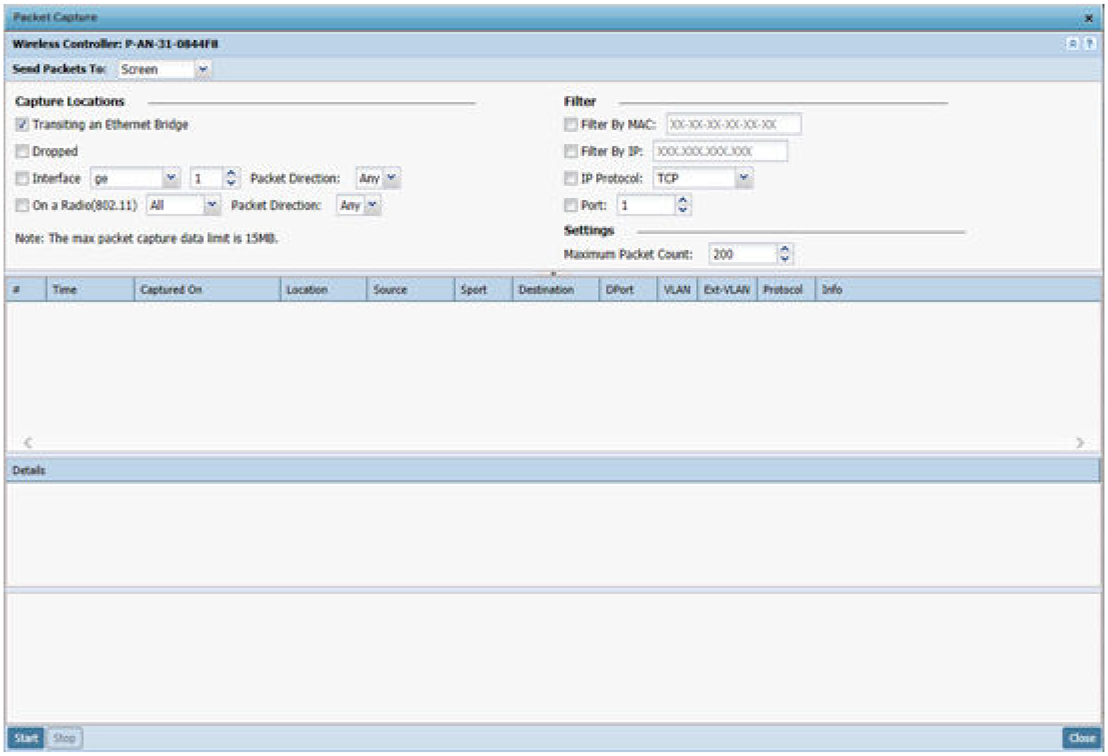
Information sent to the screen displays in the **Live Captive Portal Debug Events** field. If you have set a long message capture duration and want to end the capture early, select **Stop**.

Packet Capture

An administrator can capture connected client packet data based on the packet's address type or port on which received. Dropped client packets can also be trended to assess RF Domain client connectivity health.

To administer RF domain packet captures:

1 Select **Dashboard** → **Summary**.
2 Expand the **System** node to display managed RF domains.
3 Select and expand an RF domain and click on the down arrow to the right of the RF domain name.
4 Select **Troubleshooting**.
5 Select **Packet Capture**.


Packet Capture

Wireless Controller: P-AN-31-0844F8

Send Packets To: Screen

Capture Locations

☑ Transiting an Ethernet Bridge
☐ Dropped
☐ Interface ge 1 Packet Direction: Any
☐ On a Radio(802.11) All Packet Direction: Any

Note: The max packet capture data limit is 15MB.

Filter

☐ Filter By MAC: XX-XX-XX-XX-XX-XX
☐ Filter By IP: XXX.XXX.XXX.XXX
☐ IP Protocol: TCP
☐ Port: 1

Settings

Maximum Packet Count: 200

#	Time	Captured On	Location	Source	Sport	Destination	DPort	VLAN	Ext-VLAN	Protocol	Info

Figure 16: Packet Capture Screen

6 Refer to the following packet capture data for RF domain member connected wireless clients:

RF Domain	Displays the administrator assigned name of the selected RF domain used for wireless client packet captures. 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.
Send Data To	Use this drop-down menu to select where wireless client packet capture messages are collected. If **`Screen`** is selected, client packet capture data is sent to the Live Wireless Debug Events window at the bottom of the dialog window. If **`File`** is selected, the file location must be specified in the File Location section of the window.
Dropped	Select this option to create an event entry each time a packet is dropped from a client connected to a RF domain member device. Use this information to assess whether a particular RF domain is experiencing high levels of dropped packets that may require administration to distribute client connections more evenly.
Interface	Select this option to specify packet capture on a specific interface on the current RF domain. If you have selected this option, specify the interface name and number and specify a packet direction
On a Radio (802.11)	Select this option to capture packets only on 802.11 radios. If selecting this option, specify which radios should be used and specify a packet direction.
Filter (MAC, IP, Protocol, Port	In the Filter area, set the criteria based on which packets are filtered and captured. Select one or more of the following and specify the relevant information: • Filter by MAC • Filter By IP • IP Protocol • Port
Maximum Packet Count	In the Settings area, set the Maximum Packet Count to limit the number of packets captured for trending. Set this value between 1 - 10000 packets, with a default value of 200.

7 Select **Start** to begin the packet capture.

Information sent to the screen displays in the lower portion of the window. If the data is being sent to a file, that file populates with the packet capture information. If you have set a long message capture duration and want to end the capture early, select **Stop**.

5 Device Configuration

Device Configuration
Auto-Provisioning Policies
Managing an Event Policy
Managing MINT Policies
Password Encryption

Managed devices can either be assigned unique configurations or have existing RF Domain or Profile configurations modified (overridden) to support a requirement that dictates a device's configuration be customized from the configuration shared by its profiled peer devices.

When a device is initially managed by the controller or service platform, it requires several basic configuration parameters be set (system name, deployment location, etc.). Additionally, the number of permitted device licenses needs to be accessed to determine whether a new access point can be adopted.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement (overrides) from their original RF Domain administered design.

Profiles enable administrators to assign a common set of configuration parameters and policies to controller or service platforms and access points. Profiles can be used to assign shared or unique network, wireless and security parameters to wireless controllers and 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 controller and service platform supports both default and user defined profiles implementing new features or updating existing parameters to groups of controllers, service platforms or access points.

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

Adoption is the process an access point uses to discover controller or service platforms available in the network, pick the most desirable one, establish an association, obtain its configuration and consider itself provisioned.

At adoption, an access point solicits and receives multiple adoption responses from available controllers or service platforms on the network. Modify existing adoption policies or create new ones as needed to meet the adoption requirements of a device and its assigned profile.

Lastly, use **Configuration** → **Devices** to define and manage a critical resource policy. A critical resource policy defines a list of device IP addresses on the network (gateways, routers etc.). The support of these IP address is interpreted as critical to the health of the network. These device addresses are pinged regularly by the controller or service platform. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.

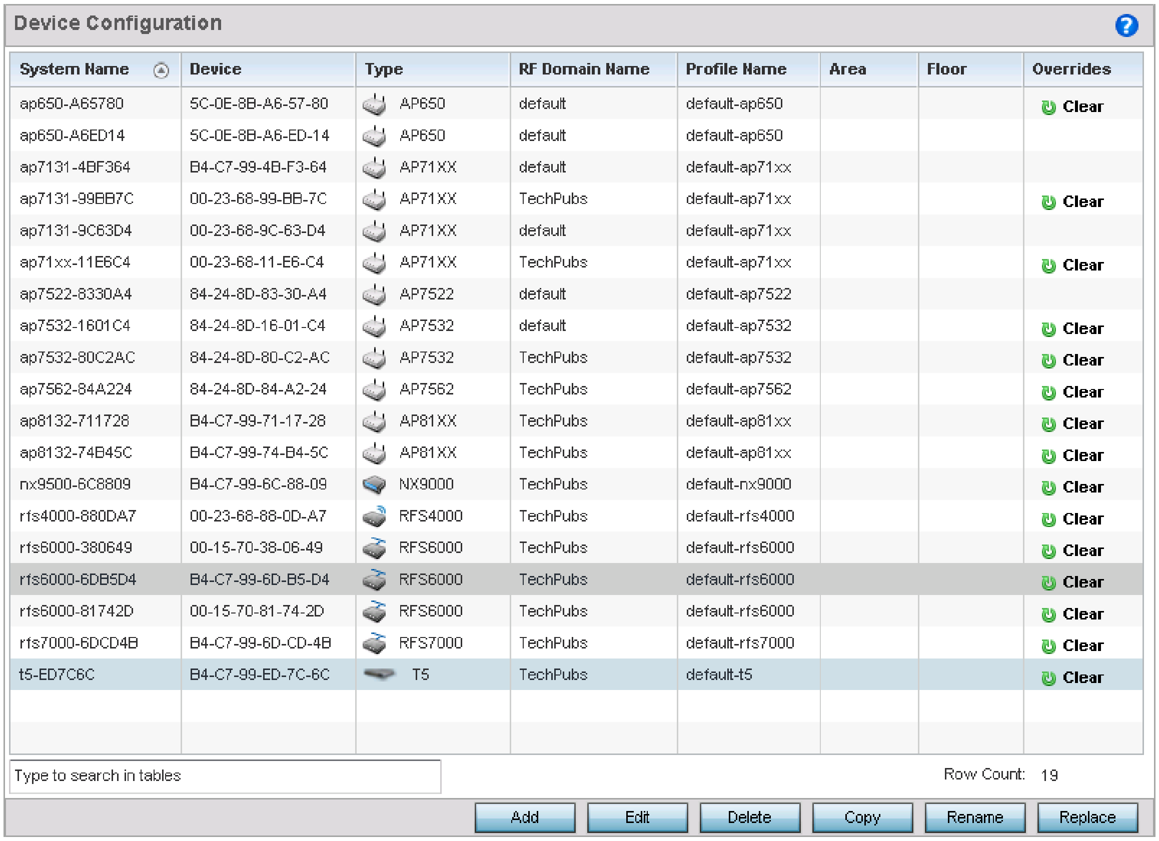
Device Configuration

When a device is initially managed by an access point, RFS controller or NX series service platform it requires several basic parameters be set (system name, deployment location, etc.). Additionally, the number of permitted device licenses needs to be assessed to determine whether additional access points can be adopted under the terms of the existing license. The Basic configuration screen affords an administrator a means of assessing devices detected by a selected access point, controller or service platform and determining whether they need minor profile or RF Domain re-assignments to be optimally deployed.

To assign a basic configuration:

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

The Device Configuration screen displays by default. This screen lists access points, controllers and service platforms within the managed network.



Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
ap650-A65780	5C-0E-8B-A6-57-80	AP650	default	default-ap650			Clear
ap650-A6ED14	5C-0E-8B-A6-ED-14	AP650	default	default-ap650			
ap7131-4BF364	B4-C7-99-4B-F3-64	AP71XX	default	default-ap71xx			
ap7131-99BB7C	00-23-68-99-BB-7C	AP71XX	TechPubs	default-ap71xx			Clear
ap7131-9C63D4	00-23-68-9C-63-D4	AP71XX	default	default-ap71xx			
ap71xx-11E6C4	00-23-68-11-E6-C4	AP71XX	TechPubs	default-ap71xx			Clear
ap7522-8330A4	84-24-8D-83-30-A4	AP7522	default	default-ap7522			
ap7532-1601C4	84-24-8D-16-01-C4	AP7532	default	default-ap7532			Clear
ap7532-80C2AC	84-24-8D-80-C2-AC	AP7532	TechPubs	default-ap7532			Clear
ap7562-84A224	84-24-8D-84-A2-24	AP7562	TechPubs	default-ap7562			Clear
ap8132-711728	B4-C7-99-71-17-28	AP81XX	TechPubs	default-ap81xx			Clear
ap8132-74B45C	B4-C7-99-74-B4-5C	AP81XX	TechPubs	default-ap81xx			Clear
nx9500-6C8809	B4-C7-99-6C-88-09	NX9000	TechPubs	default-nx9000			Clear
rfs4000-880DA7	00-23-68-88-0D-A7	RFS4000	TechPubs	default-rfs4000			Clear
rfs6000-380649	00-15-70-38-06-49	RFS6000	TechPubs	default-rfs6000			Clear
rfs6000-6DB5D4	B4-C7-99-6D-B5-D4	RFS6000	TechPubs	default-rfs6000			Clear
rfs6000-81742D	00-15-70-81-74-2D	RFS6000	TechPubs	default-rfs6000			Clear
rfs7000-6DCD4B	B4-C7-99-6D-CD-4B	RFS7000	TechPubs	default-rfs7000			Clear
t5-ED7C6C	B4-C7-99-ED-7C-6C	T5	TechPubs	default-t5			Clear

Row Count: 19

Figure 17: Device Configuration Screen - Lists the Devices Within the Network

2 Refer to the following device settings to determine whether a configuration update or RF Domain or profile change is warranted:

System Name	Displays the name assigned to the device when the basic configuration was defined. This is also the device name that appears within the RF Domain or profile the device supports.
Device	Displays the device's factory assigned MAC address used as hardware identifier. The MAC address cannot be revised with the device's configuration.
Type	Displays the device model for the listed access point, controller or service platform.
RF Domain Name	Lists RF Domain memberships for each listed device. Devices can either belong to a default RF Domain based on model type, or be assigned a unique RF Domain supporting a specific configuration customized to that device model.
Profile Name	Lists the profile each listed device is currently a member of. Devices can either belong to a default profile based on model type, or be assigned a unique profile supporting a specific configuration customized to that model.
Area	Lists the physical area where the device is deployed. This can be a building, region, campus or other area that describes the deployment location.
Floor	Lists the building Floor name representative of the location within the area or building the device was physically deployed. Assigning a building floor name is helpful when grouping devices in RF Domains and 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.
Overrides	This column contains an option to clear all profile overrides for any devices that contain overrides. This uniformly restores the device's configuration to that shared by other devices utilizing the same profile. To clear an override, select the clear button to the right of the device.

3 Click **Add** to create a new device. Click **Edit** to modify an existing device or click **Delete** to remove an existing device.

Basic Device Configuration

Setting a device's Basic configuration is required to assign a device **`name`**, deployment **`location`** and **`system time`**. Similarly, the Basic configuration screen is where profile and RF Domain assignments/ adjustments are made. 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.

Profiles enable administrators to assign a common set of configuration parameters and policies to access points, controllers and service platforms. Profiles can be used to assign *common* or *unique* network, wireless and security parameters to devices across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. Controllers and service platforms support both default and user defined profiles implementing new features or updating existing parameters to groups of devices. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations one at a time.

Note
Once devices have been assigned membership in either a profile or RF Domain, an administrator must be careful not to assign the device a configuration update that removes it from membership from a RF Domain or profile. A RF Domain or profile configuration must be re-applied to a device once its configuration has been modified in a manner that differentiates it from the configuration shared by the devices comprising the RF Domain or profile.

To set a device's basic configurations:

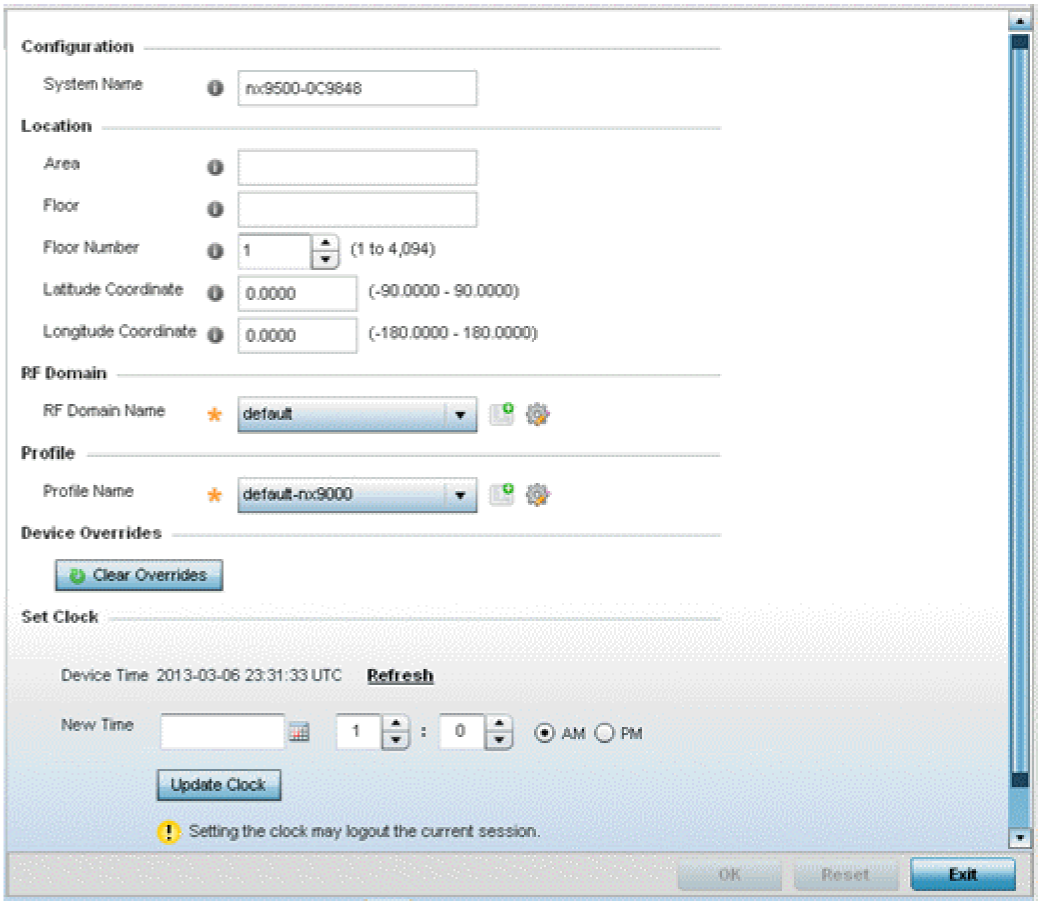
1 Select the **Configuration** → **Devices** from the Web UI.

  The Device Configuration screen displays. This screen lists the managed devices or peers. The listed devices can either be other access points, controllers or service platforms.

2 Select a target device (by double-clicking it) from amongst those displayed.

  Note
  Devices can also be selected directly from the device browser in the lower, left-hand, side of the UI.

  The Basic configuration screen displays by default.



System Name: nx9500-0C9848

Area:

Floor:

Floor Number: 1 (1 to 4,094)

Latitude Coordinate: 0.0000 (-90.0000 - 90.0000)

Longitude Coordinate: 0.0000 (-180.0000 - 180.0000)

RF Domain Name: default

Profile Name: default-nx9000

Device Time 2013-03-06 23:31:33 UTC **Refresh**

New Time: 1 : 0 ● AM ○ PM

Setting the clock may logout the current session.

Figure 18: Configuration - Devices - Basic Configuration Screen

3 Set the following basic configurations for the target device:

System Name	Provide the selected device a system name up to 64 characters. This is administrator defined device name appearing within the RF Domain or Profile the device supports.
Area	Assign the device an Area name representative of the location the access point, controller or service platform was physically deployed. The name cannot exceed 64 characters. Assigning an area name is helpful when grouping devices in RF Domains and profiles, as devices 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 a device a building Floor name representative of the location the access point, controller or service platform was physically deployed. The name cannot exceed 64 characters. Assigning a building Floor name is helpful when grouping devices within the same general coverage area.
Floor Number	Use the spinner control to assign a numerical floor designation in respect to the floor's actual location within a building. Set a value from 1 - 4094. the default setting is the 1st floor.

Latitude Coordinate	Set the latitude coordinate where devices are deployed within a floor. When looking at a floor map, latitude lines specify the east-west position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the latitude and longitude points on the earth's surface.
Longitude Coordinate	Set the longitude coordinate where devices are deployed within a floor. When looking at a floor map, longitude lines specify the north-south position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the longitude and latitude points on the earth's surface.

4. Use the RF Domain drop-down menu to select an existing RF Domain for device membership.

   If an RF Domain configuration does not exist suiting the deployment requirements of the target device, select the **Create** icon to create a new RF Domain configuration, or select the **Edit** icon to modify the configuration of a selected RF Domain.

   For more information, see RF Domains on page 747 or Managing RF Domains on page 748.
5. Use the Profile drop-down menu to select an existing RF Domain for device membership.
6. If a profile configuration does not exist suiting the deployment requirements of the target device, select the **Create** icon to create a new profile configuration, or select the **Edit** icon to modify the configuration of a selected profile.
7. If necessary, select the **Clear Overrides** button to remove all existing overrides from the device.
8. Refer to the Set Clock parameter to update the system time of the target device.
9. Refer to the Device Time parameter to assess the device's current time, or whether the device time is unavailable. Select **Refresh** as required to update the device's reported system time.
10. Use the New Time parameter to set the calendar day, hour and minute for the target device. Use the AM and PM radio buttons to refine whether the updated time is for the morning or afternoon/evening.
11. When completed, select **Update Clock** to commit the updated time to the target device.
12. Select **OK** to save the changes made to the device's basic configuration. Selecting **Reset** reverts the screen to its last saved configuration.

License Configuration

Licenses are purchased directly for the number of permissible adoptions per access point, controller, service platform or managed cluster.

Note
The Licenses screen is available only to controllers and service platforms capable of sustaining device connections, and thus requires license support to set the maximum number of device connections permitted. The License screen is not available for AP621 and AP650 model access points that are reliant on their connected controller or service platform for their management.

Managing infrastructure devices requires a license key to enable software functionality or define the number of adoptable devices allowable. My Licenses is a Web based online application enabling you to request a license key for purchased license certificates.

The Licenses screen also contains a facility where new licenses can be applied to increase the number of device adoptions permitted, or to allow the use of the advanced security features.

Each controller and service platform family has multiple models to choose from that range from zero licenses to the maximum number that can be loaded for that specific SKU.

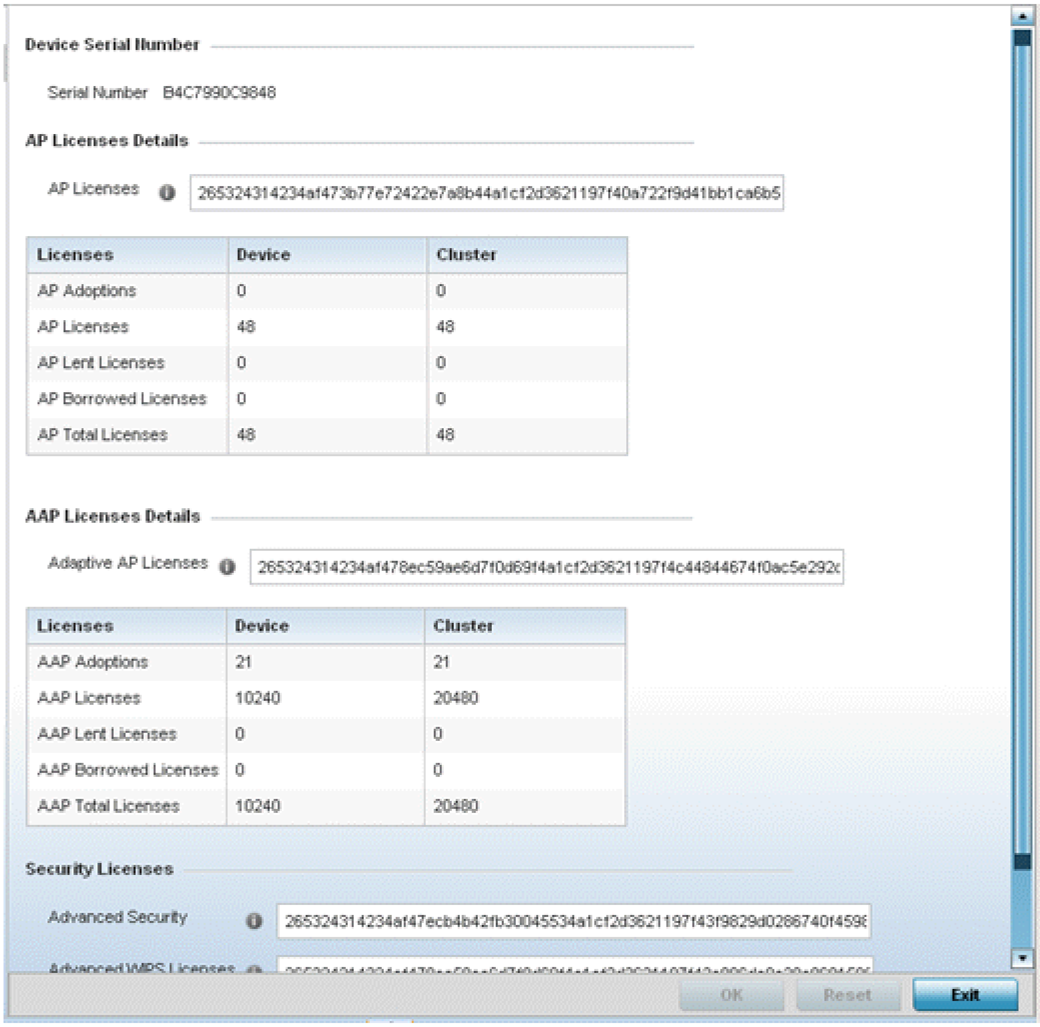
To configure a device's a license configuration:

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

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device, from the displayed list, by double-clicking on the device name. The selected device's configuration menu displays.

3 Select **Licenses**.



Device Serial Number

Serial Number B4C7990C9848

AP Licenses Details

AP Licenses 265324314234af473b77e72422e7a8b44a1cf2d3621197f40a722f9d41bb1ca6b5

Licenses	Device	Cluster
AP Adoptions	0	0
AP Licenses	48	48
AP Lent Licenses	0	0
AP Borrowed Licenses	0	0
AP Total Licenses	48	48

AAP Licenses Details

Adaptive AP Licenses 265324314234af478ec59ae6d7f0d69f4a1cf2d3621197f4c4484467410ac5e292c

Licenses	Device	Cluster
AAP Adoptions	21	21
AAP Licenses	10240	20480
AAP Lent Licenses	0	0
AAP Borrowed Licenses	0	0
AAP Total Licenses	10240	20480

Security Licenses

Advanced Security 265324314234af47ecb4b42fb30045534a1cf2d3621197f43f9829d0286740f459

Advanced WPS Licenses

Figure 19: Device Licenses Screen

The License screen displays the **Device Serial Number** of the controller or service platform generating the license key.

Note

When assessing lent and borrowed license information, it is important to distinguish between NOC controllers and site controllers.

NOC controllers are NX 95XX and NX 96XX.

The site controllers are RFS 4000, NX 5500, and NX 7510.

4 Review the AP Licenses table to assess the specific number of adoptions permitted, as dictated by the terms of the current license.

AP Adoptions	The Device column lists the total number of AP adoptions made by the controller or service platform. If the installed license count is 10 APs and the number of AP adoptions is 5, five additional APs can still be adopted under the terms of the license. The total number of APs adoptions varies by platform, as well as the terms of the license. The Cluster column lists the total number of AP adoptions made by the cluster membership (all members). If the installed license count is 100 APs and the number of AP adoptions is 50, 50 additional APs can still be adopted under the terms of the AP licenses, pooled by the cluster members.
AP Licenses	The **Device** column lists the number of APs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive APs only, and not independent mode APs. The **Cluster** column lists the number of APs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
AP Lent Licenses	Lent licenses are the total number of AP licenses the NOC controller lends (if needed) to its site controllers so that a site controller can adopt APs in excess of its own installed AP license count. AP lent licenses can be non-zero only in controllers currently configured as the NOC (NOC controller). Lent Licenses is always zero in controllers configured as the site (site controller).

AP Borrowed Licenses	Borrowed licenses are the total number of AP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AP borrowed licenses are always zero in the NOC controller. AP borrowed licenses can be non-zero only on site controllers.
AP Total Licenses	The cumulative number of both **Device** and **Cluster** AP licenses supported by the listed controller or service platform.

Note

The following is a licensing example: Assume there's two site controllers (S1 and S2) adopted to a NOC controller (N1). S1 has 3 installed AP licenses, and S2 has 4 installed AP licenses. Eight APs seek to adopt on S1, and ten APs seek to adopt on S2. N1 has 1024 installed licenses. N1 lends 5 AP licenses (8 minus 3) to S1, and 6 AP licenses (10 minus 4) to S2.

N1 displays the following in the **Device** column:

- AP Adoptions: 2 (site controllers S1 and S2)
- AP Licenses: 1024
- AP Lent Licenses: 11 (5 to S1 plus 6 to S2)
- AP Borrowed Licenses: 0
- AP Total Licenses: 1013 (1024 minus 11 lent)

S1 displays the following in the **Device** column:

- AP Adoptions: 8
- AP Licenses: 3
- AP Lent Licenses: 0
- AP Borrowed Licenses: 5
- AP Total Licenses: 8 (3 plus 5 borrowed)

S2 displays the following in the **Device** column:

- AP Adoptions: 10
- AP Licenses: 4
- AP Lent Licenses: 0
- AP Borrowed Licenses: 6
- AP Total Licenses: 10 (4 plus 6 borrowed)

---

5 Review the **Adaptive AP Licenses** table to assess the specific number of adoptions permitted, as dictated by the terms of the current license.

AAP Adoptions	The **Device** column lists the total number of AAP adoptions made by the controller or service platform. If the installed license count is 10 APs and the number of AAP adoptions is 5, five additional AAPs can still be adopted under the terms of the license. The total number of AAPs adoptions varies by platform, as well as the terms of the license. The **Cluster** column lists the total number of AAP adoptions made by the cluster membership (all members). If the installed license count is 100 APs and the number of AAP adoptions is 50, 50 additional AAPs can still be adopted under the terms of the AAP licenses, pooled by the cluster members.
AAP Licenses	The **Device** column lists the number of AAPs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive AAPs only, and not independent mode AAPs. The **Cluster** column lists the number of AAPs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
AAP Lent Licenses	Lent licenses are the total number of AAP licenses the NOC controller lends (if needed) to its site controllers so site controllers can adopt adaptive APs in excess of its own installed AAP license count. AAP lent licenses can be non-zero only in controllers currently configured as the NOC (NOC controller). Lent licenses is always zero in controllers configured as the site (site controller).
AAP Borrowed Licenses	Borrowed licenses are the total number of AAP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AAP borrowed licenses are always zero in the NOC controller. AAP borrowed licenses can be non-zero only on site controllers.
AAP Total Licenses	Lists the cumulative number of both **Device** and **Cluster** AAP licenses supported by the listed controller or service platform.

6 Refer to the **Feature Licenses** field to apply licenses and provision advanced security and analytics features:

Advanced Security	Enter the provided license key required to install the Role Based Firewall feature and increase the number of IPSec VPN tunnels. The number of IPSec tunnels varies by platform.
Analytics Licenses	Enter the provided license key required to install Analytics (an enhanced statistical management tool) for NX 95XX and NX 96XX series service platforms.

7 Refer to the **Web Filtering License** field if required to provide a 256-character maximum license string for the Web filtering feature.

Web filtering is used to restrict access to specific resources on the internet.

8 Click **OK** to save the changes made to the applied licenses.

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

Assigning Certificates

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 the CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

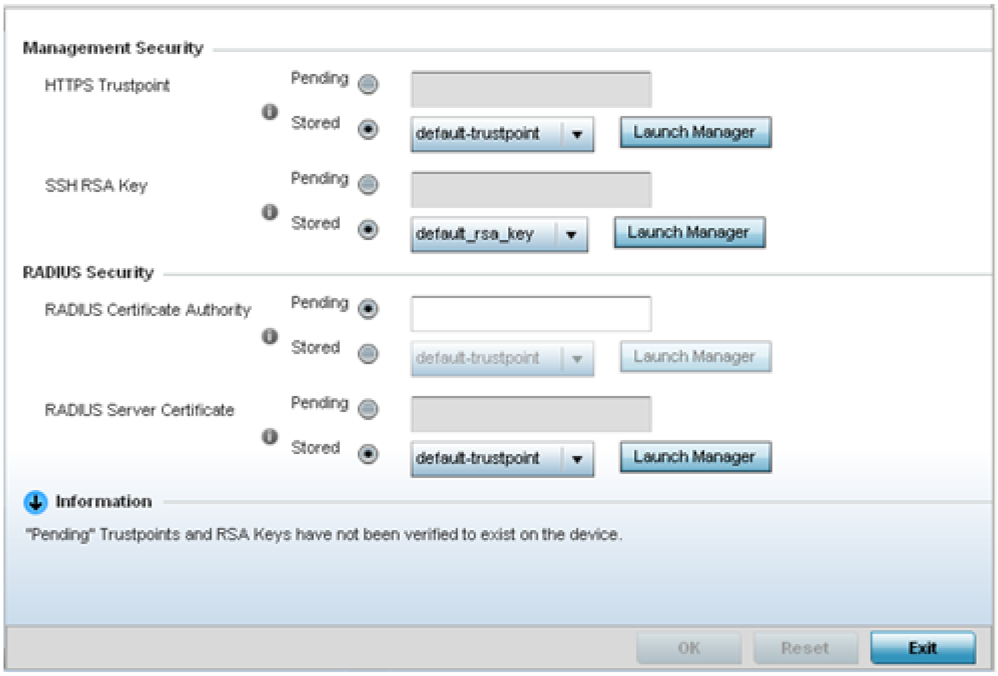
Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

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 requesting 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 controller or access point locally, while the private portion remains on a secure area of the client.

To configure certificate usage:

1 Select **Configuration** → **Devices** from the Web UI. The Device Configuration screen displays a list of managed devices or peers (other access points, controllers or service platforms).
2 Select a target device, from the displayed list, by double-clicking on the device name. The selected device's configuration menu displays.
3 Select **Certificates**.



Management Security

HTTPS Trustpoint: Pending ○ Stored ● default-trustpoint

SSH RSA Key: Pending ○ Stored ● default_rsa_key

RADIUS Security

RADIUS Certificate Authority: Pending ● Stored ○ default-trustpoint

RADIUS Server Certificate: Pending ○ Stored ● default-trustpoint

Information

"Pending" Trustpoints and RSA Keys have not been verified to exist on the device.

Figure 20: Device Certificates Screen

4 Set the following Management Security certificate configuration:

SSH RSA Key	Either use the `default_rsa_key` or select **Stored** to enable a drop-down menu where an existing certificate can be used. To use an existing key, select **Launch Manager**. For more information, see RSA Key Management on page 67.

Note

Pending trustpoints and RSA keys are typically not verified as existing on a device.

5 Set the following RADIUS Security certificate configurations:

RADIUS Certificate Authority	Either use the `default-trustpoint` or select **Stored** to enable a drop-down menu where an existing certificate can be used. To use an existing certificate, select **Launch Manager**.
RADIUS Server Certificate	Either use the `default-trustpoint` or select **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing trustpoint, select **Launch Manager**.
RADIUS Certificate Authority LDAPS	Either use the LDAP server `default-trustpoint` or select **Stored** to enable a drop-down menu where an existing certificate can be used. To use an existing certificate, select **Launch Manager**.
RADIUS Server LDAPS Trustpoint	Either use the LDAP server `default-trustpoint` or select **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing trustpoint, select **Launch Manager**.

6 Refer to the CMP Certificate field to optionally use CMP *(Certificate Management Protocol* as 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.

Either use the server `default-trustpoint` or select **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing trustpoint, select **Launch Manager**.

7 Click **OK** to save the changes made to the certificate configurations. Click **Reset** to revert the screen to its last saved configuration.

For more information on the certification activities supported, refer to the following:

- Certificate Management on page 58
- RSA Key Management on page 67
- Certificate Creation on page 73
- Generating a Certificate Signing Request on page 74

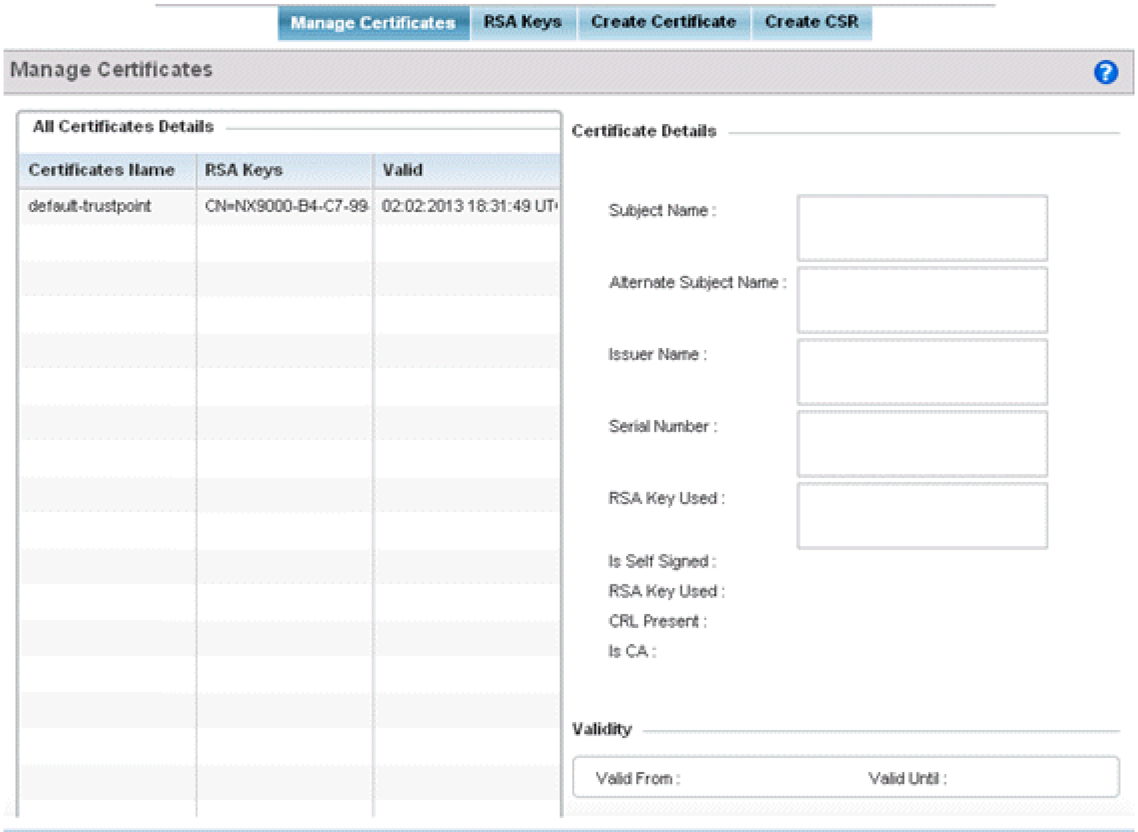
Certificate Management

A *stored* certificate can be used from a different managed device if you prefer not to use an existing certificate or key. Device certificates can be imported and exported to and from the controller or service platform to a secure remote location for archive and retrieval as required for other managed devices.

To configure trustpoints for use with certificates:

1. Select **Launch Manager** from either the HTTPS Trustpoint, SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.

   The Certificate Management screen displays with the Manage Certificates tab displayed by default.



Certificates Name	RSA Keys	Valid
default-trustpoint	CN=NX9000-B4-C7-99	02:02:2013 18:31:49 UT

Figure 21: Certificate Management - Manage Certificates Screen

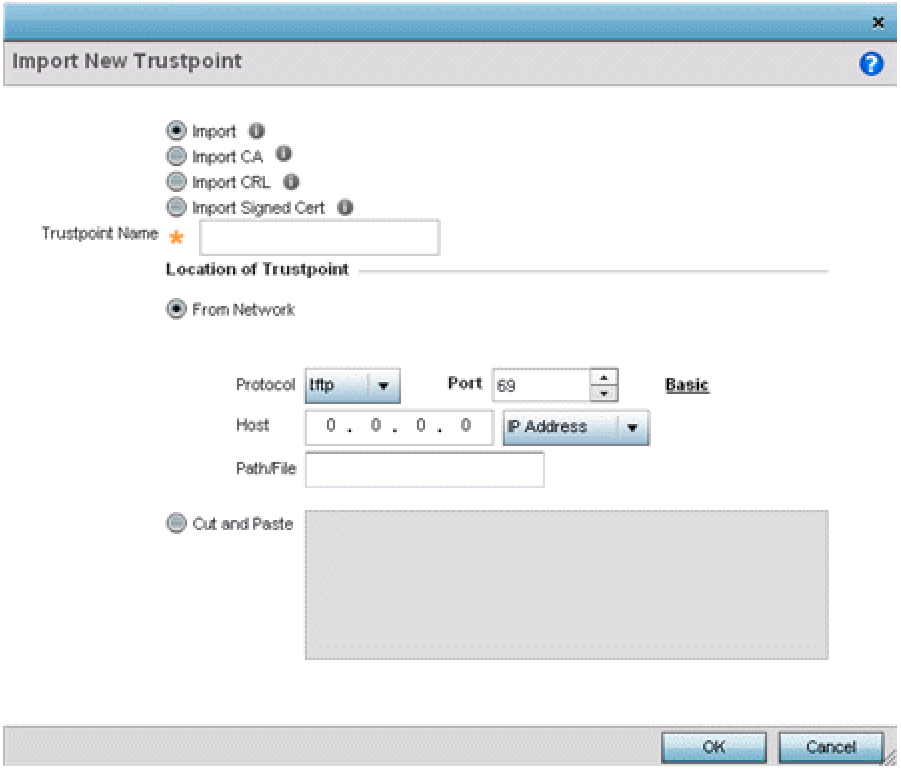
2. Select a device from among those displayed to review its certificate information.
3. Refer to **All Certificate Details** to review the certificate's properties, self-signed credentials, validity duration, and CA information.
4. To optionally import a certificate, click the **Import** button at the bottom of the Manage Certificates screen.

   The **Import New Trustpoint** screen displays. You can use this screen to import CA certificates, CRLs and signed certificates to the controller or service platform once the network credentials of the file transfer have been defined.
5. Click **OK** to import the defined trustpoint.

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

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.



Import New Trustpoint

● Import
○ Import CA
○ Import CRL
○ Import Signed Cert

Trustpoint Name *

Location of Trustpoint

● From Network

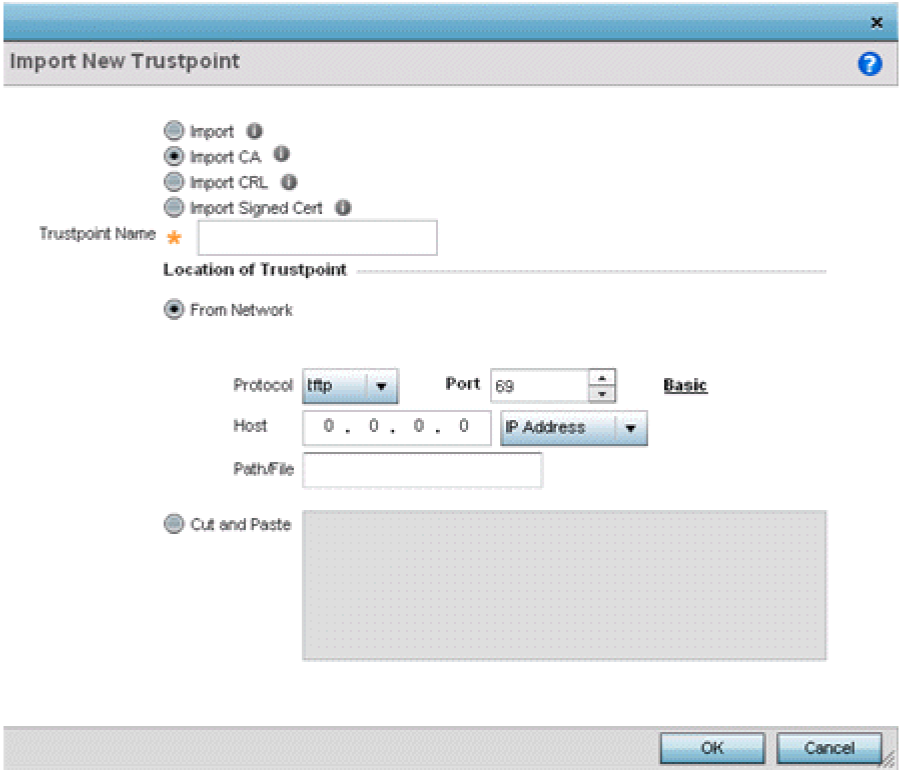
Protocol: tftp
Port: 69
Host: 0 . 0 . 0 . 0
IP Address
Path/File:

○ Cut and Paste

Figure 22: 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: • tftp • ftp • sftp • http • cf • usb1-4
Port	Set the port. This option is not valid for **`cf`** and **`usb1-4`**.

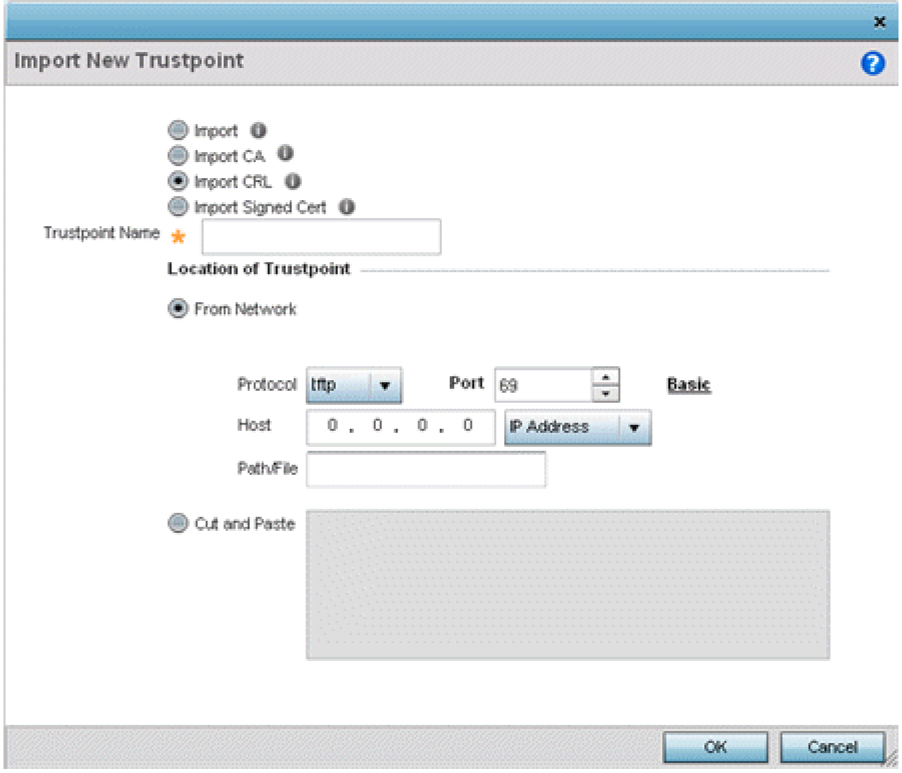
Host	Provide the hostname string or numeric IP address of the server used to import the trustpoint. Hostnames cannot include an underscore character. This option is not valid for `cf` and `usb1-4`. Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an 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.

For information on creating a CRL to use with a trustpoint, refer to Setting the Certificate Revocation List (CRL) Configuration on page 678 .



Import New Trustpoint

● Import CRL

Trustpoint Name

Location of Trustpoint

● From Network

Protocol tftp

Port 69

Host 0 . 0 . 0 . 0

IP Address

Path/File

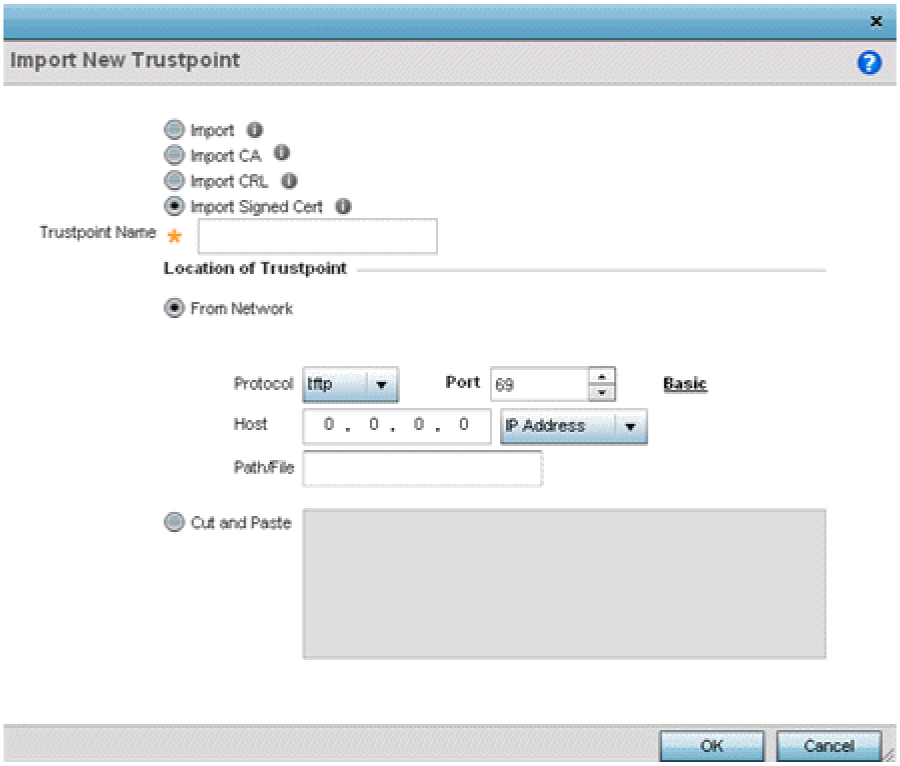
5 Define the following configuration parameters required to import a CRL:

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: • tftp • ftp • sftp • http • cf • 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`**. 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.



○ Import
○ Import CA
○ Import CRL
● Import Signed Cert
Trustpoint Name *
● From Network
Protocol tftp
Port 69
Host 0 . 0 . 0 . 0 IP Address
Path/File
○ Cut and Paste

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: • tftp • ftp • sftp • http • cf • 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`. 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

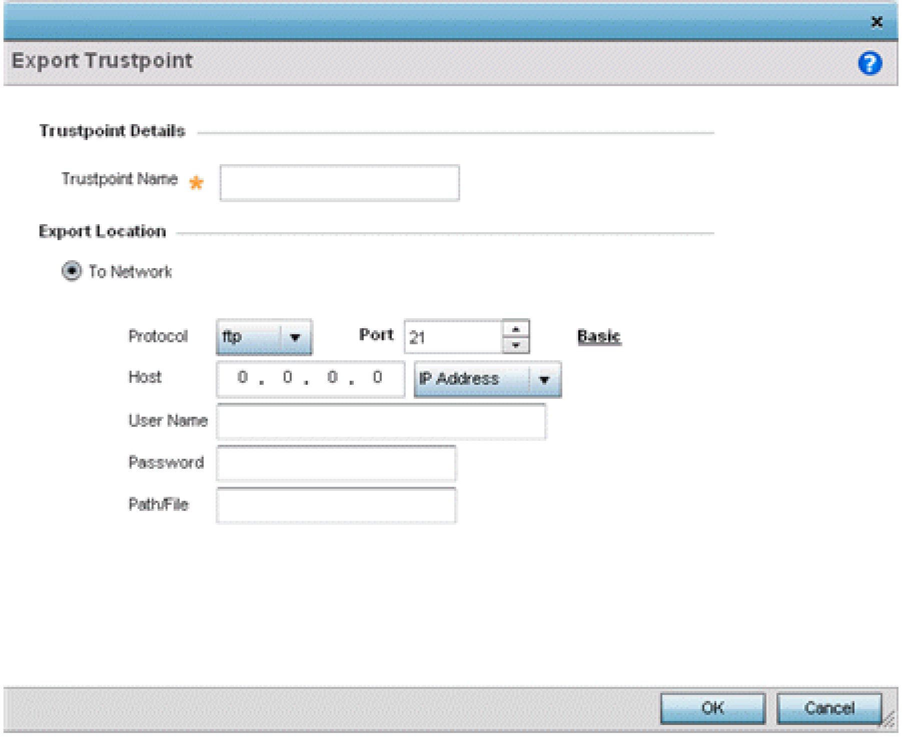
Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled 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.



● To Network

Protocol: ftp

Port: 21

Host: 0 . 0 . 0 . 0 — IP Address

User Name

Password

Path/File

Figure 23: 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: • tftp • ftp • sftp • http • cf • 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`. 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.

Delete Trutpoints

To delete a trustpoint:

1 Select **Operations → Manage Certificates**

2 To optionally delete a trustpoint, click **Delete** in the Certificate Management screen.

Provide the trustpoint name in the Delete Trustpoint screen and optionally select **Delete RSA Key** to remove the RSA key along with the trustpoint.

3 Click **OK** to proceed with the deletion.

Click **Cancel** to revert to the Certificate Management screen.

RSA Key Management

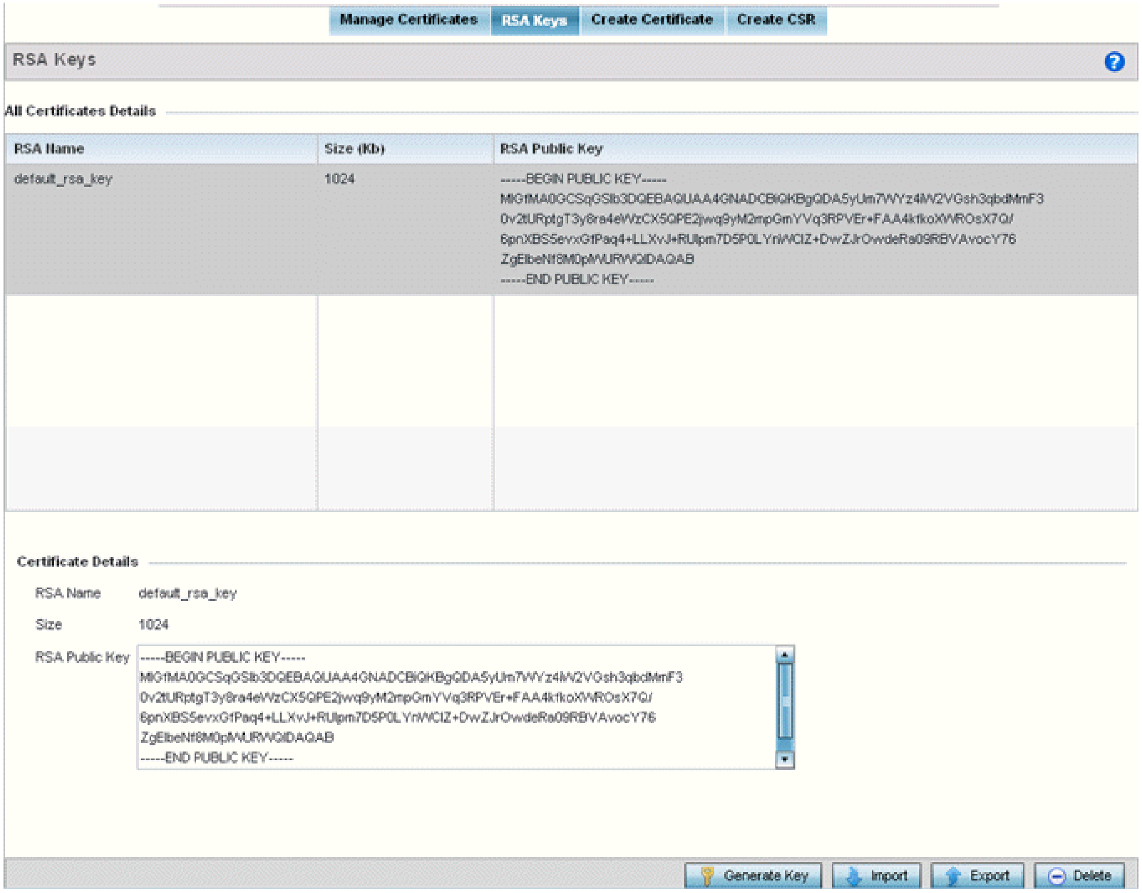
Refer to the RSA Keys screen to review existing RSA key configurations that have been applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import/export an existing key to and from a remote location.

RSA *(Rivest, Shamir, and Adleman)* is an algorithm for public key cryptography. The algorithm 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 In the Certificate Management screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.

2 Click **RSA Keys** from the Certificate Management screen.



All Certificates Details

RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5yUm7WYz4lV2VGsh3qbdMmF3 0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4k1koXWROsX7Q/ 6pnXBS5evxG1Paq4+LLXvJ+RUlpm7D5P0LYnWCIZ+DwZJrOwdeRa09RBVAvocY76 ZgElbeNf8M0pWURWQIDAQAB -----END PUBLIC KEY-----

Certificate Details

RSA Name default_rsa_key

Size 1024

RSA Public Key

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5yUm7WYz4lV2VGsh3qbdMmF3
0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4k1koXWROsX7Q/
6pnXBS5evxG1Paq4+LLXvJ+RUlpm7D5P0LYnWCIZ+DwZJrOwdeRa09RBVAvocY76
ZgElbeNf8M0pWURWQIDAQAB
-----END PUBLIC KEY-----
```

Figure 24: 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 Click **Generate Key** to create a new key with a defined size.

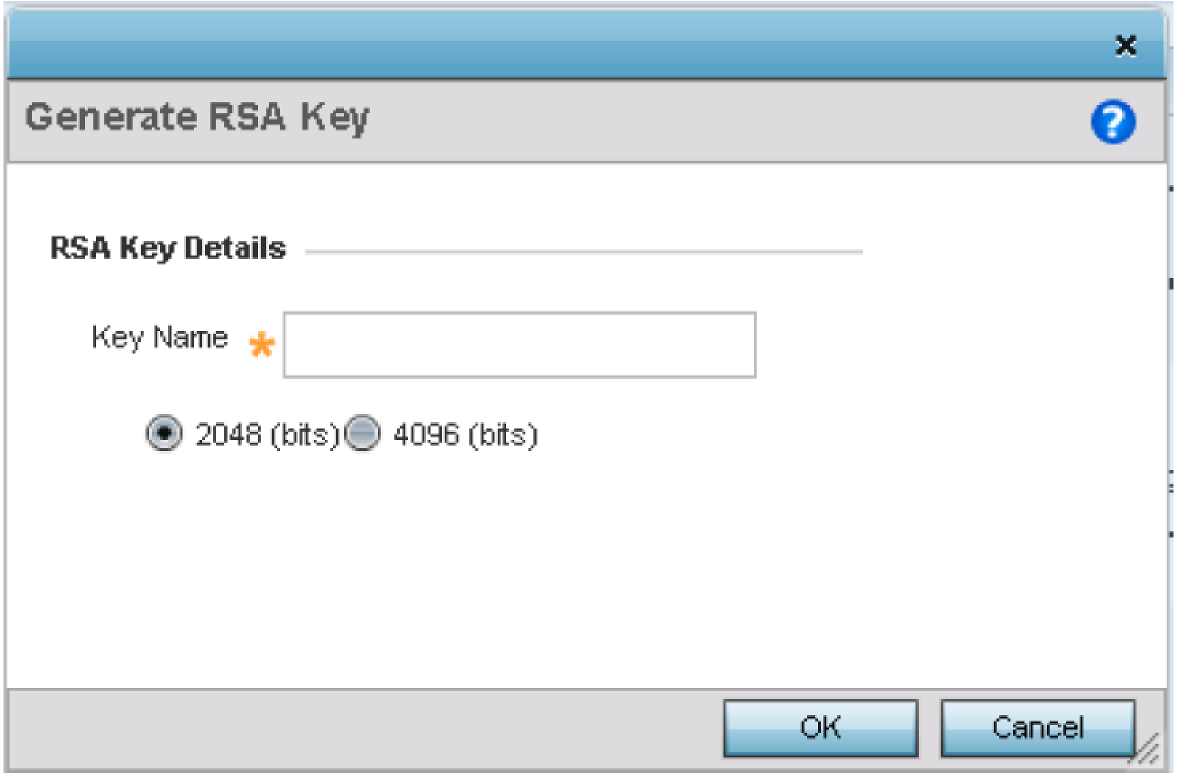


Figure 25: Certificate Management - Generate RSA Keys Screen

5 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	Set the size of the key as either 2048 (bits) or 4096 (bits). Leaving this value at the default setting of 2048 is recommended to ensure optimum functionality.

6 Click **OK** to generate the RSA key.

Click **Cancel** to revert to the 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.

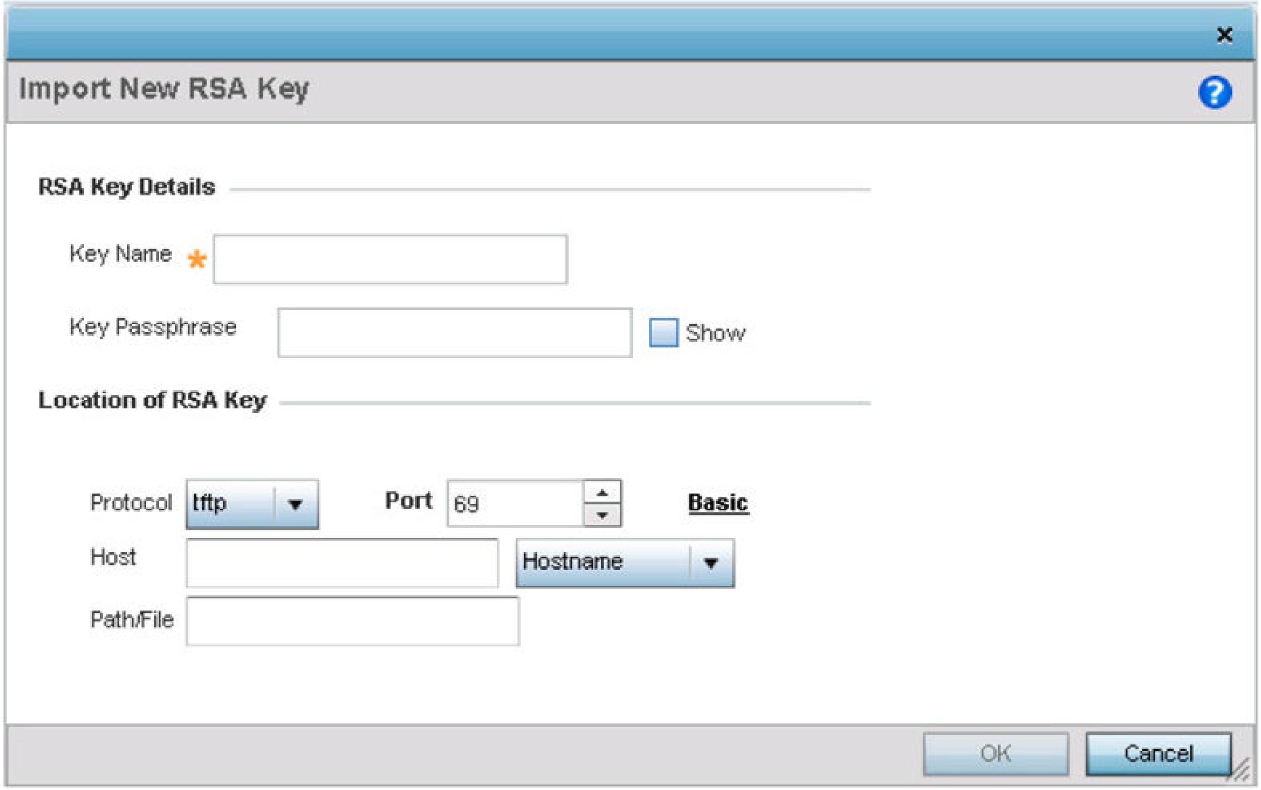


Figure 26: Certificate Management - Import New RSA Key Screen

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: • tftp • ftp • sftp • http • cf • 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`. 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

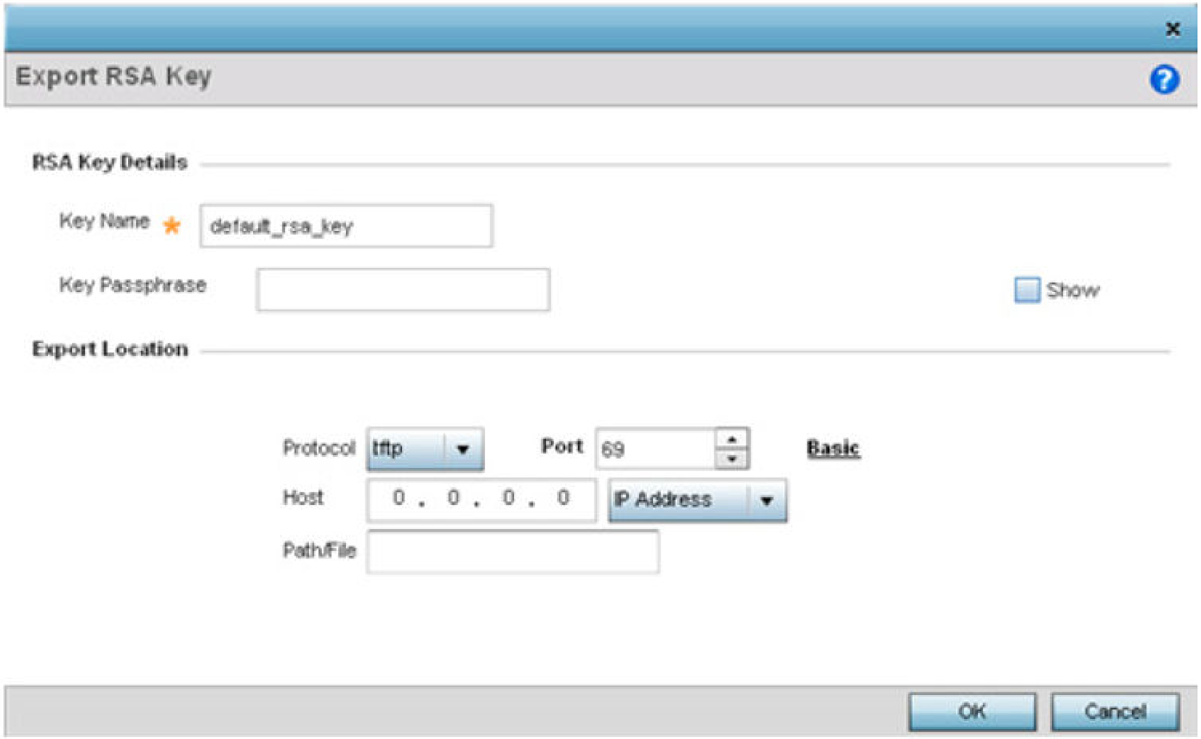
The keys utilized by a controller, service platform or access point can be exported to an external resource for archive and future use.

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.



Key Name: default_rsa_key

Protocol: tftp

Port: 69

Host: 0 . 0 . 0 . 0 IP Address

Path/File

Figure 27: 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: • tftp • ftp • sftp • http • cf • 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`. 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:

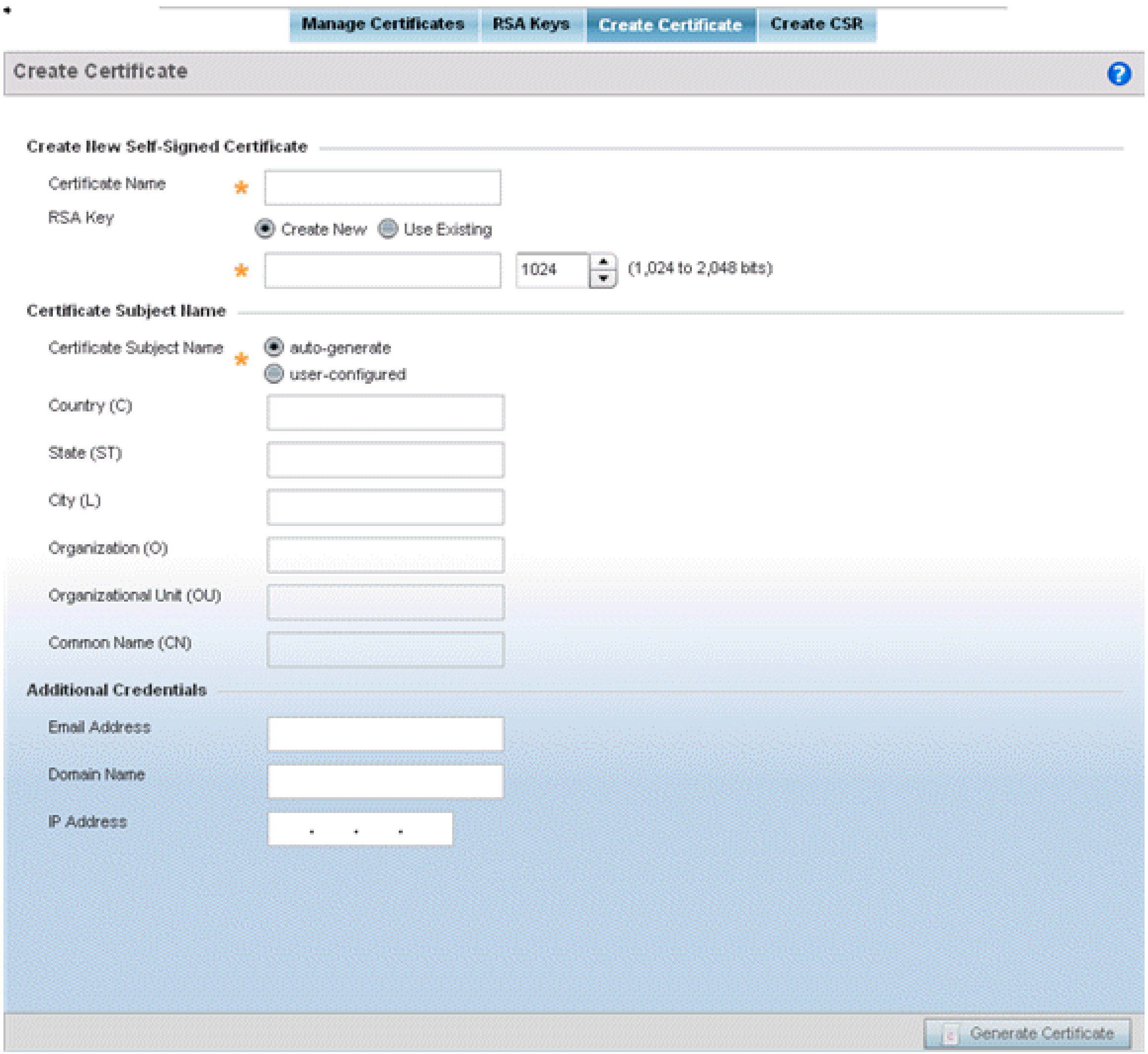
1. Select **RSA Keys** tab from the Certificate Management screen.
2. Select the **Delete** button from within the RSA Keys tab.
3. Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate.
4. Select **OK** to proceed with the deletion, or **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.



RSA Key: ● Create New ○ Use Existing 1024

Certificate Subject Name: ● auto-generate ○ user-configured

Figure 28: 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

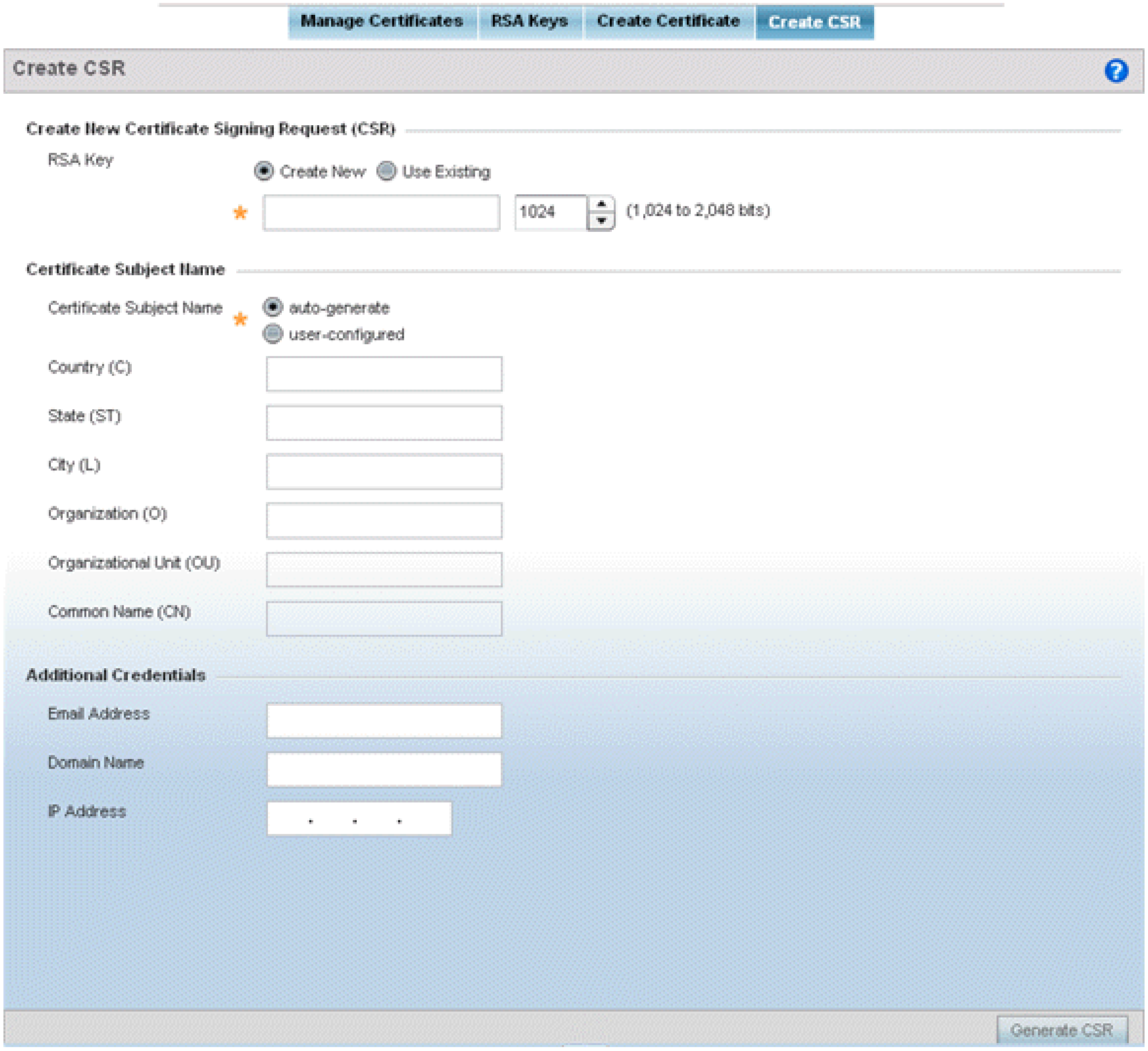
A CSR *(certificate signing request)* is a message from a requester to a certificate authority to apply for a digital certificate. The CSR is composed of a block of encrypted text generated on the server where the certificate will be used. It contains the organization name, common name (domain name), 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.



RSA Key ● Create New ○ Use Existing

1024 (1,024 to 2,048 bits)

Certificate Subject Name ● auto-generate ○ user-configured

Figure 29: 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.

Wired 802.1x Configuration

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. 802.1X allows port based access using authentication. An 802.1X enabled port can be dynamically enabled or disabled depending on user identity or device connection.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure that only the authenticated endpoint is allowed to send traffic.

To configure a device's wired 802.1x configuration:

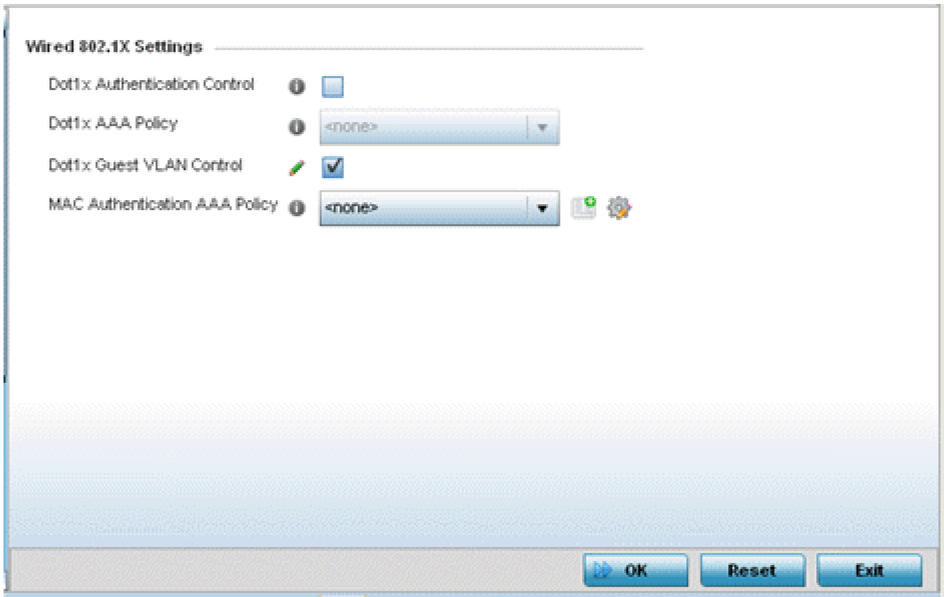
1 Select **Configuration** → **Devices** from the web UI.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Wired 802.1x** from the Device menu options.



Wired 802.1X Settings

Dot1x Authentication Control ☐

Dot1x AAA Policy <none>

Dot1x Guest VLAN Control ☑

MAC Authentication AAA Policy <none>

Figure 30: Wired 802.1x Screen

4 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.

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

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

RF Domain Overrides in Device Configuration

Use RF Domain Overrides to override the configurations set by the target device's original RF Domain assignment.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, these devices share many configuration attributes because their general client support roles are very similar. However, device configurations may need periodic refinement from their original RF Domain administered design.

A controller's or service platform's configuration contains at least one default RF Domain, but it can optionally use additional user-defined RF Domains:

- *Default RF Domain* - Automatically assigned to each controller, service platform, and associated access points by default. A default RF Domain is unique to a specific model.
- *User-Defined RF Domains* - Created by administrators and manually assigned to individual controllers, service platforms, or access points. Can be automatically assigned to access points using adoption policies.

Each controller, service platform, and access point is assigned one RF Domain at a time. However, a user-defined RF Domain can be assigned to multiple devices as required. User-defined RF Domains can be manually assigned or automatically assigned to access points using an auto-provisioning policy. The more devices assigned to a single RF Domain, the greater the likelihood one of the device's configuration requiring an override changing that device's configuration from the original RF Domain assignment shared by other devices of that model type.

To review the RF Domain's original configuration requirements and the options available for a target device, refer to Managing RF Domains on page 748.

To define a device’s RF Domain override configuration, refer to the following sections:

- RF Domain Basic Configuration on page 78
- RF Domain Sensor Configuration on page 80
- RF Domain Client Name Configuration on page 83
- WLAN Override SSID Configuration on page 84

RF Domain Basic Configuration

To override a device's RF Domain basic configuration:

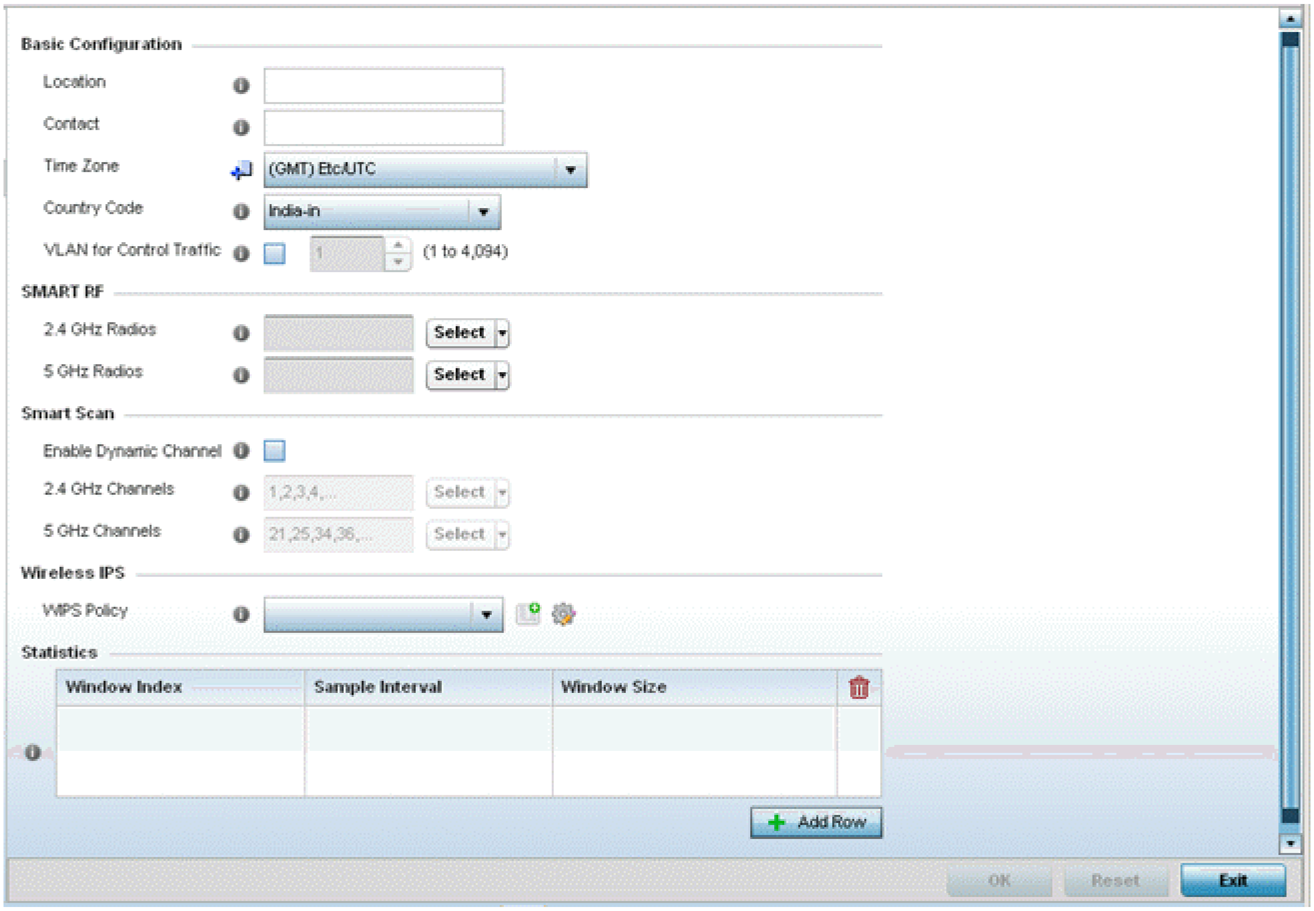
1. Select **Configuration** → **Devices** from the web UI.

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Expand the **RF Domain Overrides** menu option to display its sub-menu options.

4 Select **Basic**.

The selected RF Domain's basic configuration screen displays.



Time Zone (GMT) Etc/UTC

Country Code India-in

VLAN for Control Traffic ☐ 1 (1 to 4,094)

Enable Dynamic Channel ☐

2.4 GHz Channels 1,2,3,4,...

5 GHz Channels 21,25,34,38,...

Figure 31: RF Domain Overrides - Basic 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.

---

5 Refer to the **Basic Configuration** field to review the basic settings defined for the target device's RF Domain configuration, and optionally assign or remove overrides to and from specific parameters.

Location	Provide the 64-character maximum deployment location set for the controller or service platform as part of its RF Domain configuration.
Contact	Enter the 64-character maximum administrative contact for the controller or service platform as part of its RF Domain configuration.
Time Zone	Set the time zone set for the device as part of its RF Domain configuration.
Country Code	Set the country code set for the device as part of its RF Domain configuration. Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

6 Refer to the **Smart RF** section to configure Smart RF policy and dynamic channel settings.

2.4 GHz Radios	Select an override group of channels Smart RF can use for channel compensation adjustments in the 2.4 GHz band.
5 GHz Radios	Select an override group of channels Smart RF can use for channel compensation adjustments in the 5 GHz band.

7 Refer to the **Smart Scan** section to configure Smart RF policy and dynamic channel settings.

Enable Dynamic Channel	Select this option to enable dynamic channel switching for Smart RF radios.
2.4 GHz Channels	Select legal channels from the drop-down menu for 2.4 GHz Smart RF radios. (Device radios transmit in specific channels unique to their country of operation.)
5 GHz Channels	Select legal channels from the drop-down menu for 5 GHz Smart RF radios. (Device radios transmit in specific channels unique to their country of operation.)

8 Use the **WIPS Policy** drop-down menu to apply a WIPS policy to the RF Domain.

The *Wireless Intrusion Protection System* (WIPS) provides continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and 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 lockdown or port suppression.

Click the **Create** icon to define a new WIPS policy that can be applied to the RF Domain, or click the **Edit** icon to modify or override an existing WIPS policy.

For an overview of WIPS and instructions on how to create a WIPS policy that can be used with a RF Domain, see Intrusion Prevention on page 816.

9 Use the **Licenses** drop-down menu to obtain and leverage feature licenses from RF Domain member devices.

10 Click **OK** to save the changes and overrides made to the RF Domain configuration.

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

RF Domain Sensor Configuration

Controllers and service platforms support 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 lockdown or port suppression.

To define ADSP server credentials for WiNG controller or service platform data exchanges:

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

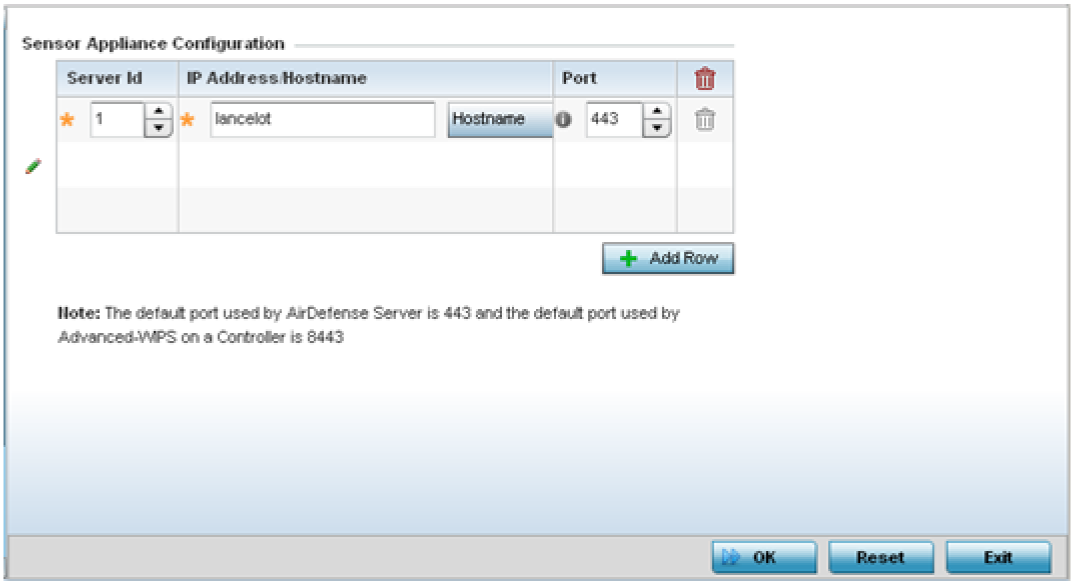
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Expand the **RF Domain Overrides** node and select **Sensor**.

The RF Domain's sensor appliance configuration screen displays.



Sensor Appliance Configuration

Server Id	IP Address/Hostname		Port
1	lancelot	Hostname	443

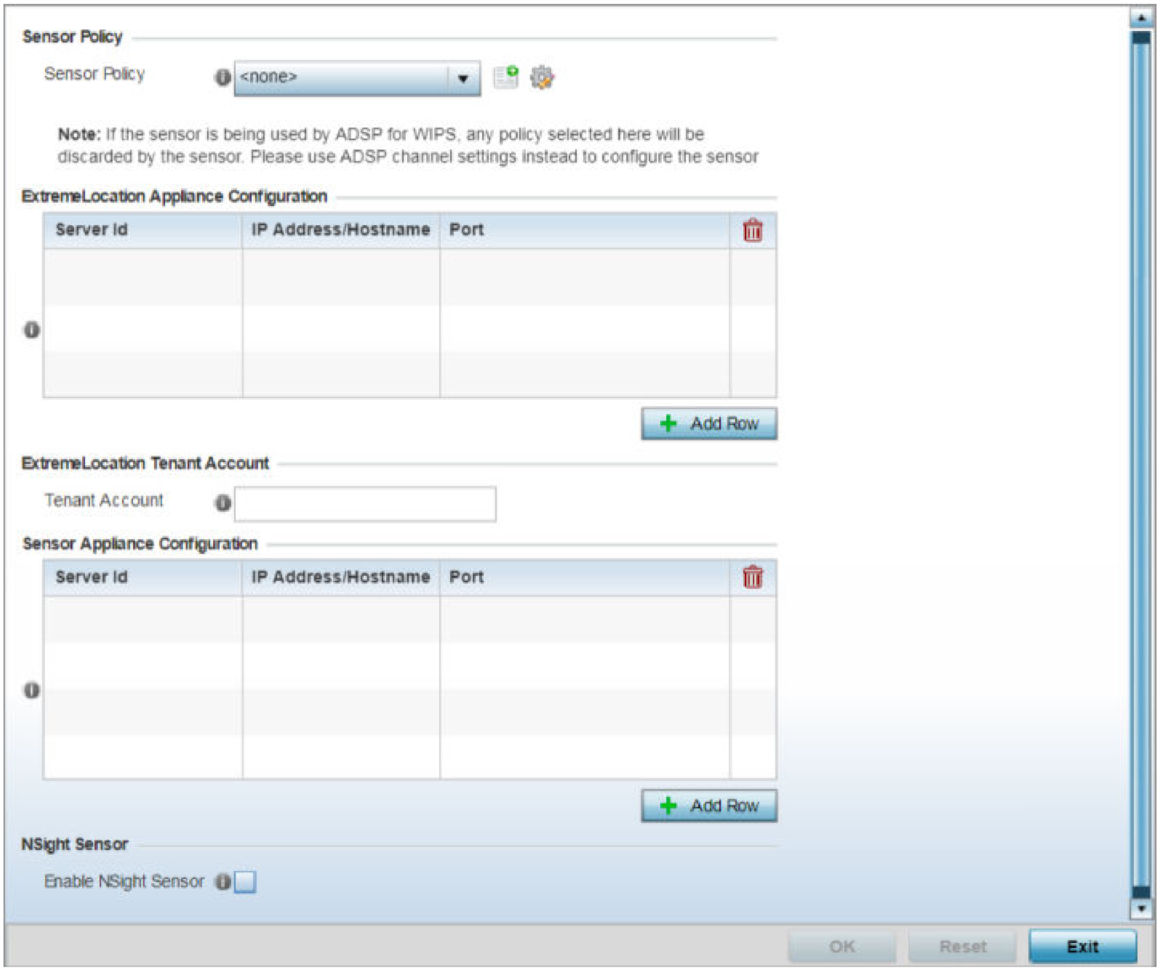
Note: The default port used by AirDefense Server is 443 and the default port used by Advanced-WIPS on a Controller is 8443

Figure 32: RF Domain Overrides - Wireless Controller/Service Platform - Sensor Screen

4 Click **+ Add Row** to populate the **Sensor Appliance Configuration** field with up to three rows for WIPS server credentials:

Server Id	Assign a numerical ID for up to three ADSP server resources. The server with the lowest defined ID is the first reached by the controller or service platform. The default ID is 1.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of each server used as a ADSP sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Specify the port of each ADSP sensor server utilized by RF member devices. The default port is 443.

5 If the device selected is an access point, configure the following settings in addition to the Sensor Appliance Configuration.



Note: If the sensor is being used by ADSP for WIPS, any policy selected here will be discarded by the sensor. Please use ADSP channel settings instead to configure the sensor

Figure 33: RF Domain Overrides - Access Point - Sensor screen

Sensor Policy	Use the Sensor Policy drop-down menu to select a Sensor policy. If no Sensor policy exists, use the **Create** icon to create a new Sensor policy. Or, use the **Edit** icon to edit an existing Sensor policy if required. 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.

6 Enter the ExtremeLocation Tenant's account number in the Tenant Account field. 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.

7 Select the **+ Add Row** button to populate the ExtremeLocation Appliance Configuration field with ExtremeLocation server details:

Server Id Policy	Use the spinner control to assign a numerical ID for the ExtremeLocation server resource. Note: As of now only one server is supported.
IP Address/Hostname	Provide the hostname of the ExtremeLocation server used by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore. Note: Enter the ExtremeLocation server's hostname and not the IP address, as the IP address is likely to periodically change in order to balance load across multiple Location servers.

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

9 Click **OK** to save the changes to the sensor configuration.

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

RF Domain Client Name Configuration

To override the device's RF Domain client name configuration:

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

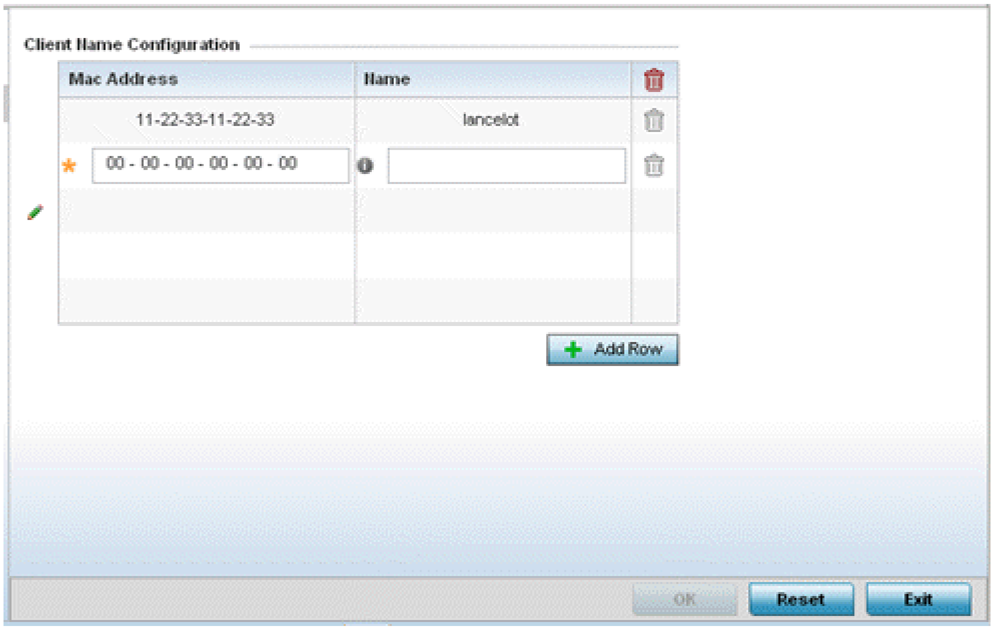
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

The selected device's configuration menu displays.

3 Expand the **RF Domain Overrides** node and select **Client Name**.

The Client Name Configuration screen displays.



Client Name Configuration

Mac Address	Name
11-22-33-11-22-33	lancelot
00 - 00 - 00 - 00 - 00 - 00	

Figure 34: RF Domain Overrides - 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 Select **OK** to save the changes to the configuration.

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

WLAN Override SSID Configuration

To override an RF Domain's WLAN configurations:

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

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

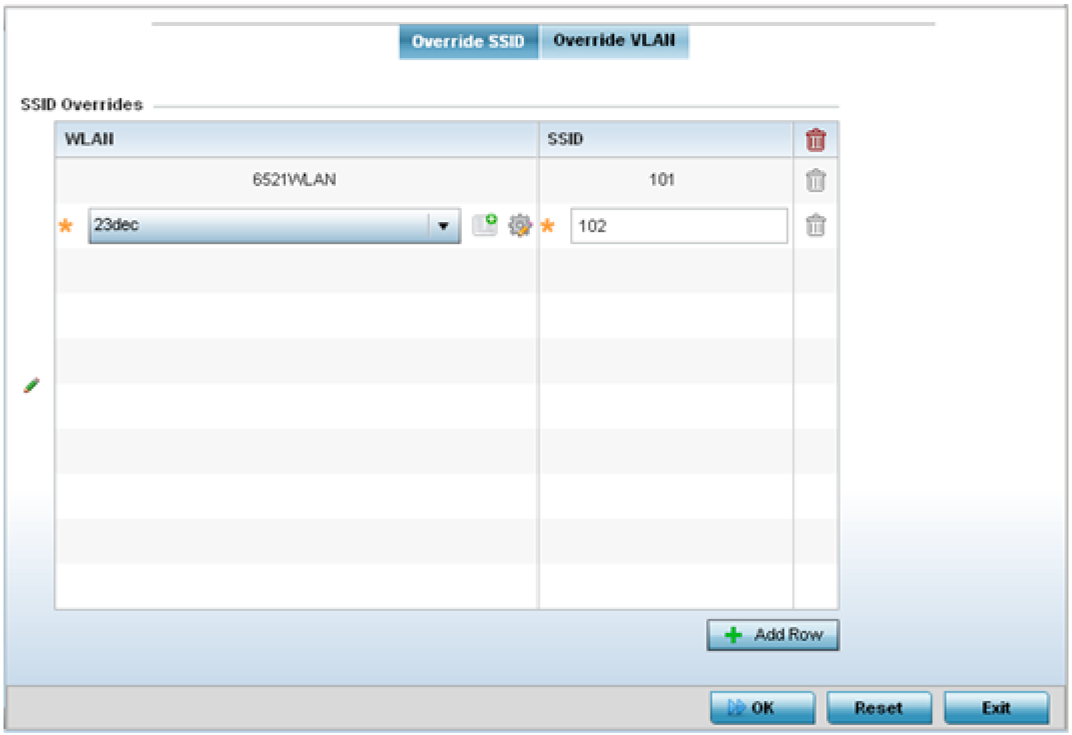
You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Expand the **RF Domain Overrides** menu and select **WLAN Override**.

Note

The **WLAN Override** option is available only for access points – not for controllers or service platforms.

The WLAN Override screen displays with the Override SSID tab selected by default.



SSID Overrides

WLAN	SSID
6521WLAN	101
23dec	102

Figure 35: WLAN Override screen - Override SSID Tab

4 Define up to three overrides for the listed WLAN SSID assignment:

WLAN	Optionally use the drop-down menu to change the WLAN assignment for the listed access point. Click the **Create** icon to define a new WLAN configuration, or click the **Edit** icon to modify an existing WLAN configuration.
SSID	Optionally change the SSID associated with the WLAN. The WLAN name is auto-generated using the SSID until it is changed (overridden). The maximum number of characters used for the SSID is 32.

5 Click **+ Add Row** as needed to add additional WLAN SSID overrides.

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.

6 Click **OK** to save the changes and overrides.

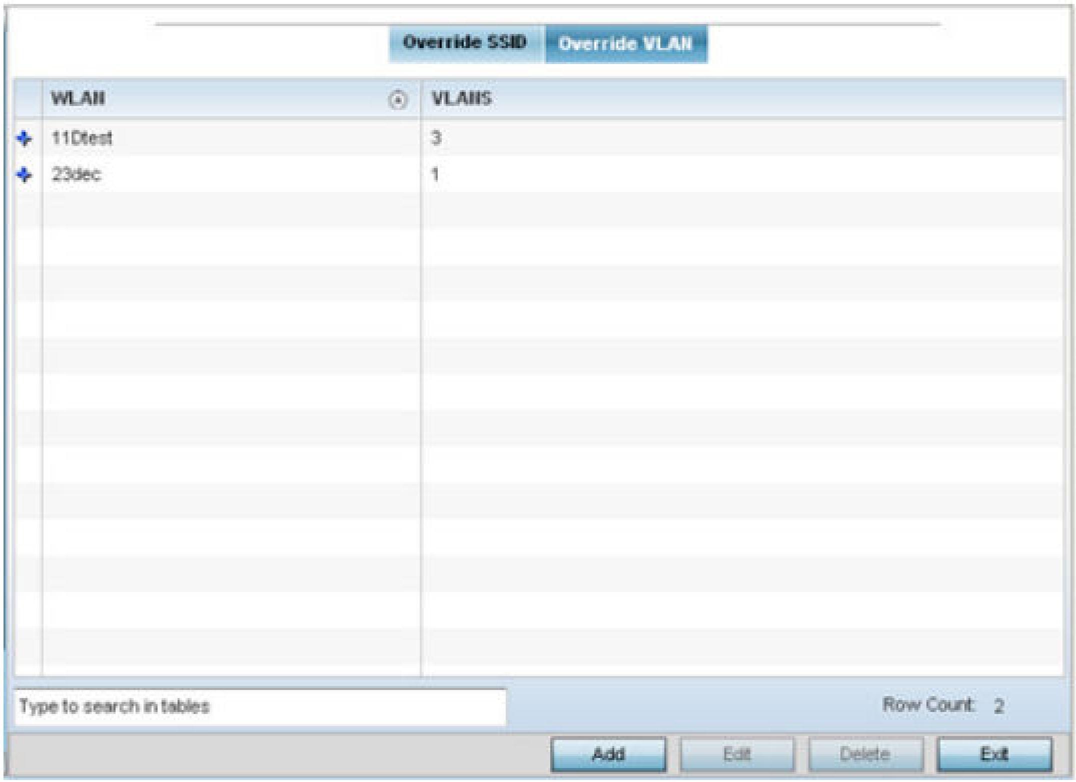
Click **Reset** to revert to the last saved configuration.

WLAN Override VLAN Configuration

1 Select the Override VLAN tab.

The Override VLAN tab displays VLANs assigned to the access point's WLAN. Review existing VLAN assignment overrides, add new configurations or edit existing configurations.

The Override VLAN main screen displays. This screen lists existing WLAN to VLAN assignments.



	WLAN	VLANS
✚	11Dtest	3
✚	23dec	1

Figure 36: WLAN Override - Override VLAN Screen

2 Select **Add** to create a new WLAN to VLAN assigment. Or, select an existing configuration and click **Edit** to modify it.

The VLAN Overrides screen diplays.

3 If creating a new WLAN to VLAN assignment, use the WLAN drop-down menu and select the WLAN.

4 In the Override VLAN table, click **+ Add Row** to create a new client limit for a specific WLAN and VLAN, or click **Edit** to modify an existing configuration.

5 Optionally define a VLAN's wireless client limit override configuration.

VLANS	Set a virtual interface ID (1 - 4094).
Wireless Client Limit	Set the number of users permitted on the VLAN. Set the value to 0 to have an unlimited number of users.

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.

6 Click **OK** to save the changes and overrides.

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

Device Profile Overrides

Profiles enable administrators to assign a common set of parameters and policies to controllers, service platforms and access points. Profiles can be used to assign shared or *unique* network, wireless and security parameters within a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. Controllers and service platforms support both default and user defined profiles implementing new features or updating existing parameters to groups of controllers or access points. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations. Power and Adoption overrides apply specifically to access points, while Cluster configuration overrides apply to only controller 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.

Use Profile Overrides to define configurations overriding the parameters set by the target device's original profile assignment.

General Overrides

To review a profile's original configuration requirements and the options available for a target device, refer to General Profile Configuration on page 531.

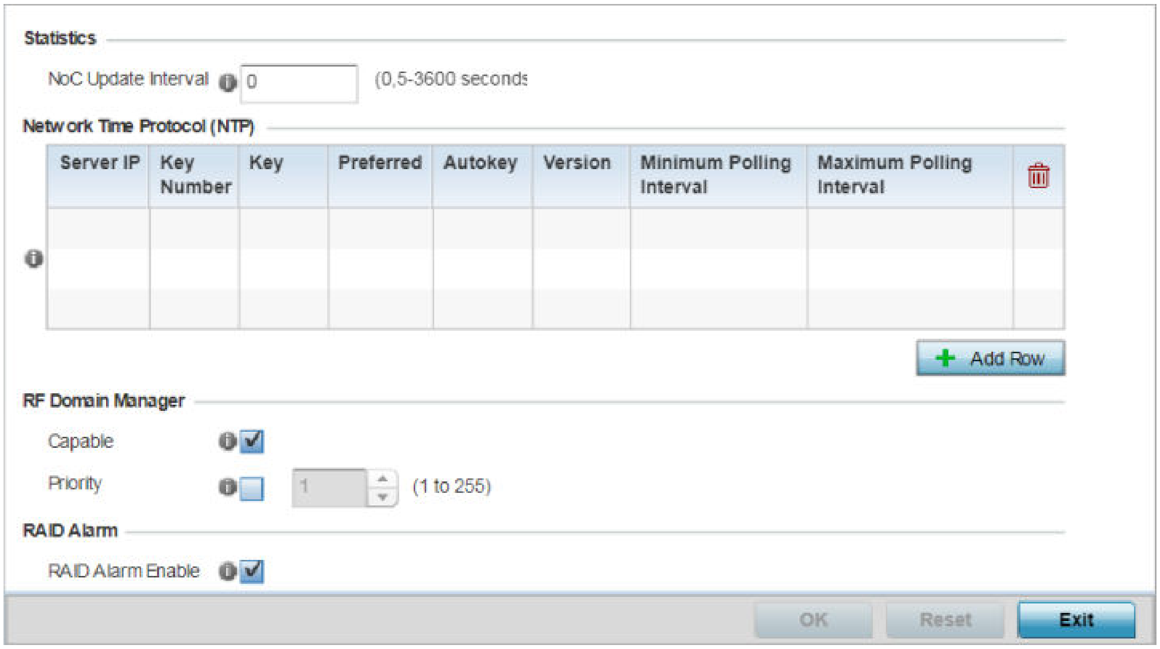
To override the selected device's general profile configuration:

1 Go to **Configuration** → **Devices**. The Device Configuration screen displays by default. This screen lists the devices or peer controllers within the managed network. The listed devices can be other controllers or access points.

2 Select a device, from the displayed list, by double-clicking on the device name. The selected device's configuration menu displays.

Note
Devices can also be selected directly from the device browser in the lower, left-hand side of the UI.

3 Expand the **Profile Overrides** node. The General configuration screen displays by default.



Statistics

NoC Update Interval: 0 (0,5-3600 seconds

Network Time Protocol (NTP)

Server IP	Key Number	Key	Preferred	Autokey	Version	Minimum Polling Interval	Maximum Polling Interval

RF Domain Manager

Capable ☑

Priority ☐ 1 (1 to 255)

RAID Alarm

RAID Alarm Enable ☑

Figure 37: Configuration - Device Configuration - Profile Overrides - General 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 the **Clear Overrides** button. This removes all overrides from the device.

4 Set a **NoC Update Interval** from 5-36500 seconds for updates from the RF Domain manager to the controller. This is the interval at which the RF Domain manager sends updates to its adopting controller.

The default value is 0 seconds, which indicates the auto mode. In the auto mode the controller automatically adjusts the interval based on the information load.

5 Select **+ Add Row** below the NTP *(Network Time Protocol)* table to define (or override) the configurations of NTP server resources the controller uses it obtain its system time. Set the following parameters to define the NTP configuration:

Server IP	Set the IP address of each server as a potential NTP resource.
Key Number	Select the number of the associated *Authentication Key* for the NTP resource.
Key	If an autokey is not being used, manually enter a 64 character maximum key the controller or service platform and NTP resource share to securely interoperate.
Preferred	Select the radio button to designate this particular NTP resource as preferred. If using multiple NTP resources, preferred resources are given first opportunity to connect to the controller and provide NTP calibration.
AutoKey	Select the radio button to enable an *Autokey* configuration for the controller and 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.

6 Refer to the RF Domain Manager field to elect RF Domain Manager devices and assign them a priority in the election process

Capable	Select this option to elect this controller a RF Domain manager capable of storing and provisioning configuration and firmware images for other members of the RF Domain. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain. This setting is enabled by default.
Priority	Select this option to set the priority of this device becoming the RF Domain Manager versus other capable RF Domain members. The higher the value (1 - 255) the higher priority assigned to the device in the RF Domain Manager election process.

7 Refer to the RAID Alarm field to either enable or disable the chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on series service platform.

RAID controller drive arrays are available within the NX 95XX and NX 96XX series service platforms.

These service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. With the WiNG 5.5 release, an administrator can manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface and is not required to reboot the service platform BIOS.

8 Click **OK** to save the changes and overrides made to the general profile configuration.

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

Power Overrides (APs Only)

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 CPLD *(complex programmable logic device)* 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 Navigate to **Configuration** → **Devices**.

The Device Configuration screen displays. This screen lists devices or peer controllers service platforms and access points within the managed network.

2 Select a target device (by double-clicking it) from amongst those displayed on the screen.

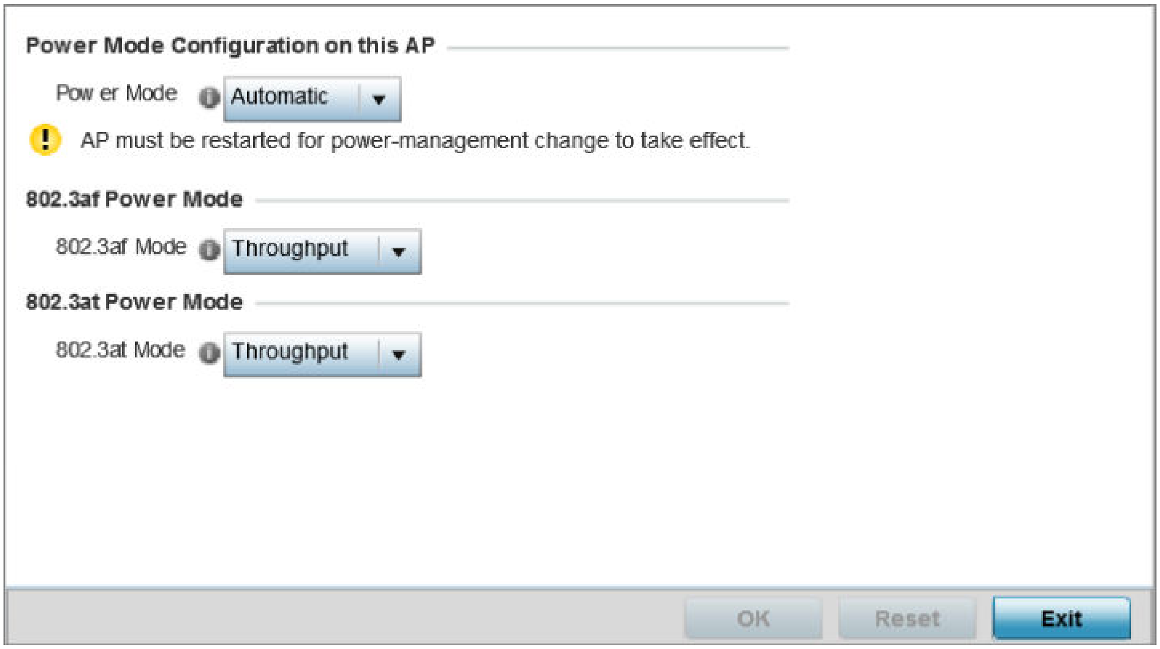
The selected device's configuration menu displays,

Note
Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Expand the **Profile Overrides** node and select **Power**.

Note
The Power option is available only for access points.

The selected access point's power mode configuration screen displays.



Power Mode Configuration on this AP

Pow er Mode: Automatic

AP must be restarted for power-management change to take effect.

802.3af Power Mode

802.3af Mode: Throughput

802.3at Power Mode

802.3at Mode: Throughput

Figure 38: Device Configuration - System Profile - Power Screen

4. 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.

5. 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.

6. Click **OK** to save the changes made to the access point power configuration.

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

Cluster Configuration Overrides (Controllers & Service Platforms Only)

A redundancy group (cluster) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the redundancy group, members discover and establish connections to other peers and provide wireless self-healing support in the event of cluster member failure.

A cluster's AP load balance is typically distributed evenly amongst the controllers or service platforms in the cluster. Define how often this profile is load balanced for AP radio distribution as often as you feel required, as radios can come and go and members can join and exit the cluster. For information on setting a profile's original cluster configuration (before applying an override), see Profile Cluster Configuration (Controllers Only) on page 533.

As cluster memberships increase or decrease and their load requirements change, a profile may need an override applied to best suit a site's cluster requirements.

To apply an override (if required) to a profile cluster configuration:

1. Navigate to **Configuration** → **Devices**.

   The Device Configuration screen displays. This screen lists devices or peer controllers service platforms and access points within the managed network.

2 Select a target device (by double-clicking it) from amongst those displayed on the screen.

The selected device's configuration menu displays,

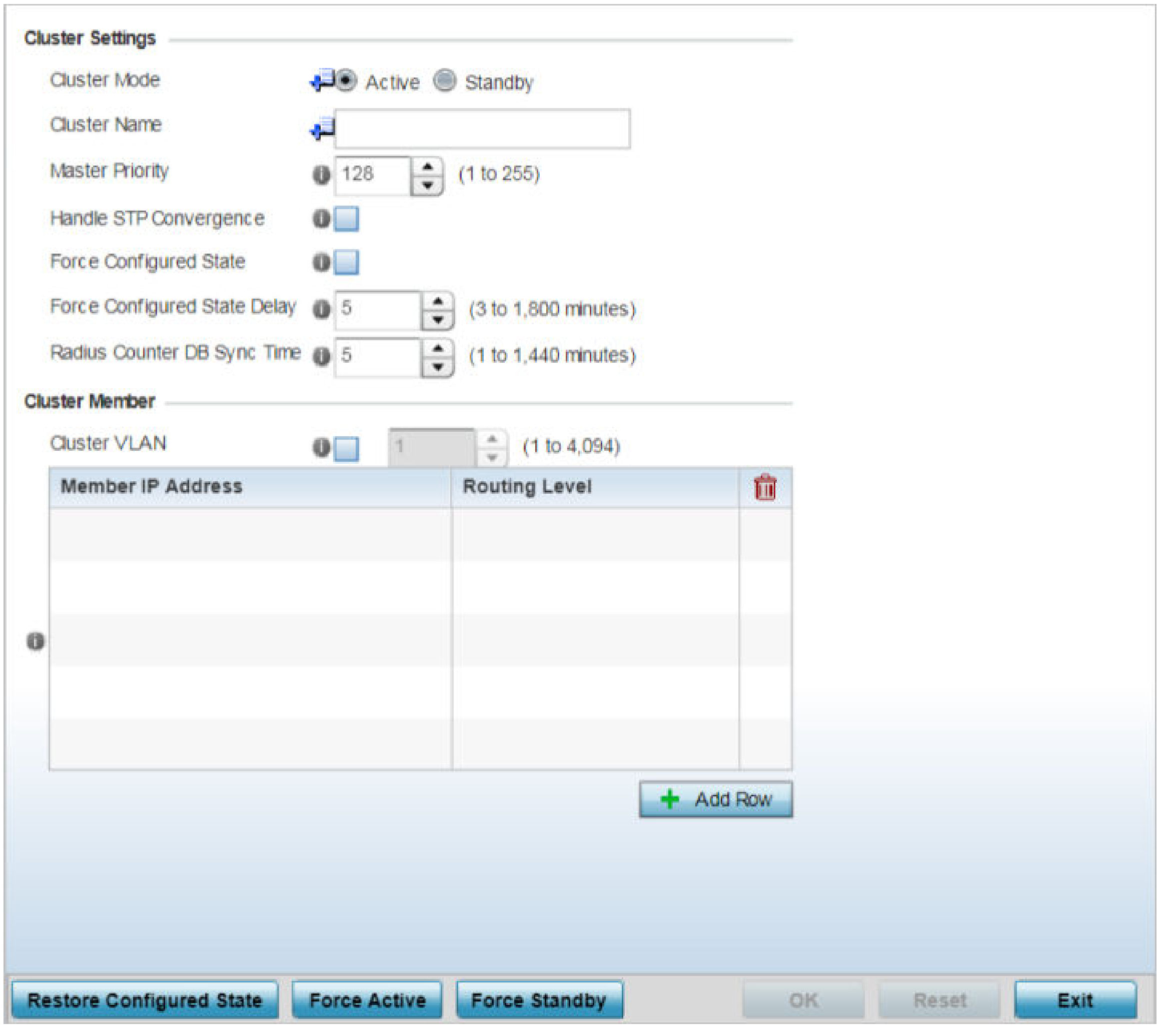
Note

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

---

3 Expand the **Profile Overrides** node and select **Cluster**.

The Cluster override configuration screen displays.



Cluster Settings

Cluster Mode ● Active ○ Standby

Cluster Name

Master Priority 128 (1 to 255)

Handle STP Convergence ☐

Force Configured State ☐

Force Configured State Delay 5 (3 to 1,800 minutes)

Radius Counter DB Sync Time 5 (1 to 1,440 minutes)

Cluster Member

Cluster VLAN ☐ 1 (1 to 4,094)

Member IP Address	Routing Level

Figure 39: Device Configuration - Profile Overrides - Cluster Configuration Override Screen

4 Define the following Cluster Settings overrides:

Cluster Mode	A member can be in either an Active or Standby mode. All active member controllers or service platforms can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point that’s not yet adopted. The default cluster mode is Active and enabled for use with the profile.
Cluster Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
Master Priority	Set a priority value from 1 and 255 with the higher value being given higher priority. This configuration is the device’s priority to become cluster master. In cluster environment one device from cluster members is elected as cluster master. This configuration is the device’s priority to become cluster master. The default is 128.
Handle STP Convergence	Select the radio button to enable Spanning Tree Protocol (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 controller or service platform. The spanning tree protocol disables redundant connections and uses the least costly path to maintain a connection between any two controllers or service platforms in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup. The default setting is disabled.
Force Configured State	Select the radio button to allow this controller or service platform to take over for an active member if it were to fail. A standby controller or service platform in the cluster takes over APs adopted by the failed active member. If the failed active member were to come back up, the active member starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby member releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active member goes down and comes up during the Auto Revert Delay interval. The default value is disabled.
Force Configured State Delay	Specify a delay interval in minutes (3 - 1,800). This is the interval a standby member waits before releasing adopted APs and goes back to a monitoring mode when an active cluster member becomes active again after a failure. The default interval is 5 minutes.
Radius Counter DB Sync Time	Specify a sync time (from 1 - 1,440 minutes) a RADIUS counter database uses as its synchronization interval with the dedicated NTP server resource. The default interval is 5 minutes.

5 Within the Cluster Member field, select **Cluster VLAN** to enable a spinner control to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 - 4094.

Specify the IP addresses of the VLAN’s cluster members using the Member IP Address table.

6 Select **Restore Configured State** to restore this cluster member back into role of taking over for an active member if it were to fail.

7 Select **Force Active** to revert this cluster member back into its default active state and provide the ability to adopt access points.

8 Select **Force Standby** to only adopt access points when an active member has failed or sees an access point that’s not yet adopted

9 Select **OK** to save the changes and overrides made to the profile’s cluster configuration.

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

Controller Adoption Overrides (Controllers Only)

Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the requesting device. Adoption settings are configurable and supported within a profile and applied to other access points supported by the profile.

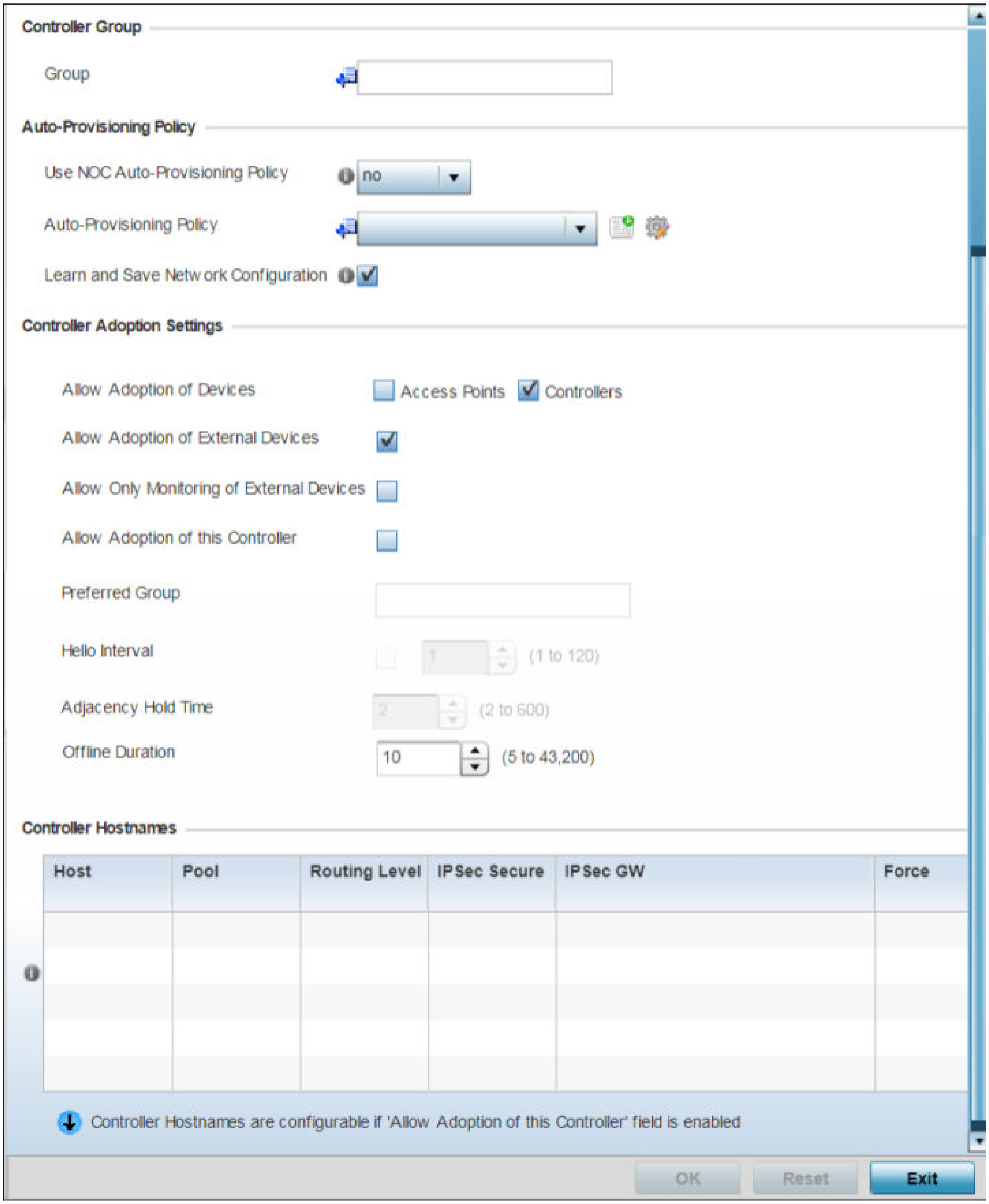
To define a controller or service platform’s adoption capabilities:

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

The Device Configuration screen displays in the right-hand UI. This screen lists all devices within the managed network.

2 Select a controller or service platform from the list. The selected device's configuration menu displays.

3 Go to **Profile Overrides** → **Adoption**. A screen displays, where the selected controller or service platform’s adoption configuration can be set or overridden for a profile.



Controller Group

Group:

Auto-Provisioning Policy

Use NOC Auto-Provisioning Policy: no

Auto-Provisioning Policy:

Learn and Save Network Configuration: ☑

Controller Adoption Settings

Allow Adoption of Devices: ☐ Access Points ☑ Controllers

Allow Adoption of External Devices: ☑

Allow Only Monitoring of External Devices: ☐

Allow Adoption of this Controller: ☐

Preferred Group:

Hello Interval: ☐ 1 (1 to 120)

Adjacency Hold Time: 2 (2 to 600)

Offline Duration: 10 (5 to 43,200)

Controller Hostnames

Host	Pool	Routing Level	IPSec Secure	IPSec GW	Force

Controller Hostnames are configurable if 'Allow Adoption of this Controller' field is enabled

Figure 40: Configuration - Device - Profile Overrides - Adoption

4 Within the Controller Group field, use the Group item to provide the controller group this controller or service platform belongs to. A preferred group can also be selected for the adoption of this controller or service platform. The name of the preferred group cannot exceed 64 characters.

5 Set the following Auto Provision Policy parameters:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC's auto provisioning policy instead of the policy local to the controller or service platform. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default.
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 Set the following Controller Adoption Settings:

Allow Adoption of Devices	Select either **`access points`**, **`Controllers`** or both to refine whether this controller or service platform can adopt 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.

7 In the Controller Hostnames field, select **+ Add Row** and populate the table with IP addresses or hostnames used as access point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) IP Address or a Hostname. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
Force	Enable this setting to create a forced link between an access point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

8 Select **OK** to save the changes to the controller or service platform profile adoption configuration. Select **Reset** to revert to the last saved configuration.

Overriding a Profile's Interface Configuration

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS 4000 controllers and NX 5500 and NX 7500 series service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces.

A controller or service platform 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.

If the profile is configured to support an access point radio, an additional radios option is available, unique to the access point's radio configuration.

Each profile interface configuration can have overrides applied to customize the configuration to a unique deployment. However, once an override is applied to this configuration it becomes independent from the profile that may be shared by a group of devices in a specific deployment and my need careful administration until a profile can be re-applied to the target device. For more information, refer to the following:

- Ethernet Port Override Configuration on page 96
- Virtual Interface Override Configuration on page 109
- Port Channel Override Configuration on page 126
- Overriding VM Interface Configuration on page 134
- Radio Override Configuration on page 139
- Overriding WAN Backhaul Configuration on page 158
- Overriding PPPoE Configuration on page 160
- Overriding Bluetooth Configuration on page 163

Ethernet Port Override Configuration

Use an Ethernet port override to modify a device's Ethernet port configuration.

The following ports are available on RFS 4000 model controllers: ge1, ge2, ge3, ge4, ge5, up1.

The following ports are available to NX series service platform models:

- NX 5500: ge1, ge2
- NX 7500: ge1-ge10, xge1-xge2

GE ports are RJ-45 ports supporting 10/100/1000Mbps.

UP ports supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone because it has a non-blocking 1gbps connection unlike the GE ports.

The following ports are available on access points:

- AP 6522: GE1/POE (LAN)
- AP 6562: GE1/POE (LAN)
- AP 7161: GE1/POE (LAN), GE2 (WAN)
- AP 7502: GE1, fe1, fe2, fe3
- AP-7522: GE1/POE (LAN), GE2 (WAN)

- AP 7562: GE1/POE (LAN), GE2 (WAN)
- AP 7602: GE1/POE (LAN), GE2 (WAN)
- AP-7612: GE1/POE (LAN), GE2 (WAN)
- AP 7622: GE1/POE (LAN)
- AP7632: GE1/POE (LAN)
- AP7662: GE1/POE (LAN), GE2 (WAN)
- AP-8163: GE1/POE (LAN), GE2 (WAN)

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2. (T5 controller managed CPE devices have ports fe1 - fe2).

To set an Ethernet port configuration and potentially apply overrides to the profile's configuration:

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

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device by double-clicking on the device name.

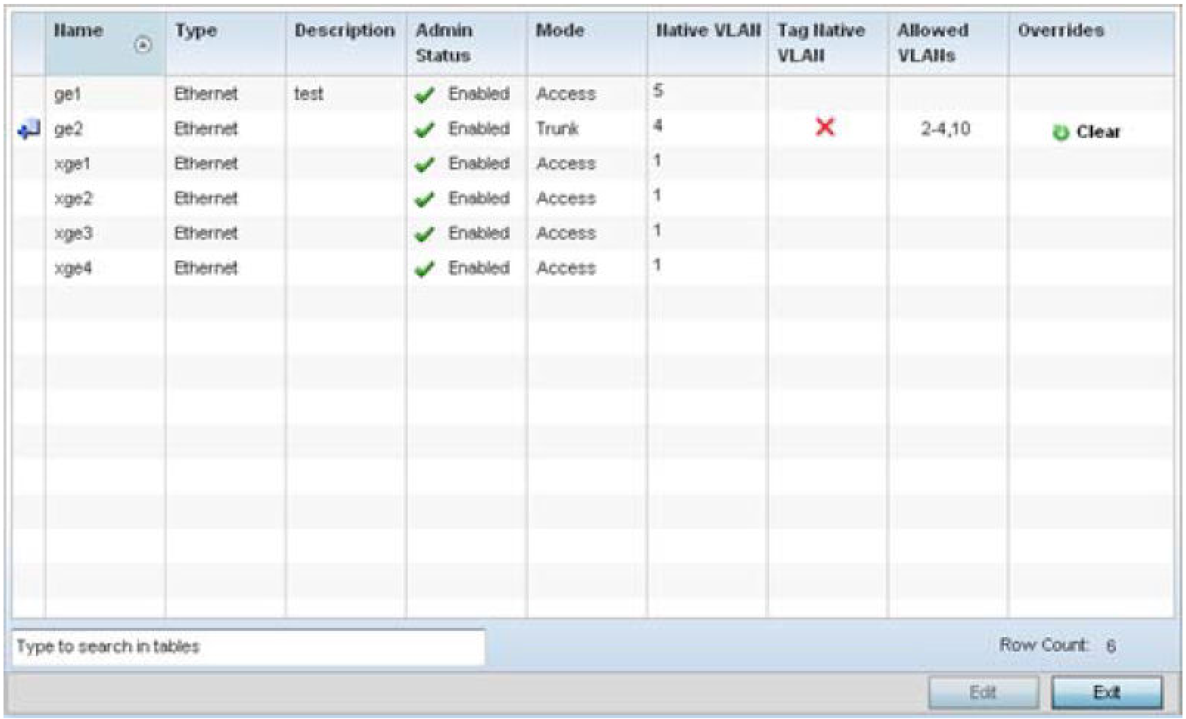
  The selected device's configuration menu displays.

3 Got to **Profile Overrides** → **Interface**.

4 Select **Ethernet Ports**.

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.



	Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs	Overrides
	ge1	Ethernet	test	✓ Enabled	Access	5			
↵	ge2	Ethernet		✓ Enabled	Trunk	4	✗	2-4,10	Clear
	xge1	Ethernet		✓ Enabled	Access	1			
	xge2	Ethernet		✓ Enabled	Access	1			
	xge3	Ethernet		✓ Enabled	Access	1			
	xge4	Ethernet		✓ Enabled	Access	1			

Row Count: 6

Figure 41: Device Overrides - Ethernet Ports Screen

5 Refer to the following to review port status and assess whether an override is warranted:

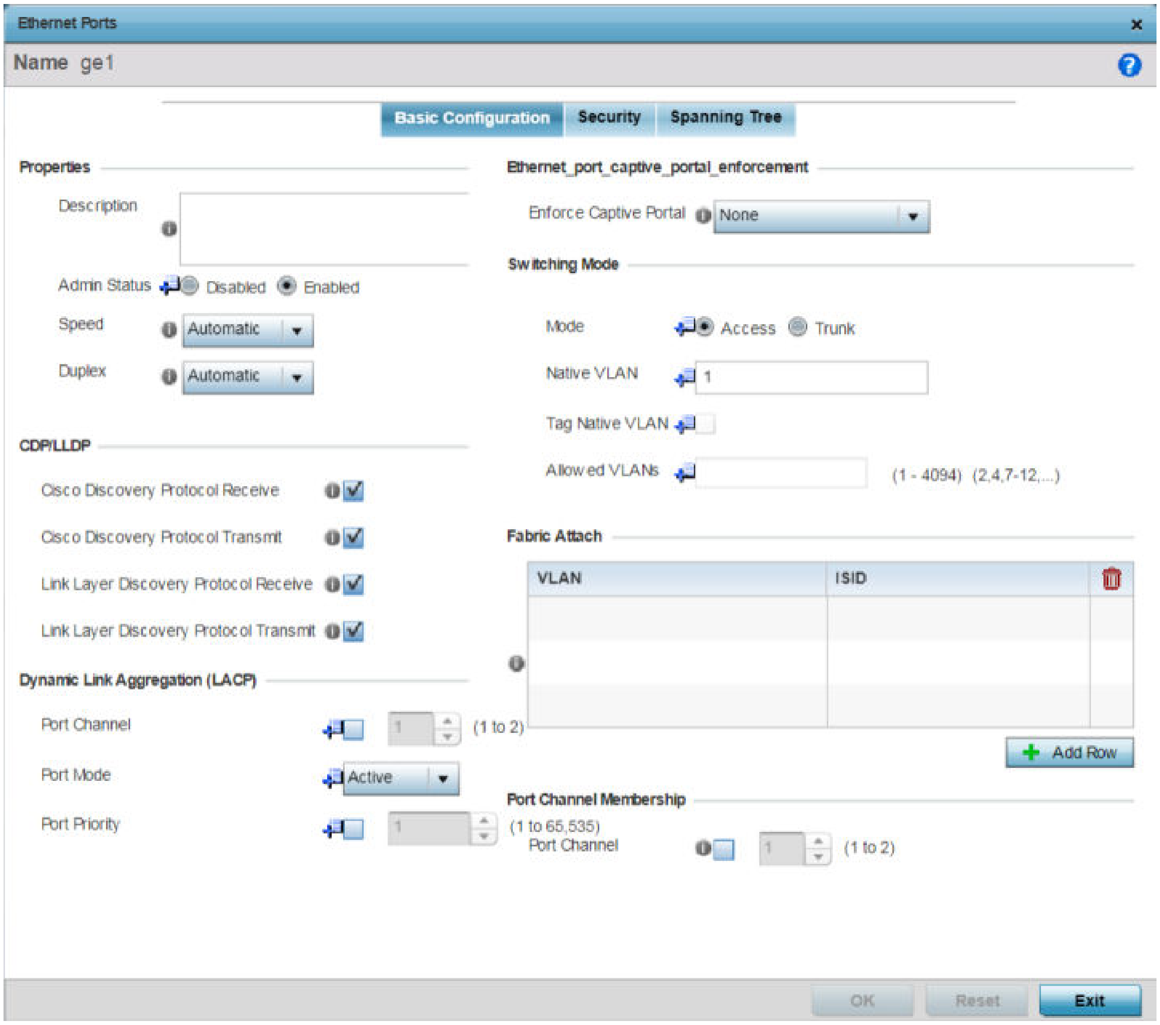
Name	The name of the physical port reporting runtime data and statistics. Supported ports vary by model. • RFS 4000: ge1, ge2, ge3, ge4, ge5, up1 • NX 5500: ge1, ge2 • NX 7500: ge1-ge10, xge1-xge2
Type	The physical port type. `Cooper` is used on RJ45 Ethernet ports, and `Optical` materials are used on fiber optic gigabit Ethernet ports.
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). 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. 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. 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	If overrides have been applied to the port configuration, click **Clear** to clear the overrides and revert to the configuration originally defined by the administrator for this interface.

Overriding Basic Configuration

To edit or override the configuration of an existing port:

1 Select the port from those displayed on the screen and click **Edit**.

The Ethernet Port Basic Configuration screen displays.



Name ge1

Description:
Admin Status: ○ Disabled ● Enabled
Speed: Automatic
Duplex: Automatic
Cisco Discovery Protocol Receive ☑
Cisco Discovery Protocol Transmit ☑
Link Layer Discovery Protocol Receive ☑
Link Layer Discovery Protocol Transmit ☑
Port Channel ☐ 1 (1 to 2)
Port Mode ☐ Active
Port Priority ☐ 1 (1 to 65,535)
Enforce Captive Portal: None
Mode: ● Access ○ Trunk
Native VLAN: 1
Tag Native VLAN ☐
Allowed VLANs: (1 - 4094) (2,4,7-12,...)
Port Channel ☐ 1 (1 to 2)

Figure 42: Ethernet Ports - Basic Configuration Screen

2 Set or override 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 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. 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. 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 port at the same time. Using full duplex, the port can send data while receiving data as well. 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 Set or override the following **Power Over Ethernet (PoE)** parameters (if supported and applicable):

Enable PoE	Select this option to configure the selected controller or service platform port to use PoE *(Power over Ethernet)*. To disable PoE on a port, uncheck this option. PoE is supported on RFS 4000 model controllers. When enabled, the controller or service platform supports 802.3af PoE on each of its ge ports. 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 PoE on the ge port. Set a value from 0 - 40 watts.
Power Priority	Set the power priority for the listed port to either to either **`Critical`**, **`High`**, or **`Low`**. This is the priority assigned to this port versus the power requirements of the other supports available on the controller or service platform.

5 Select **Enforce Captive Portal** to automatically apply captive portal access permission rules to data transmitted over this specific Ethernet port.

This setting is disabled by default.

A captive portal is an access policy for providing temporary and restrictive 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 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.

For information on configuring a captive portal policy, see Captive Portal Policies on page 834.

6 Set or override the following **Switching Mode** parameters to apply to the Ethernet port configuration:

Mode	Set the VLAN switching mode over the port: either **`Access`** or **`Trunk`**. If you select **Access**, 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. If you select **Trunk**, the port allows 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. **`Access`** is the default mode.
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 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: AP 7562, AP 7602, AP-7612, AP-8432, AP-8533, NX 5500, NX 7500, NX 95XX, NX 96XX and VX 9000. 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. 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 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. 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. The passive port only responds to LACPDU received from its corresponding active port. 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. 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.

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. Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port. 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. 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 **Port Channel** in the Port Channel Membership area, and define or override a setting from 1 - 8 using the spinner control.

   This sets the channel group for the port.
10. Click **OK** to save the changes and overrides made to the Ethernet port's basic configuration.

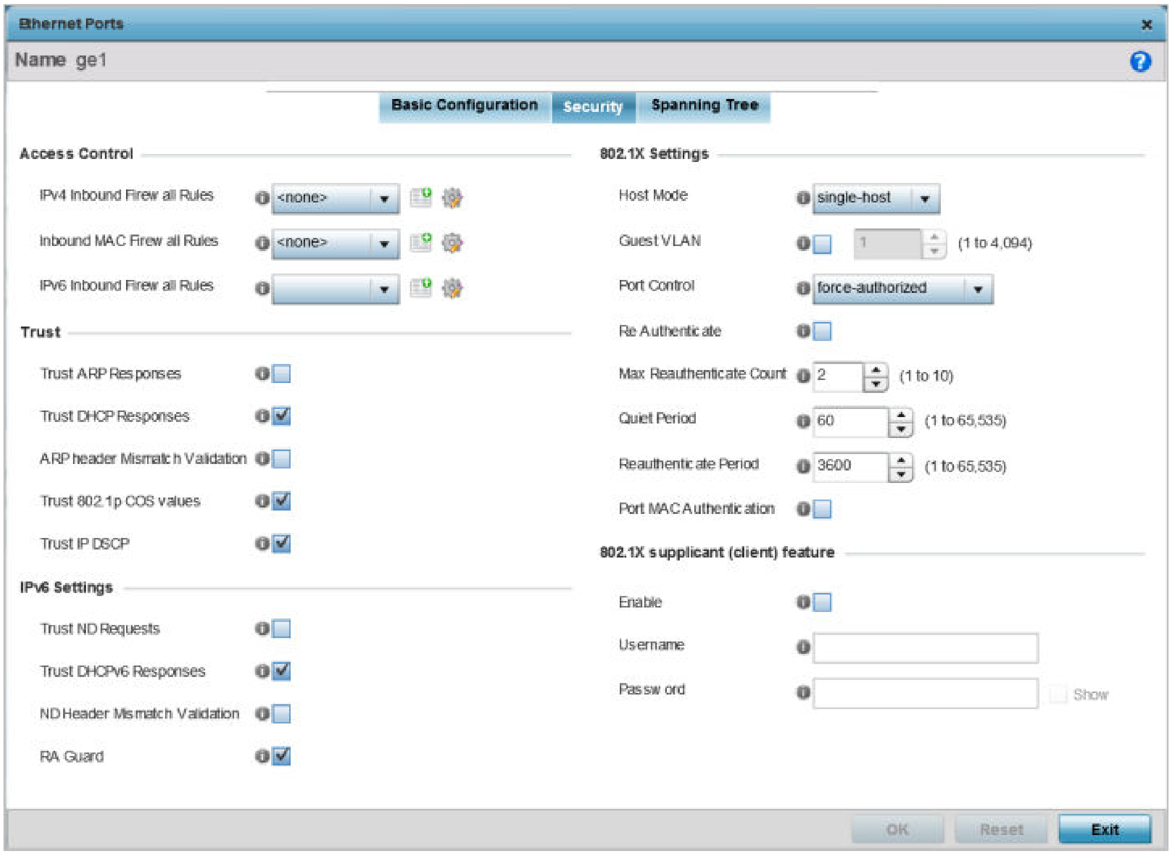
    Click **Reset** to revert to the last saved configuration.

Overriding Security Configuration

To edit or override security configuration of a port:

1. Select the **Security** tab.

   The selected port's security configuration screen displays.



Name ge1

Access Control

IPv4 Inbound Firewall Rules: <none>

Inbound MAC Firewall Rules: <none>

IPv6 Inbound Firewall Rules:

Trust

Trust ARP Responses ☐

Trust DHCP Responses ☑

ARP header Mismatch Validation ☐

Trust 802.1p COS values ☑

Trust IP DSCP ☑

IPv6 Settings

Trust ND Requests ☐

Trust DHCPv6 Responses ☑

ND Header Mismatch Validation ☐

RA Guard ☑

802.1X Settings

Host Mode: single-host

Guest VLAN ☐ 1 (1 to 4,094)

Port Control: force-authorized

Re Authenticate ☐

Max Reauthenticate Count: 2 (1 to 10)

Quiet Period: 60 (1 to 65,535)

Reauthenticate Period: 3600 (1 to 65,535)

Port MAC Authentication ☐

802.1X supplicant (client) feature

Enable ☐

Username:

Password: ☐ Show

Figure 43: Ethernet Ports - Security Screen

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.

   a. Use the **MAC Inbound Firewall Rules** drop-down menus to select the 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.

   b. Use the **IPv4 Inbound Firewall Rules** 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.

   c. Use the **IPv6 Inbound Firewall Rules** 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.

   d. If no firewall rules meet the data protection needs of the target port configuration, select the **Create** icon to define a new firewall rule or the **Edit** icon to modify an existing firewall rule.

      For more information, see Configuring IP Firewall Rules on page 789 or Wireless Firewall on page 771.

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	Select the port mode for 802.1X authentication. Select **`single-host`** to bridge traffic from a single authenticated host. Select **`multi-host`** 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. Select one of the following options: • **`Automatic`** – The port is set to the state as received from the authentication server. • **`force-authorized`** – Any traffic on the port is considered authenticated and is bridged as configured. • **`force-unauthorized`** – Any traffic on the port is considered unauthenticated and is not bridged. The default setting is **`force-authorized`**.
Reauthenticate	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 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 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	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 RFS 4000 model controllers. 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, select **Enable** 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.

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.

Overriding Spanning Tree Configuration

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.

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.

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.

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.

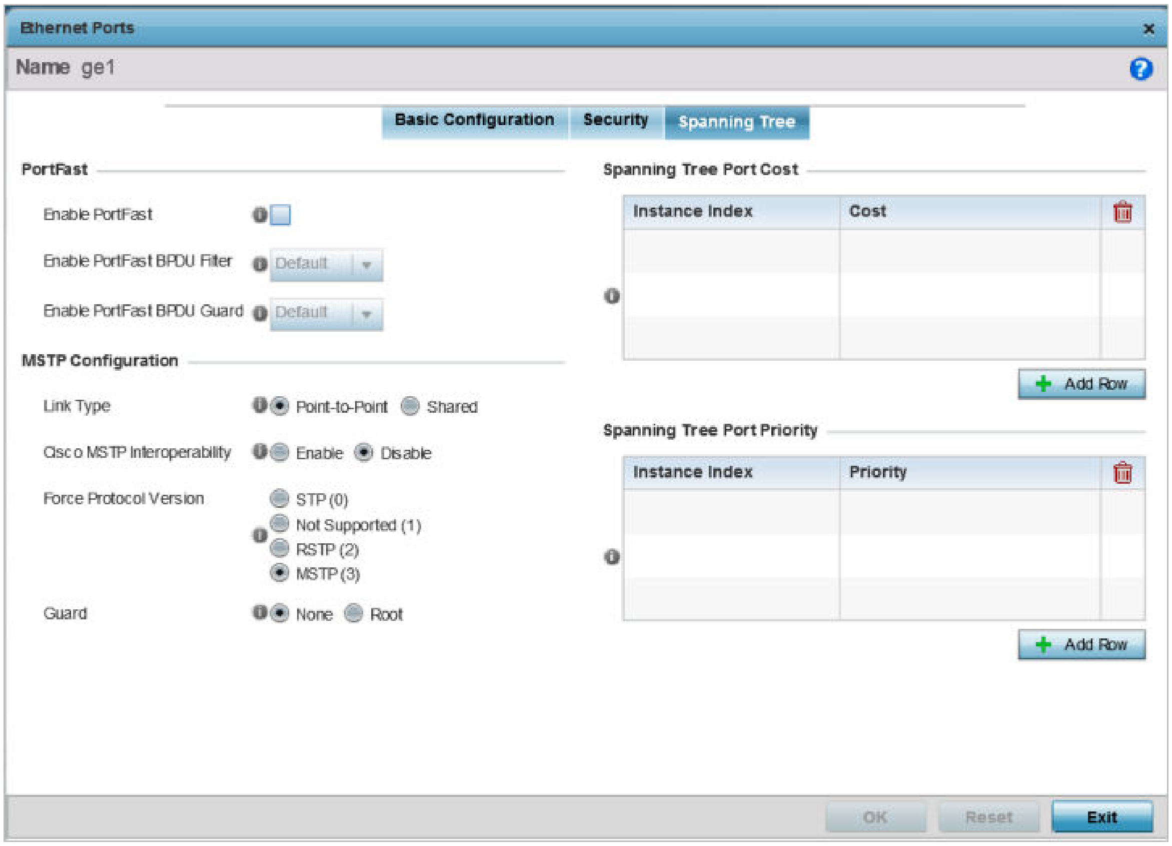
If there is only one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

An MSTP supported deployment uses multiple MST regions with multiple MSTIs *(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 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.

To edit or override spanning tree configuration of the selected port:

1 Select **Spanning Tree** tab.



Name ge1

Enable PortFast ☐

Enable PortFast BPDU Filter Default

Enable PortFast BPDU Guard Default

Link Type ● Point-to-Point ○ Shared

Cisco MSTP Interoperability ○ Enable ● Disable

Force Protocol Version ○ STP (0) ○ Not Supported (1) ○ RSTP (2) ● MSTP (3)

Guard ● None ○ Root

Figure 44: Ethernet Ports - Spanning Tree Screen

2 Set the following **MSTP Configuration** settings:

Enable as Edge Port	Select this option to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port.
Link Type	Select either **`Point-to-Point`** or **`Shared`**. When *Point-to-Point* is selected, the port is treated as connected to a point-to-point link. When *Shared* is selected, the port is shared between multiple devices. An example of a **`Point-to-Point`** connection is a port that is connected to a controller or service platform. An example of a **`Shared`** connection is a port that is connected to a hub.
Cisco MSTP Interoperability	**`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	Select **`STP`** to use the standard Spanning Tree Protocol. Select **`RSTP`** to use Rapid Spanning Tree Protocol. Select **`MSTP`** to use Multiple Spanning Tree Protocol. Select **`Not Supported`** to disable spanning tree protocol for this interface. MSTP is the default setting.
Guard	Select **Root** radio to ensure that 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. Select **None** to disable this feature.

Enable PortFast	Select this option to enable drop-down menus for both the **`Enable PortFast BPDU Filter`** and **`Enable PortFast BPDU Guard`** options for the port.
Enable PortFast BPDU Filter	Select this option 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.
Enable PortFast BPDU Guard	Select this option to invoke a BPDU guard for this PortFast enabled port. Enabling the BPDU guard feature means that this PortFast enabled port will shut down when it receives BPDU messages.

3 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 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.

Table 3: 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.

4 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.

The lower the priority, the greater likelihood of the port becoming a designated port. Applying a higher override value impacts the port's likelihood of becoming a designated port..

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

5 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.

Virtual Interface Override 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** from the web UI.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

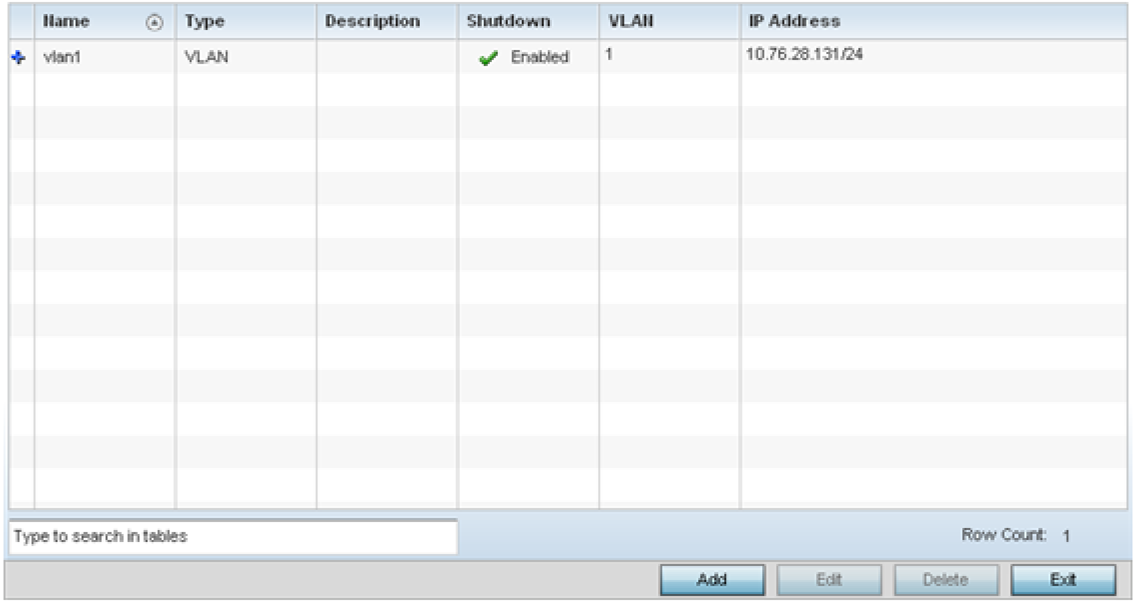
  You can also select a target device by double-clicking it in the list in the Device Configuration screen.

  The selected device's configuration menu displays.

3 Select **Profile Overrides** → **Interface**.

4 Select **Virtual Interfaces**.

Note
A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove overrides from a device, go to the Basic Configuration screen for the device and select **Clear Overrides**.



	Name	Type	Description	Shutdown	VLAN	IP Address
✚	vlan1	VLAN		✓ Enabled	1	10.76.28.131/24

Row Count: 1

Figure 45: Profile Overrides - Virtual Interfaces Screen

5 Review the following parameters unique to each virtual interface configuration to determine whether a parameter override is warranted:

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.

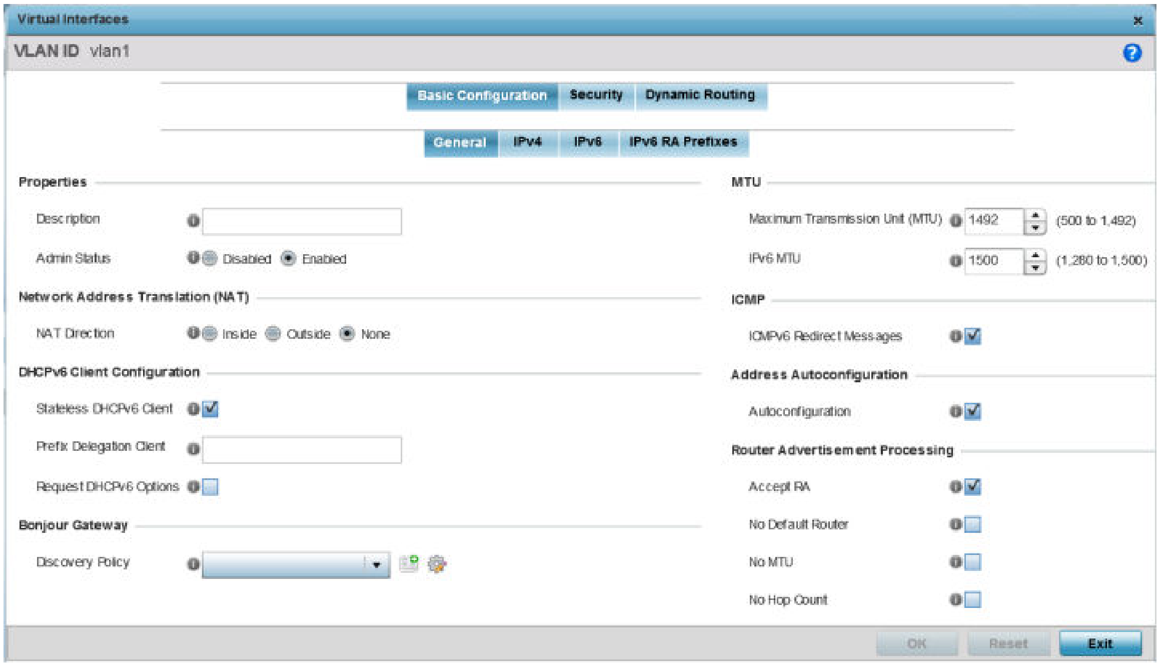
After reviewing the configurations of existing virtual interfaces, determine whether a new interface needs to be created, an existing virtual interface needs to be edited (overridden), or an existing virtual interface needs to be deleted.

Overriding General Configuration

To override 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.



VLAN ID vlan1

Properties
Description
Admin Status ○ Disabled ● Enabled

Network Address Translation (NAT)
NAT Direction ○ Inside ○ Outside ● None

DHCPv6 Client Configuration
Stateless DHCPv6 Client ☑
Prefix Delegation Client
Request DHCPv6 Options ☐

Bonjour Gateway
Discovery Policy

MTU
Maximum Transmission Unit (MTU) 1492 (500 to 1,492)
IPv6 MTU 1500 (1,280 to 1,500)

ICMP
ICMPv6 Redirect Messages ☑

Address Autoconfiguration
Autoconfiguration ☑

Router Advertisement Processing
Accept RA ☑
No Default Router ☐
No MTU ☐
No Hop Count ☐

Figure 46: 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.

Note

Refer to Setting the Profile's NAT Configuration on page 698 for instructions on creating a profile's NAT configuration.

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.

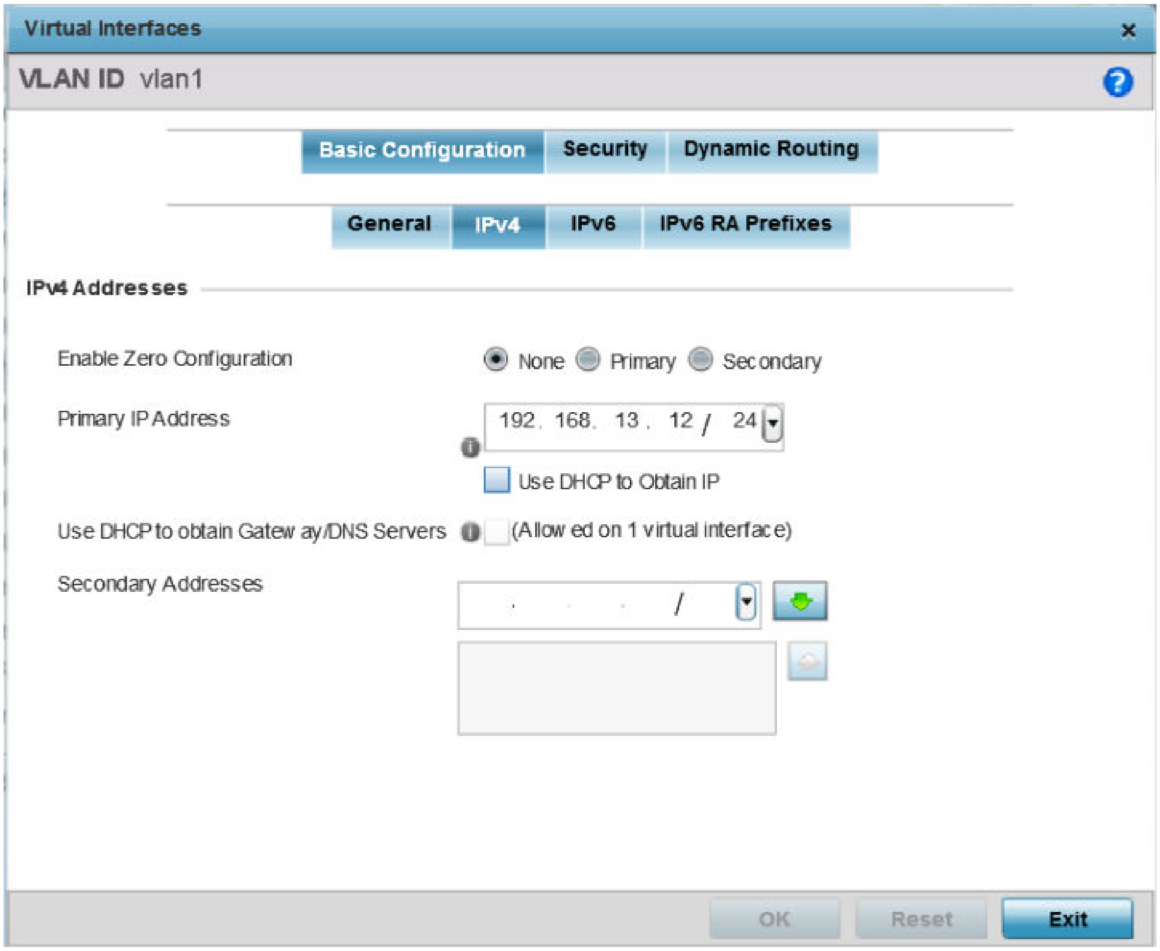
Click **Reset** to revert to the last saved configuration.

Overriding IPv4 Configuration

To override 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).



VLAN ID vlan1

IPv4 Addresses

Enable Zero Configuration ● None ○ Primary ○ Secondary

Primary IP Address 192.168.13.12 / 24

☐ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ☐ (Allowed on 1 virtual interface)

Secondary Addresses

Figure 47: 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 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the virtual interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
DHCP Relay	Provide IP addresses for DHCP server relay resources. 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.

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

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

Overriding 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 override the VLAN IPv6 configuration:

1 Select the **IPv6** tab.

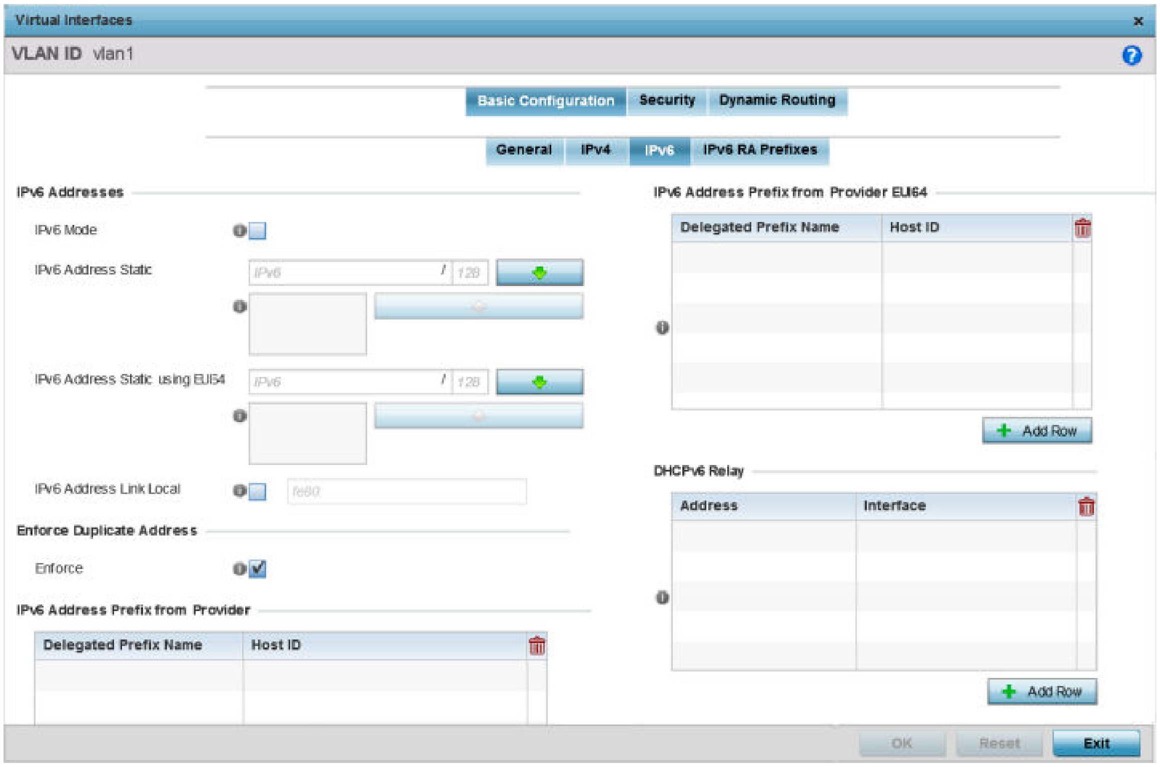


Figure 48: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab

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.

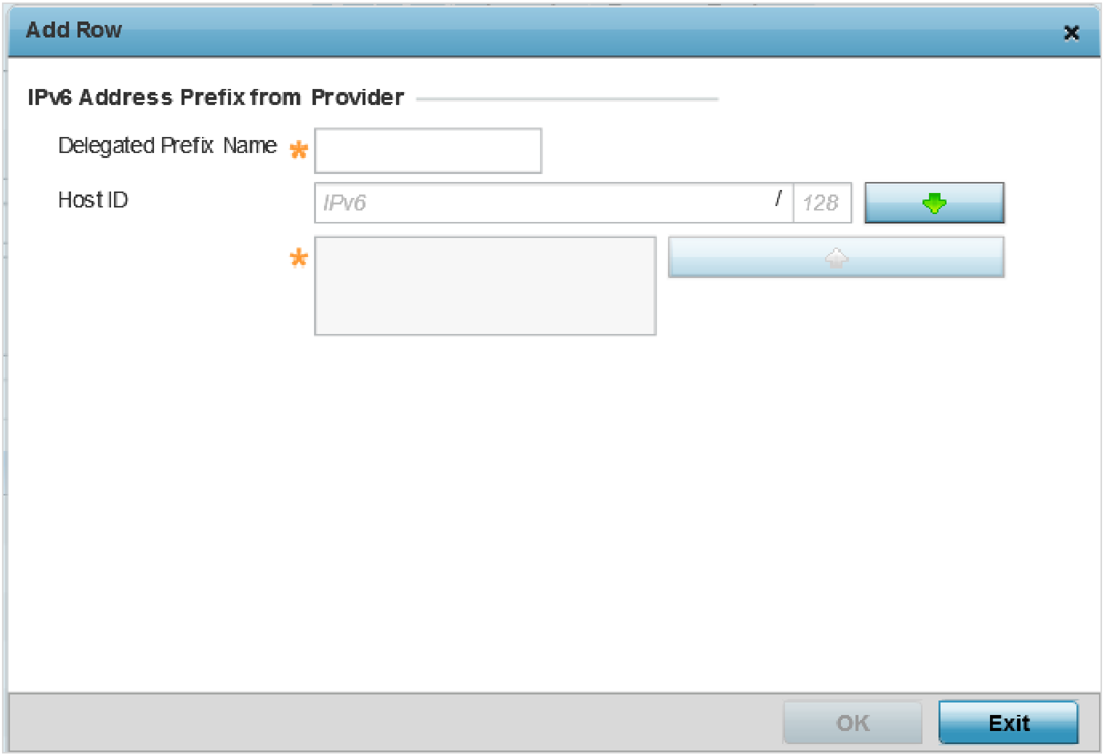


Figure 49: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider

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.

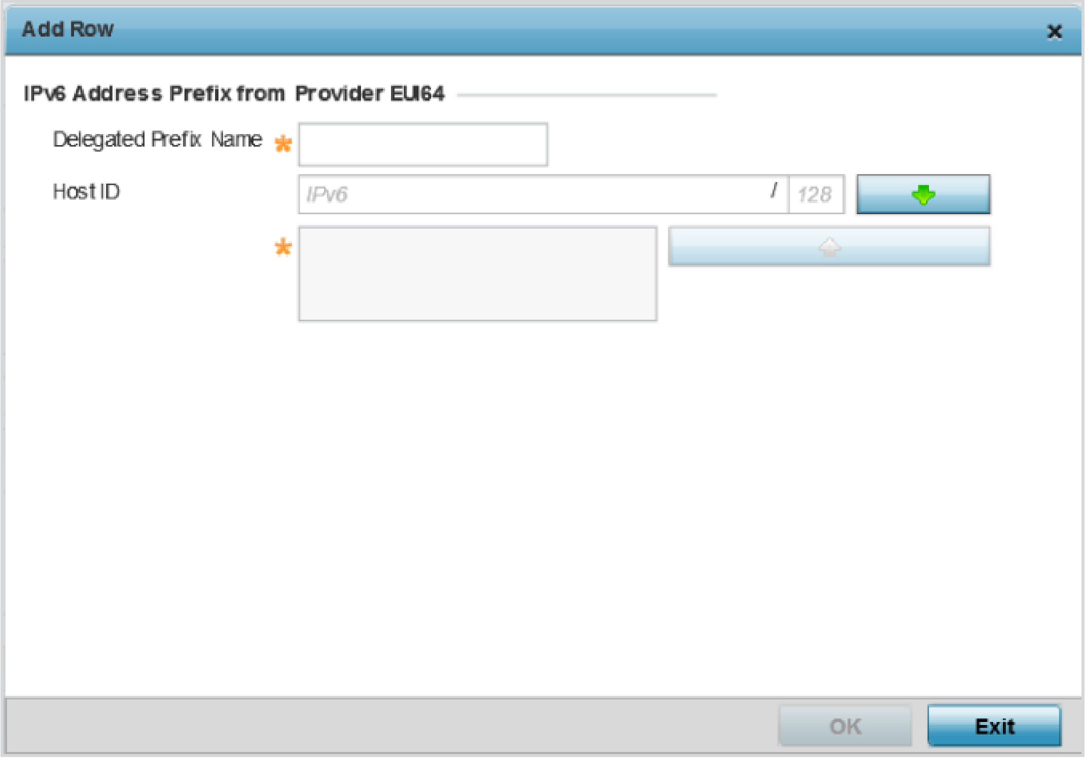


Figure 50: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64

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.

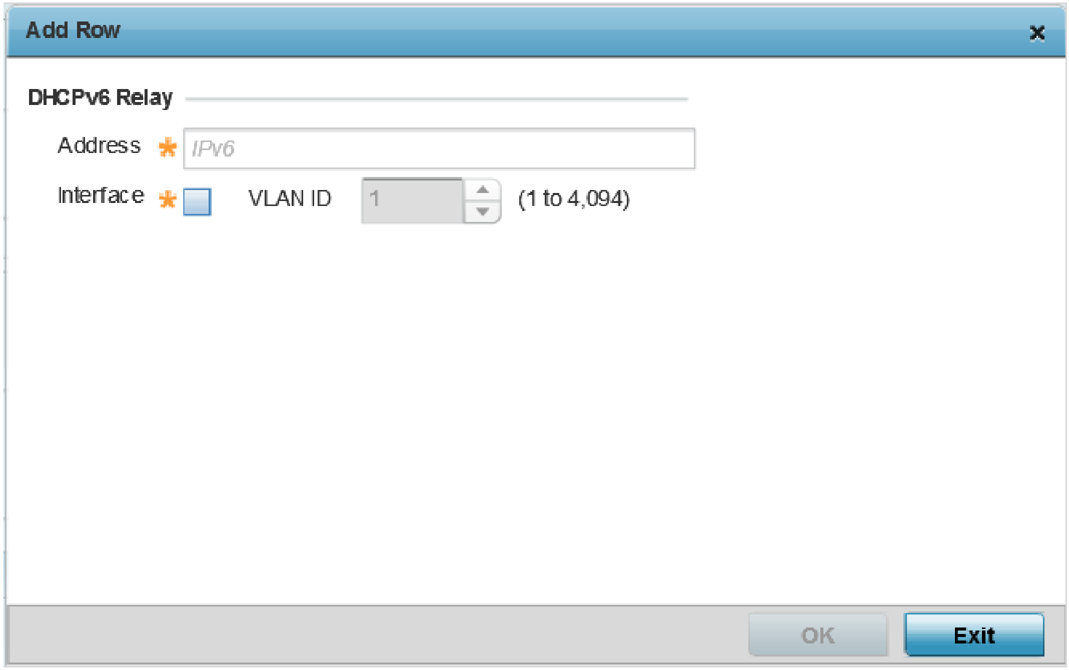


Figure 51: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add DHCPv6 Relay

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.

Overriding IPv6 RA Prefixes

To override the VLAN IPv6 RA Prefixes configuration:

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

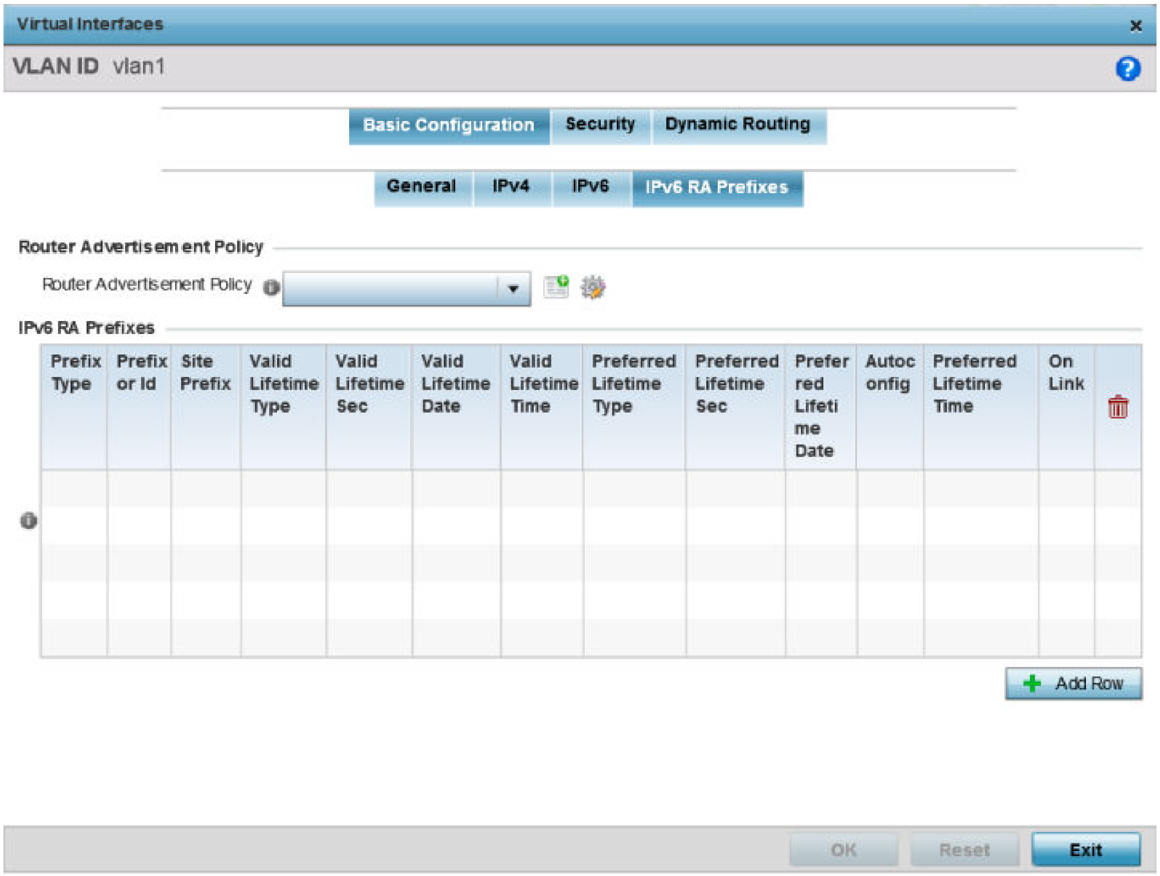


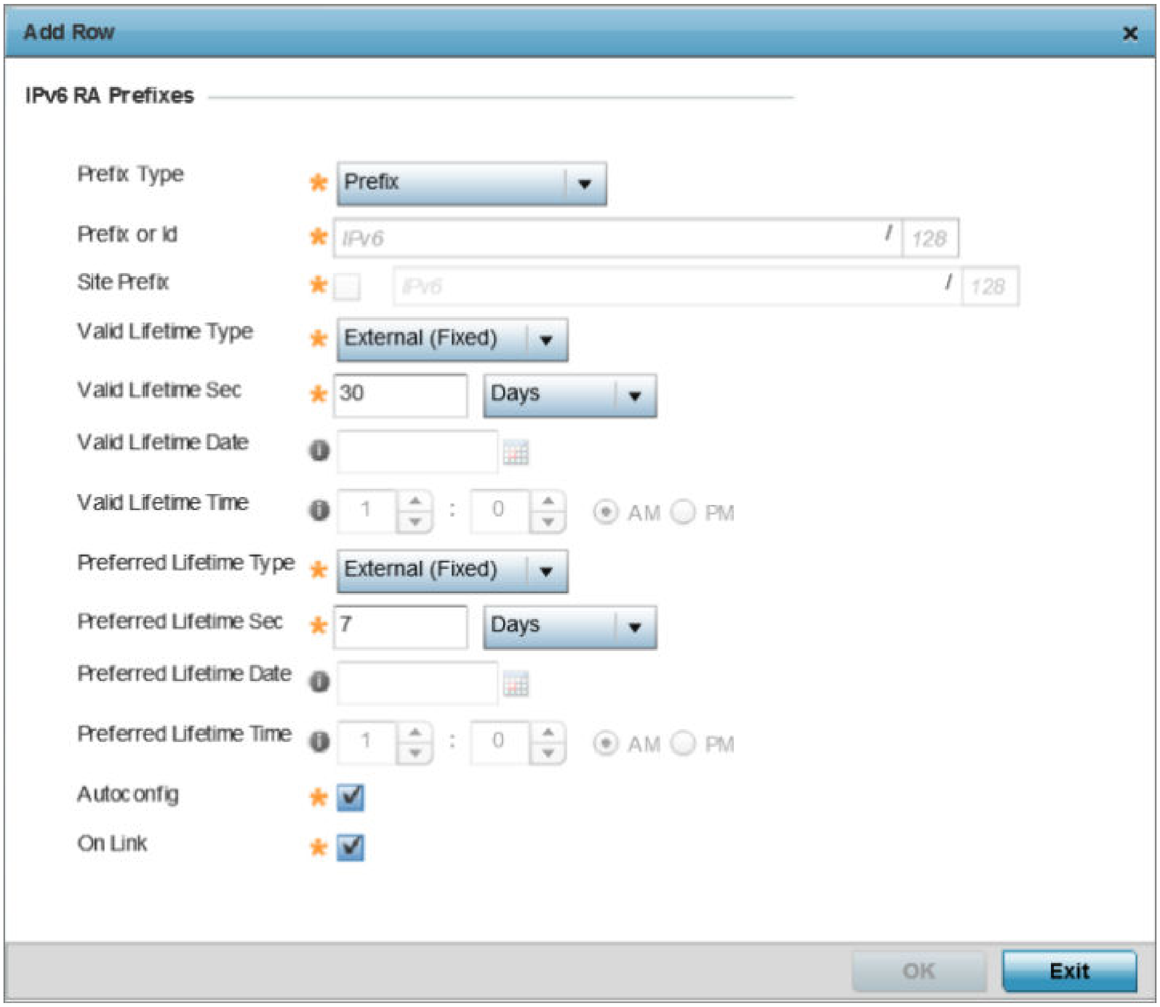
Figure 52: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab

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.



Prefix Type Prefix
Prefix or Id IPv6 / 128
Site Prefix ☐ IPv6 / 128
Valid Lifetime Type External (Fixed)
Valid Lifetime Sec 30 Days
Valid Lifetime Date
Valid Lifetime Time 1 : 0 ● AM ○ PM
Preferred Lifetime Type External (Fixed)
Preferred Lifetime Sec 7 Days
Preferred Lifetime Date
Preferred Lifetime Time 1 : 0 ● AM ○ PM
Autoconfig ☑
On Link ☑

Figure 53: 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.
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.
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.

Overriding Security Configuration

To override the VLAN 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 771.

1 Select the **Security** tab.

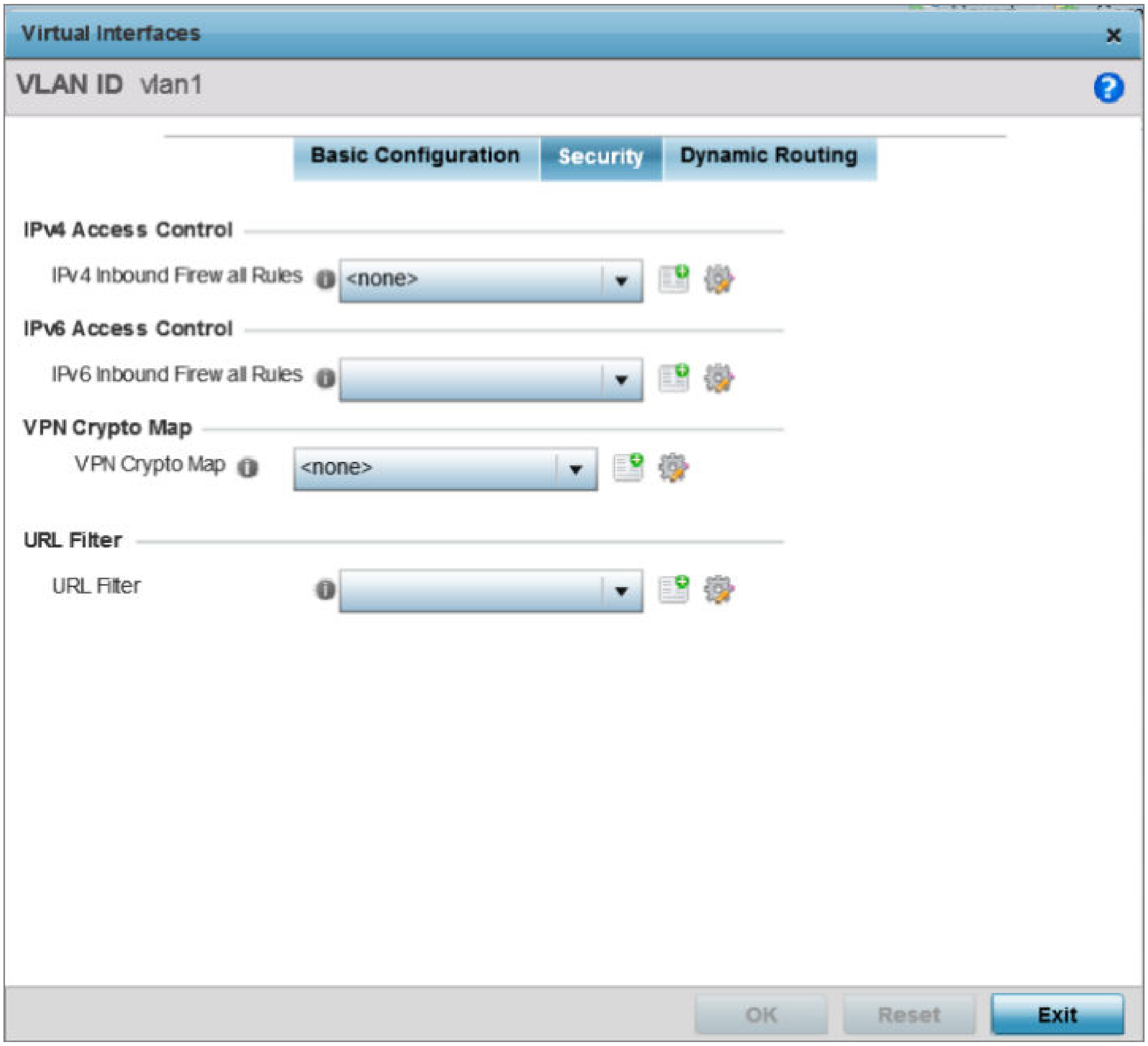


Figure 54: Profile Overrides - Virtual Interfaces Security Screen

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).

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 789.
4. Use the **VPN Crypto Map** drop-down menu to select or override the Crypto Map configuration applied to this virtual interface.

   Crypto Map entries are sets of configuration parameters for encrypting packets that pass through the VPN Tunnel. If there is no Crypto Map configuration that meets the needs of this virtual interface, click the **Create** icon to define a new Crypto Map configuration or click the **Edit** icon to modify an existing configuration. For more information, see Overriding VPN Configuration on page 257.
5. 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.
6. Click **OK** to save the changes and overrides to the Security screen.

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

Overriding Dynamic Routing Configuration

To override the VLAN Dynamic Routing configuration:

1 Select the **Dynamic Routing** tab.

Note
The Dynamic Routing tab is not available for controllers or service platfrorms.

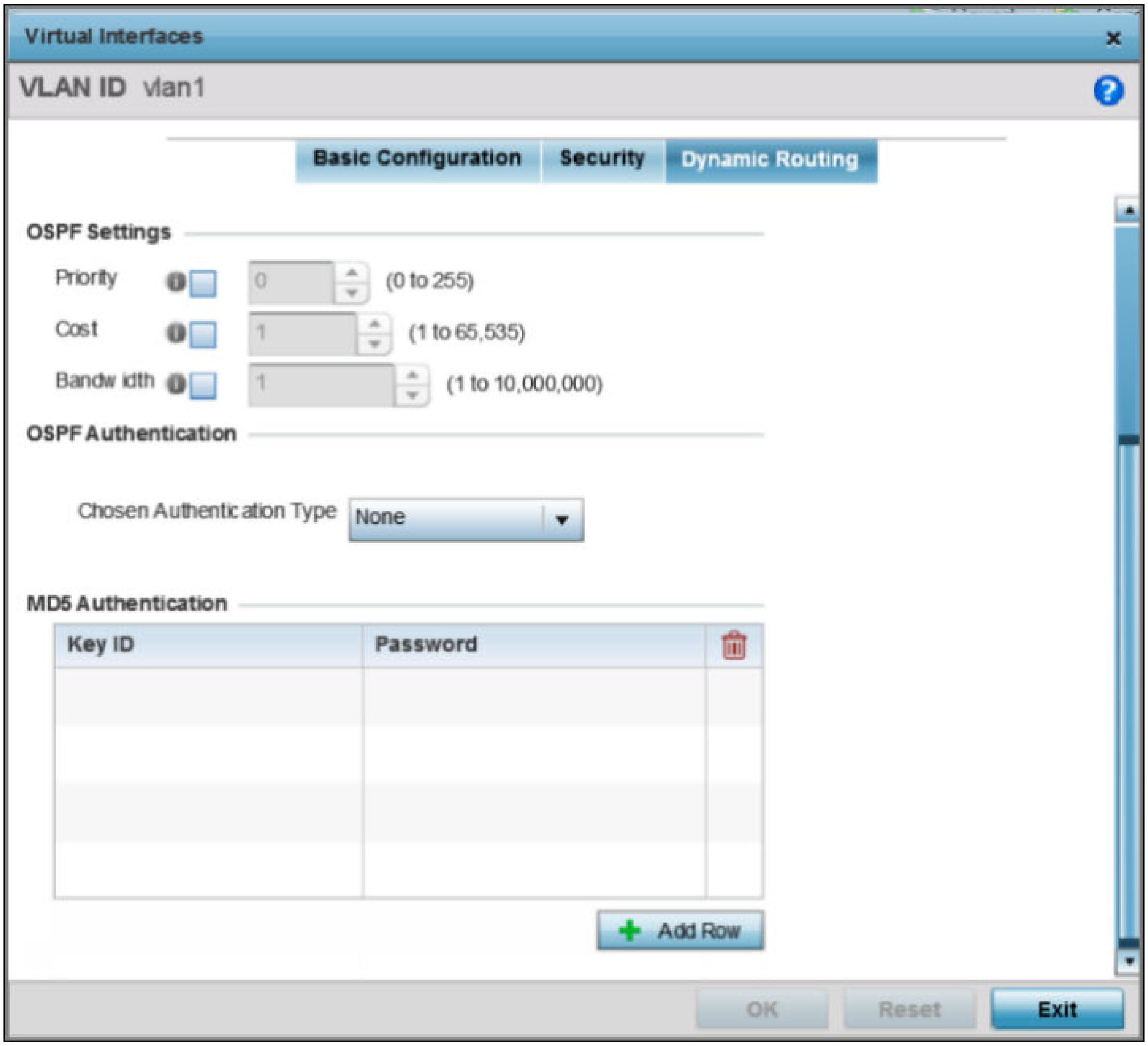


Figure 55: Profile Overrides - Virtual Interfaces Dynamic Routing Screen

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

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 bandwidth from 1 - 10,000,000 KBps.

3 From the **Chosen Authentication Type** drop-down list, select the authentication type used to validate credentials within the OSPF dynamic route.

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

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.

   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 changes and overrides to the Security screen.

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

Port Channel Override Configuration

Profiles can utilize customized port channel configurations as part of their interface settings. Existing port channel profile configurations can be overridden as they become obsolete for specific device deployments.

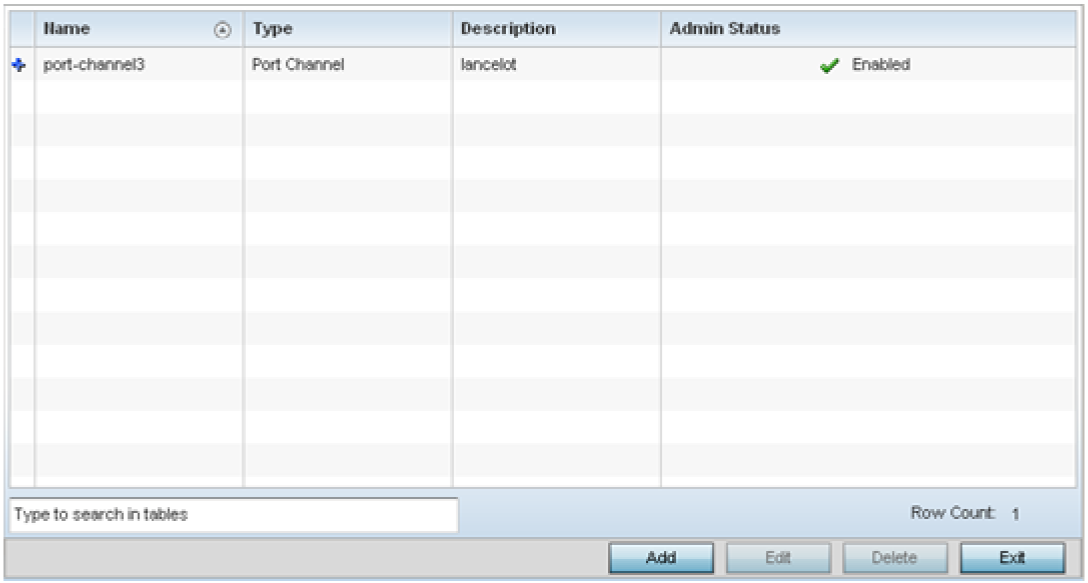
To define or override a port channel configuration on a profile:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.

   The selected device's configuration menu displays.
3. Select **Port Channels**.



	Name	Type	Description	Admin Status
✚	port-channel3	Port Channel	lancelot	✓ Enabled

Figure 56: Device Overrides - Port Channels 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 Refer to the following to 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.

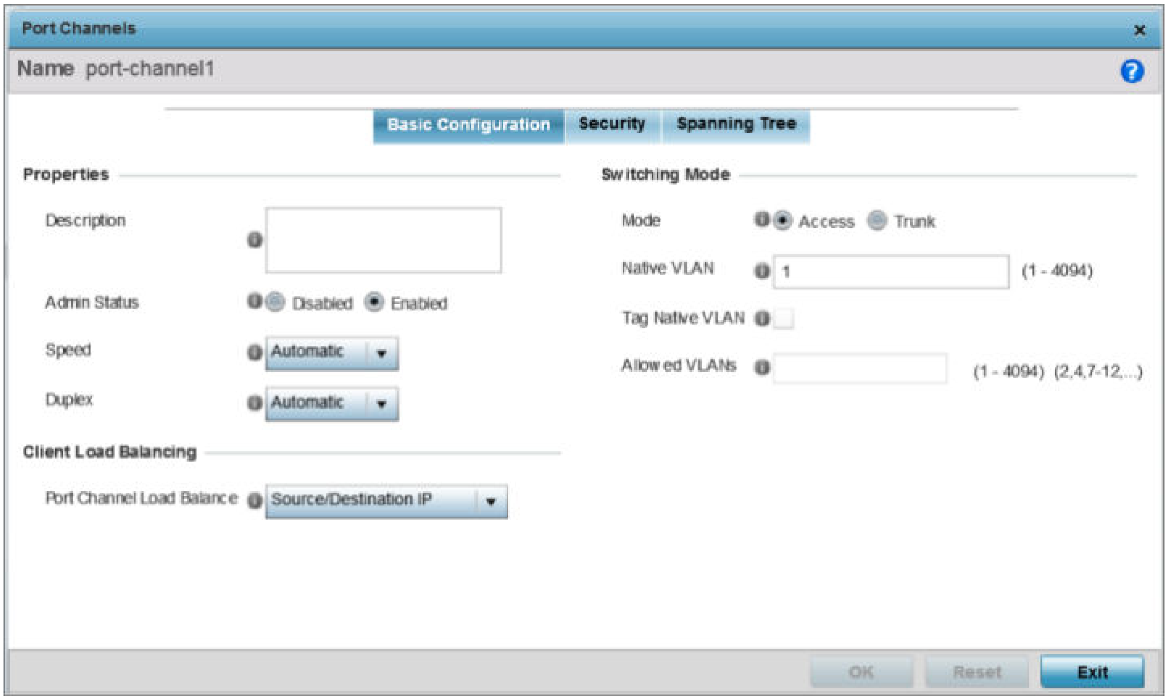
After reviewing the configurations of existing port channel interfaces, determine whether a new interface needs to be created, an existing interface needs to be edited (overridden), or an existing interface needs to be deleted.

Overriding Basic Configuration

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

1 Select **Add** to add a new port channel. Select **Edit** to edit an existing port channel configuration.

The Basic Configuration screen displays by default.



Port Channels

Name port-channel1

Properties

Description

Admin Status ○ Disabled ● Enabled

Speed Automatic

Duplex Automatic

Client Load Balancing

Port Channel Load Balance Source/Destination IP

Switching Mode

Mode ● Access ○ Trunk

Native VLAN 1 (1 - 4094)

Tag Native VLAN ☐

Allowed VLANs (1 - 4094) (2,4,7-12,...)

Figure 57: Device Overrides - Port Channels - 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. Automatic is the default setting.
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. Automatic is the default setting.

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

The *Source/Destination IP* option is the default setting.

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. Access is the default setting.
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. Note: This option is enabled when the switching mode is set as **`Trunk`**.
Allowed VLANs	Add VLANs that exclusively send packets over the port channel. Note: This option is enabled when the switching mode is set as **`Trunk`**.

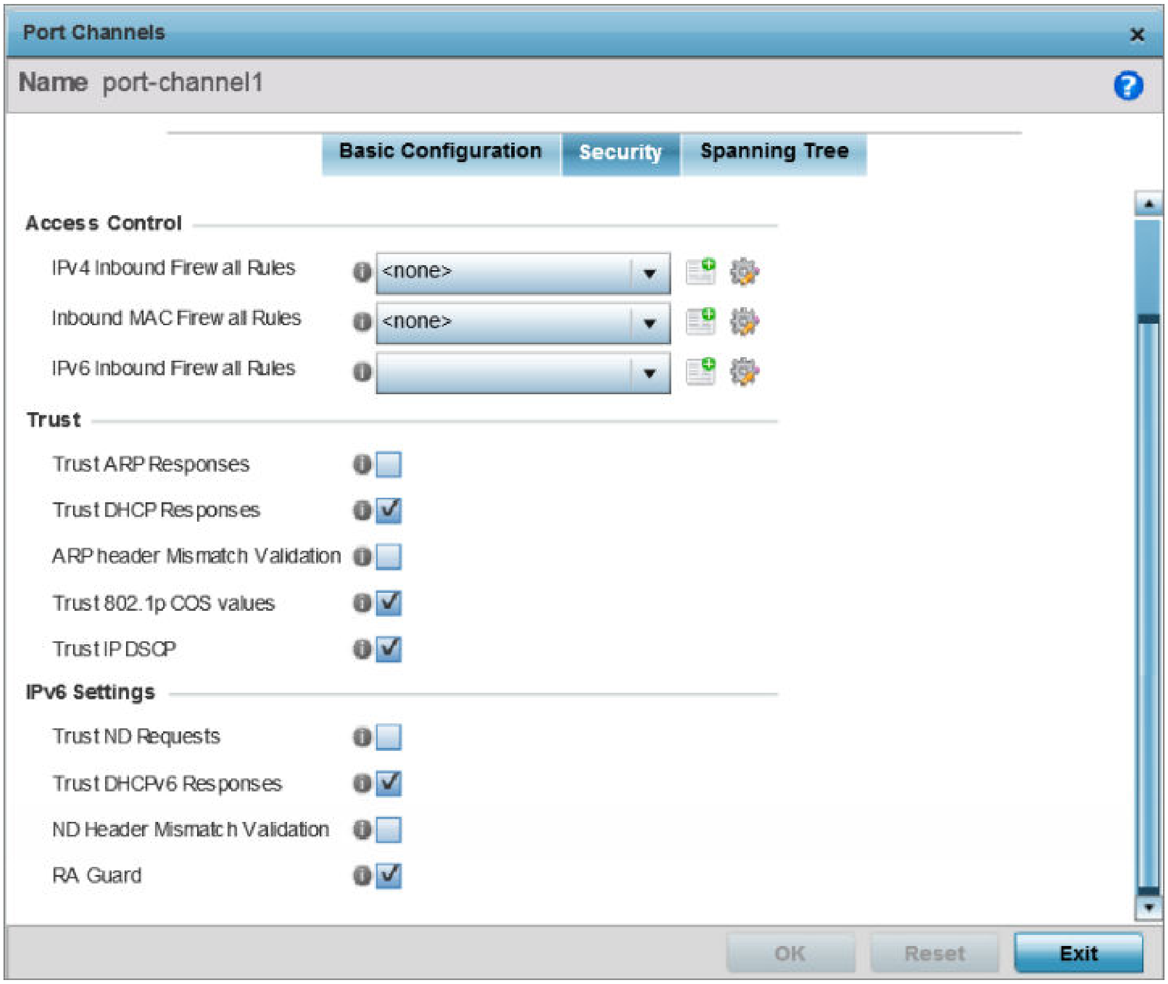
5. Click **OK** to save the changes and overrides to the port channel Basic Configuration.

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

Overriding Security Configuration

To configure the port channel's security configuration:

1 Select the **Security** tab.



Name port-channel1

Access Control

IPv4 Inbound Firewall Rules <none>

Inbound MAC Firewall Rules <none>

IPv6 Inbound Firewall Rules

Trust

- ☐ Trust ARP Responses
- ☑ Trust DHCP Responses
- ☐ ARP header Mismatch Validation
- ☑ Trust 802.1p COS values
- ☑ Trust IP DSCP

IPv6 Settings

- ☐ Trust ND Requests
- ☑ Trust DHCPv6 Responses
- ☐ ND Header Mismatch Validation
- ☑ RA Guard

Figure 58: Device Overrides - Port Channels - Security Screen

2 Refer to the Access Control section.

As part of the port channel's security configuration, Inbound IPv4 IP, IPv6 IP, and MAC address firewall rules are required.

Use the drop-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 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.

4 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 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.

5 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.

6 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 enabled 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 disabled by default.

7 Set the following IPv6 Settings:

Trust ND Requests	Select this option to enable neighbor discovery (ND) request trust on this port channel (neighbor discovery requests received on this port are considered trusted). Neighbor discovery allows the discovery of an adjacent device's MAC addresses, similar to *Address Resolution Protocol* (ARP) on Ethernet in IPv4. The default value is disabled.
Trust DHCPv6 Responses	Select this option to enable DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. The default value is enabled.
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. Router advertisements are periodically sent to hosts or sends in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is disabled by default.

8 Click **OK** to save the changes and overrides to the security configuration.

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

Overriding Spanning Tree Configuration

To configure the port channel's spanning tree configuration:

1 Select the **Spanning Tree** tab.

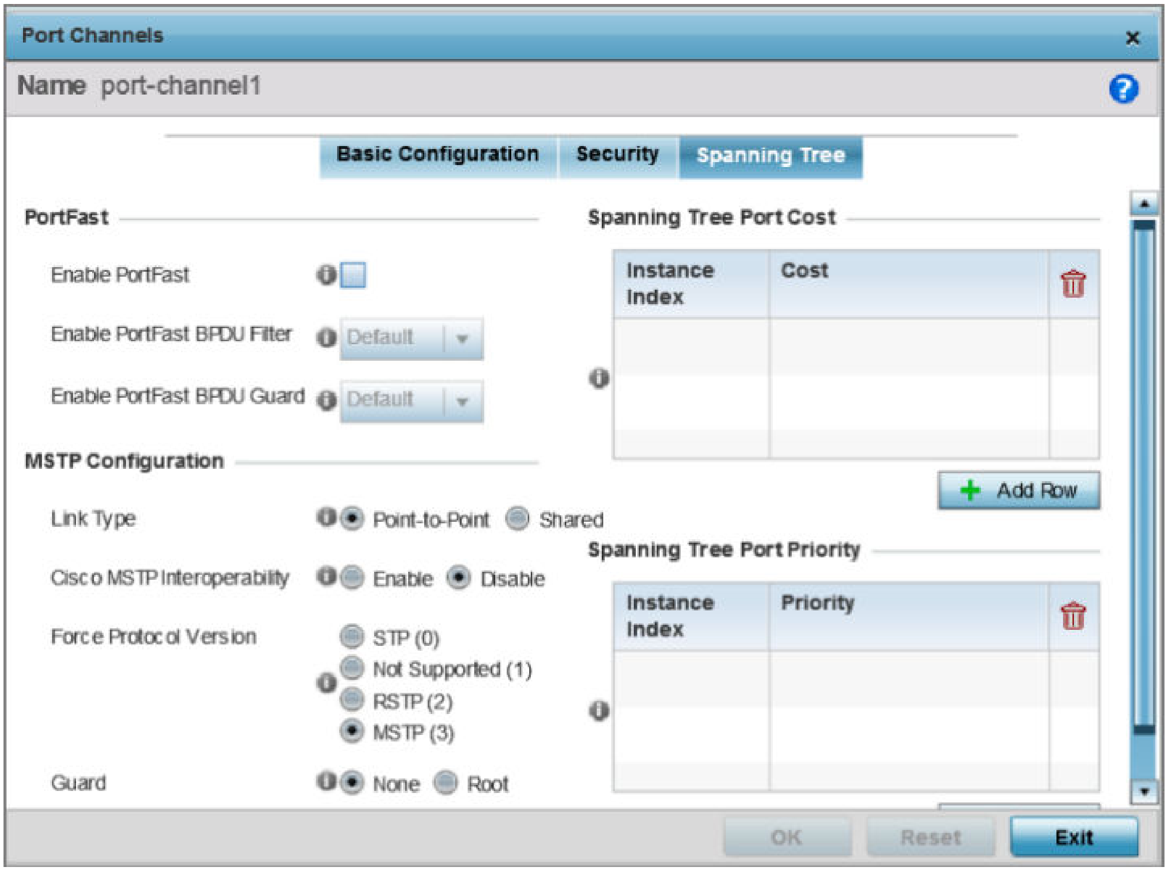


Figure 59: Port Channels - Spanning Tree Screen

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

Enable PortFast	Select this option to enable drop-down menus for the **`Enable PortFast BPDU Filter`** and **`Enable PortFast BPDU Guard`** options. This setting is disabled by default.
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: Default, Enable and Disable. • Default — This is the default setting. This option makes the bridge BPDU filter value to take effect. • Enable — Enables BPDU filtering. • 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: • Default — This is the default setting. This option makes the bridge BPDU guard value to take effect. • Enable — Enables shutting down of port. • Disable — Disables shutting down of port.

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

Enable as Edge Port	Select this option 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 `Point-to-Point` or `Shared`. When **Point-to-Point** is selected, the port is treated as connected to a point-to-point link. Selecting **Shared** means this port should be treated as having a shared connection. Note: 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. Point-to-Point is the default setting.
Cisco MSTP Interoperability	`Enable` or `Disable` interoperability with Cisco's version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP. This setting is disabled by default.
Force Protocol Version	Set the protocol version to either `STP(0)`, `Not Supported(1)`, `RSTP(2)`, or `MSTP(3)`. MSTP(3) 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.

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 4: 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.

Overriding VM Interface Configuration

WiNG provides a dataplane bridge for external network connectivity for VMs *(virtual machines)*. VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enable remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of 16 VMF ports on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1, by default, is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.

To define or override a VM interface configuration:

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

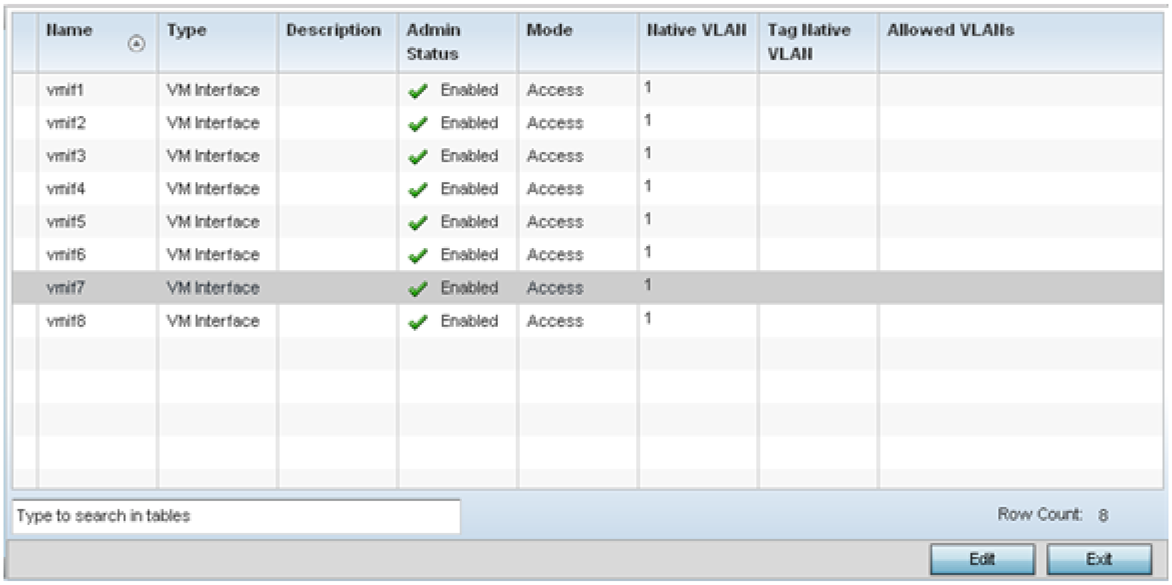
   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.

   The selected device's configuration menu displays.
3. Go to **Profile Overrides** → **Interface**.

4 Select **VM Interfaces**.

The VM Interfaces screen displays.



Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
vmif1	VM Interface		✓ Enabled	Access	1		
vmif2	VM Interface		✓ Enabled	Access	1		
vmif3	VM Interface		✓ Enabled	Access	1		
vmif4	VM Interface		✓ Enabled	Access	1		
vmif5	VM Interface		✓ Enabled	Access	1		
vmif6	VM Interface		✓ Enabled	Access	1		
vmif7	VM Interface		✓ Enabled	Access	1		
vmif8	VM Interface		✓ Enabled	Access	1		

Row Count: 8

Figure 60: Profile Overrides - VM Interfaces 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.

5 Refer to the following to review existing configurations and status to determine whether a parameter requires an override:

Name	The VM interface numerical identifier assigned when the VM interface was created. The numerical name cannot be modified as part of the edit process.
Type	Whether the type is VM interface.
Description	A short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
Admin Status	A green check mark means the listed VM interface is active and currently enabled with the profile. A red “X” means the VM interface is currently disabled and not available for use. The interface status can be modified with the VM Interface Basic Configuration screen as required.
Mode	The layer 3 mode of the VM interface: either `Access` or `Trunk` (as defined within the VM Interfaces Basic Configuration screen). If `Access` is selected, the listed VM interface 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. If set to `Trunk`, the port allows packets from a list of VLANs added to the trunk. A VM interface configured as `Trunk` supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged.

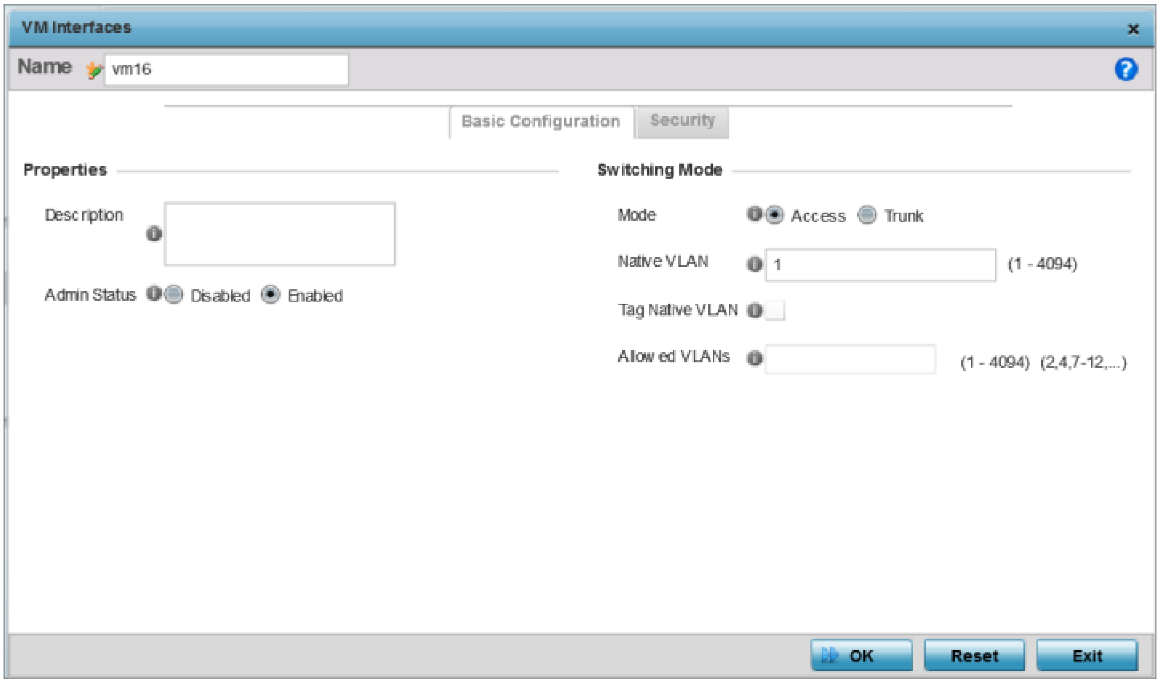
Native VLAN	The numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a VM interface in trunk mode.
Tag Native VLAN	A green check mark means the native VLAN is tagged. A red "X" means the native VLAN is untagged. When a frame is tagged, the 12-bit frame VLAN ID is added to the 802.1Q header so upstream VM interface ports 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 VM interface classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows a VM interface 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 VM interface. Allowed VLANs are listed only when the mode has been set to `Trunk`.

Overriding Basic Configuration

You can add a new VM interface configuration or edit an existing configuration.

1 To edit or override the configuration of an existing VM interface, select it from among those displayed and click **Edit**.

The VM Interface Basic Configuration screen displays by default.



Name: vm16

Description:

Admin Status: ○ Disabled ● Enabled

Mode: ● Access ○ Trunk

Native VLAN: 1 (1 - 4094)

Tag Native VLAN: ☐

Allowed VLANs: (1 - 4094) (2,4,7-12,...)

Figure 61: Profile Overrides - VM Interfaces Basic Configuration Screen

2 Set or override the following VM interface **Properties**:

Description	Enter a description for the controller or service platform VM interface (64 characters maximum).
Admin Status	Select **Enabled** to define this VM interface as active to the profile it supports. Select **Disabled** to disable this VM interface in the profile. It can be activated at any time when needed. This option is disabled by default.
Mode	Select either **`Access`** or **`Trunk`** to set the VLAN switching mode over the VM interface. If *Access* is selected, the VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VMF port are expected as untagged and mapped to the native VLAN. If set to *Trunk*, the port allows packets from a list of VLANs you add to the trunk. A VM interface 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	Define the numerical VLAN ID (1 - 4094) for the native VLAN. The native 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. 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 VMIF that the frame belongs. If the upstream VMIF does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between VM interface ports, both VM interfaces 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 VM interfaces know which VLAN ID the frame belongs to. The 12-bit VLAN ID is read and the frame is forwarded to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VMIF classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows a VM interface 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 VM interface. The available range is from 1 - 4094. The maximum number of entries is 256.

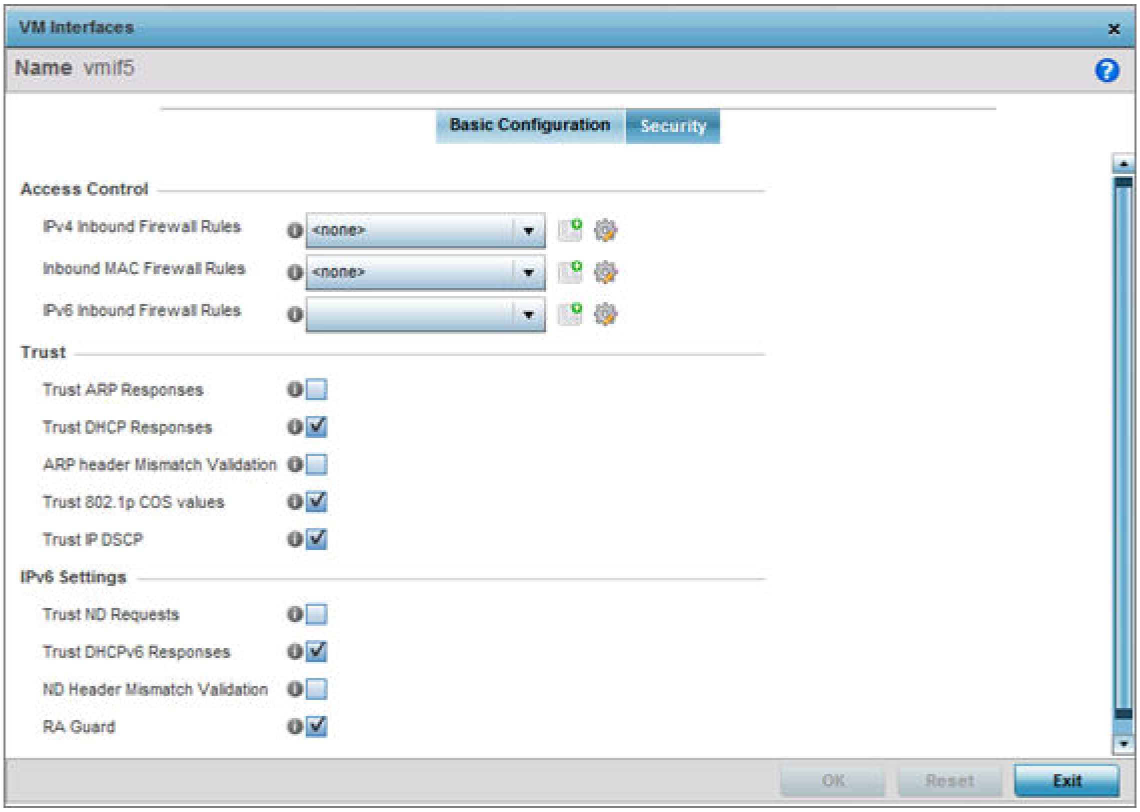
3 Click **OK** to save the changes and overrides made to the VM interface basic configuration.

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

Overriding Security Configuration

To override the VM interface security configuration:

1. Select **Security**.



Name vmif5

Access Control

IPv4 Inbound Firewall Rules <none>
Inbound MAC Firewall Rules <none>
IPv6 Inbound Firewall Rules

Trust

Trust ARP Responses ☐
Trust DHCP Responses ☑
ARP header Mismatch Validation ☐
Trust 802.1p COS values ☑
Trust IP DSCP ☑

IPv6 Settings

Trust ND Requests ☐
Trust DHCPv6 Responses ☑
ND Header Mismatch Validation ☐
RA Guard ☑

Figure 62: Profile Overrides - VM Interfaces Security Screen

2. Refer to the Access Control field.

   As part of the VM interface's security configuration, IPv4 and IPv6 Inbound and MAC Inbound address firewall rules are required.

   You will use the drop-down menus to select the firewall rules to apply to this profile's VM interface configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

3. Use the **IPv4 Inbound Firewall Rules** drop-down menu to select the IPv4 specific firewall rules to apply to this profile's VM interface 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.

4. Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific firewall rules to apply to this profile's VM interface 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.

5. If there is no firewall rule that meets the data protection needs of the target VM interface configuration, click the **Create** icon to define a new rule configuration, or click the **Edit** icon to modify an existing firewall rule configuration.

6 Refer to the Trust field to define or override the following:

Trust ARP Responses	Select this option to enable ARP trust on this VM interface. ARP packets received on this port are considered trusted, and the information from these packets is used to identify rogue devices. This option is disabled by default.
Trust DHCP Responses	Select this option to enable DHCP trust on this VM interface. 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 enabled by default.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this VM interface. This option is enabled by default.
Trust IP DSCP	Select this option to enable IP DSCP values on this VM interface. This option is disabled by default.

7 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 VM interface. This option is disabled by default.
Trust DHCPv6 Responses	Select this option to trust all DHCPv6 responses on this VM interface. 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. 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 VM interface. Router advertisements are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is disabled by default.

8 Click **OK** to save the changes and overrides made to the VM interface configuration.

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

Radio Override Configuration

An access point can have its radio profile configuration overridden after its radios have successfully associated to the network.

To define a radio configuration override from the access point's associated controller or service platform:

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

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

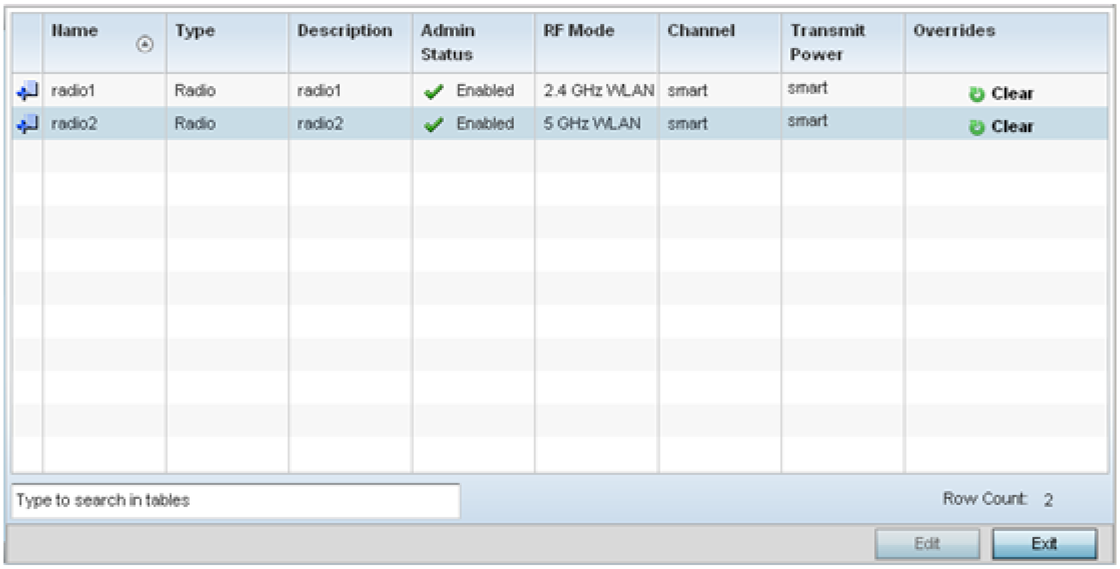
2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

The selected device's configuration menu displays.

3 Go to **Profile Overrides** → **Interface**.

4 Select **Radios**.



Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power	Overrides
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart	Clear
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart	Clear

Figure 63: Device Overrides - Radios 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.

5 Review the following radio configuration data to determine whether a radio configuration needs to be modified or overridden to better support the managed network:

Name	Displays whether the reporting radio is the access point's radio1, radio2 or radio3.
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.

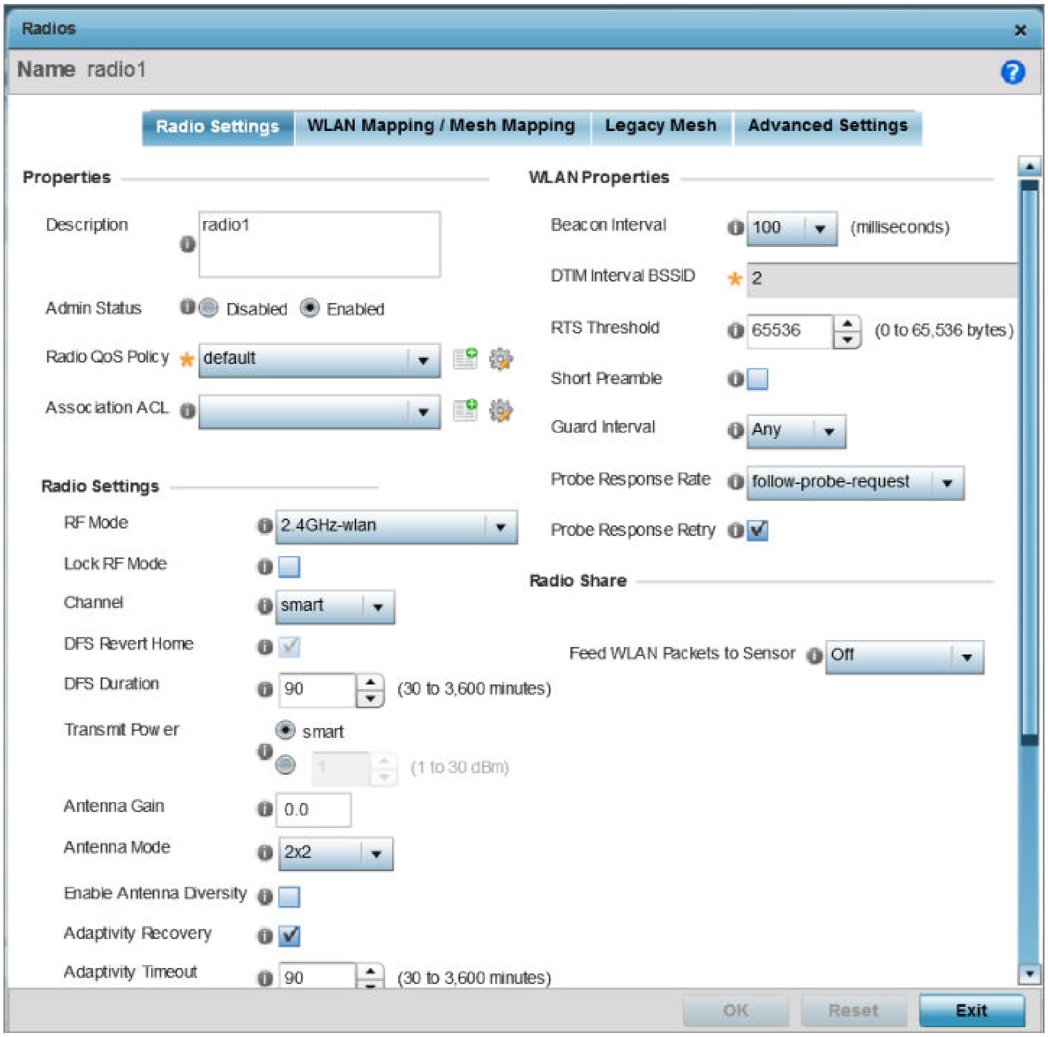
Transmit Power	Lists the transmit power for each radio displayed as a value in milliwatts. Selecting `smart` allows the radio to perform power adjustments to compensate for failed neighboring radios.
Overrides	A Clear option appears for each radio configuration that has an override applied to the profile's configuration. Select `Clear` to revert this specific radio configuration to the profile configuration originally defined by the administrator for this radio.

Overriding Radio Settings

If required, you can modify or override a radio's basic configurations at the device level.

1 Select a radio and click **Edit**.

The Radio Settings tab displays by default.



Name radio1

Properties

Description: radio1
Admin Status: ○ Disabled ● Enabled
Radio QoS Policy: default
Association ACL:

Radio Settings

RF Mode: 2.4GHz-wlan
Lock RF Mode: ☐
Channel: smart
DFS Revert Home: ☑
DFS Duration: 90 (30 to 3,600 minutes)
Transmit Power: ● smart ○ 1 (1 to 30 dBm)
Antenna Gain: 0.0
Antenna Mode: 2x2
Enable Antenna Diversity: ☐
Adaptivity Recovery: ☑
Adaptivity Timeout: 90 (30 to 3,600 minutes)

WLAN Properties

Beacon Interval: 100 (milliseconds)
DTIM Interval BSSID: 2
RTS Threshold: 65536 (0 to 65,536 bytes)
Short Preamble: ☐
Guard Interval: Any
Probe Response Rate: follow-probe-request
Probe Response Retry: ☑

Radio Share

Feed WLAN Packets to Sensor: Off

Figure 64: Access Point Radio - Radio Settings Tab

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. For more information, see Radio QoS Policies on page 392.
Association ACL	Specify an existing Association ACL policy to apply to the access point radio. An Association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a managed Access Point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller or service platform packets. When a packet is received on an interface, the controller or service platform compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. 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 or override the following Radio Settings for the selected access point radio:

RF Mode	Set the mode to either 2.4 GHz WLAN or 5 GHz WLAN depending on the radio's intended client support requirement. Set the mode to **`sensor`** if you are using the radio for rogue device detection. To set a radio as a detector, disable sensor support on the other access point radio. Set the mode to **`scan-ahead`** in DFS-aware countries to allow a mesh point's 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.
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. 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. Note: 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. Select the **smart** option 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. Note: 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 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.
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. Note: The Data Rates drop-down menu is disabled for radios running as sensors. 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). 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.
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. Note: Most access point models can support up to 256 clients per access point radio.
Rate Selection Methods	Specify a radio selection method for the radio. The selection methods are: Standard: Standard monotonic radio selection method will be used. Opportunistic: Sets ORLA *(opportunistic radio link adaptation)* as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput. The ORLA rate selection mode is supported only on the AP 7161 and AP-8163 model access points.

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. 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. 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. 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.

This feature can be enabled in two modes:

- In **`Inline`** mode, the WIPS sensor receives the packets from the radios with each radio operating in normal mode.
- In **`Promiscuous`** mode, 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 the packets.

In both **`Inline`** and **`Promiscuous`** modes, the packets the radio is switching can also be used by the WIPS analysis module.

6 Click **OK** to save the changes and overrides to the Radio Settings screen.

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

Overriding WLAN / Mesh Mapping

To override the radio's WLAN or Mesh assignment:

1 Select the **WLAN Mapping / Mesh Mapping** tab.

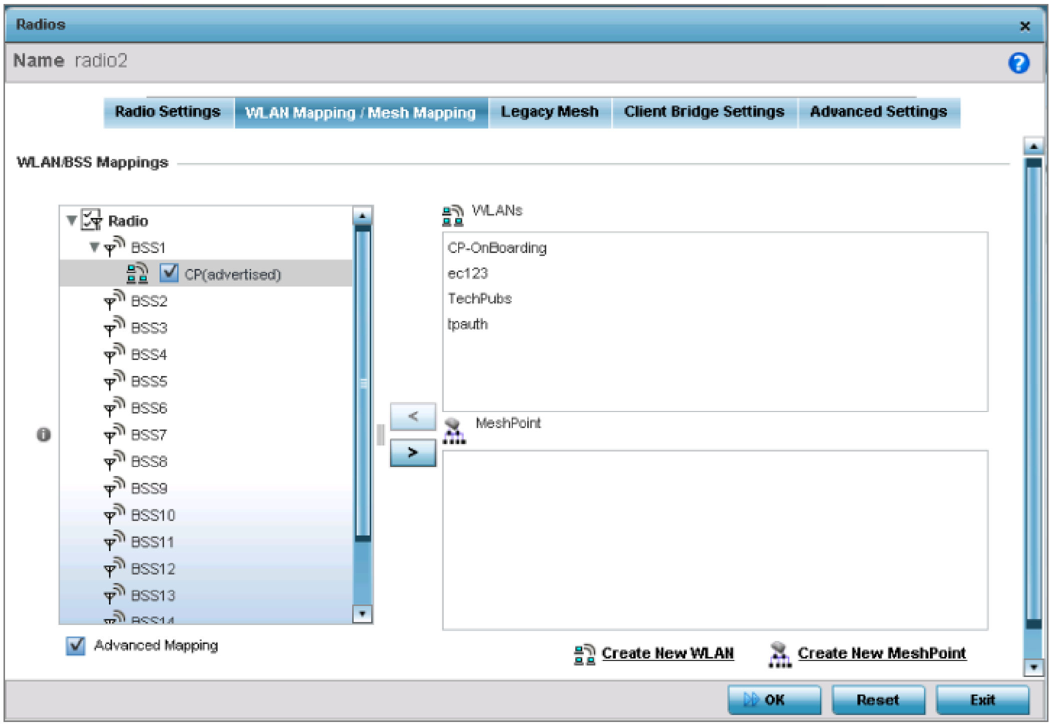


Figure 65: Access Point Radio - WLAN Mapping / Mesh Mapping Tab

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.

Administrators can assign each WLAN its own BSSID. For dual-radio access points, there are sixteen BSSIDs for the 802.11b/g/n radio and sixteen BSSIDs for the 802.11a/n radio.

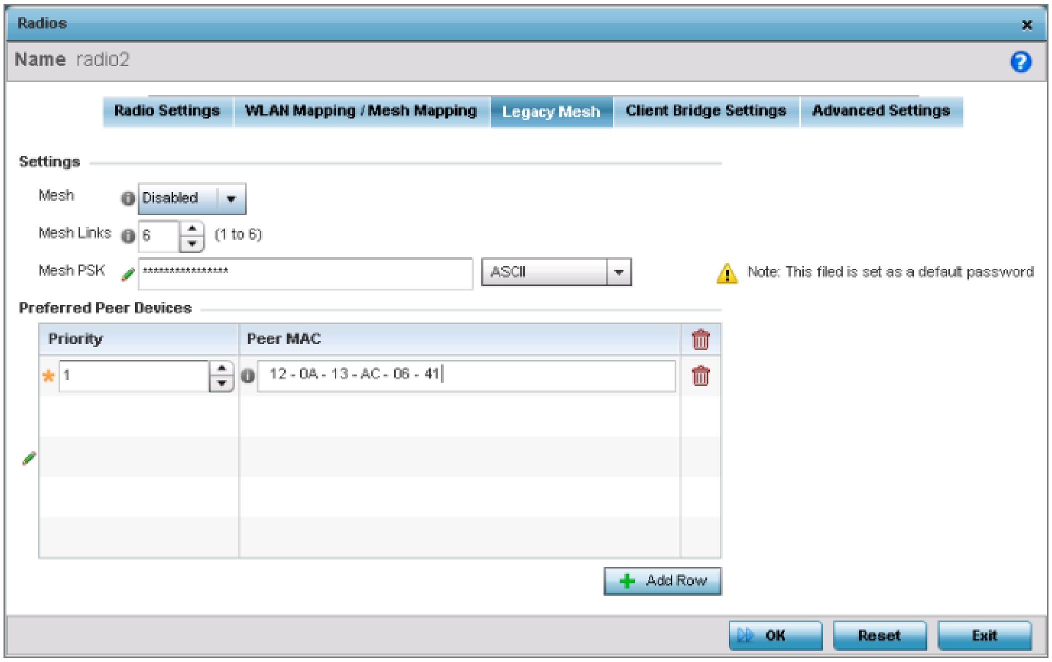
3 Click **OK** to save the changes and overrides to the Radio Settings screen.

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

Overriding Legacy Mesh Settings

To override the selected radio's mesh configuration:

1 Select the **Legacy Mesh** tab.



Name radio2

Settings

Mesh: Disabled

Mesh Links: 6 (1 to 6)

Mesh PSK: **************** ASCII

Note: This filed is set as a default password

Preferred Peer Devices

Priority	Peer MAC
1	12 - 0A - 13 - AC - 06 - 41

Figure 66: Access Point Radio - Legacy Mesh Tab

Use the Mesh Legacy screen to define or override how mesh connections are established and the number of links available among access points within the Mesh network.

2 Define the following legacy mesh **Settings**:

Mesh	Set the mesh mode for this radio – either **`Client`**, **`Portal`**, or **`Disabled`**. Setting the mesh mode to *Client* enables the radio to operate as a mesh client that scans and connects to mesh portals or nodes connected to portals. Setting the mesh mode to *Portal* turns the radio into a mesh portal. This starts the radio beaconing immediately and will accept connections from other mesh nodes. Setting the mesh mode to *Disabled* deactivates all mesh activity on this radio.
Mesh Links	Specify the number of mesh links allowed by the radio. The radio can have from 1- 6 mesh links when the radio is configured as a portal.
Mesh PSK	Provide the encryption key in either ASCII or Hex format. Administrators must ensure that this key is configured on the access point when staged for mesh, added to both the mesh client and the portal access point’s configuration on the controller or service platform. Select **Show** to display the characters used in the PSK.

Note

Only single-hop mesh links are supported at this time.

3 Refer to the **Preferred Peer Devices** table to add mesh peers.

For each peer being added, enter its MAC address and a priority from 1 - 6. The lower the priority number assigned, the higher the priority the peer is given when it connects to the mesh infrastructure.

Click **+ Add Row** to add preferred peer devices for the radio to connect to in mesh mode.

4 Click **OK** to save the changes and overrides to the Mesh configuration.

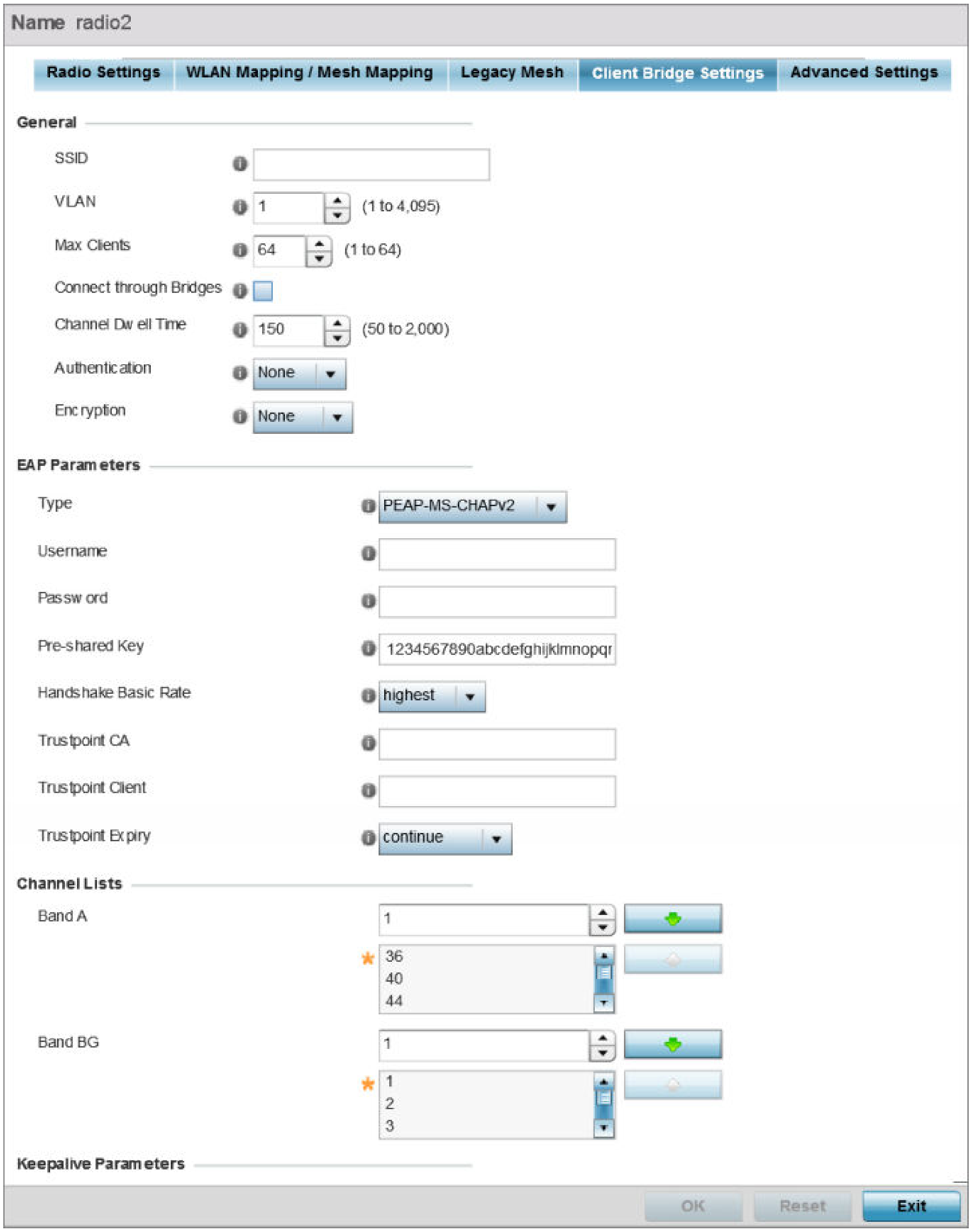
Click **Reset** to revert to the last saved configuration.

Overriding 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. This feature is supported only on the , Ap7522, AP7532, AP7562, AP7602, and AP7622.

To override the selected radio's client bridge settings:

1 Select the **Client Bridge Settings** tab to configure the selected radio as a client-bridge.



Name radio2

General

SSID

VLAN 1 (1 to 4,095)

Max Clients 64 (1 to 64)

Connect through Bridges ☐

Channel Dwell Time 150 (50 to 2,000)

Authentication None

Encryption None

EAP Parameters

Type PEAP-MS-CHAPv2

Username

Password

Pre-shared Key 1234567890abcdefghijklmnopqr

Handshake Basic Rate highest

Trustpoint CA

Trustpoint Client

Trustpoint Expiry continue

Channel Lists

Band A 1

36
40
44

Band BG 1

1
2
3

Keepalive Parameters

Figure 67: Access Point Radio - Client Bridge Settings Tab

2 Define the following General settings:

Before configuring the client-bridge parameters, set the radio's **rf-mode** to **`bridge`**.

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. For information on WLAN authentication, see Configuring WLAN Security on page 334.
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. For information on WLAN encryption, see Configuring WLAN Security on page 334.

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. 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. 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. 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. discontinue – Terminates the CB once the certificate (CA/client) has expired. Note: 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 462.

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. 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.

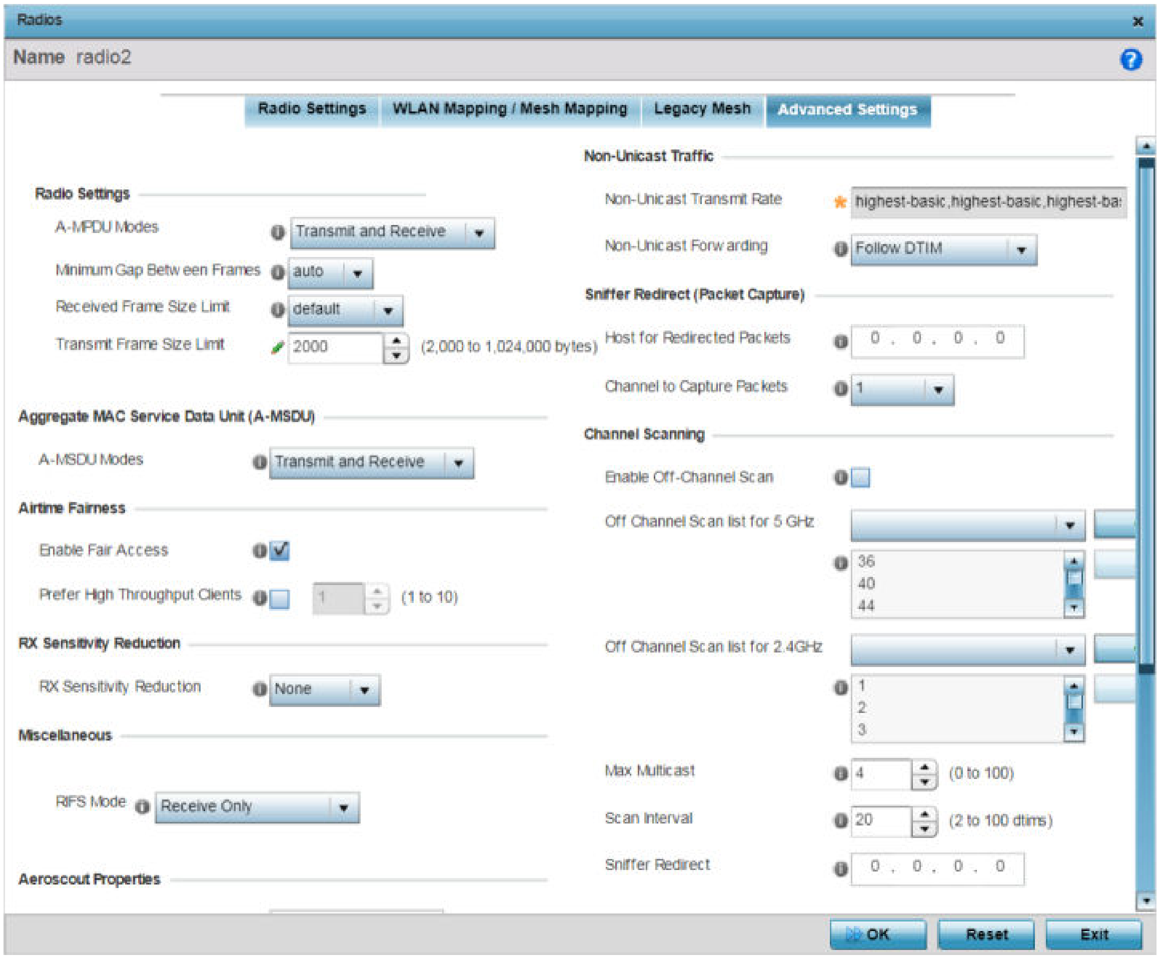
8 Click **OK** to save the changes and overrides to the client bridge settings screen.

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

Overriding Advanced Settings

To override the selected radio's advanced settings:

1 Select the **Advanced Settings** tab.



Radios

Name radio2

Radio Settings

A-MPDU Modes: Transmit and Receive

Minimum Gap Between Frames: auto

Received Frame Size Limit: default

Transmit Frame Size Limit: 2000 (2,000 to 1,024,000 bytes)

Aggregate MAC Service Data Unit (A-MSDU)

A-MSDU Modes: Transmit and Receive

Airtime Fairness

Enable Fair Access: ☑

Prefer High Throughput Clients: ☐ 1 (1 to 10)

RX Sensitivity Reduction

RX Sensitivity Reduction: None

Miscellaneous

RIFS Mode: Receive Only

Aeroscout Properties

Non-Unicast Traffic

Non-Unicast Transmit Rate: highest-basic,highest-basic,highest-ba

Non-Unicast Forwarding: Follow DTIM

Sniffer Redirect (Packet Capture)

Host for Redirected Packets: 0 . 0 . 0 . 0

Channel to Capture Packets: 1

Channel Scanning

Enable Off-Channel Scan: ☐

Off Channel Scan list for 5 GHz: 36 40 44

Off Channel Scan list for 2.4GHz: 1 2 3

Max Multicast: 4 (0 to 100)

Scan Interval: 20 (2 to 100 dtims)

Sniffer Redirect: 0 . 0 . 0 . 0

2 Refer to the Radio Settings field to 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: • **`0`** – Configures the minimum gap as 0 microseconds • **`1`** – Configures the minimum gap as 1 microseconds • **`2`** – Configures the minimum gap as 2 microseconds • **`4`** – Configures the minimum gap as 4 microseconds • **`8`** – Configures the minimum gap as 8 microseconds • **`16`** – Configures the minimum gap as 16 microseconds • **`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: • **`8191`** - Advertises the maximum received frame size limit as 8191 bytes. • **`16383`** - Advertises the maximum received frame size limit as 16383 bytes. • **`32767`** - Advertises the maximum received frame size limit as 32767 bytes. • **`65535`** - Advertises the maximum received frame size limit as 65535 bytes. • **`128000`** - Advertises the maximum received frame size limit as 128000 bytes. • **`256000`** - Advertises the maximum received frame size limit as 256000 bytes. • **`512000`** - Advertises the maximum received frame size limit as 512000 bytes. • **`1024000`** - Advertises the maximum received frame size limit as 1024000 bytes. • **`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. For 802.11ac capable APs, the range is as follows: • **`2000 - 65,535 bytes`** - For radio 1, the range is 2000 - 65,535 bytes. The default value is 65,535 bytes. Note: 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. • **`2000 - 1,024,000 bytes`** - For radio 2, the range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes. Note: The WiNG 802.11ac capable APs are: AP7522, AP7532, AP7562, AP7602, AP7612, AP7632, AP7662, AP8432, and AP8533. For non 802.11ac capable APs the range is as follows: • **`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 Use the **A-MSDU Modes** drop-down menu in the **Aggregate MAC Service Data Unit (A-MSDU)** section 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. The default value is *Transmit and Receive*.

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

Select **Enable Fair Access** to enable this feature and provide equal access client access to radio resources. Select **Prefer High Throughput Clients** 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 or override the following **Miscellaneous** advanced radio settings:

RIFS Mode	Define an RIFS mode to determine whether interframe spacing is applied to access point transmissions or received packets, both, or neither The default mode is **`Transmit and Receive`**. 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. Consider setting this value to **`None`** for high priority traffic to reduce packet delay.
STBC Mode	Select a STBC *(space–time block coding)* option to transmit multiple data stream copies across access point antennas to improve signal reliability. An access point's transmitted signal traverses a problematic environment, with scattering, reflection and refraction all prevalent. The signal can be further corrupted by noise at the receiver. Consequently, some of the received data copies are less corrupt and better than others. This redundancy means there's a greater chance of using one, or more, of the received copies to successfully decode the signal. STBC effectively combines all the signal copies to extract as much information from each as possible.
Transmit Beamforming	Enable beamforming to steer signals to peers in a specific direction to enhance signal strength and improve throughput among meshed devices (not clients). Each access point radio support up to 16 beamforming capable mesh peers. When enabled, a beamformer steers its wireless signals to its peers. A beamformee device assists the beamformer with channel estimation by providing a feedback matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a steering matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself. Transmit beamforming is available only on the AP-8163) model access point, and it is disabled by default.

7 Set or override the following **Aeroscout Properties** for the selected access point radio.

Forwarding Host	Specify the Aeroscout engine's IP address. When specified, the AP forwards Aeroscout beacons directly to the Aeroscout locationing engine without proxying through the controller or RF Domain manager. Note: Aeroscout beacon forwarding is supported only on theAP 6532, AP 7502, AP-7522, AP 7532, AP 7562, AP-8432, and AP-8533 model access points.
Forwarding Port	Set the port on which the Aeroscout engine is reachable.
MAC to be forwarded	Specify the MAC address to be forwarded.

8 Set or override the following **Ekahau Properties** for the selected access point radio.

Forwarding 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 Port	Set the Ekahau TZSP port used for processing information from locationing tags.
MAC to be forwarded	Specify the MAC address to be forwarded with location data requests.

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	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 toward the channel scan and does not negatively impact client support.
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 If an AP 7161 access point is deployed, set an **Extended Range** (from 1 - 25 kilometers) to allow AP 7161 access points to transmit and receive with their clients at greater distances without being timed out.

13 Click **OK** to save the changes and overrides to the Advanced Settings screen.

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

MCS Data Rates

The following tables define 802.11n MCS rates for with and without *short guard intervals* (SGI):

Table 5: 802.11n MCS rates: No of Streams 1

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 6: 802.11n MCS rates: No of Streams 2

MCS 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 7: 802.11n MCS rates: No of Streams 3

MCS 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	364.7	405
7	3	195	216.7	405	450

The following table defines 802.11ac MCS rates for both with and without SGI:

Table 8: 802.11ac MCS rates, 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

Overriding WAN Backhaul Configuration

A WWAN *(Wireless Wide Area Network)* card is a specialized network interface card that allows a device to connect, transmit and receive data over a Cellular Wide Area Network.

The RFS 4000 controller has a PCI Express card slot that supports 3G WWAN cards.

The WWAN card uses PPP *(point to point protocol)* to connect to the ISP *(Internet Service Provider)* 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 HDLC *(High Speed Data Link Control)* for packet encapsulation.

To define a WAN Backhaul configuration override:

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

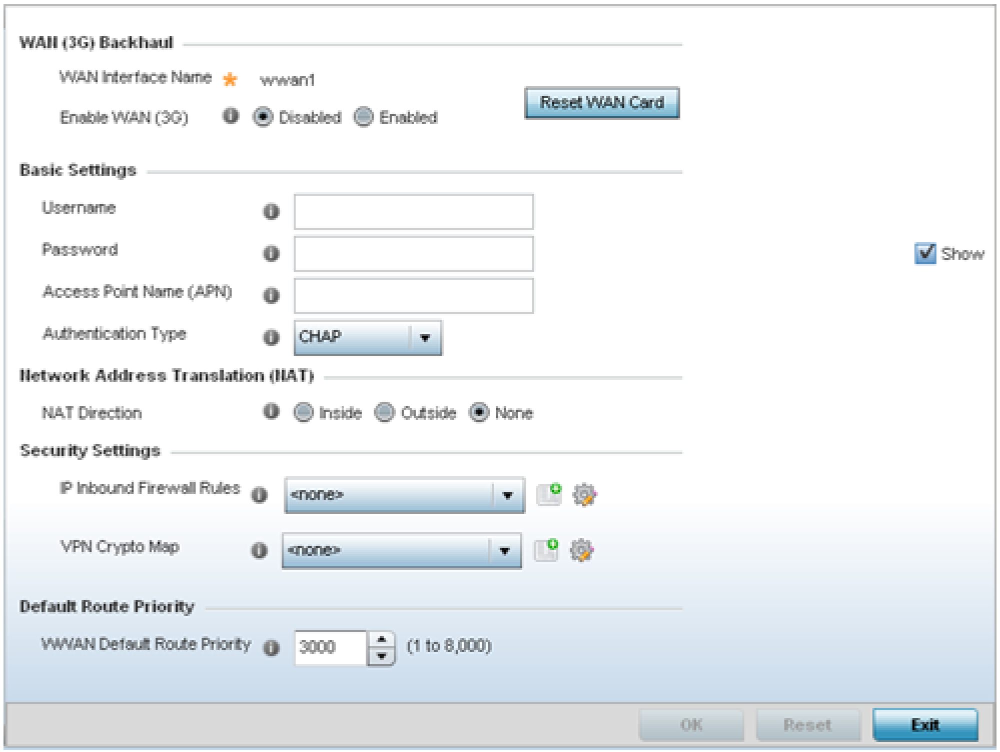
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Profile Overrides** → **Interface**.

4 Select **WAN Backhaul**.



WAN Interface Name * wwan1

Enable WAN (3G) ● Disabled ○ Enabled

Authentication Type CHAP

NAT Direction ○ Inside ○ Outside ● None

IP Inbound Firewall Rules <none>

VPN Crypto Map <none>

WWAN Default Route Priority 3000 (1 to 8,000)

Figure 68: Profile Overrides - WAN Backhaul 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.

5 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	The WAN Interface name for the WAN 3G Backhaul card.
Reset WAN Card	If the WAN Card becomes unresponsive or experiences other errors, click **Reset WAN Card** to power cycle and reboot the WAN card.
Enable WAN (3G)	Select to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work properly.

6 Define or override the following authentication parameters in the **Basic Settings** field:

Username	Provide a username for authentication support by the cellular data carrier.
Password	Provide a 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 and Asia.
Authentication Type	Specify the authentication type used by the cellular data provider. Supported authentication types are **`None`**, **`PAP`**, **`CHAP`**, **`MSCHAP`**, and **`MSCHAP-v2`**.

7 Define or override the following NAT parameter in the **Network Address Translation (NAT)** field:

NAT Direction	Define the NAT *(Network Address Translation)* direction. Options include: 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 controller or service platform 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 network. None – No NAT activity takes place. This is the default setting.

8 Define or override the following security parameters in the **Security Settings** field:

IP Inbound Firewall Rules	Select an inbound IPv4 ACL to associate with traffic on the WAN backhaul. This setting pertains to IPv4 inbound traffic only and not IPv6. 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. If an appropriate IP ACL does not exist, click **Add** to create a new one.
VPN Crypto Map	If necessary, specify a crypto map for the wireless WAN. A crypto map can be up to 256 characters long. If a suitable crypto map is not available, click **Create** button to configure a new one.

9 Define or override the following route parameter in the **Default Route Priority** field:

WWAN Default Route Priority	Use the spinner control to define a priority from 1 - 8,000 for the default route learned by the wireless WAN. The default value is 3000.

10 Click **OK** to save the changes and overrides made to the WAN Backhaul screen.

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

Overriding PPPoE Configuration

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 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

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.

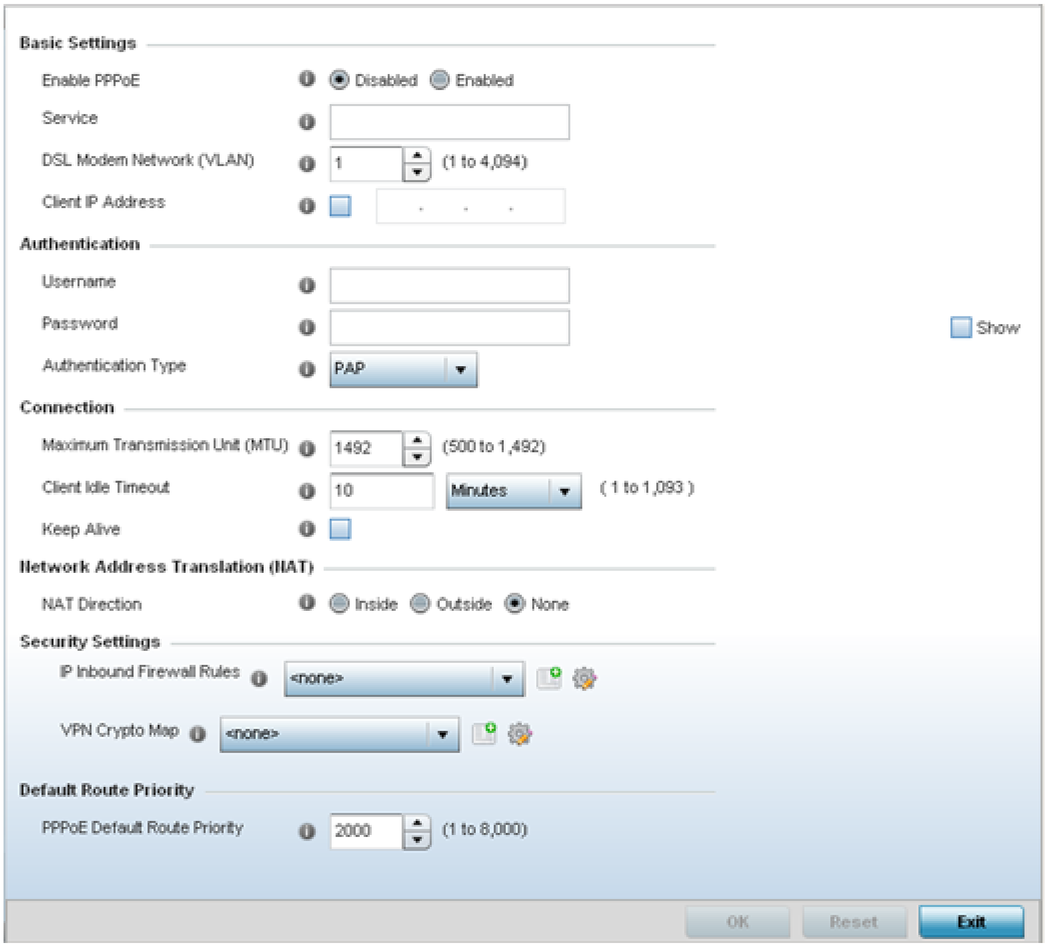
When the access point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

To create a PPPoE point-to-point configuration:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.
3. Select Profile **Profile Overrides** → **Interface**.

4 Select **PPPoE**.



Basic Settings

Enable PPPoE ● Disabled ○ Enabled

Service

DSL Modem Network (VLAN) 1 (1 to 4,094)

Client IP Address ☐

Authentication

Username

Password ☐ Show

Authentication Type PAP

Connection

Maximum Transmission Unit (MTU) 1492 (500 to 1,492)

Client Idle Timeout 10 Minutes (1 to 1,093)

Keep Alive ☐

Network Address Translation (NAT)

NAT Direction ○ Inside ○ Outside ● None

Security Settings

IP Inbound Firewall Rules <none>

VPN Crypto Map <none>

Default Route Priority

PPPoE Default Route Priority 2000 (1 to 8,000)

Figure 69: Device Overrides - PPPoE 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.

5 Use the Basic Settings field to enable PPPoE and define a PPPoE client.

Admin Status	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.

6. 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**.

7. 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.

8. 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).

9. 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 771.
VPN Crypto Map	Use the drop-down menu to apply an existing crypto map configuration to this PPPoE interface.

10. Set the **Default Route Priority** for the default route learned using PPPoE.

    Select from 1 - 8,000. The default setting is 2,000.

11. 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.

Overriding Bluetooth Configuration

AP-8432 and AP-8533 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.

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 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.

To define a Bluetooth radio interface configuration:

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

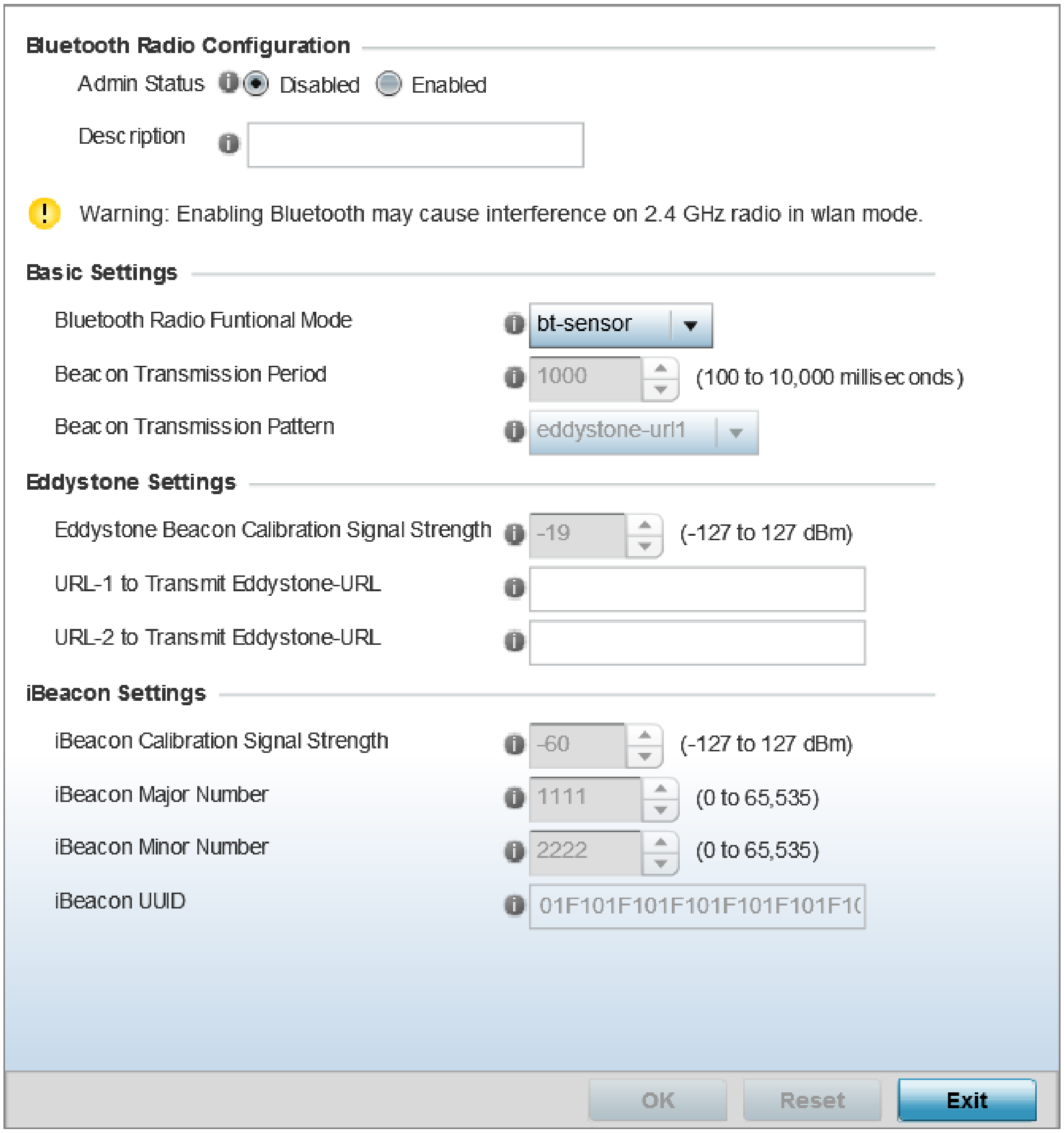
   The Device Configuration screen displays in the right-hand UI. This screen lists managed devices or peer controllers, service platforms, or access points.

2 Select a target access point in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Profile Overrides** → **Interface**.

4 Select **Bluetooth**.



Bluetooth Radio Configuration

Admin Status ● Disabled ○ Enabled

Description

Warning: Enabling Bluetooth may cause interference on 2.4 GHz radio in wlan mode.

Basic Settings

Bluetooth Radio Funtional Mode: bt-sensor

Beacon Transmission Period: 1000 (100 to 10,000 milliseconds)

Beacon Transmission Pattern: eddystone-url1

Eddystone Settings

Eddystone Beacon Calibration Signal Strength: -19 (-127 to 127 dBm)

URL-1 to Transmit Eddystone-URL

URL-2 to Transmit Eddystone-URL

iBeacon Settings

iBeacon Calibration Signal Strength: -60 (-127 to 127 dBm)

iBeacon Major Number: 1111 (0 to 65,535)

iBeacon Minor Number: 2222 (0 to 65,535)

iBeacon UUID: 01F101F101F101F101F101F1(

Figure 70: Profile Overrides - Bluetooth Screen

5 Set the following Bluetooth Radio Configuration parameters:

Admin Status	`Enable` or `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.

6 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`**. Use **`bt-sensor`** mode for ADSP Bluetooth classic sensing. Use **`le-beacon`** mode to have the access point transmit both ibeacon and Eddystone-URL low energy beacons. The *bt-sensor* option is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. 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`**. 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. 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.

7 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. The encoding process is for getting the URL to fit within the beacon's payload.
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. The encoding process is for getting the URL to fit within the beacon's payload.

8 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 UUID. The UUID classification contains 32 hexadecimal digits The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

9 Click **OK** to save the changes made to the Bluetooth configuration.

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

Profile Overrides - Network Overview

Refer to the following for overriding the selected device's profile network configurations.

- Profile Overrides - DNS Configuration on page 167
- Profile Overrides - ARP Configuration on page 169
- Profile Overrides - L2TPv3 General Settings on page 170
- GRE Tunnel Configuration on page 178
- IGMP Snooping Configuration on page 182
- MLD Snooping Configuration on page 184
- QoS Traffic Shaping Basic Configuration on page 186
- Profile Overrides - IPv4 Routing on page 191
- BGP Configuration on page 213
- Forwarding Database Configuration on page 226
- Profile Overrides - Bridge VLAN on page 227
- CDP Configuration on page 234
- LLDP Configuration on page 235
- Miscellaneous Network Configurations on page 236
- Network Basic Alias on page 239
- IPv6 Neighbor Configuration on page 247

Profile Overrides - 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 override DNS configuration:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device by double-clicking on the device name.

   You can also select a target device from the lower, left-hand pane of the Web UI.

   The selected device's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **DNS**.

The selected device's DNS configuration screen displays.

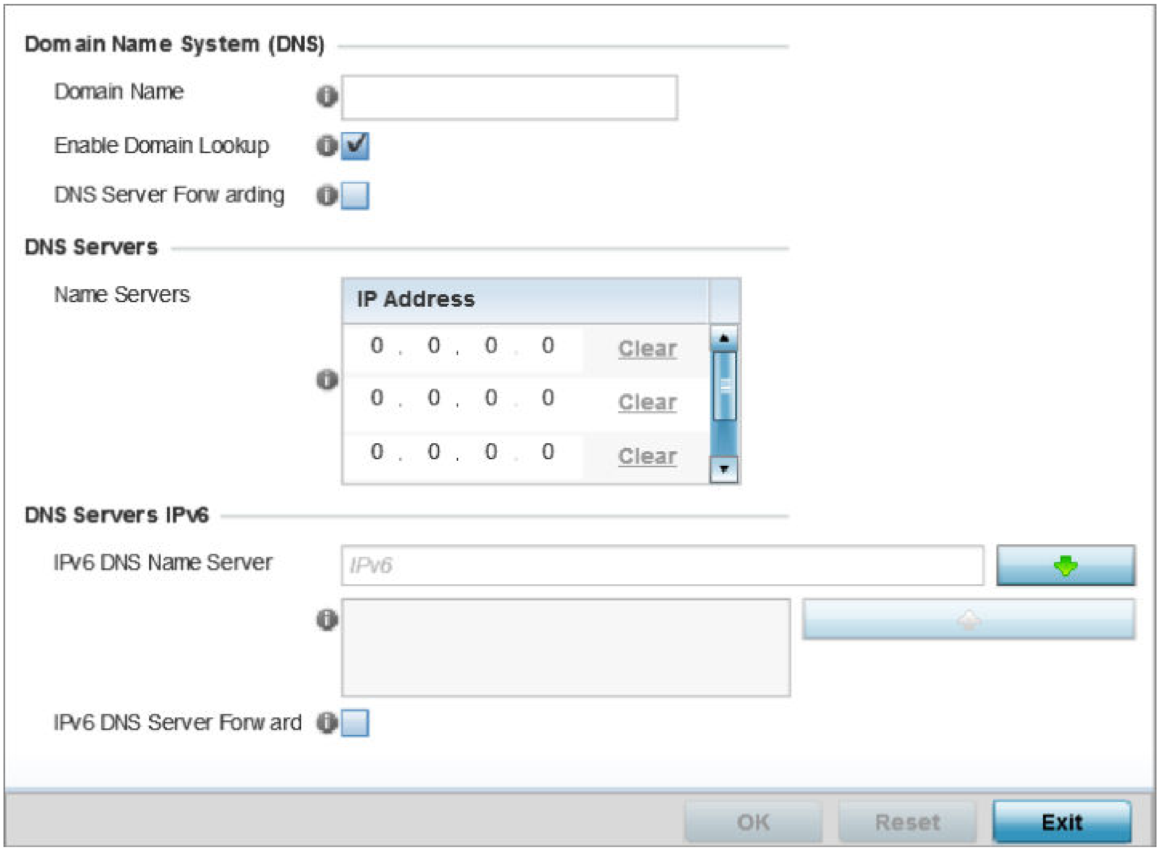


Figure 71: Profile Overrides - Network DNS Configuration Screen

4 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.

5 In the DNS Servers field, provide the IP addresses of up to three Name Server resources available to the access point.

6 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.

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

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

Profile Overrides - 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 configure or override ARP configuration:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device by double-clicking on the device name.

   You can also select a target device from the lower, left-hand pane of the Web UI.

   The selected device's configuration menu displays.

3 Expand **Profile Overrides** → **Network** and select **DNS**.

The selected device's DNS configuration screen displays.

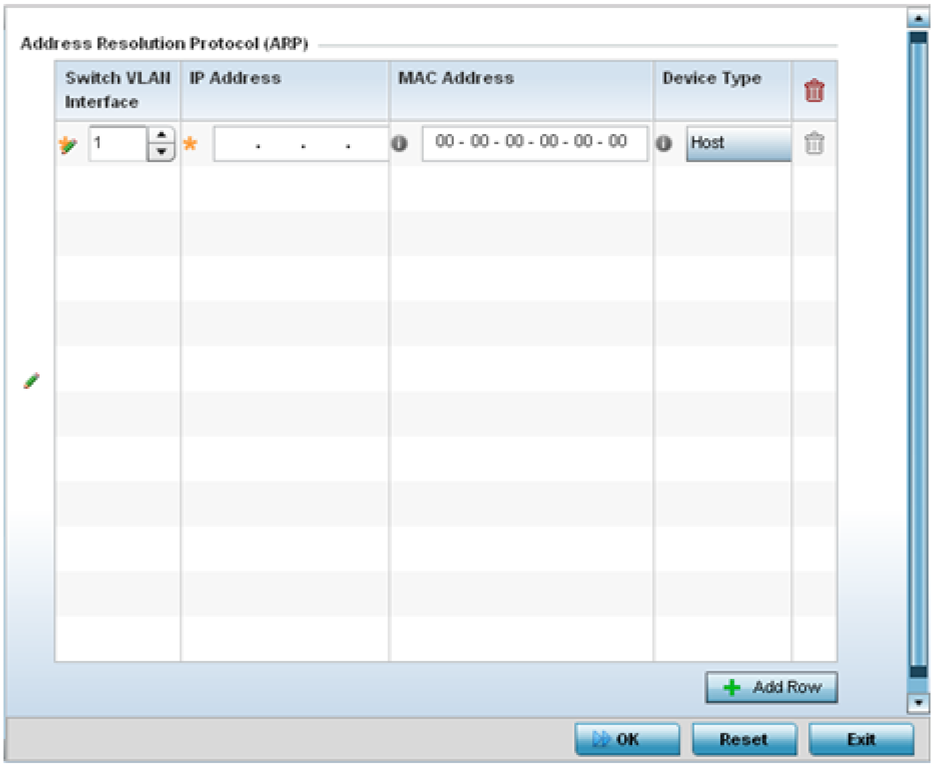


Figure 72: ARP Configuration Screen

4 Set the following ARP configurations:

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 To add additional ARP settings select **+ Add Row** and enter the configuration information.

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.

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*.

To override the profile's L2TPv3 general configuration:

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

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device by double-clicking on the device name.

  You can also select a target device from the lower, left-hand pane of the Web UI.

  The selected device's configuration menu displays.

3 Expand the **Network** node and select **L2TPv3**.

The L2TPv3 general configuration screen displays.

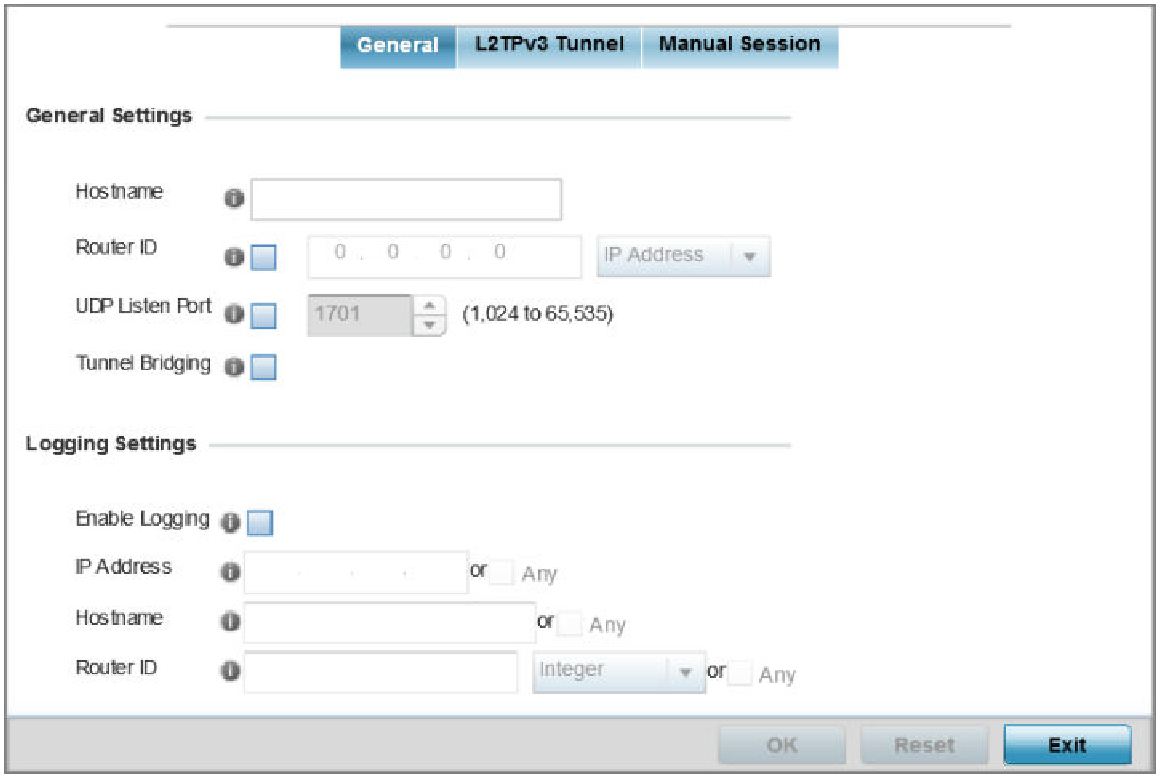


Figure 73: L2TPv3 - General Configuration Screen

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 tunnelled 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.

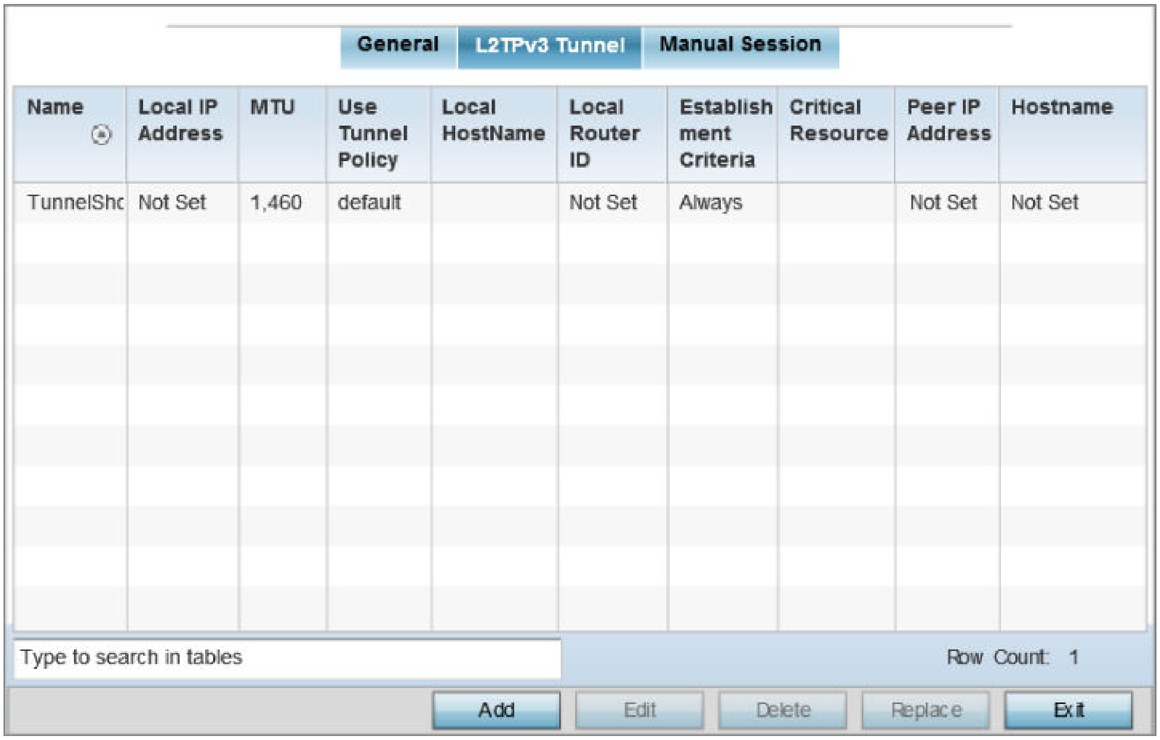
Click **Reset** to revert to the last saved configuration.

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.



Name	Local IP Address	MTU	Use Tunnel Policy	Local HostName	Local Router ID	Establishment Criteria	Critical Resource	Peer IP Address	Hostname
TunnelShc	Not Set	1,460	default		Not Set	Always		Not Set	Not Set

Figure 74: 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.

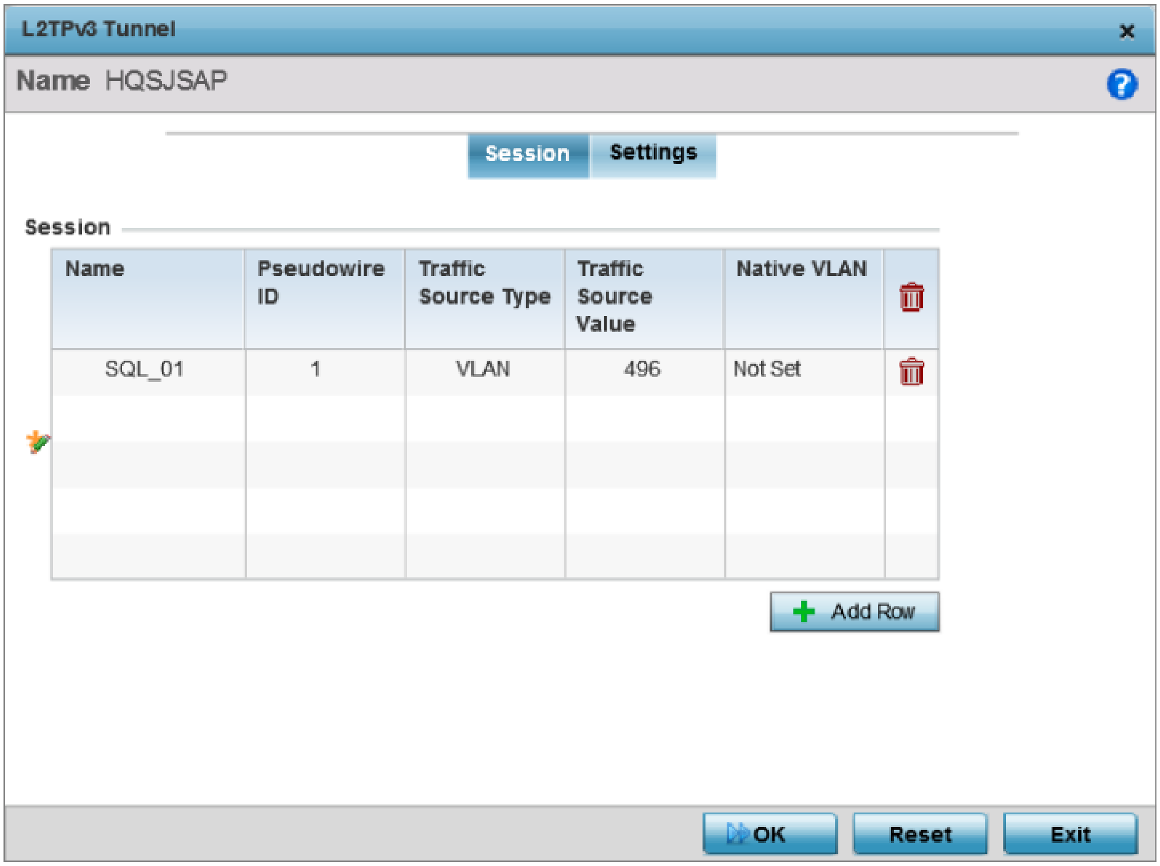
Local Router ID	Specifies the router ID sent in the tunnel establishment messages.
Establishment Criteria	Specifies tunnel criteria between two peers.
Critical Resource	Specifies the critical resource that should exist for a tunnel between two peers to be created and maintained. Critical resources are 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.



Name HQSJSAP

Session

Name	Pseudowire ID	Traffic Source Type	Traffic Source Value	Native VLAN
SQL_01	1	VLAN	496	Not Set

Figure 75: 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.

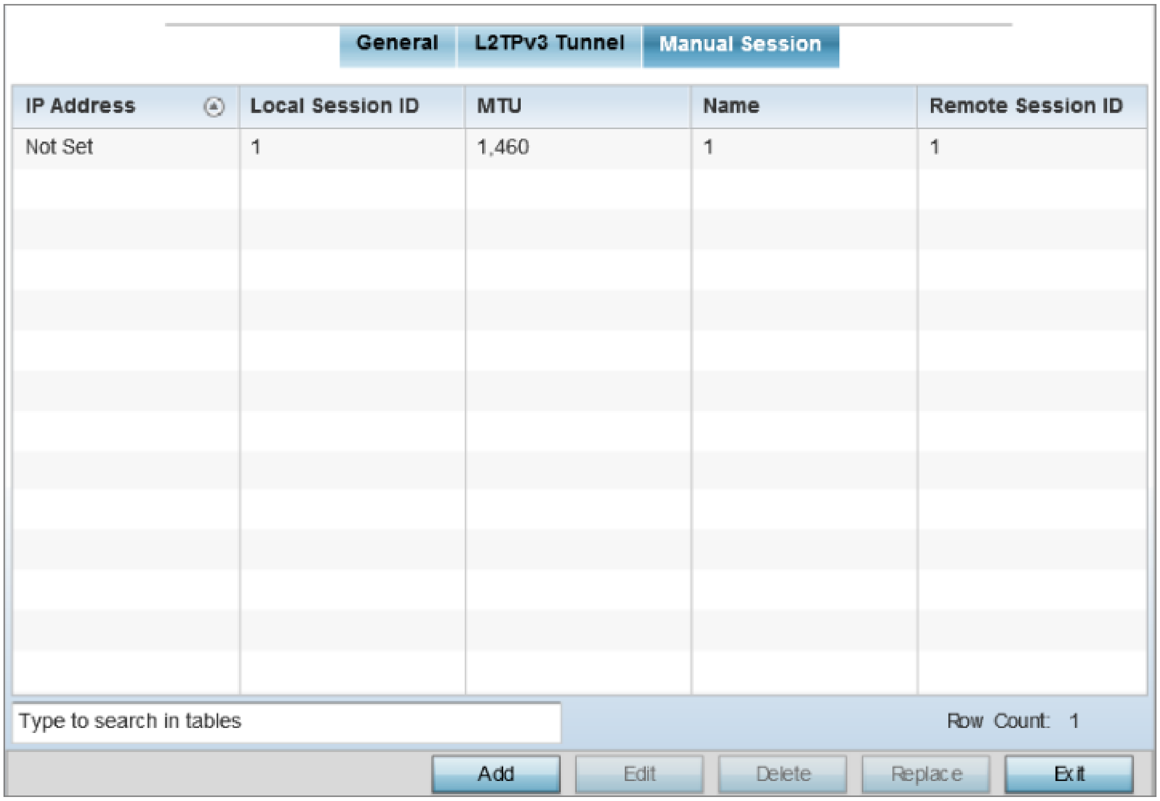
5 Click **OK** to save the L2TPv3 Tunnel session changes.

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.



IP Address	Local Session ID	MTU	Name	Remote Session ID
Not Set	1	1,460	1	1

Figure 76: 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

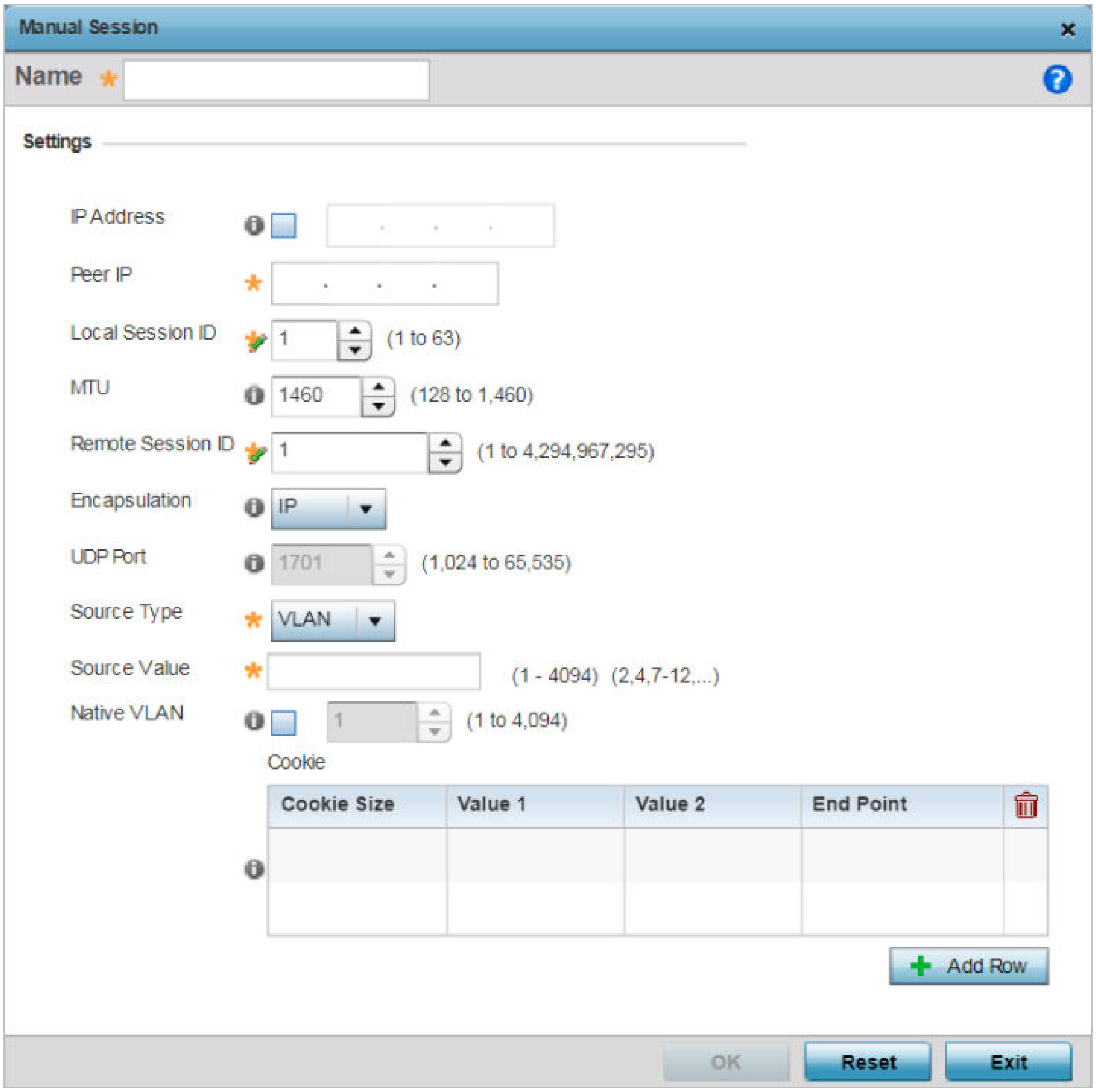
You can add a new L2TPv3 manual session configuration or edit an existing configuration.

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.



Manual Session

Name *

Settings

IP Address ☐

Peer IP *

Local Session ID 1 (1 to 63)

MTU 1460 (128 to 1,460)

Remote Session ID 1 (1 to 4,294,967,295)

Encapsulation IP

UDP Port 1701 (1,024 to 65,535)

Source Type * VLAN

Source Value * (1 - 4094) (2,4,7-12,...)

Native VLAN ☐ 1 (1 to 4,094)

Cookie

Cookie Size	Value 1	Value 2	End Point

Figure 77: 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.

GRE Tunnel Configuration

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.

The GRE tunnel main screen displays existing GRE Tunnel configuration. Select and review an existing tunnel configuration to determine if a new configuration needs to be created or an existing configuration needs to be modified.

To override an access point's GRE tunnel configuration.

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

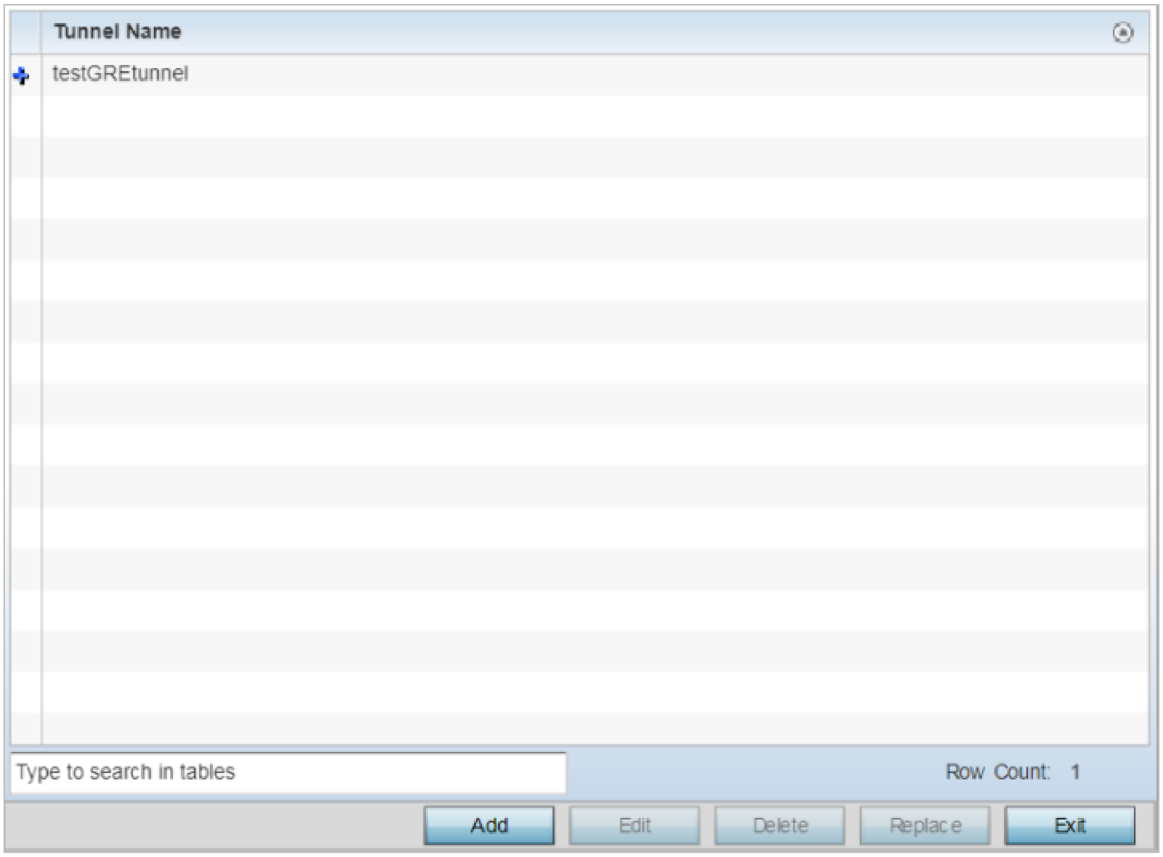
  The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

  The selected device's configuration screen displays.

3 Expand the **Network** node and select **GRE**.

  The GRE Tunnel screen displays.



Tunnel Name
testGREtunnel

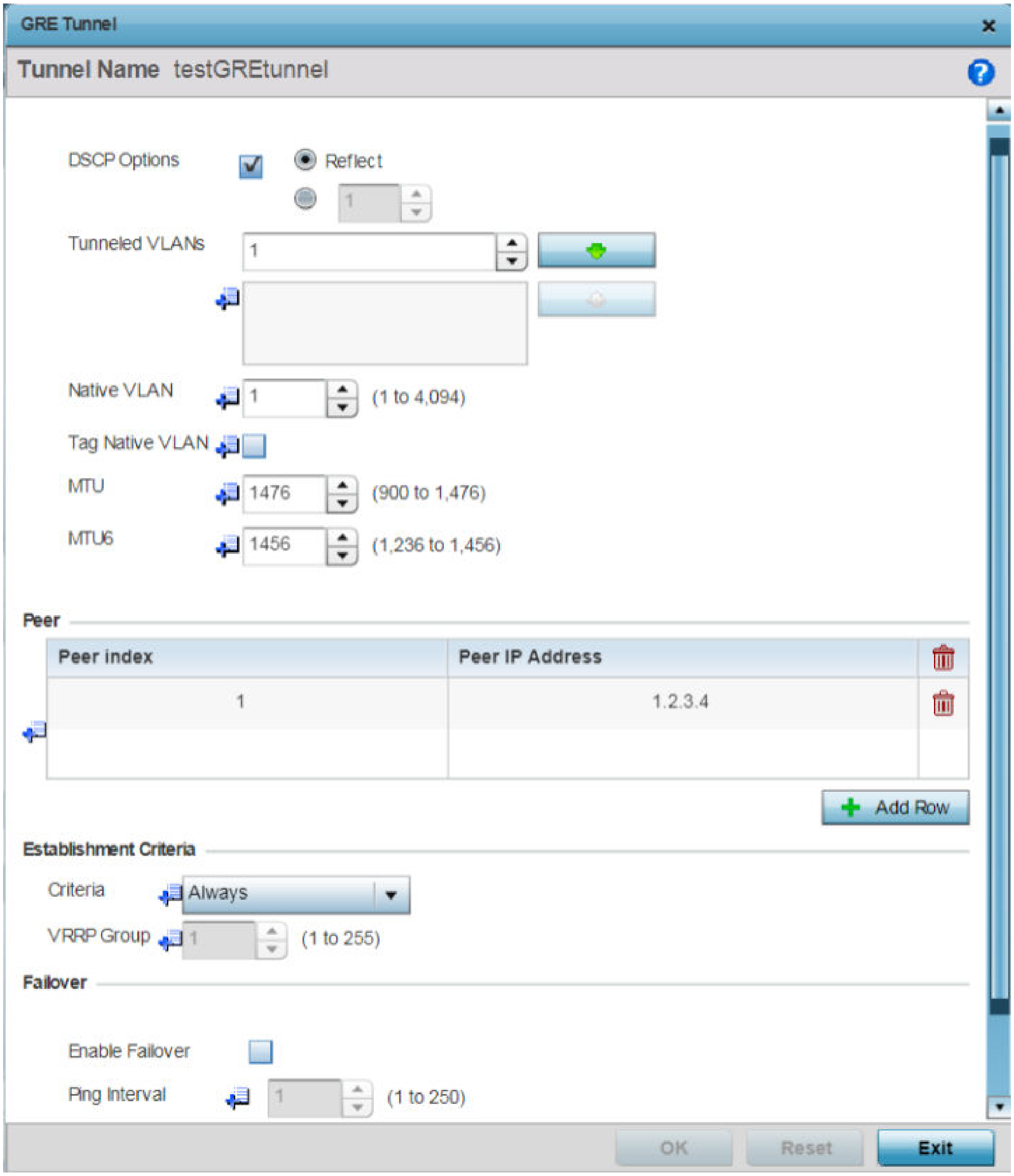
Figure 78: Profile Overrides - Network - GRE Configuration Main Screen

Adding and Editing GRE Tunnel

You can add a new GRE tunnel configuration or edit an existing configuration.

1 Select the **Add** button 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.

The GRE tunnel configuration screen displays.



Tunnel Name testGREtunnel

DSCP Options ☑ ● Reflect ○ 1

Tunneled VLANs 1

Native VLAN 1 (1 to 4,094)

Tag Native VLAN ☐

MTU 1476 (900 to 1,476)

MTU6 1456 (1,236 to 1,456)

Peer

Peer index	Peer IP Address
1	1.2.3.4

Establishment Criteria

Criteria Always

VRRP Group 1 (1 to 255)

Failover

Enable Failover ☐

Ping Interval 1 (1 to 250)

Figure 79: GRE Tunnel - Add/Edit 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 the **Clear Overrides** button. This removes all overrides from the device.

2 If creating a new GRE configuration, assign it a 31 character maximum `Name` to distinguish its configuration.

3 Define the following settings for the GRE configuration:

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 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.

4 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.

5 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. Depending on which of the following options is selected, the GRE is established: • **`vrrp-master`** - The tunnel is created only if the master node is the VRRP master. • **`cluster-master`** - The tunnel is created only if the master node is the cluster master. • **`rf-domain-manager`** - The tunnel is created only if the master node is the RF Domain manager. • **`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 enables 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.

6 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.

7 Select the **OK** button located to save the changes.

Select **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.

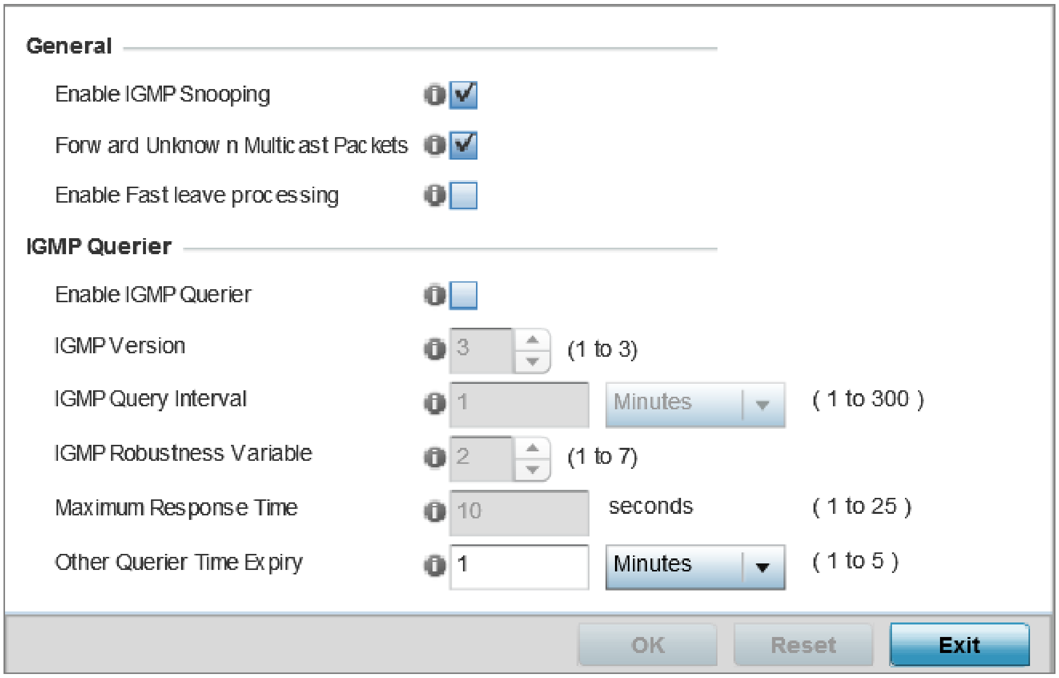
1 Go to **Configuration** → **Devices**.

The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand the **Network** node and select **IGMP Snooping**.



General

Enable IGMP Snooping ☑

Forward Unknown Multicast Packets ☑

Enable Fast leave processing ☐

IGMP Querier

Enable IGMP Querier ☐

IGMP Version 3 (1 to 3)

IGMP Query Interval 1 Minutes (1 to 300)

IGMP Robustness Variable 2 (1 to 7)

Maximum Response Time 10 seconds (1 to 25)

Other Querier Time Expiry 1 Minutes (1 to 5)

Figure 80: 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 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. 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.

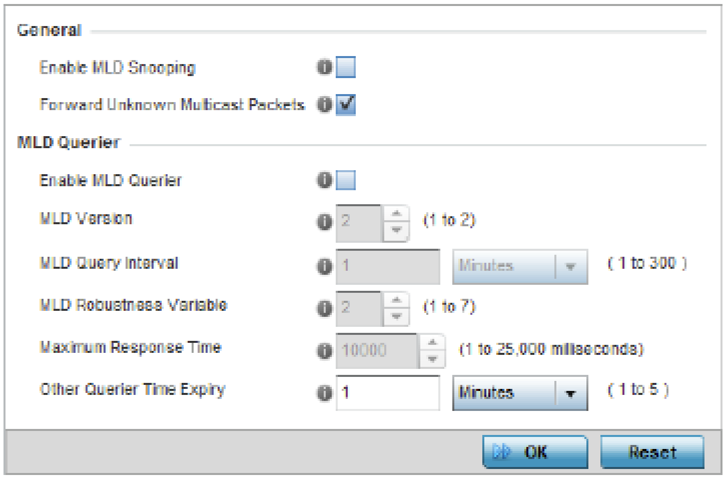
To set an MLD snooping configuration:

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

   The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.
2. Select a device from the list displayed.

   The selected device's configuration screen displays.

3 Expand the **Network** node and select **MLD Snooping**.



General

Enable MLD Snooping ☐

Forward Unknown Multicast Packets ☑

MLD Querier

Enable MLD Querier ☐

MLD Version 2 (1 to 2)

MLD Query Interval 1 Minutes (1 to 300)

MLD Robustness Variable 2 (1 to 7)

Maximum Response Time 10000 (1 to 25,000 milliseconds)

Other Querier Time Expiry 1 Minutes (1 to 5)

Figure 81: 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 Click 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 priority of service to some packets over others. 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 applied to a packet.

To define an QoS configuration for DSCP mappings:

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

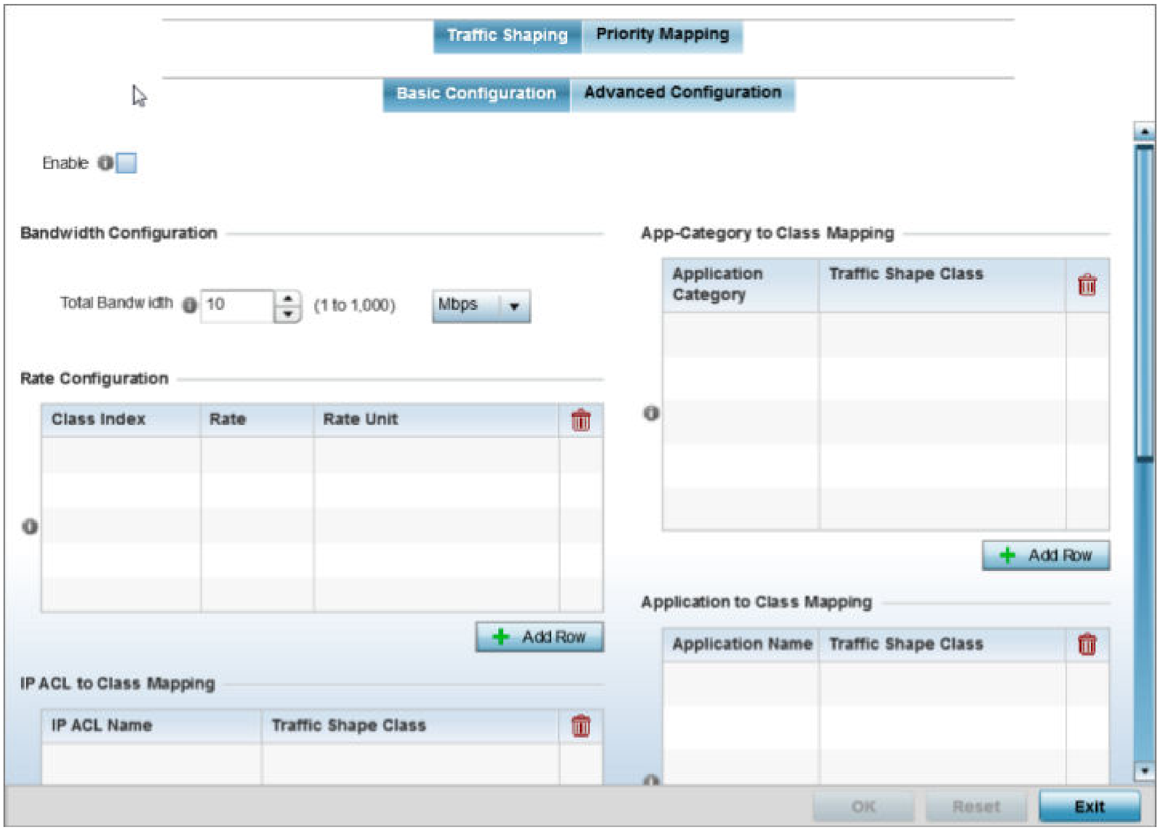
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand the **Network** node and select **Quality of Service (QoS)**.

The Traffic Shaping screen displays with the Basic Configuration tab selected by default.



Enable ☐

Total Bandwidth 10 Mbps

Figure 82: Profile Overrides - Network 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. For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 789 and Setting an IPv4 or IPv6 Firewall Policy on page 789.

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. For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 789 and Setting an IPv4 or IPv6 Firewall Policy on page 789.

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 509.

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 509.

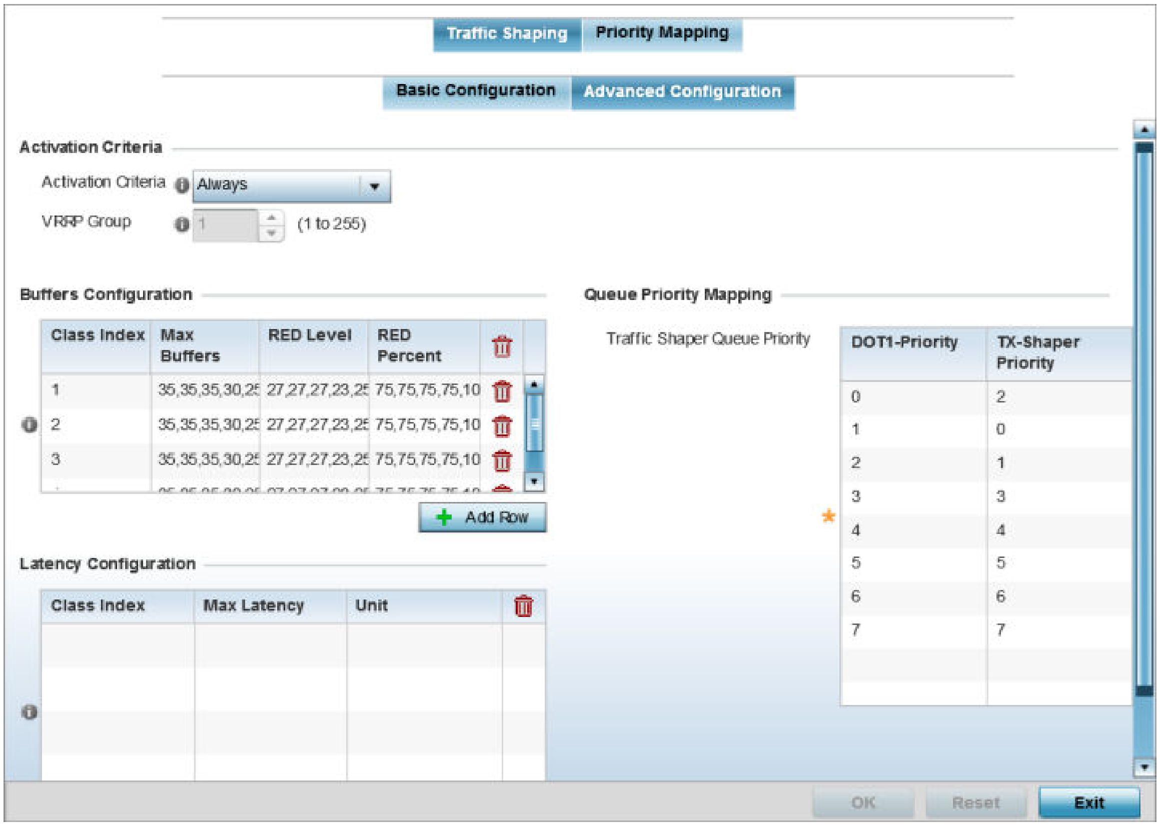
11 Click the **OK** button located to save the changes to the traffic shaping basic configuration.

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

QoS Traffic Shaping Advanced Configuration

1 Select the **Advanced Configuration** tab.

The **Traffic Shaping** → **Advanced Configuration** screen displays.



Activation Criteria: Always

VRRP Group: 1 (1 to 255)

Class Index	Max Buffers	RED Level	RED Percent
1	35,35,35,30,25	27,27,27,23,25	75,75,75,75,10
2	35,35,35,30,25	27,27,27,23,25	75,75,75,75,10
3	35,35,35,30,25	27,27,27,23,25	75,75,75,75,10

Class Index	Max Latency	Unit

Traffic Shaper Queue Priority

DOT1-Priority	TX-Shaper Priority
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 83: 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.

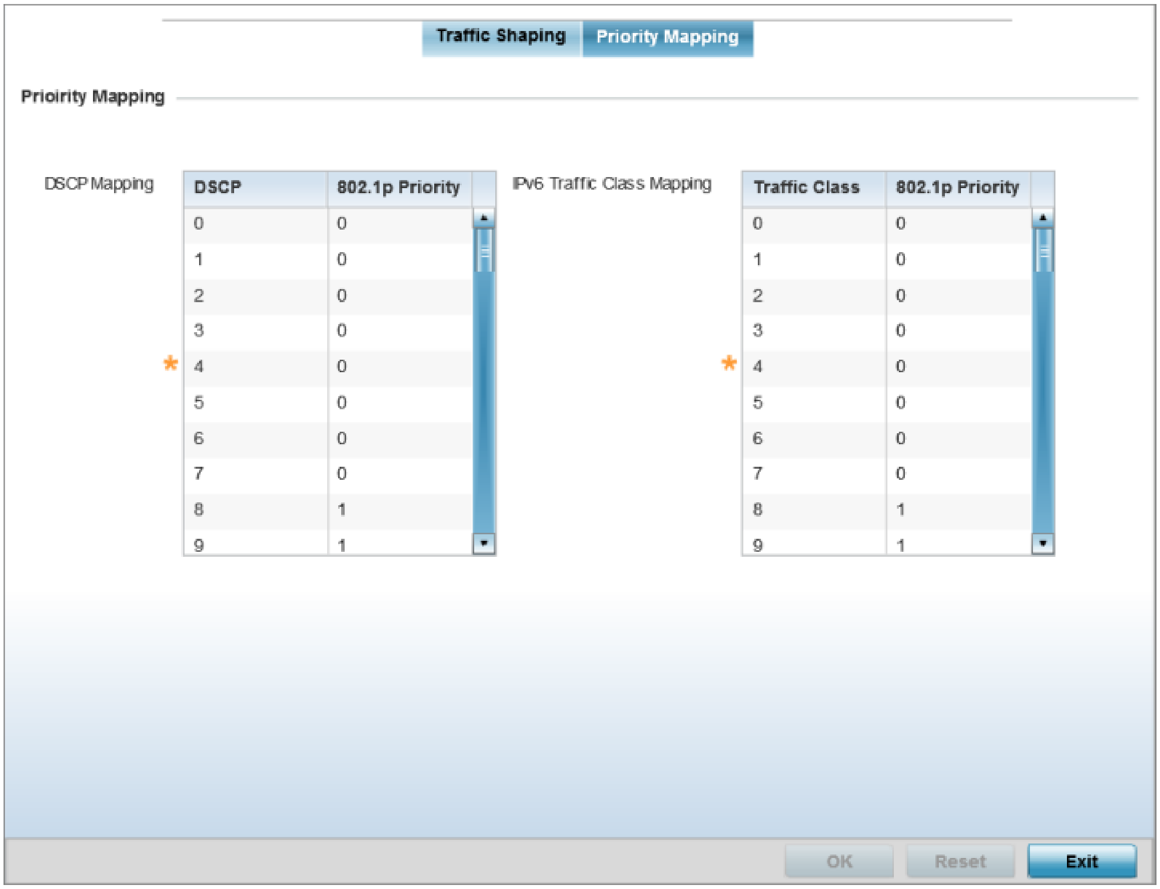
6 Select **OK** to save the traffic shaping advanced configuration changes.

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.



DSCP Mapping

DSCP	802.1p Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1

IPv6 Traffic Class Mapping

Traffic Class	802.1p Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1

Figure 84: 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: • 0 – *Best Effort* • 1 – *Background* • 2 – *Spare* • 3 – *Excellent Effort* • 4 – *Controlled Load* • 5 – *Video* • 6 – *Voice* • 7 – *Network Control* Note: 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: • 0 – *Best Effort* • 1 – *Background* • 2 – *Spare* • 3 – *Excellent Effort* • 4 – *Controlled Load* • 5 – *Video* • 6 – *Voice* • 7 – *Network Control*

4 Select **OK** to save the priority mapping 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**.

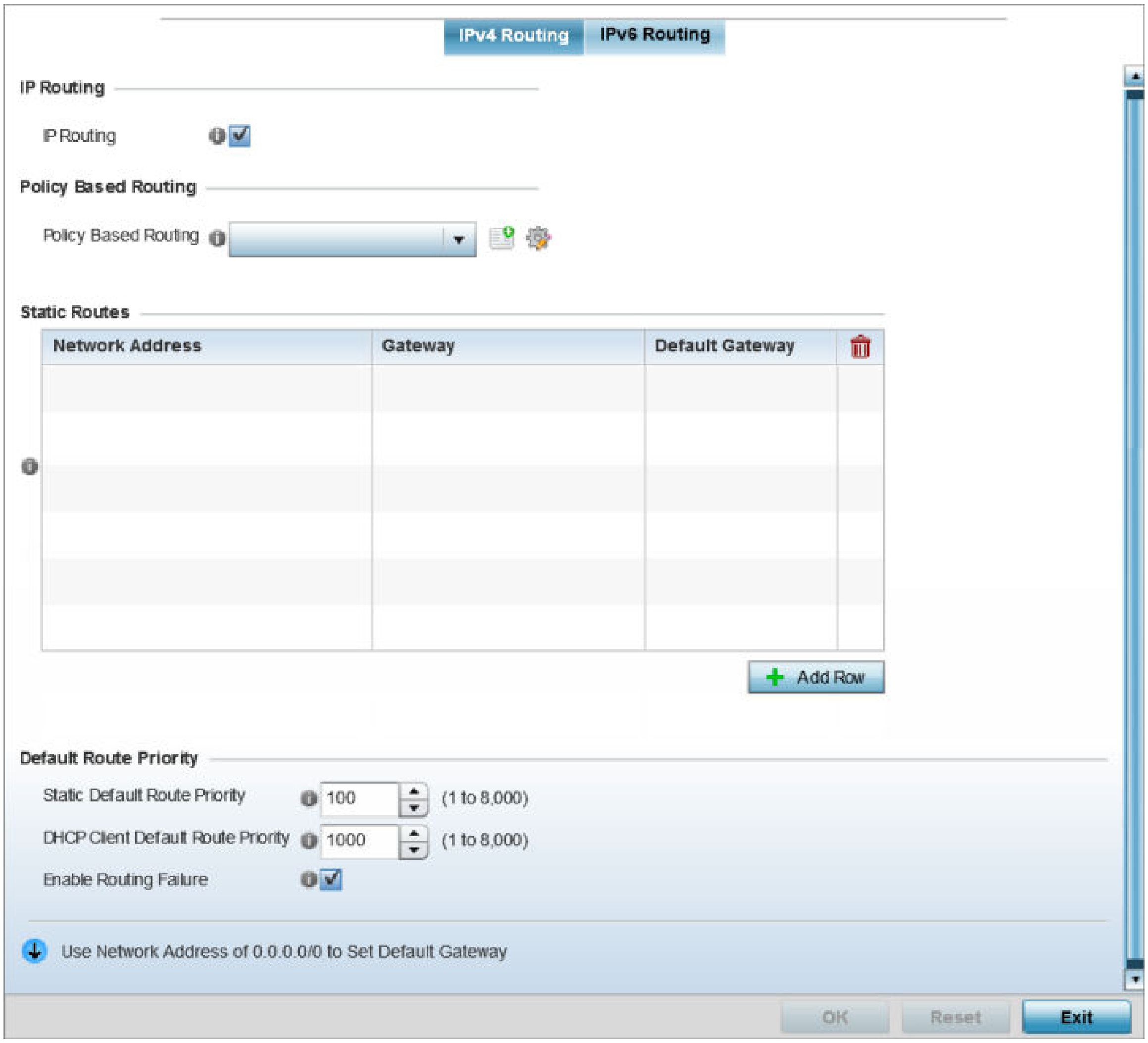
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand **Network** and select **Routing**.

The IPv4 Routing configuration screen displays.



IP Routing ☑

Policy Based Routing

Static Default Route Priority 100 (1 to 8,000)

DHCP Client Default Route Priority 1000 (1 to 8,000)

Enable Routing Failure ☑

Use Network Address of 0.0.0.0/0 to Set Default Gateway

Figure 85: 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 454.

6 In the Static Routes table, click **Add Row +** and provide the following static 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 Click the **OK** button to save the IPv4 routing configuration changes.

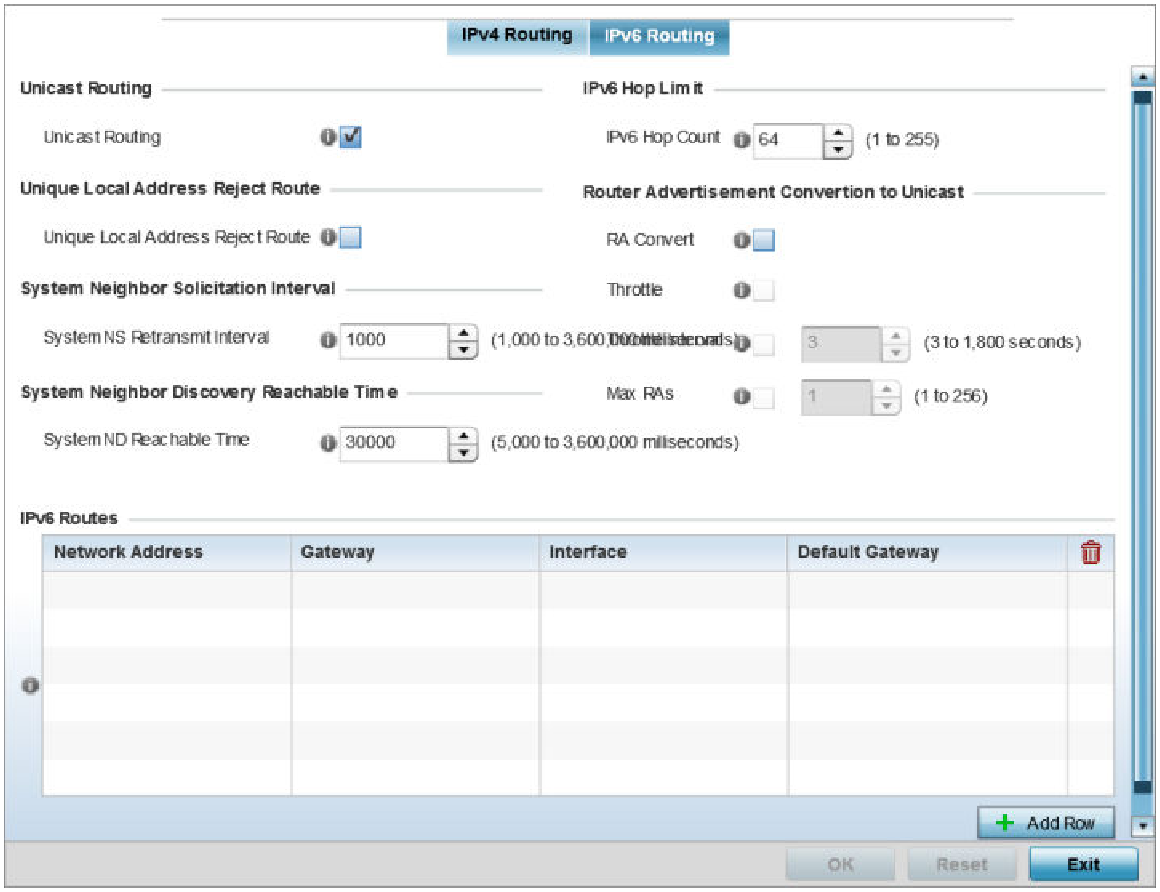
Click **Reset** to revert to the last saved configuration.

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.



Unicast Routing

Unicast Routing ☑

Unique Local Address Reject Route

Unique Local Address Reject Route ☐

System Neighbor Solicitation Interval

System NS Retransmit Interval 1000 (1,000 to 3,600,000 milliseconds)

System Neighbor Discovery Reachable Time

System ND Reachable Time 30000 (5,000 to 3,600,000 miliseconds)

IPv6 Hop Limit

IPv6 Hop Count 64 (1 to 255)

Router Advertisement Convertion to Unicast

RA Convert ☐

Throttle ☐

☐ 3 (3 to 1,800 seconds)

Max RAs ☐ 1 (1 to 256)

Network Address	Gateway	Interface	Default Gateway

Figure 86: 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.

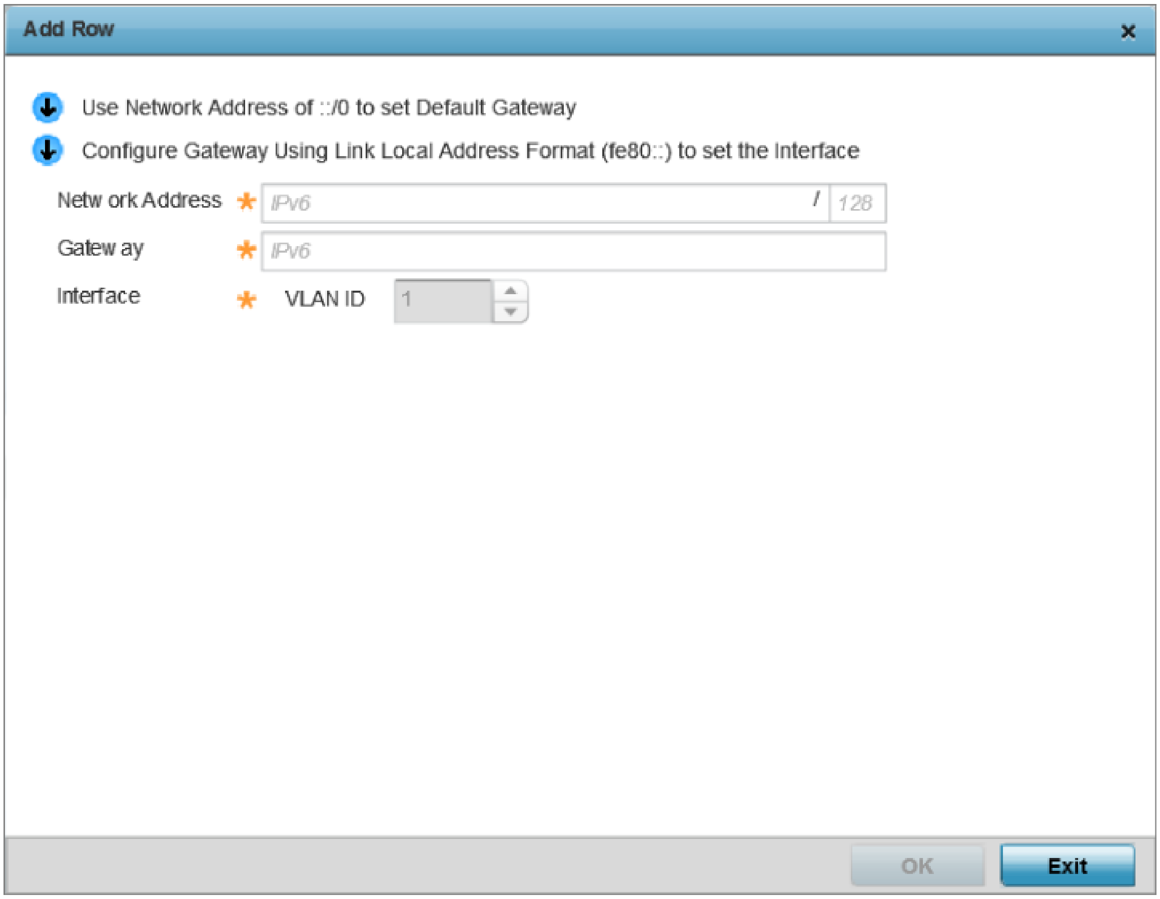

Add Row
Use Network Address of ::/0 to set Default Gateway
Configure Gateway Using Link Local Address Format (fe80::) to set the Interface
Netw ork Address
IPv6
/
128
Gatew ay
IPv6
Interface
VLAN ID
1
OK
Exit

Figure 87: 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.

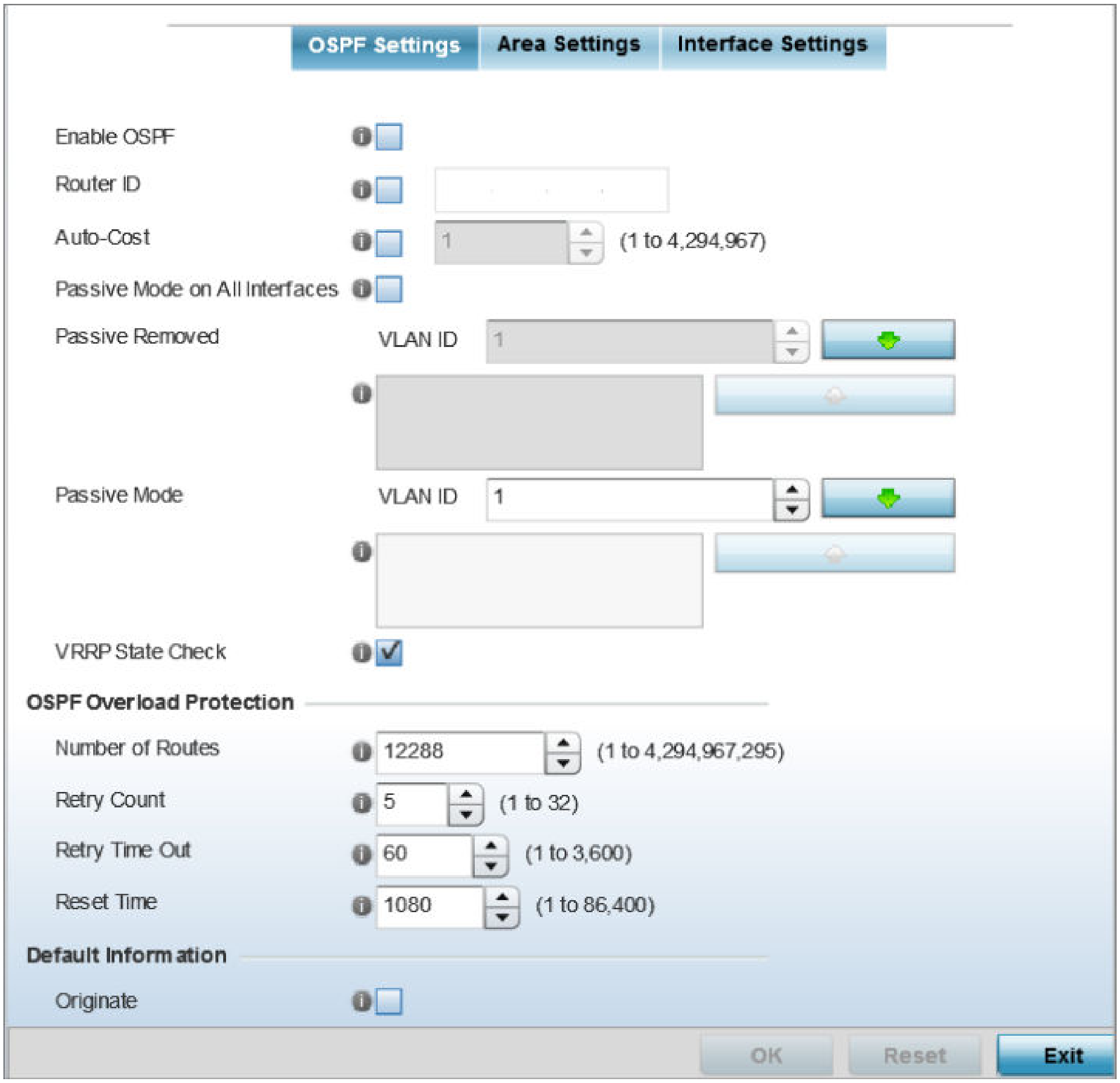
To override a profile's OSPF configurations:

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

   The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.
2. Select a device from the list displayed.

   The selected device's configuration screen displays.
3. Expand **Profile Overrides** → **Network** and select **OSPF**.

   The **OSPF** → **OSPF Settings** configuration screen displays.



Enable OSPF ☐
Router ID ☐
Auto-Cost ☐ 1 (1 to 4,294,967)
Passive Mode on All Interfaces ☐
Passive Removed VLAN ID 1
Passive Mode VLAN ID 1
VRRP State Check ☑

OSPF Overload Protection
Number of Routes 12288 (1 to 4,294,967,295)
Retry Count 5 (1 to 32)
Retry Time Out 60 (1 to 3,600)
Reset Time 1080 (1 to 86,400)

Default Information
Originate ☐

Figure 88: 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.

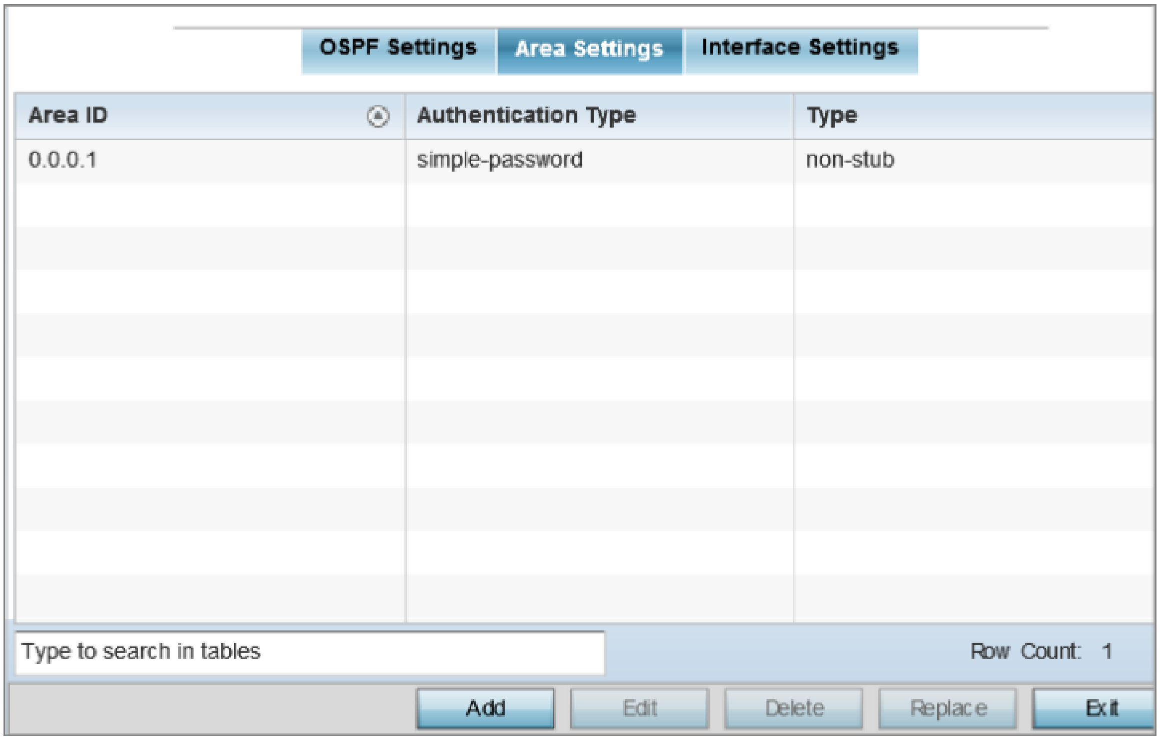
11 Click **OK** to save the OSPF setting changes.
Click **Reset** to revert to the last saved configuration.

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.



Area ID	Authentication Type	Type
0.0.0.1	simple-password	non-stub

Figure 89: OSPF - Area Setting Configuration Screen

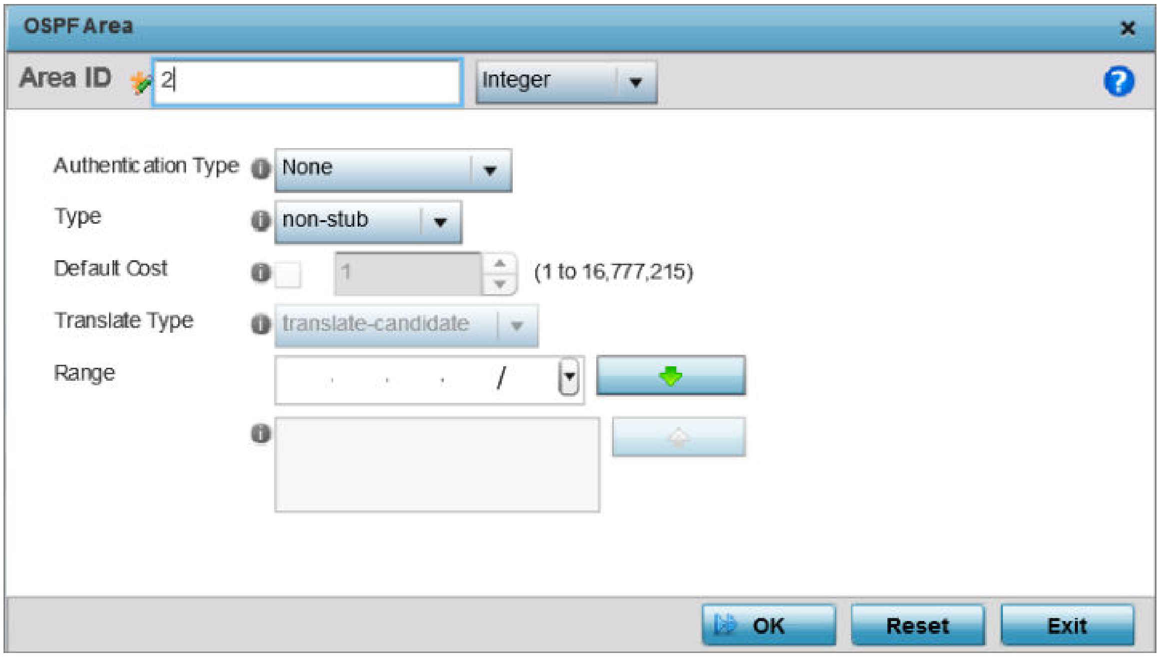
2 Review existing **Area Settings** configurations:

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.



Area ID: 2

Figure 90: 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.

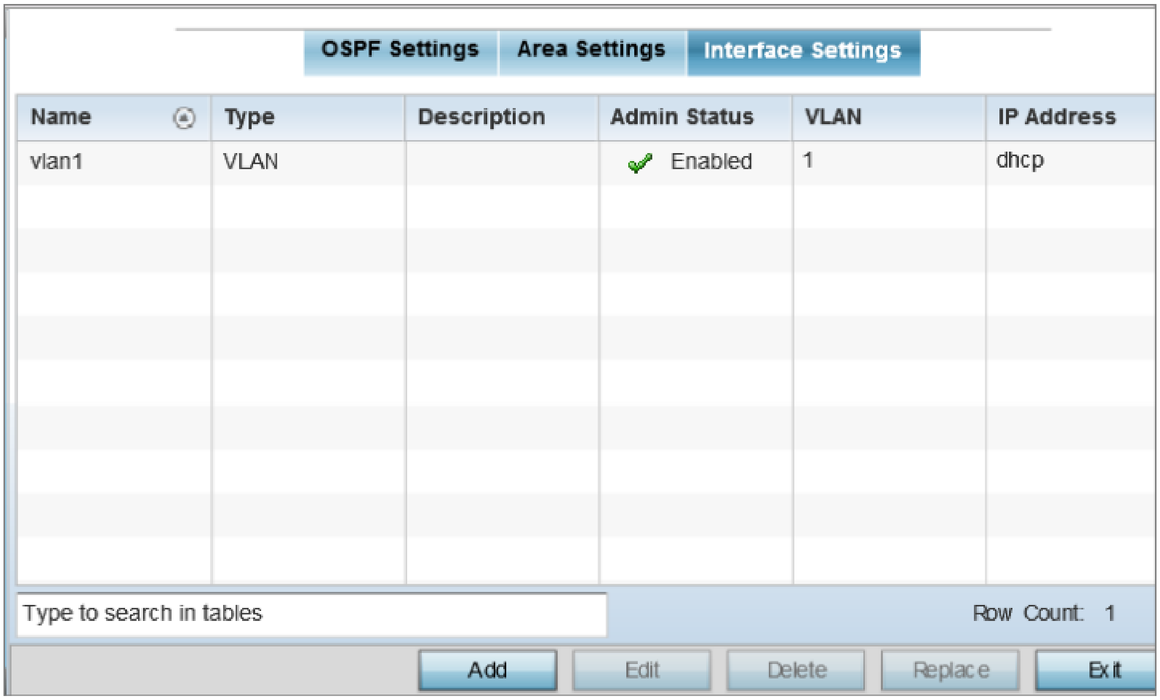
Click **Reset** to revert to the last saved configuration.

OSPF - Interface Settings

To override the access point profile's OSPF interface settings:

1 Select the **Interface Settings** tab.

The OSPF interface configuration displays.



Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		✓ Enabled	1	dhcp

Figure 91: 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.

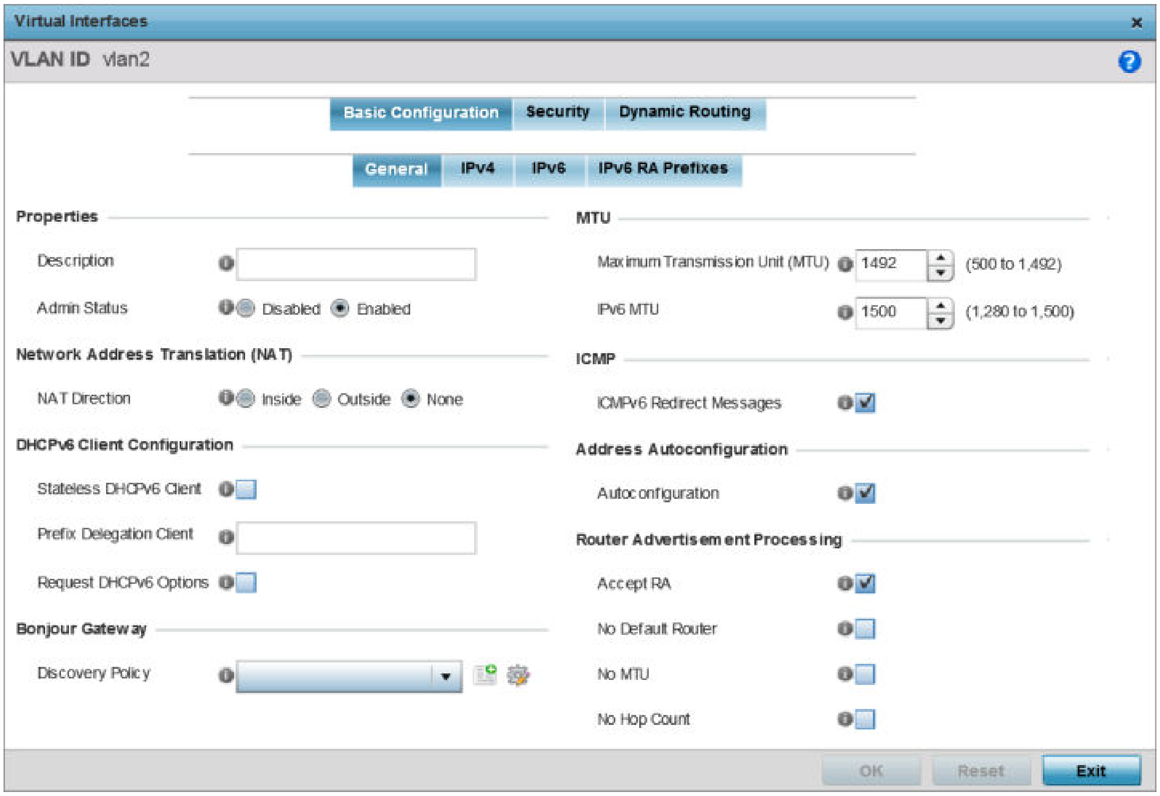
OSPF Basic General Settings

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.



VLAN ID vlan2

Properties
Description
Admin Status ○ Disabled ● Enabled

Network Address Translation (NAT)
NAT Direction ○ Inside ○ Outside ● None

DHCPv6 Client Configuration
Stateless DHCPv6 Client ☐
Prefix Delegation Client
Request DHCPv6 Options ☐

Bonjour Gateway
Discovery Policy

MTU
Maximum Transmission Unit (MTU) 1492 (500 to 1,492)
IPv6 MTU 1500 (1,280 to 1,500)

ICMP
ICMPv6 Redirect Messages ☑

Address Autoconfiguration
Autoconfiguration ☑

Router Advertisement Processing
Accept RA ☑
No Default Router ☐
No MTU ☐
No Hop Count ☐

Figure 92: 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.

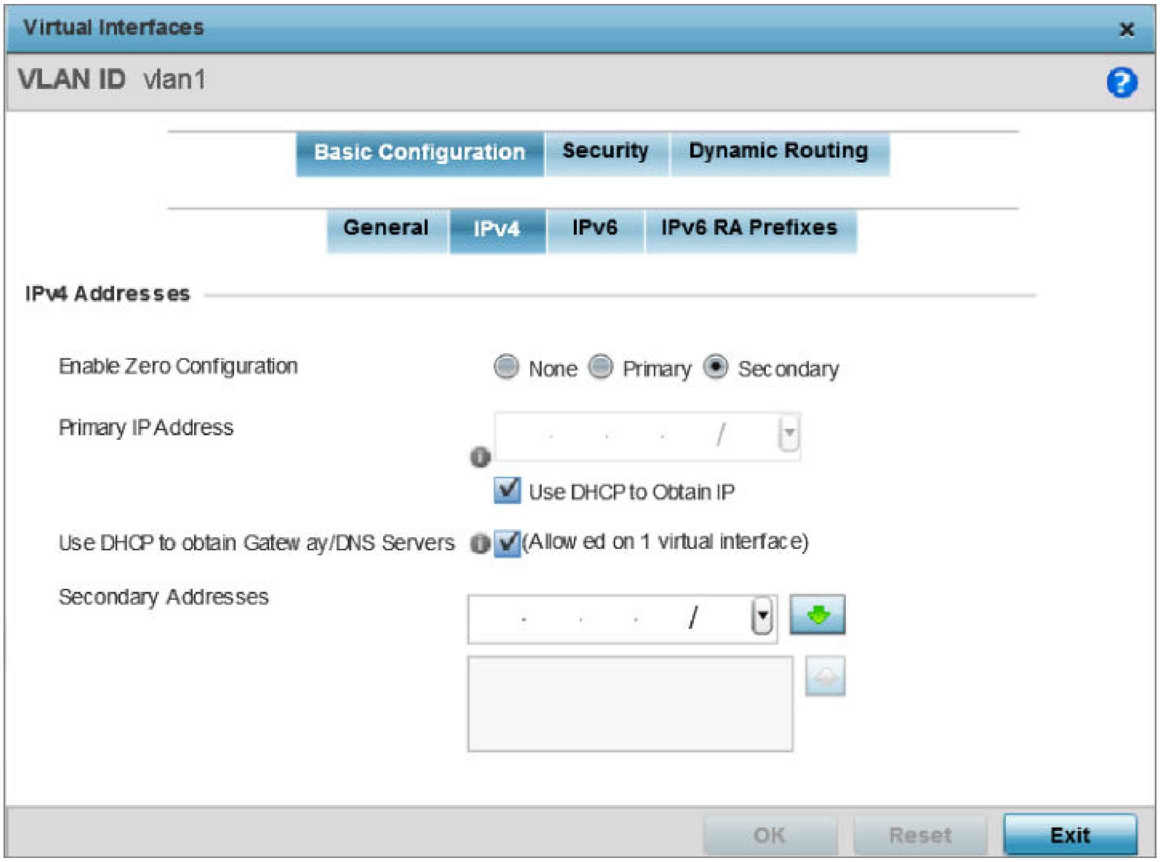
OSPF IPv4 Settings

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.



Enable Zero Configuration ○ None ○ Primary ● Secondary

Primary IP Address . . . /

☑ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ☑ (Allowed on 1 virtual interface)

Secondary Addresses . . . /

Figure 93: 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.

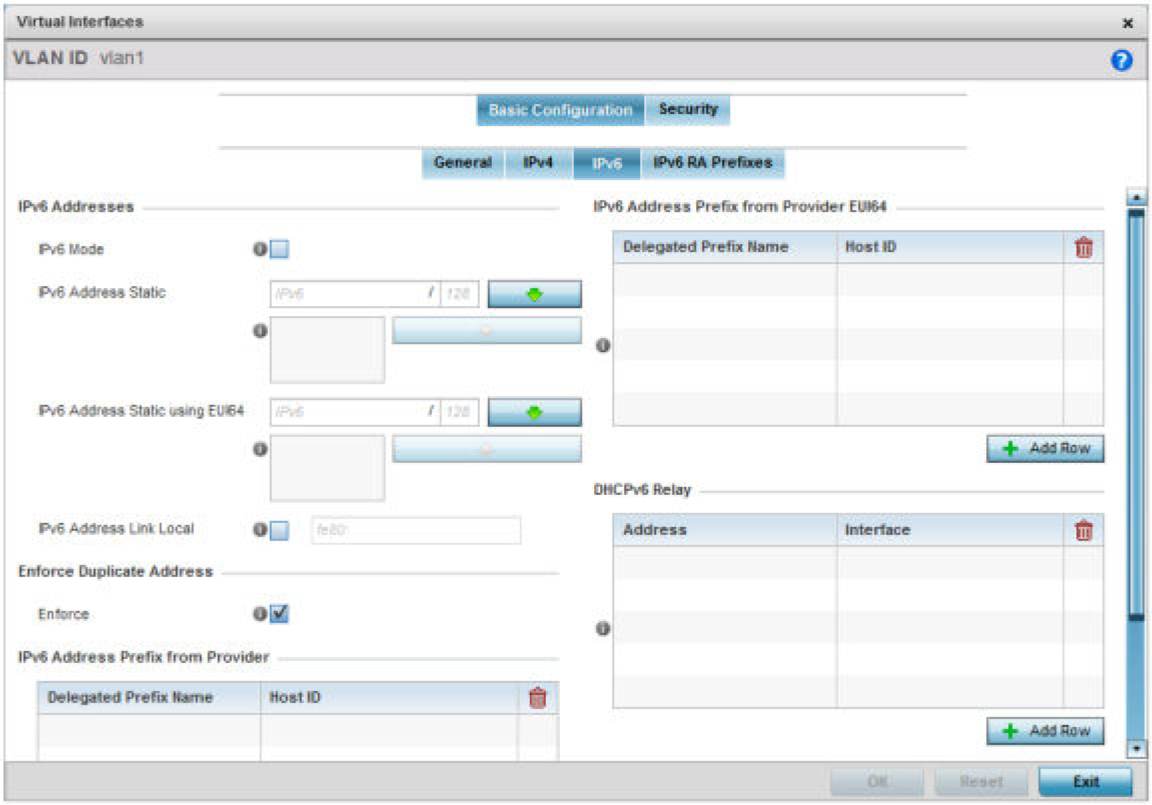


Figure 94: OSPF - VLAN Interface IPv6 Configuration Screen

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.

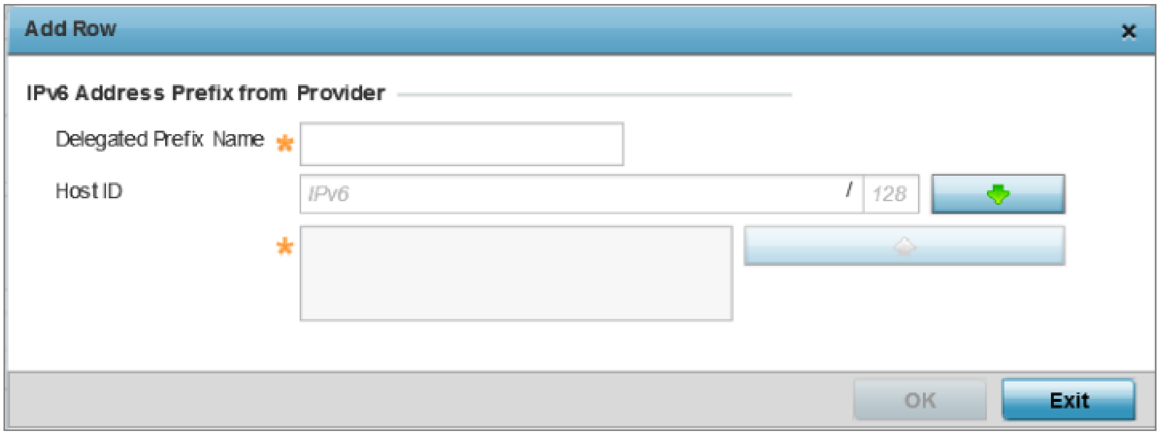


Figure 95: OSPF - IPv6 Add IPv6 Address Prefix from Provider Screen

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.

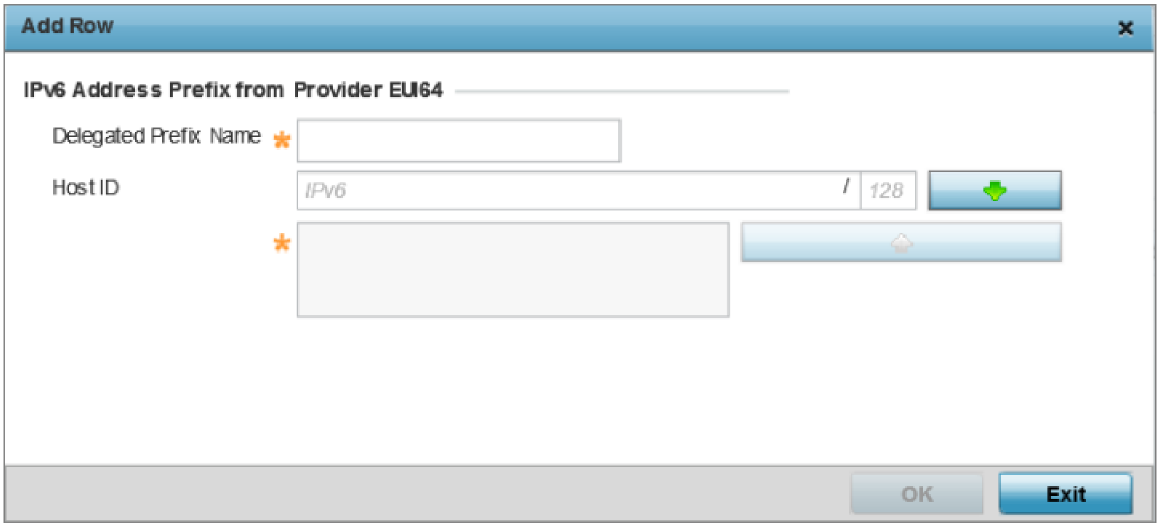


Figure 96: OSPF - IPv6 Add Address Prefixes from Provider EU164

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.

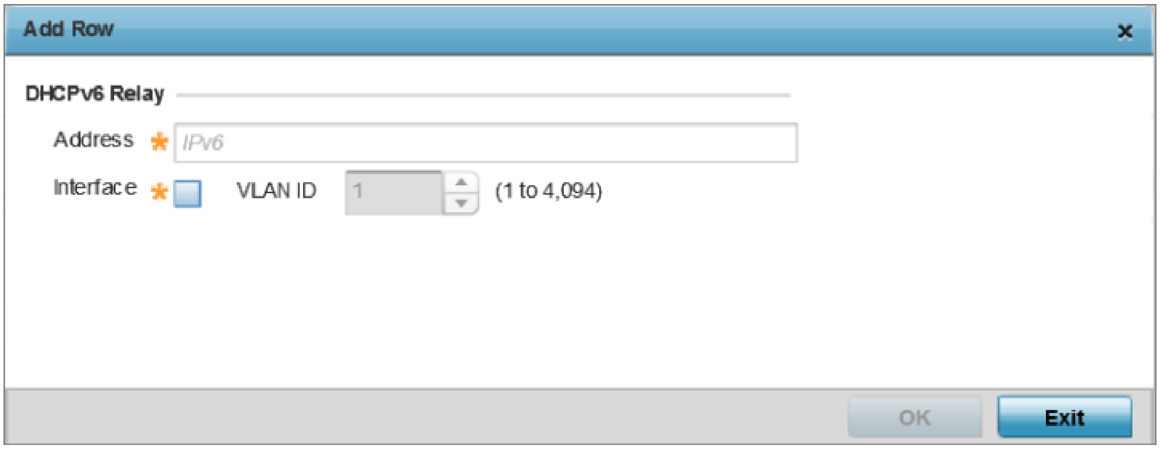


Figure 97: OPSF - VLAN Interface DHCPv6 Relay Configuration Screen

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.

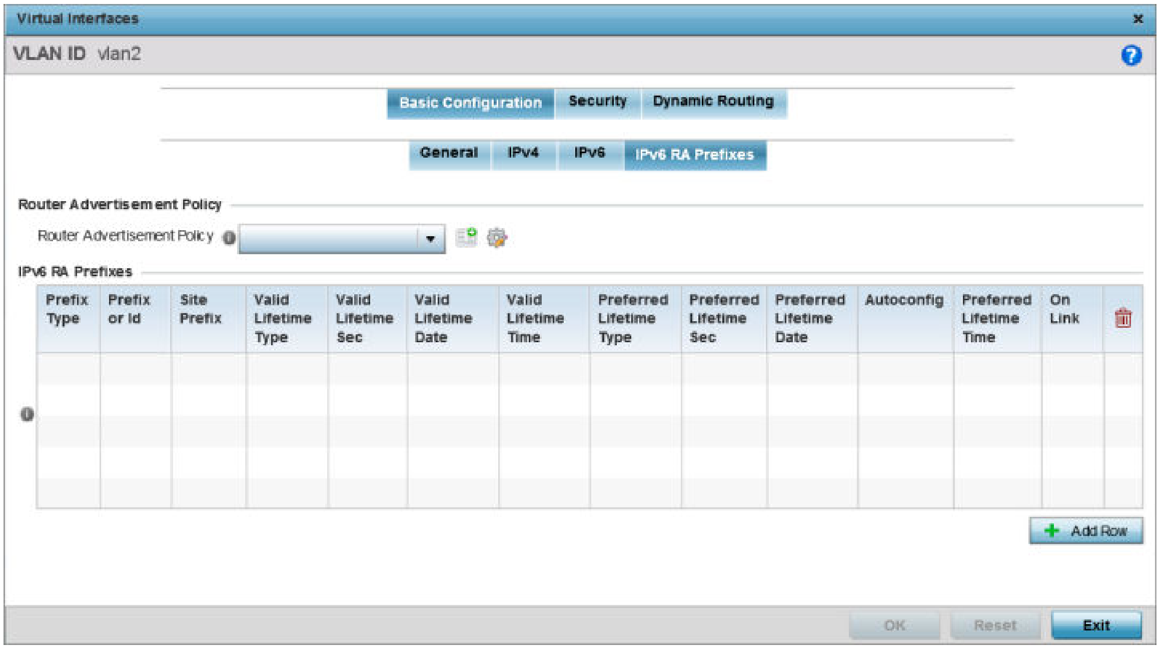


Figure 98: OSPF - VLAN Interface IPv6 RA Prefix Configuration Screen

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 481.

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.

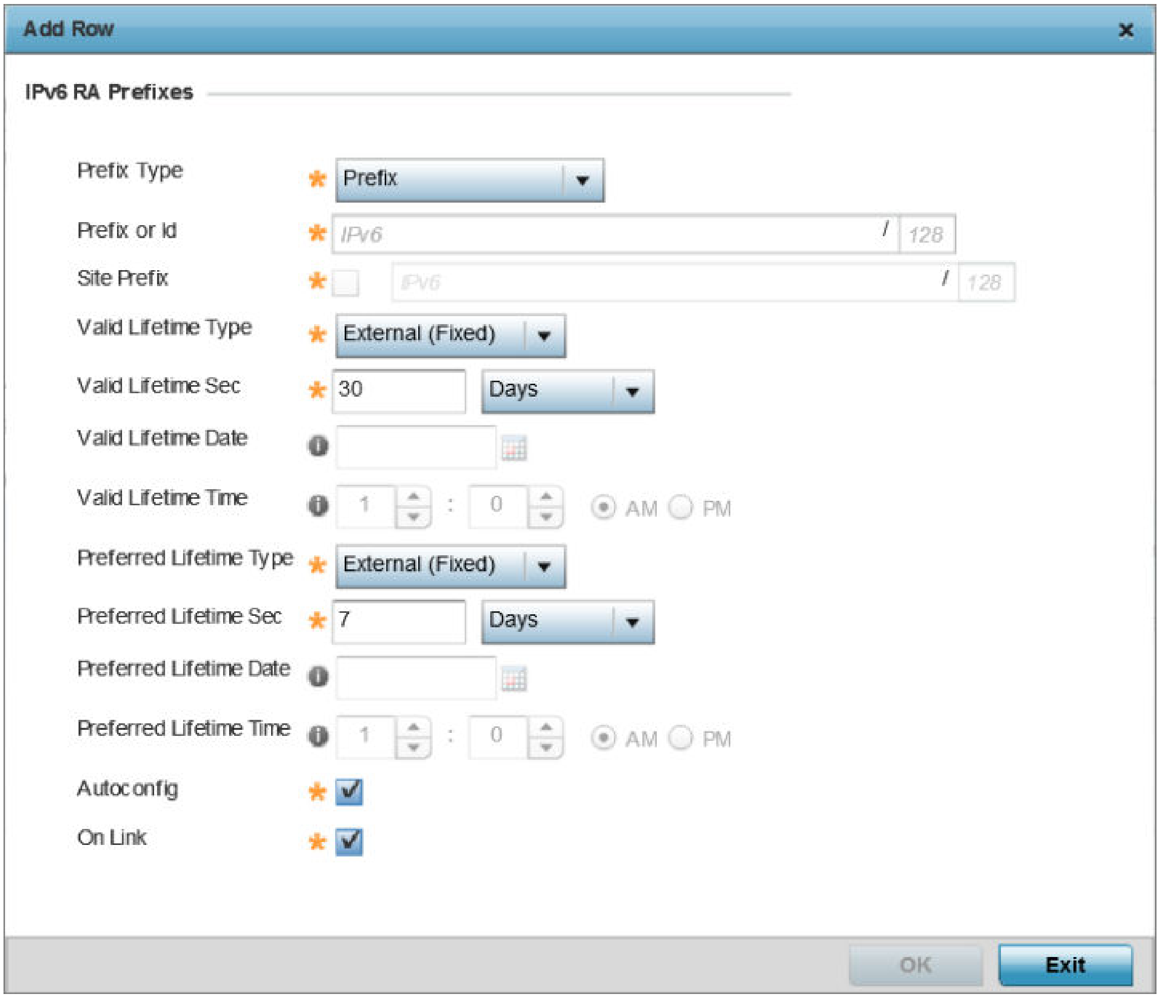


Figure 99: Add/Edit IPv6 RA Prefixes Configuration Screen

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.

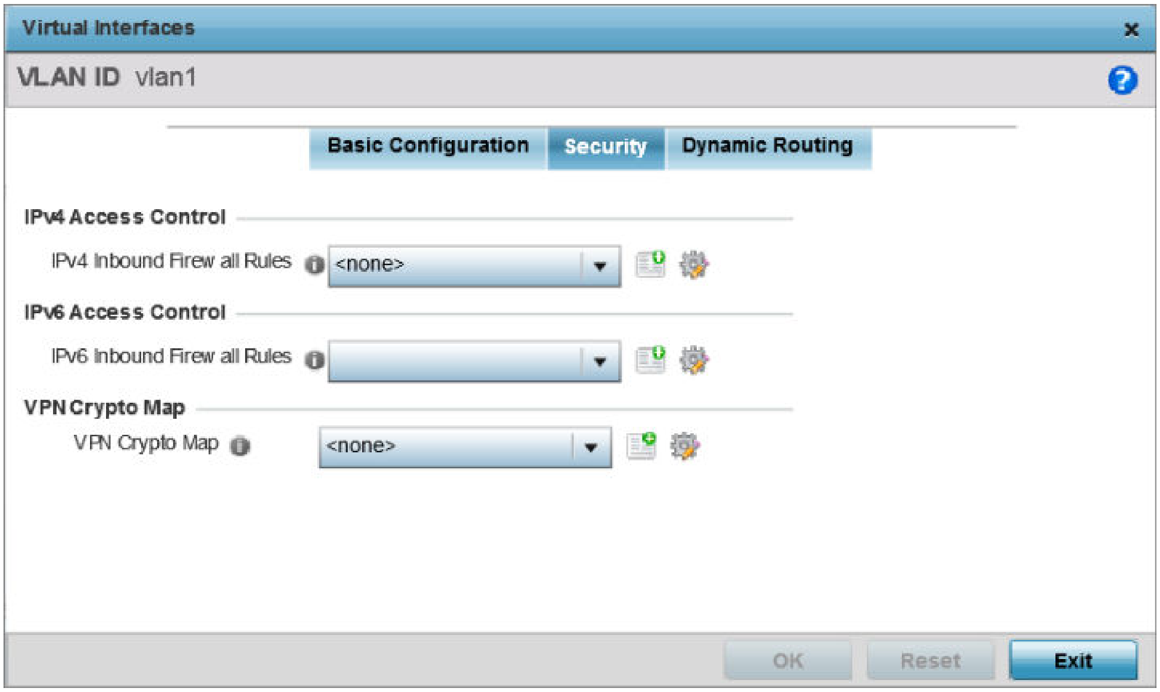


Figure 100: OSPF - VLAN Interface Security Configuration Screen

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 789.

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 789.

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.

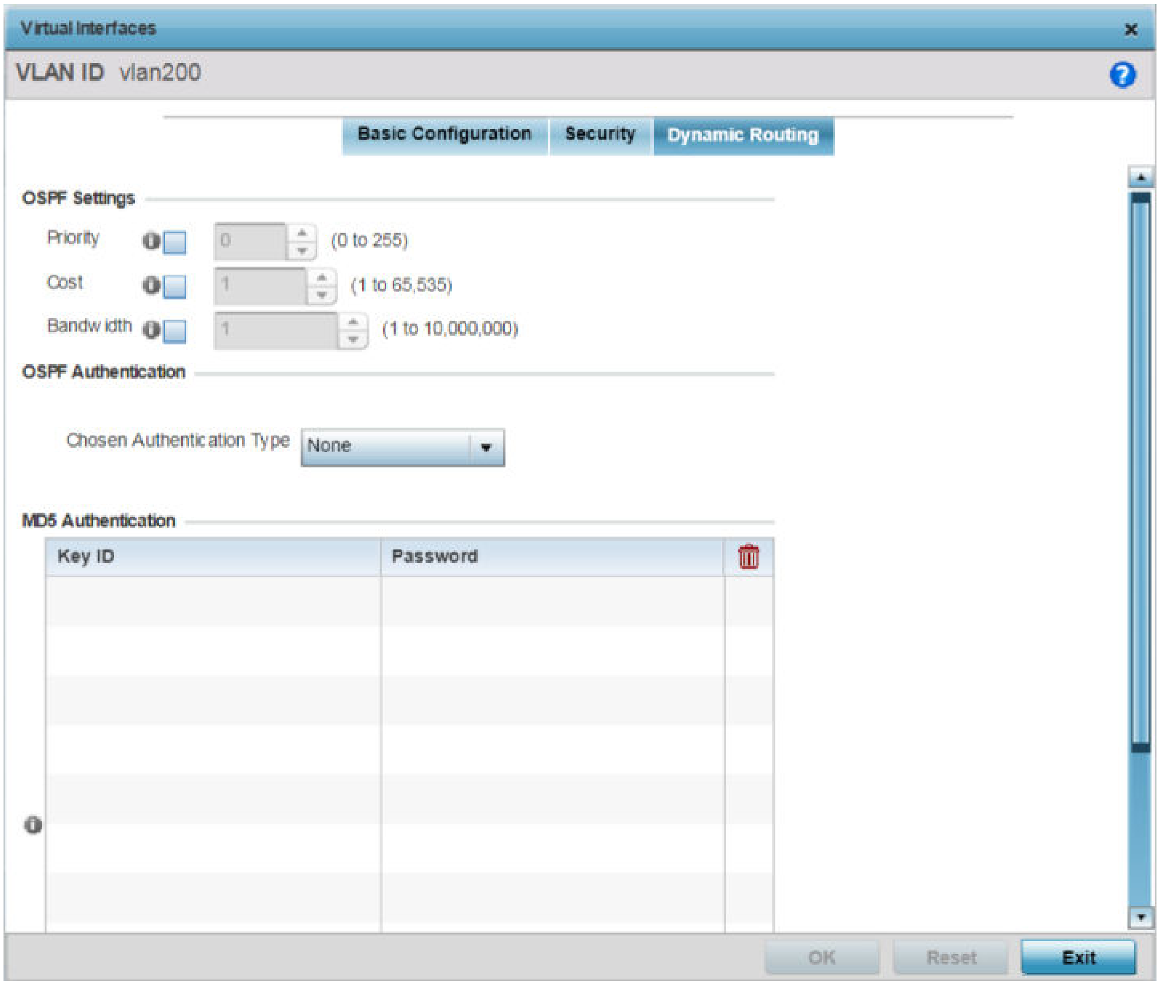


Figure 101: OSPF - VLAN Interface Dynamic Routing Screen

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.

BGP Configuration

BGP *(Border Gateway Protocol)* is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between AS *(Autonomous Systems)* on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An AS is a set of routers under the same administration that use IGP *(Interior Gateway Protocol)* and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed).

To define BGP configuration:

1 Go to **Configuration → Devices**.

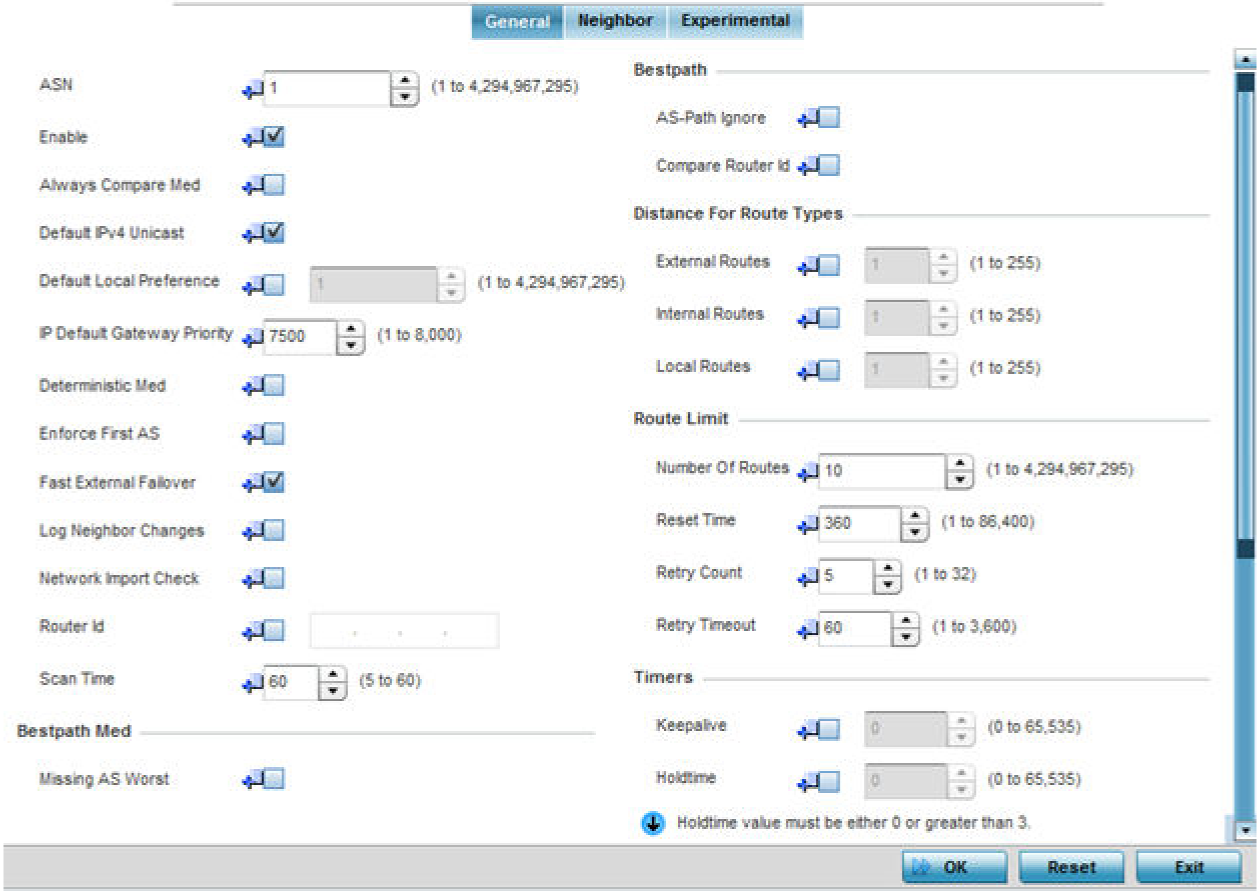
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand the **Network** node and select **BGP**.

The BGP **General** configuration tab displays by default.



ASN: 1 (1 to 4,294,967,295)
Enable: ☑
Always Compare Med: ☐
Default IPv4 Unicast: ☑
Default Local Preference: ☐ 1 (1 to 4,294,967,295)
IP Default Gateway Priority: 7500 (1 to 8,000)
Deterministic Med: ☐
Enforce First AS: ☐
Fast External Failover: ☑
Log Neighbor Changes: ☐
Network Import Check: ☐
Router Id: ☐ . . .
Scan Time: 60 (5 to 60)

Bestpath Med
Missing AS Worst: ☐

Bestpath
AS-Path Ignore: ☐
Compare Router Id: ☐

Distance For Route Types
External Routes: ☐ 1 (1 to 255)
Internal Routes: ☐ 1 (1 to 255)
Local Routes: ☐ 1 (1 to 255)

Route Limit
Number Of Routes: 10 (1 to 4,294,967,295)
Reset Time: 360 (1 to 86,400)
Retry Count: 5 (1 to 32)
Retry Timeout: 60 (1 to 3,600)

Timers
Keepalive: ☐ 0 (0 to 65,535)
Holdtime: ☐ 0 (0 to 65,535)
Holdtime value must be either 0 or greater than 3.

Figure 102: Border Gateway Protocol - General tab

4 Define the following BGP general configuration parameters:

ASN	Define the ASN *(Autonomous System Number)*. ASN is a set of routers under the same administration that use IGP and common metrics to define how to route packets. Select a value from 1 - 4,294,967,295.
Enable	Enable to start BGP on this controller or service platform. BGP is only supported on RFS 4000, NX 95XX and NX 96XX model controllers and service platforms. The default is disabled.
Always Compare MED	MED *(Multi-exit Discriminator)* is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is always selected over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the **`Deterministic MED`** option.
Default IPv4 Unicast	Select this option to enable IPv4 unicast traffic for neighbors. This option is disabled by default.

Default Local Preference	Select this option to enable a local preference for the neighbor. When enabled, set the local preference value (1 - 4,294,967,295).
IP Default Gateway Priority	Set the default priority value for the IP Default Gateway. Set a value from 1 - 8000. The default is 7500.
Deterministic MED	MED is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the **`Always Compare MED`** option.
Enforce First AS	Select this option to deny any updates received from an external neighbor that does not have the neighbor's configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS. This setting is disabled by default.
Fast External Failover	Select this option to immediately reset the BGP session on the interface once the BGP connection goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in Holdtime parameter before bringing down the interface. This setting is enabled by default.
Log Neighbor Changes	Select this option to enable logging of changes in routes to neighbor BGP peers. This enables the logging of only the changes in neighbor routes. All other events must be explicitly turned on using debug commands. This setting is disabled by default.
Network Import Check	Select this option to enable a network import check to ensure consistency in advertisements. This setting is disabled by default.
Router ID	Select this option to manually configure the router ID for this BGP supported controller or service platform. The router ID identifies the device uniquely. When no router ID is specified, the IP address of the interface is considered the router ID. This setting is disabled by default.
Scan Time	Select this option to set the scanning interval for updating BGP routes. This interval is the period between two consecutive scans the BGP device checks for the validity of routes in its routing table. To disable this setting, set the value to Zero (0). The default setting is 60 seconds.

5. Optionally, in the Bestpath Med field, select the **Missing AS Worst** option to treat any path that does not contain a MED value as the least preferable route. This setting is disabled by default.
6. Set the following Bestpath parameters

AS-Path Ignore	Select this option to prevent an AS path from being considered as a criteria for selecting a preferred route. The route selection algorithm uses the AS path as one of the criteria when selecting the best route. When this option is enabled, the AS path is ignored.
Compare Router ID	Select this option to use the router ID as a selection criteria when determining a preferred route. The route selection algorithm uses various criteria when selecting the best route. When this option is enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower route ID is selected over a route with a higher route id.

7. Set or override the following Distance for Route Types.

   The distance parameter is a rating of route trustworthiness. The greater the distance, the lower the trust rating. The distance can be set for each type of route indicating its trust rating:

External Routes	External routes are those routes learned from a neighbor of this BGP device. Set a value from 1 - 255.
Internal Routes	Internal routes are those routes learned from another router within the same AS. Set a value from 1 - 255.
Local Routes	Local routes are those routes being redistributed from other processes within this BGP router. Set a value from 1 - 255.

8 Set or override the following Route Limit parameters:

Number of Routes	Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router. Configure a value from 1 - 4,294,967,295. The default value is 9,216 routes.
Reset Time	Configures the reset time. This is the time limit after which the Retry Count value is set to Zero (0). Set a value from 1- 86,400 seconds.
Retry Count	Configures the number of time the BGP process is reset before it is shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed its number of routes. Set a value from 1 - 32.
Retry Timeout	Configures the time duration in seconds the BGP process is shutdown temporarily before a reset of the process is attempted. Set a value from 1 - 3,600 seconds.

9 Set the following Timers:

Keepalive	Set the duration, in seconds, for the keep alive timer used to maintain connections between BGP neighbors. Set a value from 1 - 65,535 seconds.
Holdtime	Set the time duration, in seconds, for the hold (delay) of packet transmissions.

10 Set the following Aggregate Address fields:

Aggregate addresses are used to minimize the size of the routing tables. Aggregation combines the attributes of several different routes and advertises a single route. This creates an aggregation entry in the BGP routing table if more specific BGP routes are available in the specified address range.

IP Prefix	Enter an IP address and mask used as the aggregate address.
Summary Only	Select this option to advertise the IP Prefix route to the BGP neighbor while suppressing the detailed and more specific routes.
AS Set	Generates AS set path information. Select to enable. When selected, it creates an aggregate entry advertising the path for this route, consisting of all elements contained in all the paths being summarized. Use this parameter to reduce the size of path information by listing the AS number only once, even if it was included in the multiple paths that were aggregated.

11 Set the following Distance for IP Source Prefix fields:

IP Source Prefix	Enter an IP address and mask used as the prefix source address
Admin Distance	Use the spinner control to set the BGP route’s admin distance from 1 - 255.
IP Access List	Provide the IP address used to define the prefix list rule.

12 Configure the following **Network** values:

Network	Configure an IP address to broadcast to neighboring BGP peers. This network can be a single IP address or a range of IP addresses in A.B.C.D/ M format.
Pathlimit	Configure the maximum path limit for this AS. Set a value from 1 - 255 AS hops.
Backdoor	Select this option to indicate to border devices this network is reachable using a backdoor route. A backdoor network is treated the same as a local network, except it is not advertised. This setting is disabled by default.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

13 Configure the following **Route Redistribute** values:

Route Type	Use the drop-down menu to define the route type as either `connected`, `kernal`, `ospf` or `static`.
Metric	Select this option to set a numeric route metric used for route matching and permit designations.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

14 Select the **Neighbor** tab.

The BGP Neighbor **Identifier** screen displays. This screen displays a list of configured BGP neighbor devices identified by their IP address.

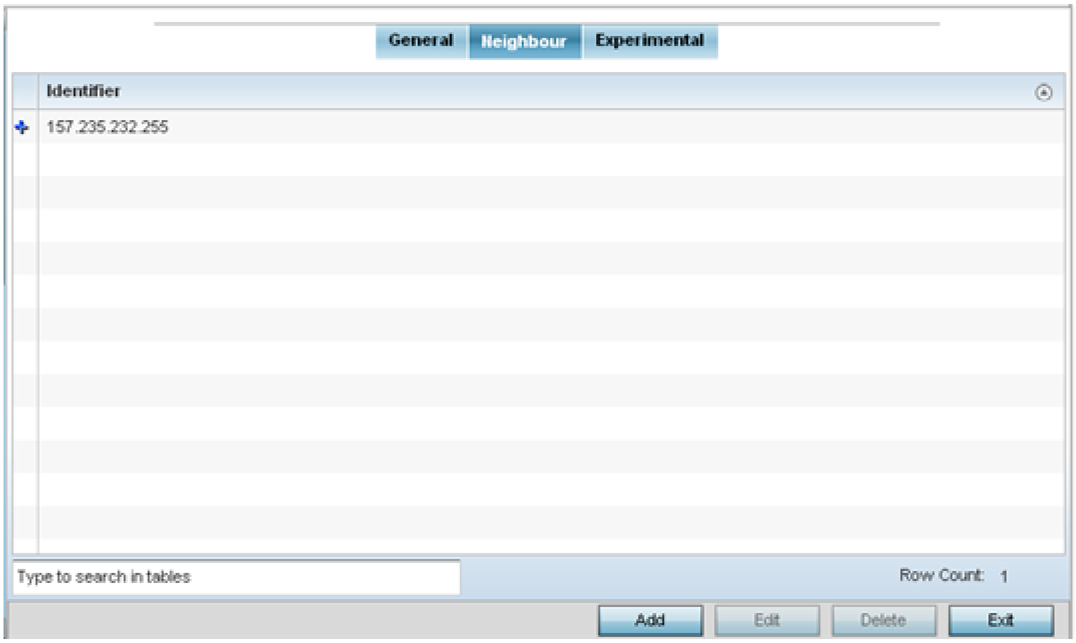
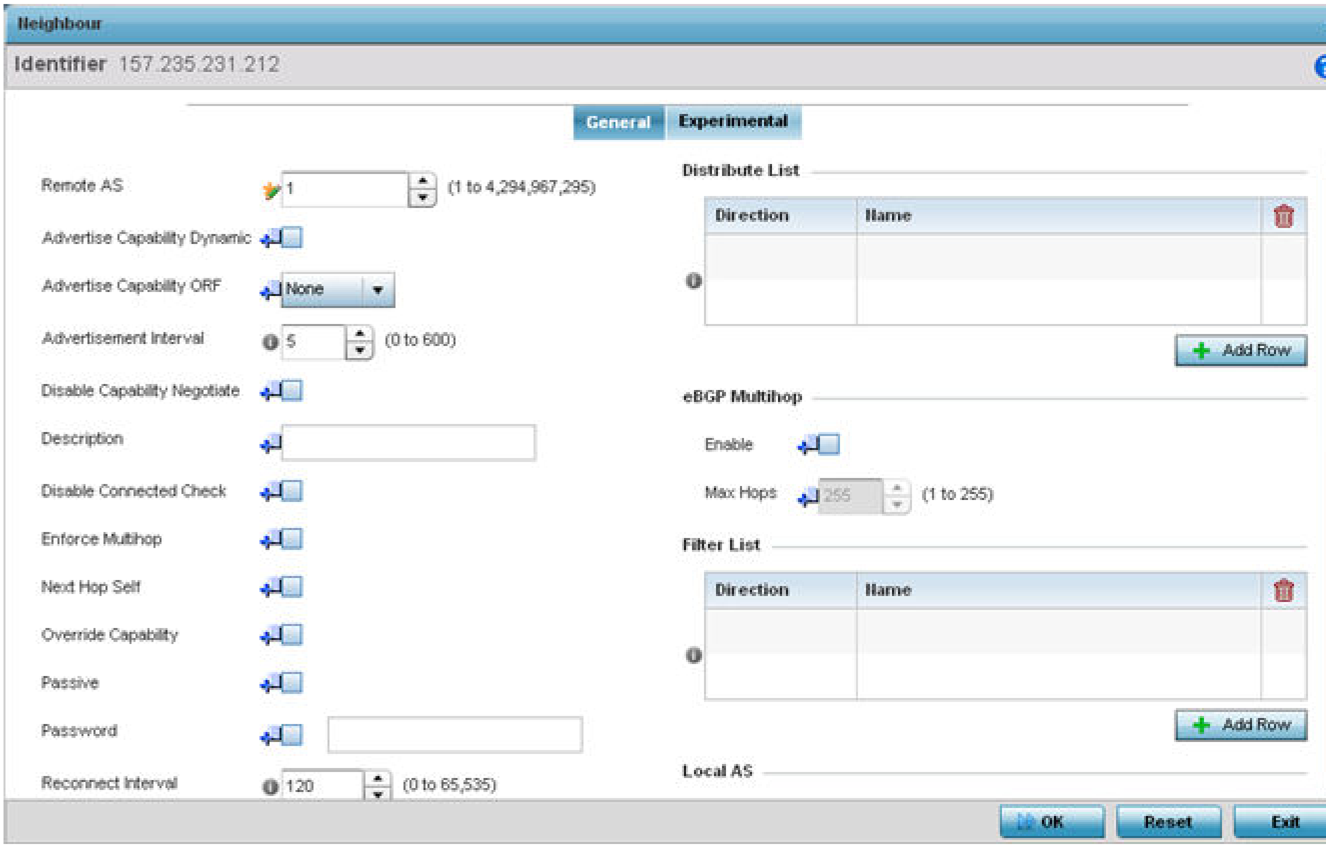


Figure 103: Border Gateway Protocol - Neighbor tab

15 Select **Add** to add a new BGP neighbor configuration or select an existing Identifier and select **Edit** to modify it. The following screen displays with the General tab selected by default.



Neighbour

Identifier 157.235.231.212

Remote AS 1 (1 to 4,294,967,295)

Advertise Capability Dynamic ☐

Advertise Capability ORF None

Advertisement Interval 5 (0 to 600)

Disable Capability Negotiate ☐

Description

Disable Connected Check ☐

Enforce Multihop ☐

Next Hop Self ☐

Override Capability ☐

Passive ☐

Password ☐

Reconnect Interval 120 (0 to 65,535)

Distribute List

Direction	Name

eBGP Multihop

Enable ☐

Max Hops 255 (1 to 255)

Filter List

Direction	Name

Local AS

Figure 104: Border Gateway Protocol - Add/Edit - Neighbor - General Tab

16 If adding a new neighbor, in the Identifier field, provide the BGP neighbor's IP address. Click **Continue**.

17 Configure the following common parameters:

Remote AS	Define the ASN for the neighbor BGP device. ASN is a set of routers under the same administration that use IGP and common metrics to define how to route packets within the AS. Set a value from 1 - 4,294,967,295.
Advertise Capability Dynamic	Select this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This setting is disabled by default.
Advertise Capability ORF	Select this option to enable ORF *(Outbound Router Filtering)* and advertise this capability to peer devices. ORFs send and receive capabilities to lessen the number of updates exchanged between BGP peers. By filtering updates, ORF minimizes update generation and exchange overhead. The local BGP device advertises ORF in the send mode. The peer BGP device receives the ORF capability in receive mode. The two devices exchange updates to maintain the ORF for each router. Only a peer group or an individual BGP router can be configured to be in receive or send mode. A member of a peer group cannot be configured.

Advertisement Interval	Use this option to set the minimum interval between sending BGP router updates. Sending too many router updates creates flapping of routes leading to possible disruptions. Set a minimum interval so that the BGP routing updates are sent after the set interval in seconds. The default is 5 seconds.
Disable Capability Negotiate	Select to disable capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the open messages between peers. This setting id disabled by default.
Description	Provide a 80 character maximum description for this BGP neighbor device.
Disable Connected Check	If utilizing loopback interfaces to connect single-hop BGP peers, enable this option before establishing a the BGP peering session. This setting is disabled by default.
Enforce Multihop	A multihop route is a route to external peers on indirectly connected networks. Select to enforce neighbors to perform multi-hop check. This setting is disabled by default.
Next Hop Self	Select to enable Next Hop Self. Use this to configure this device as the next hop for a BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor. This setting is disabled by default.
Override Capability	Select this to enable the ability to override capability negotiation result. This setting is disabled by default.
Passive	Select this option to set this BGP neighbor as passive. When a neighbor is set as passive, the local device should not attempt to open a connection to this device. This setting is disabled by default.
Password	Select this option, and set a password for this BGP neighbor. This will make all sessions with this neighbor password protected.
Reconnect Interval	Set a reconnection interval for peer BGP devices from 0 - 65,535 seconds. The default setting is 120 seconds.
Send Community	Select this option to ensure the community attribute is sent to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.
Shutdown	Select this option to administratively shutdown this BGP neighbor. This setting is disabled by default.
Soft Reconfiguration Inbound	Select this option to store updates for inbound soft reconfiguration. Soft reconfiguration can be used in lieu of BGP route refresh capability. Selecting this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device. When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.
Update Source	Select this option to allow internal BGP sessions to use any operational interface for TCP connections. Use Update Source in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections. This setting is disabled by default.

Unsuppress Map	Enable this option to selectively advertise more precise routing information to this neighbor. Use this in conjunction with the `Route Aggregate` option. The route aggregate command creates a route map with a IP/mask address that consolidates the subnets under it. This enables a reduction in number of route maps on the BGP device to one entry that encompasses all the different subnets. Use `Unsuppress Map` to selectively allow/deny a subnet or a set of subnets. Use the **Create** icon to create a new route map. Use the **Edit** icon to edit an existing route map list after selecting it.
Weight	Select to set the weight of all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

18 Configure or set the following Default Originate parameters. Default originate is used by the local BGP router to send the default route 0.0.0.0 to its neighbor for use as a default route.

Enable	Select to enable Default Originate on this BGP neighbor. This setting is disabled by default.
Route Map	Use the drop-down menu to select a route map (enhanced packet filter) to use as the Default Originate route.

19 Configure or set the following Route Map parameters. This configures how route maps are applied for this BGP neighbor.

Direction	Use the drop-down menu to configure the direction on which the selected route map is applied. Select one from `in`, `out`, `export` or `import`.
Route Map	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the **Create** icon to create a new route map. Use the **Edit** icon to edit an existing route map after selecting it.

20 Configure or set the following Distribute List parameters. Up to 2 distribute list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP access list is applied. Select either in or out.
Name	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the **Create** icon to create a new IP Access.

21 Configure or set the following eBGP Multihop parameters. This configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.

Enable	Select to enable eBGP Multihop on this BGP neighbor.
Max Hops	Set the maximum number of hops between eBGP neighbors not connected directly. Select a value from 1 - 255.

22 Configure or set the following Filter List parameters. Up to 2 filter list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected AS Path list is applied. Select either `in` or `out`.
Name	Use the drop-down menu to select the AS Path list to use with this BGP neighbor. Use the **Create** icon to create a new AS Path list. Use the **Edit** icon to edit an existing AS Path list after selecting it.

23 Configure or set the following Local AS parameters:

This is an experimental feature and its actual operation may be unpredictable.

AS Number	Specify the local Autonomous System (AS) number. Select from 1 - 4,294,967,295.
No Prepend	Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers.

24 Configure or set the following Maximum Prefix value. This configures the maximum number of prefix that can be received from a BGP neighbor.

Prefix Limit	Sets the maximum number of prefix that can be received from a BGP neighbor. Select from 1 - 4,294,967,295. Once this threshold is reached, the BGP peer connection is reset.
Threshold Percent	Sets the threshold limit for generating a log message. When this percent of the Prefix Limit is reached, a log entry is generated. For example, if the Prefix Limit is set to 100 and Threshold Percent is set to 65, then after receiving 65 prefixes, a log entry is created.
Restart Limit	Sets the number of times a reset BGP peer connection is restarted. Select a value from 1 - 65535.
Warning Only	Select to enable. When the number of prefixes specified in Prefix Limit field is exceeded, the connection is reset. However, when this option is enabled, the connection is not reset and an event is generated instead. This setting is disabled by default.

25 Configure or set the following Prefix List parameters. Up to 2 prefix list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP prefix list is applied. Select either **`in`** or **`out`**.
Name	Use the drop-down menu to select the IP prefix list to use with this BGP neighbor. Use the **Create** icon to create a new IP prefix list or select the **Edit** icon to edit an existing IP prefix list after selecting it.

26 Set or override the following Timers for this BGP neighbor.

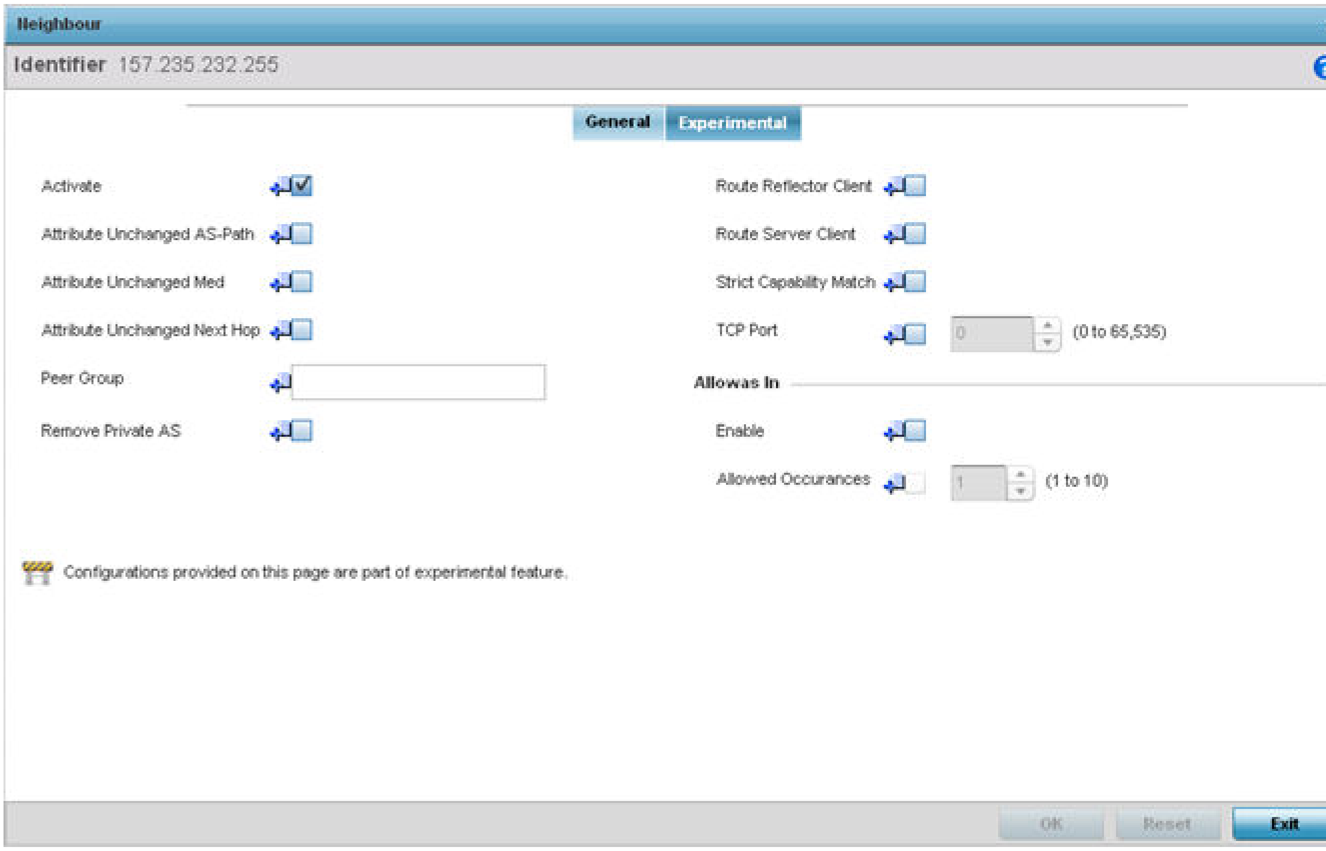
Keepalive	Set the time duration in seconds for keepalive. The keep alive timer is used to maintain connections between BGP neighbors. Set a value from 1 - 65,535 seconds.
Holdtime	Set the time duration in seconds for the hold time.

27 Select **OK** to save the changes and overrides.

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

28 Select the **Experimental** tab.

This is an experimental feature and its actual operation may be unpredictable.



Neighbour
Identifier 157.235.232.255
General
Experimental
Activate ☑
Attribute Unchanged AS-Path ☐
Attribute Unchanged Med ☐
Attribute Unchanged Next Hop ☐
Peer Group
Remove Private AS ☐
Route Reflector Client ☐
Route Server Client ☐
Strict Capability Match ☐
TCP Port ☐ 0 (0 to 65,535)
Allowas In
Enable ☐
Allowed Occurances 1 (1 to 10)
Configurations provided on this page are part of experimental feature.
OK
Reset
Exit

Figure 105: Border Gateway Protocol - Add/Edit - Neighbor - Experimental Tab

29 Set the following Experimental BGP neighbor parameters:

Activate	Enable an address family for this neighbor. This setting is enabled by default.
Attribute Unchanged AS-Path	Select to enable propagating AS path BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.
Attribute Unchanged Med	Select to enable propagating MED BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.
Attribute Unchanged Next Hop	Select to enable propagating the next hop BGP attribute value unchanged to this neighbor BGP device. This setting is enabled by default.
Peer Group	Set the peer group for this BGP neighbor device. Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists. The peer group can be configured as a single entity. Any changes made to the peer group is propagated to all members.

Remove Private AS	Select this option to remove the private AS number from outbound updates. Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.
Route Reflector Client	Select this option to enable this BGP neighbor as a route reflector client for the local router. Route reflectors control large numbers of iBGP peering. Using route reflection, the number of iBGP peers is reduced. This option configures the local BGP device as a route reflector and the neighbor as its route reflector client. This setting is disabled by default.
Route Server Client	Select this option to enable this neighbor BGP device to act as a route server client. This setting is disabled by default.
Strict Capability Match	Select this option to enable a strict capability match before allowing a neighbor BGP peer to open a connection. When capabilities do not match, the BGP connection is closed. This setting is disabled by default.
TCP Port	Select to enable configuration of non-standard BGP port for this BGP neighbor. By default the BGP port number is 179. To configure a non standard port for this BGP neighbor, use the control to set the port number. Select a value from 1 - 65,535.

30 Configure or set the following Allowas In parameters.

This configures the PE *(Provider Edge)* routers to allow the re-advertisement of all prefixes containing duplicate ASN. This creates a pair of VRF *(VPN Routing/Forwarding)* instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the CE *(Customer Edge)* routers and re-advertises them to all PE routers in the configuration.

Enable	Select this option to enable re-advertisement of all prefixes containing duplicate ASNs.
Allowed Occurrences	Set the maximum number of times an ASN is advertised. Select a value in the rage 1 - 10.

31 Select **OK** to save the changes and overrides.

Select **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

32 Select the **Experimental** tab from the BGP main screen.

This is an experimental feature and its actual operation may be unpredictable.

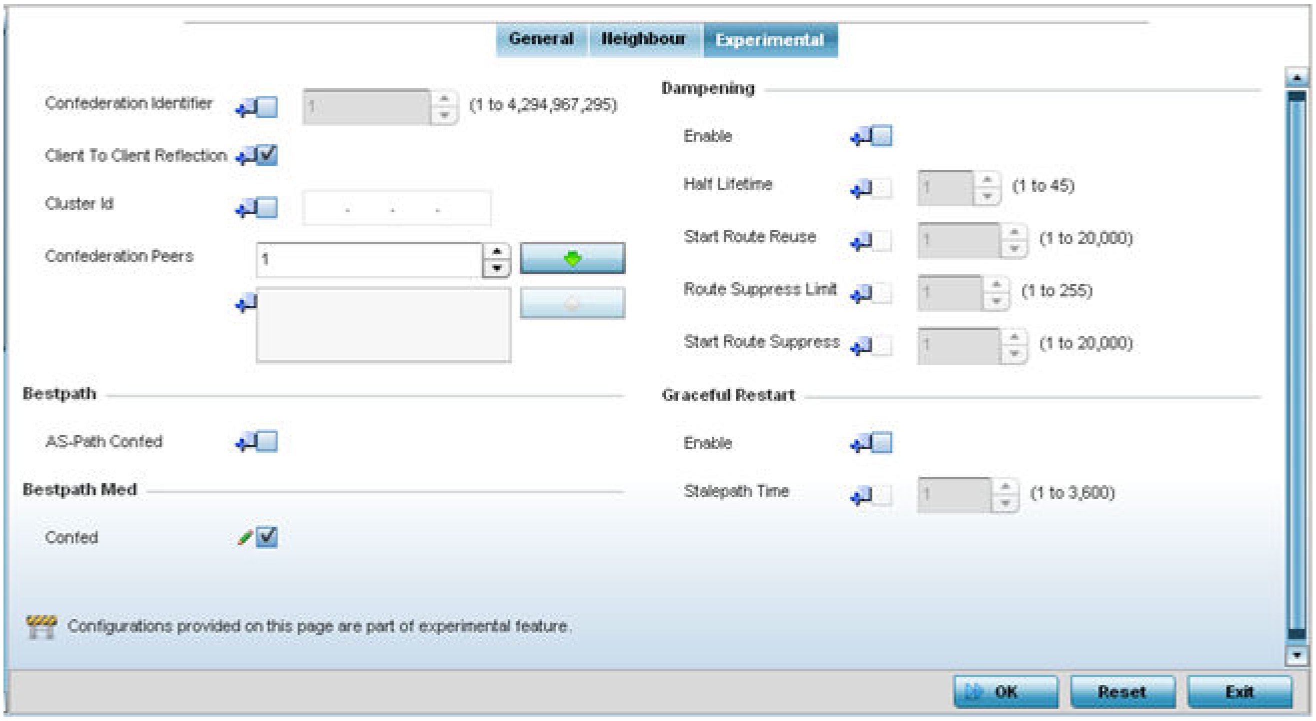


Figure 106: Border Gateway Protocol - Experimental tab

33 Set the following Experimental BGP features:

Confederation Identifier	Enable and set a confederation identifier to allow an AS to be divided into several ASs. This confederation is visible to external routers as a single AS. Select a value from 1 - 4,294,967,295.
Client to Client Reflection	Select to enable client-to-client route reflection. Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. The default is enabled.
Cluster ID	Select to enable and set a Cluster ID if the BGP cluster has more than one route-reflectors. A cluster generally consists of a single router reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase the redundancy, a cluster might have more than one route-reflectors configured. In this case, all route-reflectors in the cluster are identified by the Cluster ID. Select a value from 1 - 4,294,967,295.
Confederation Peers	Use this spinner to select the confederation members. Once selected, select the Down Arrow button next to this control to add the AS as a confederation member. Multiple AS configurations can be added to the list of confederation members. To remove an AS as a confederation member, select the AS from the list and select the Up Arrow button next to the list.

34 Configure or set the following **Bestpath** parameter:

AS-Path Confed	Select this option to allow the comparison of the confederation AS path length when selecting the best route. This indicates the AS confederation path length must be used, if available, in the BGP path when deciding the best path.

35 Configure or set the following **Bestpath Med** parameter:

Confed	Select to enable. Use this option to allow comparing MED when selecting the best route when learned from confederation peers. This indicates that MED must be used, when available, in the BGP best path when deciding the best path between routes from different confederation peers.

36 Configure or set the following **Dampening** parameters

Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the `Route Suppress Limit` value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in Half Lifetime occurs. Once the penalty becomes lower than the value specified in Start Route Reuse, the advertisement of the route is un-suppressed.

Enable	Select to enable dampening on advertised routes. When this option is selected, other configuration fields in this Dampening field are enabled. This setting is disabled by default.
Half Lifetime	Select to enable and configure the half lifetime value. A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Set a value from 1 - 45 in minutes. The default is 1 second.
Start Route Reuse	Select to enable and configure the route reuse value. When the penalty for a suppressed route decays below the value specified in Start Route Reuse field, the route is un-suppressed. Set a value from 1 - 20000.
Route Suppress Limit	Select to enable and configure the maximum duration in minutes a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Set a value from 1 - 255 minutes.
Start Route Suppress	Select to enable and configure the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified in Route Suppress Limit, the route is suppressed. Set a value from 1 - 20000.

37 Configure or set the **Graceful Restart** parameters. This provides a graceful restart mechanism for a BGP session reset in which the BGP daemon is not restarted, so that any changes in network configuration that caused the BGP reset does not affect packet forwarding.

Enable	Select to enable a graceful restart on this BGP router. This section is disabled by default.
Stalepath Time	Configure the maximum time to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor is preserved. All stale paths, unless reinstated by the neighbor after reestablishment, are deleted at the expiry of this timer value. Set a value from 1 - 3600 seconds.

38 Click **OK** to save the changes and overrides.

Click **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

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

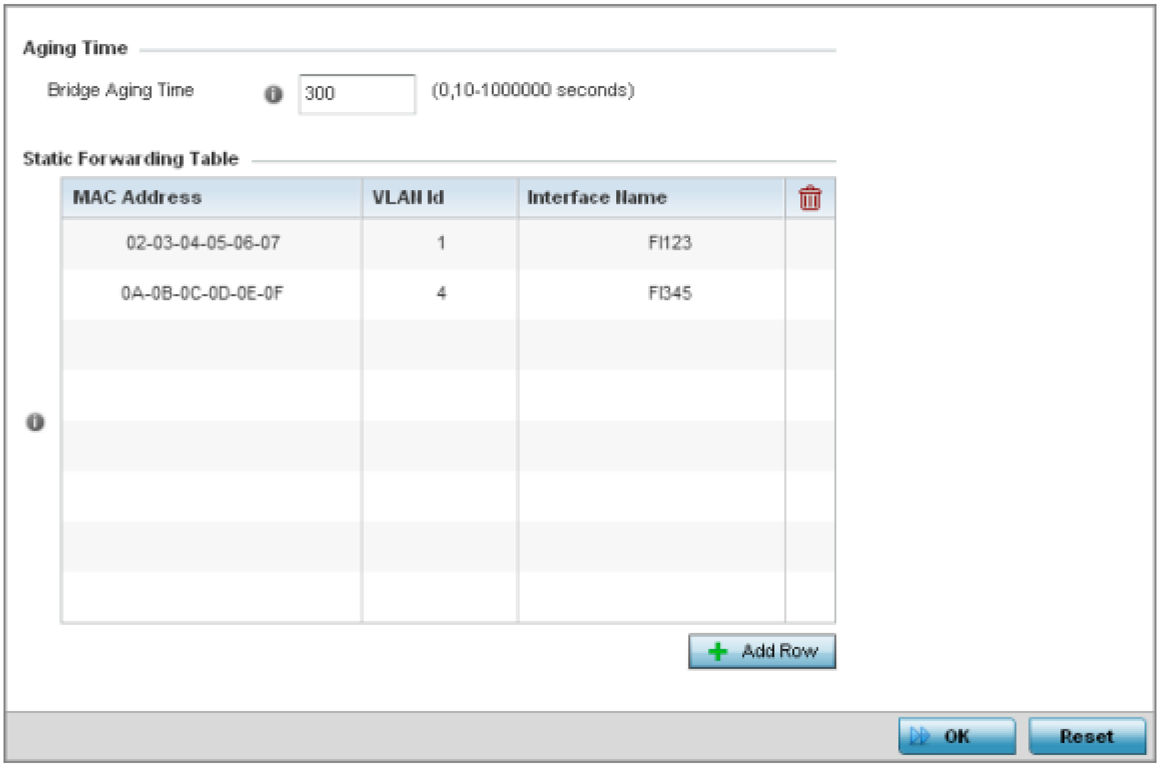
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand **Profile Overrides** → **Network** and select **Forwarding Database**.

The Forwarding Database configuration screen displays.



Aging Time

Bridge Aging Time: 300 (0,10-1000000 seconds)

Static Forwarding Table

MAC Address	VLAN Id	Interface Name
02-03-04-05-06-07	1	FI123
0A-0B-0C-0D-0E-0F	4	FI345

Figure 107: Network - Forwarding Database 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 Use the **+Add Row** button to create a new row within the Static Forwarding Table.

6 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).

7 Define the target **VLAN ID** if the destination MAC is on a different network segment.

8 Provide an **Interface Name** used as the target destination interface for the target MAC address.

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

Click **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.

To override an device profile's Bridge VLAN configuration:

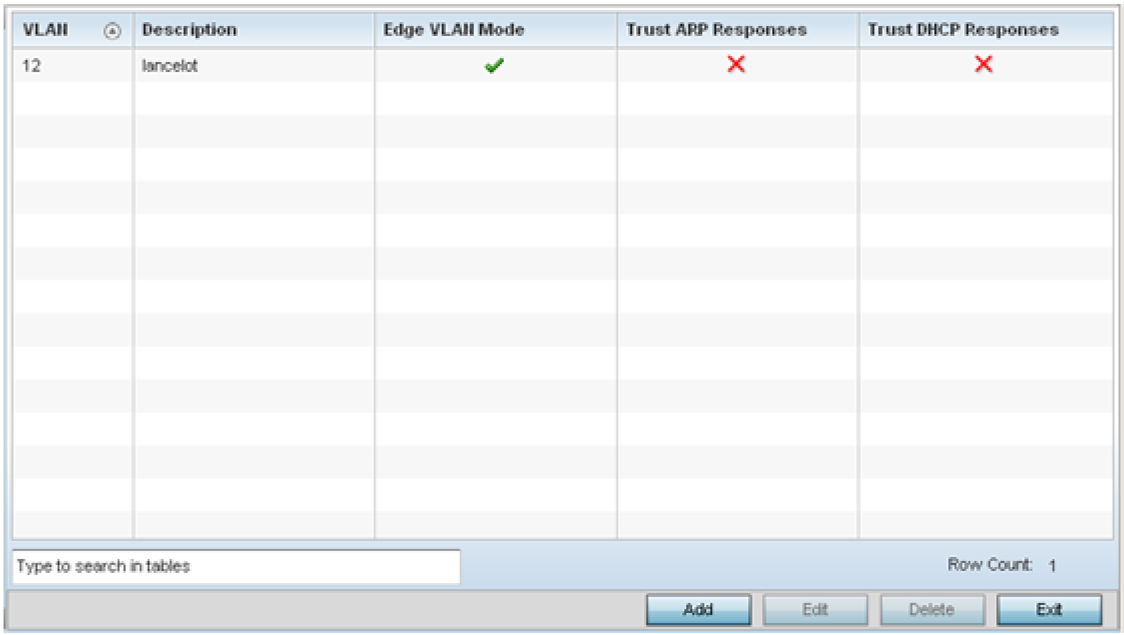
1 Go to **Configuration** → **Devices**.

The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand the **Network** node and select **Bridge VLAN**. The Bridge VLAN Main screen displays. This screen displays existing Bridge VLAN configurations.



VLAN	Description	Edge VLAN Mode	Trust ARP Responses	Trust DHCP Responses
12	lancelot	✓	✗	✗

Row Count: 1

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.

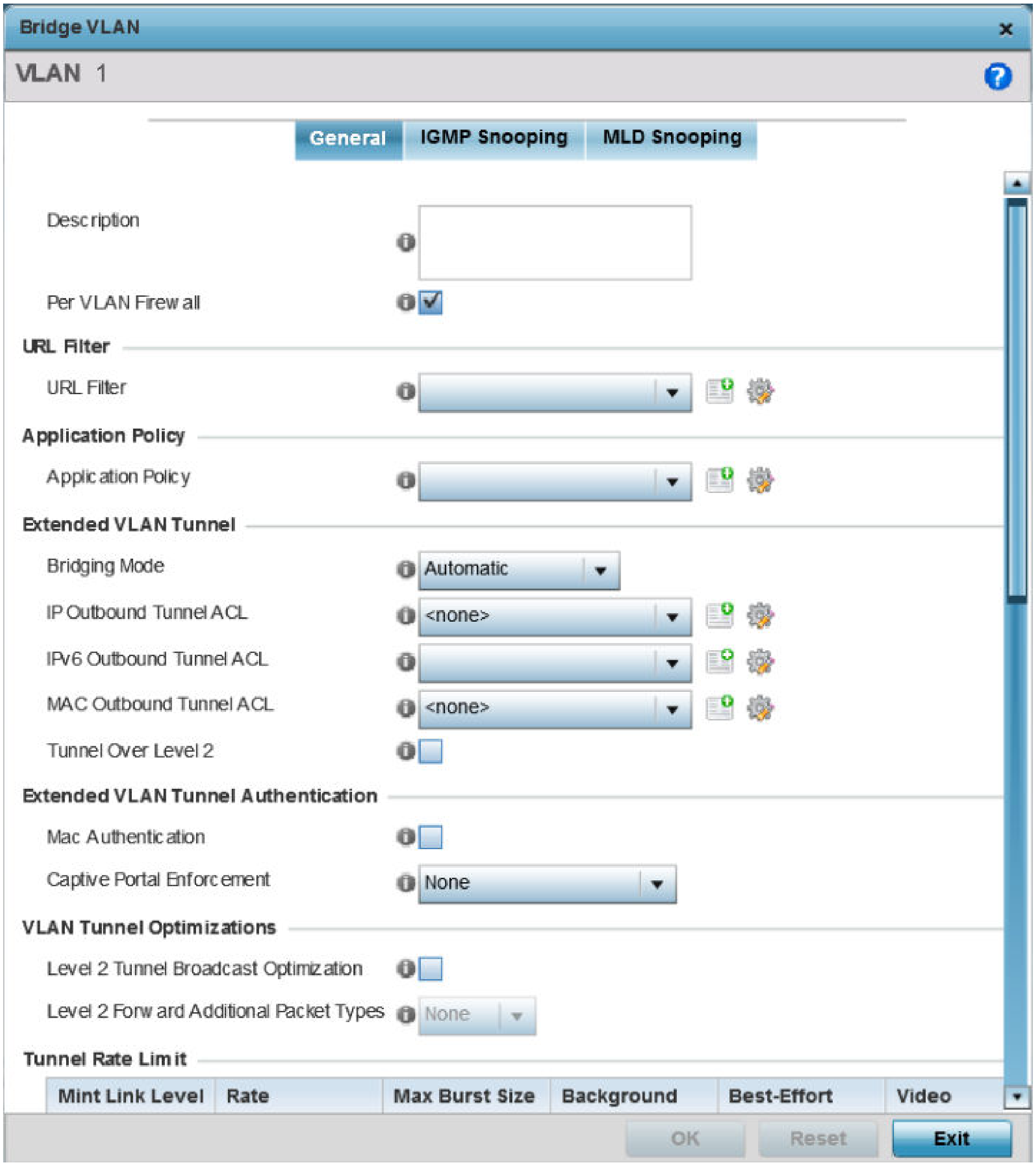
5 Clcik **Add** to define a new bridge VLAN configuration, **Edit** to modify an existing bridge VLAN configuration or **Delete** to remove a VLAN configuration.

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.



Description

Per VLAN Firewall ☑

URL Filter

URL Filter

Application Policy

Application Policy

Extended VLAN Tunnel

Bridging Mode: Automatic

IP Outbound Tunnel ACL: <none>

IPv6 Outbound Tunnel ACL

MAC Outbound Tunnel ACL: <none>

Tunnel Over Level 2 ☐

Extended VLAN Tunnel Authentication

Mac Authentication ☐

Captive Portal Enforcement: None

VLAN Tunnel Optimizations

Level 2 Tunnel Broadcast Optimization ☐

Level 2 Forward Additional Packet Types: None

Tunnel Rate Limit

Mint Link Level	Rate	Max Burst Size	Background	Best-Effort	Video

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. *Automatic*: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN. *Local*: Select Local to use local bridging mode for bridging traffic on the VLAN. *Tunnel*: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. *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: **None** – No Authentication mode used. This is the default setting. **Authentication Failure** – Configures MAC Authentication as the primary and Captive-Portal Authentication as the fall-back authentication mode. **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.

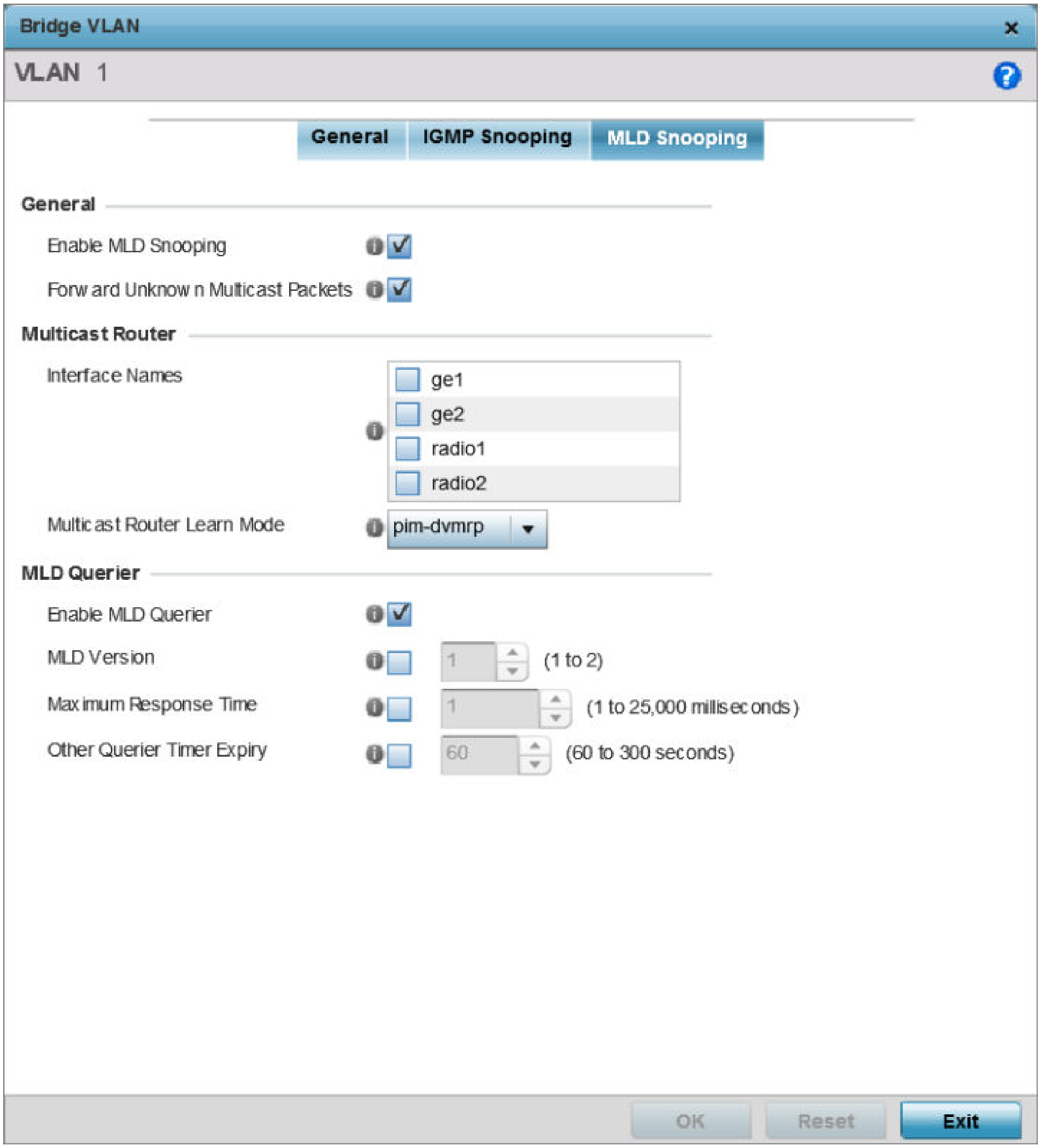
MLD Snooping

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.



Bridge VLAN

VLAN 1

General | IGMP Snooping | MLD Snooping

General

Enable MLD Snooping ☑

Forward Unknown Multicast Packets ☑

Multicast Router

Interface Names ☐ ge1 ☐ ge2 ☐ radio1 ☐ radio2

Multicast Router Learn Mode pim-dvmrp

MLD Querier

Enable MLD Querier ☑

MLD Version ☐ 1 (1 to 2)

Maximum Response Time ☐ 1 (1 to 25,000 milliseconds)

Other Querier Timer Expiry ☐ 60 (60 to 300 seconds)

Figure 108: 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.

CDP Configuration

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 a profile's CDP configurations:

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

The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand **Profile Overrides** → **Network** and select **CDP**.

The CDP configuration screen displays.

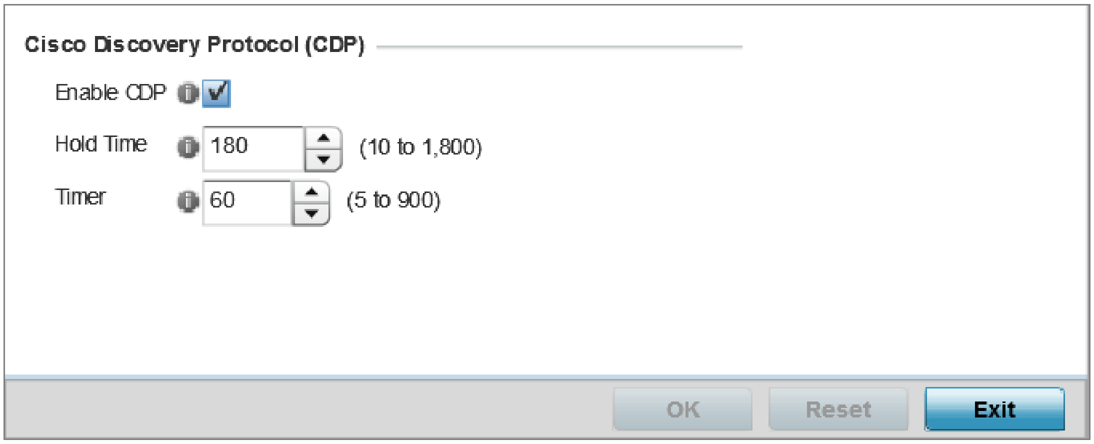


Figure 109: Profile Overrides - CDP Configuration Screen

4 Configure 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. Note: This option 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. Note: The default setting is 1,800 seconds.
Timer	Use the spinner control to set the interval for CDP packet transmissions. Note: The default setting is 60 seconds.

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

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

LLDP 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 override/define LLDP configurations:

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

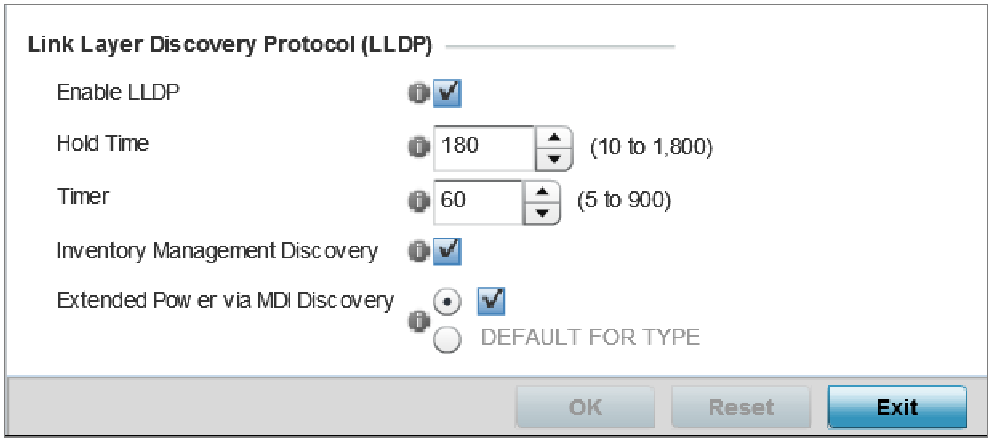
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand **Profile Overrides** → **Network** and select **LLDP**.

The LLDP configuration screen displays.



Link Layer Discovery Protocol (LLDP)

Enable LLDP ☑

Hold Time 180 (10 to 1,800)

Timer 60 (5 to 900)

Inventory Management Discovery ☑

Extended Power via MDI Discovery ● ☑ ○ DEFAULT FOR TYPE

Figure 110: Profile Overrides - LLDP Configuration Screen

4 Set the following LLDP parameters:

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

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

Miscellaneous Network Configurations

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

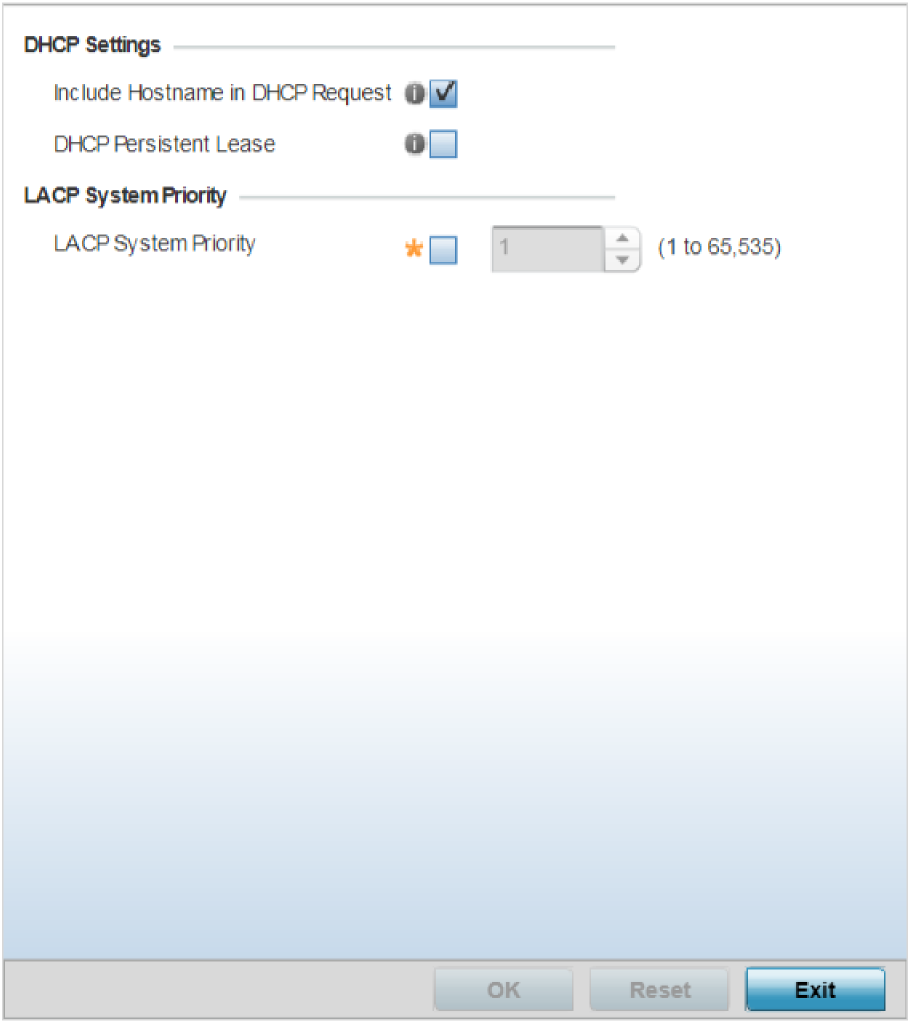
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a device from the list displayed.

The selected device's configuration screen displays.

3 Expand **Profile Overrides** → **Network** and select **Miscellaneous**.

The Miscellaneous configuration screen displays.



DHCP Settings

Include Hostname in DHCP Request ☑

DHCP Persistent Lease ☐

LACP System Priority

LACP System Priority * ☐ 1 (1 to 65,535)

4 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.

5 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.

6 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.

7 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.

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**.

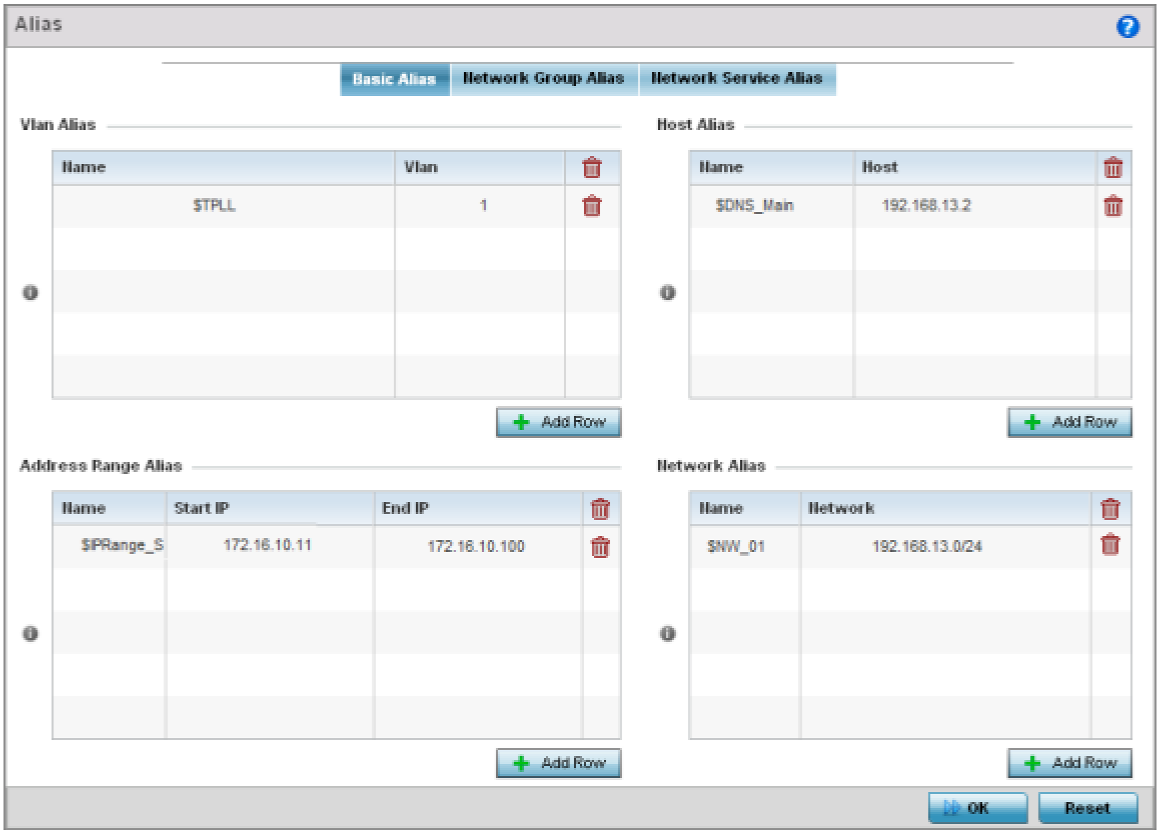
The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a target device.

The selected device's configuration screen displays.

3 Expand **Profile Overrides** → **Network** and select **Alias**.

The Basic Alias screen displays.



Vlan Alias

Name	Vlan
$TPLL	1

Host Alias

Name	Host
$DNS_Main	192.168.13.2

Address Range Alias

Name	Start IP	End IP
$IPRange_S	172.16.10.11	172.16.10.100

Network Alias

Name	Network
$NW_01	192.168.13.0/24

Figure 111: 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. 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

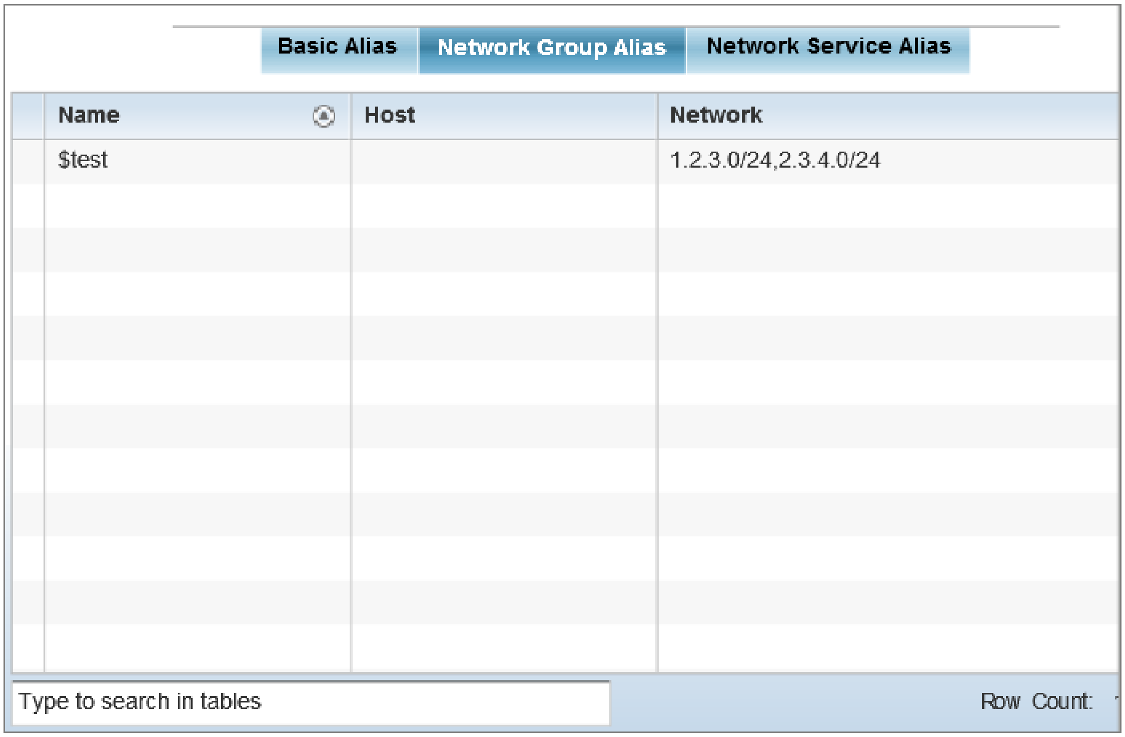
A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address,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



Name	Host	Network
$test		1.2.3.0/24,2.3.4.0/24

Figure 112: 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.

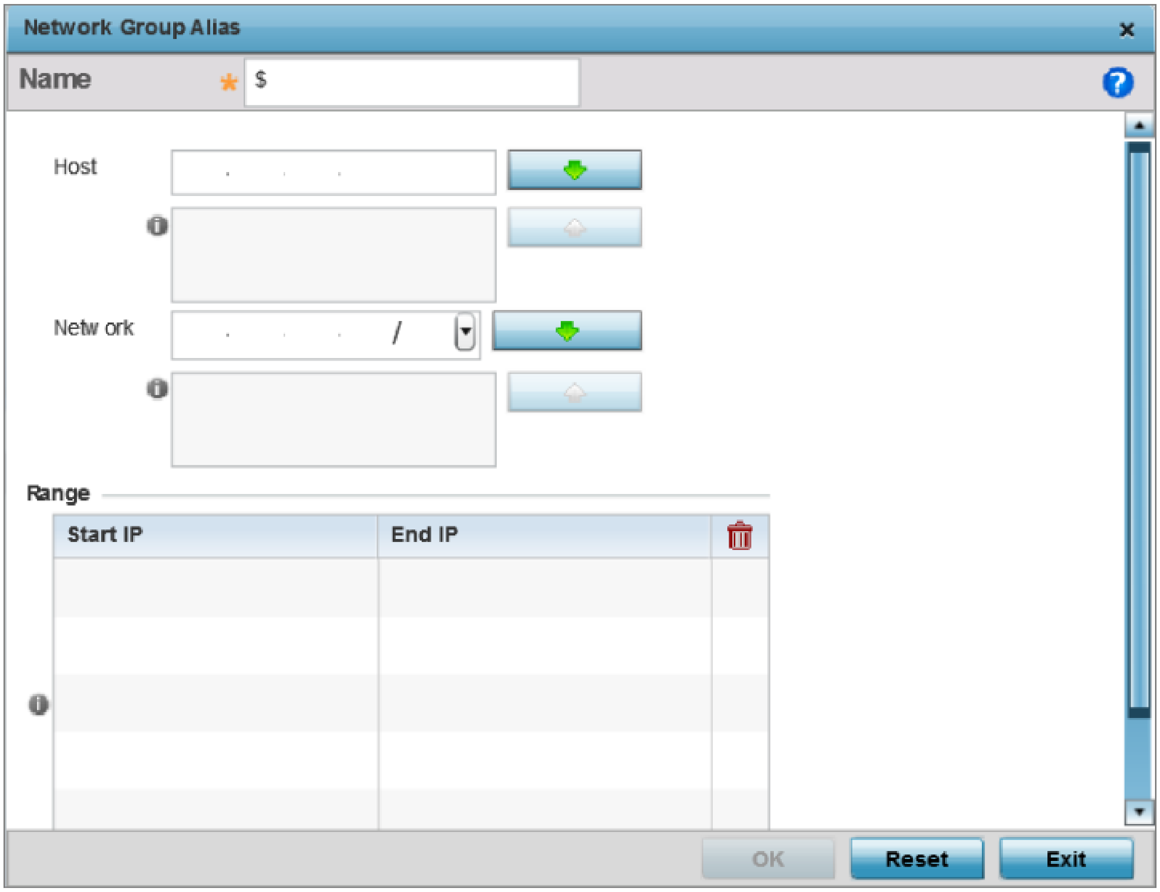


Figure 113: Network Alias - Network Group Alias Add Screen

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.

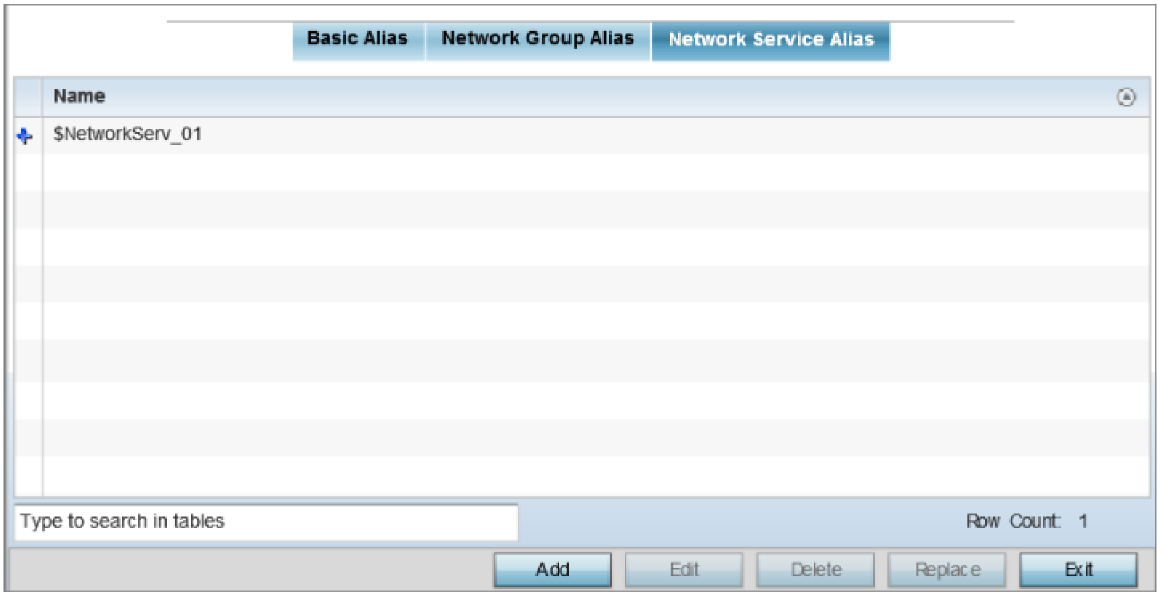


Figure 114: Network Alias - Network Service Alias Screen

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.

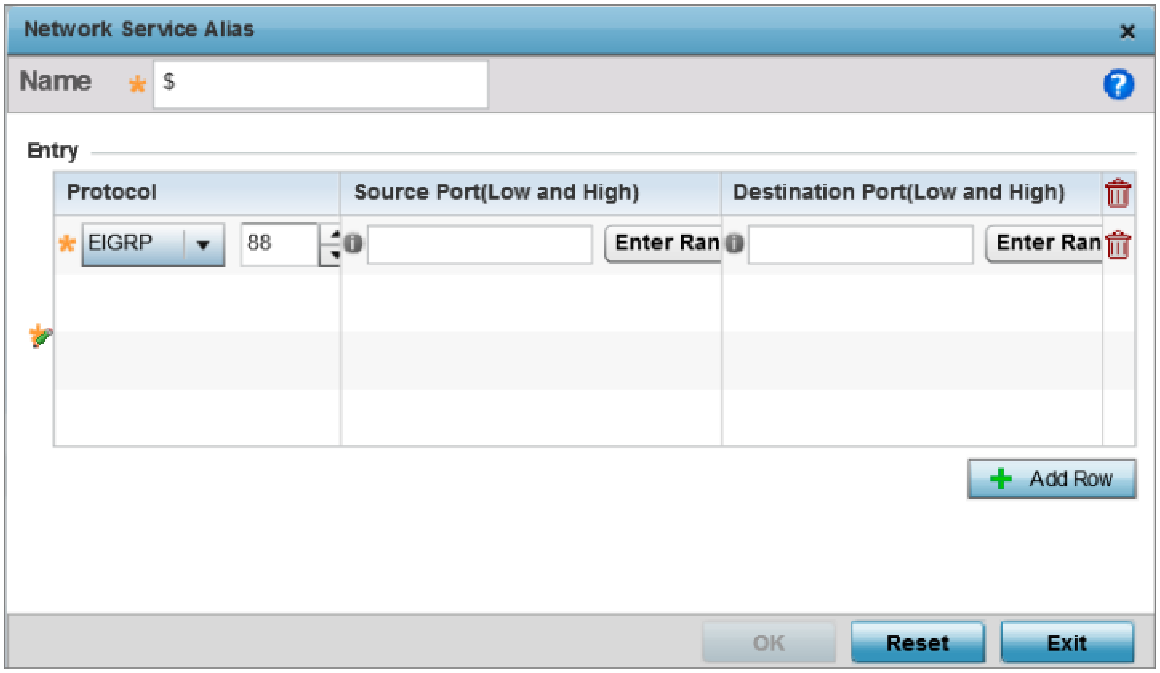


Figure 115: Network Alias - Network Service Alias Add screen

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*. 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*. 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.

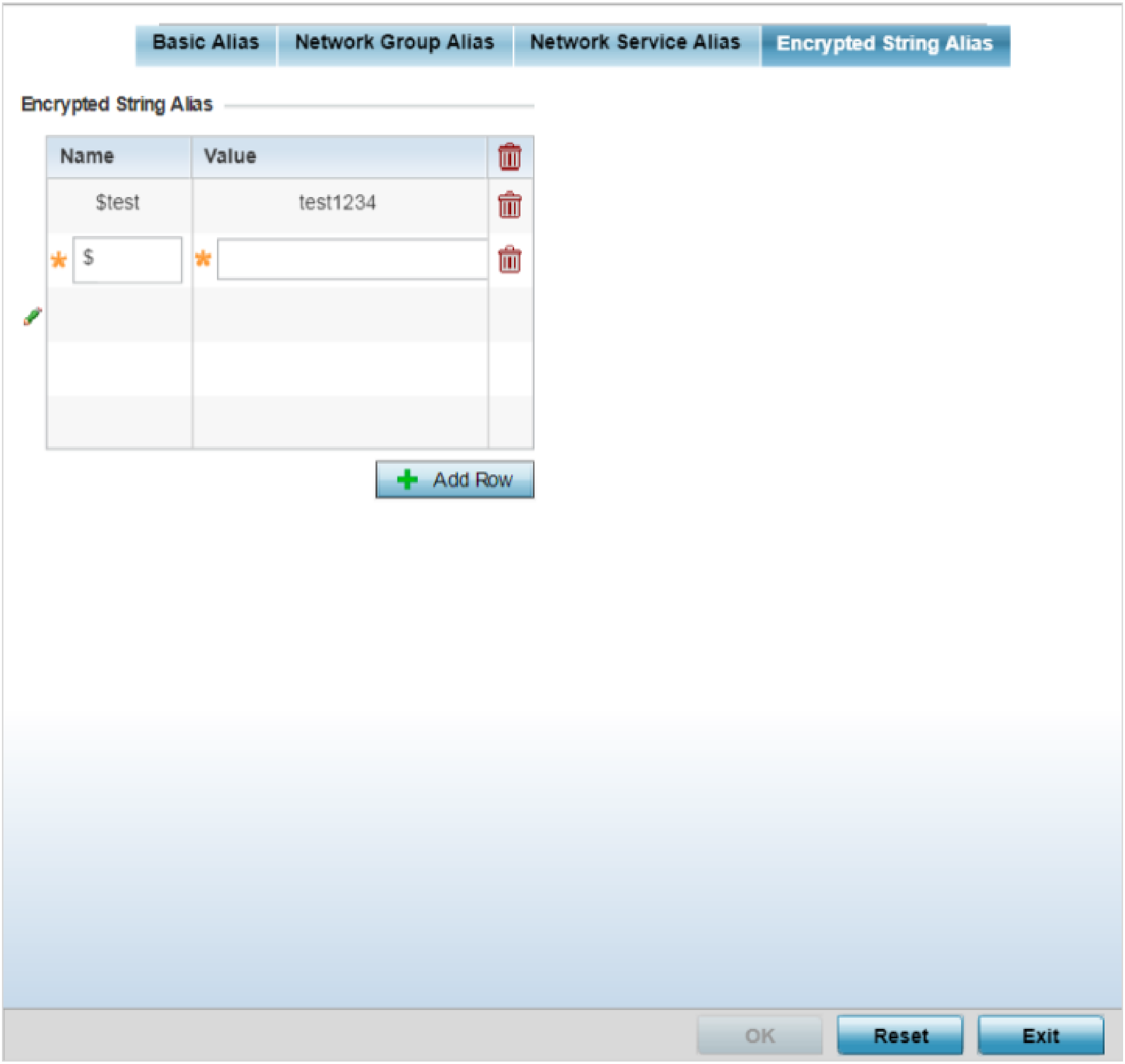
Encrypted String Alias

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.



Encrypted String Alias

Name	Value
$test	test1234
$	

Figure 116: 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. Note: 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 Click **OK** when completed to update the encrypted string alias rules.

Click **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:

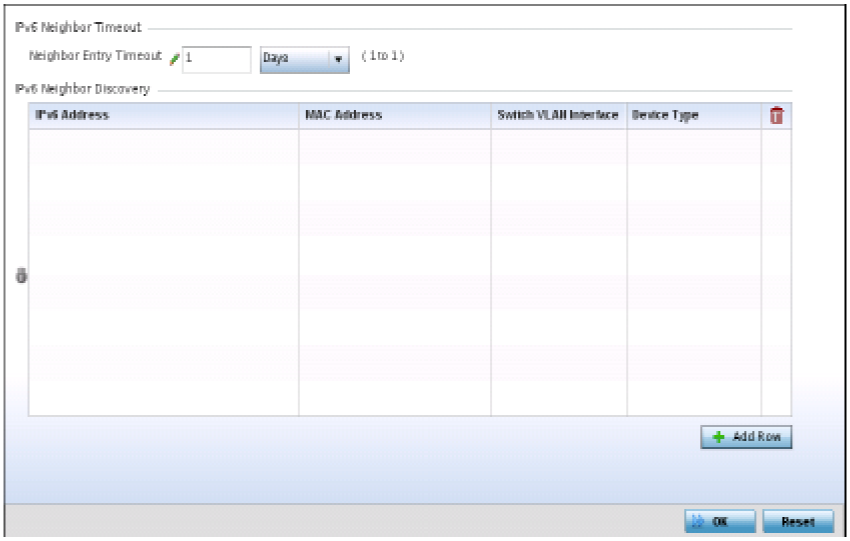
1 Go to **Configuration → Devices**.

The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Select a target device from the device browser in the lower, left-hand side of the UI.

The selected device's configuration screen displays.

3 Expand **Profile Overrides → Network** and select **IPv6 Neighbor**.



Neighbor Entry Timeout 1 Days (1 to 1)

Figure 117: 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 Internet Control Message Protocol version 6 (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. 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 Click **OK** to save the changes. Click **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.

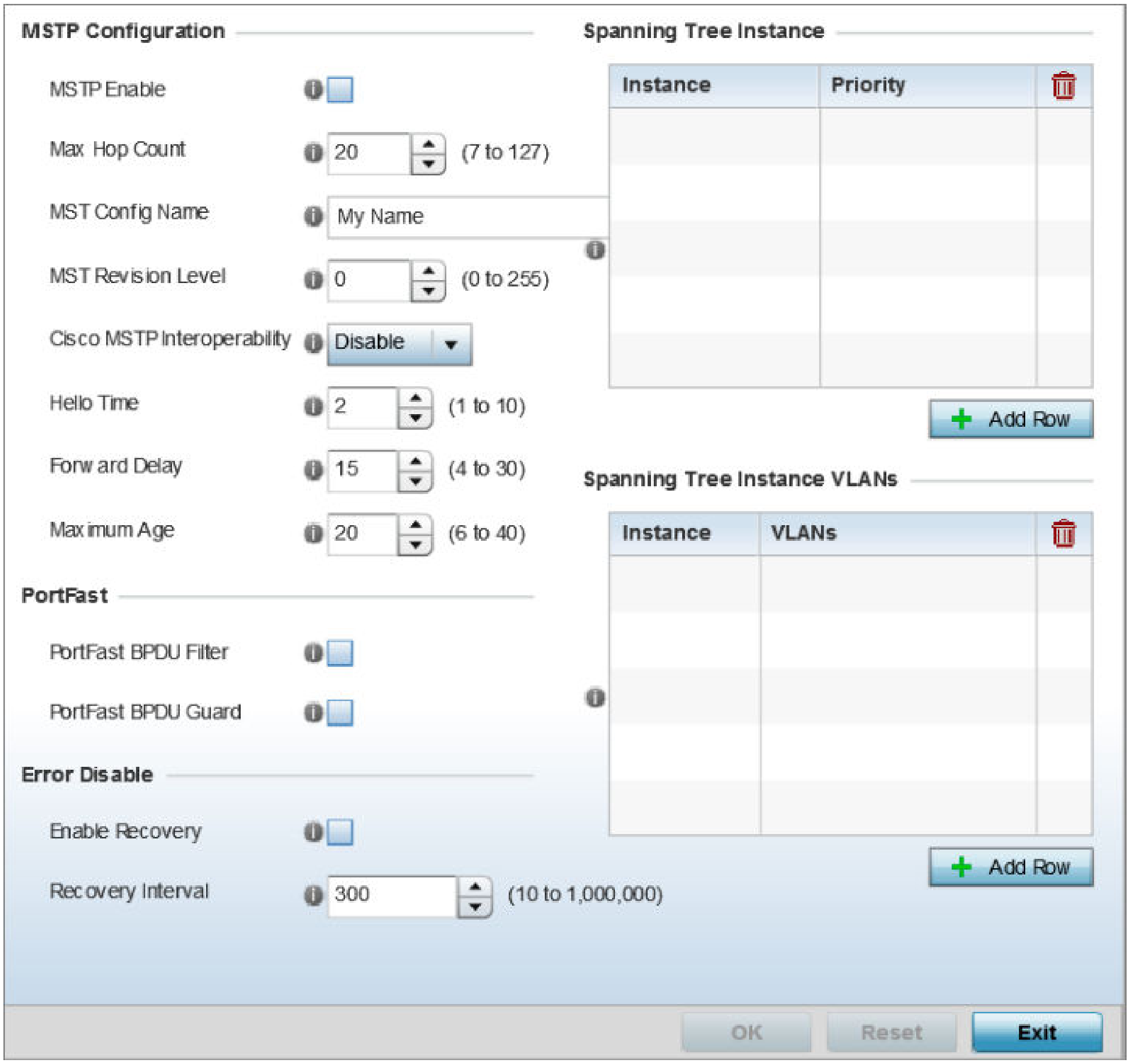
To define the spanning tree configuration:

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

   The **Device Configuration** screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.
2. Select a device from the list displayed.

   The selected device's configuration screen displays.

3 Expand the **Network** node and select **Spanning Tree**.



MSTP Enable ☐
Max Hop Count 20 (7 to 127)
MST Config Name My Name
MST Revision Level 0 (0 to 255)
Cisco MSTP Interoperability Disable
Hello Time 2 (1 to 10)
Forward Delay 15 (4 to 30)
Maximum Age 20 (6 to 40)
PortFast BPDU Filter ☐
PortFast BPDU Guard ☐
Enable Recovery ☐
Recovery Interval 300 (10 to 1,000,000)

Figure 118: 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 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.

Overriding a Profile's Security Configuration

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy, and VPN policy (controllers and service platforms only) applied. If an existing firewall, client role, or NAT policy is unavailable, an administrator can be navigated from the **Profiles** portion of the UI to the **Configuration** > **Security** portion to create the required security policy configuration. Once created, a policy's configuration can have an override applied to meet the changing data protection requirements of a device's environment. When this is done, however, the device must now be managed separately from the profile configuration shared by other devices within the managed network.

For more information on applying an override to an existing device profile, refer to the following sections:

- Overriding General Security Settings on page 252
- Overriding a Certificate Revocation List (CRL) Configuration on page 254
- Overriding RADIUS Trustpoint Configuration on page 255
- Overriding VPN Configuration on page 257
- Overriding Auto IPSec Tunnel Settings on page 265
- Overriding NAT Configuration on page 268
- Overriding a Bridge NAT Configuration on page 278
- Overriding Application Visibility Settings on page 281

Overriding General 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.

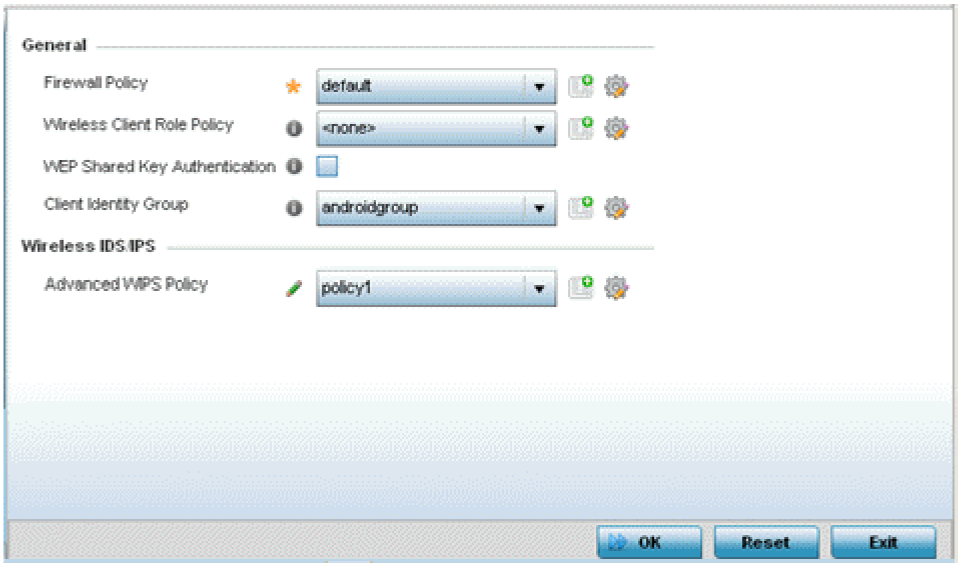
To configure a profile's security settings and overrides:

1. Select **Configuration** > **Devices** from the web UI.

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Select **Profile Overrides** → **Security**.

4 Select **Settings**.



General

Firewall Policy: default

Wireless Client Role Policy: <none>

WEP Shared Key Authentication: ☐

Client Identity Group: androidgroup

Wireless IDS/IPS

Advanced WIPS Policy: policy1

Figure 119: Device Overrides - Security Settings 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.

5 Refer to the General field to assign or override the following:

Firewall Policy	Select an existing Firewall policy to use as an additional security mechanism with a profile. 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 that both block and permit data traffic within the network. If an existing firewall policy does not meet your requirements, click the **Create** icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and overridden as needed using the **Edit** icon.
Wireless Client Role Policy	Select a client role policy used to strategically filter client connections based on a pre-defined set of filter rules and connection criteria. If an existing Wireless Client Role policy does not meet your requirements, click the **Create** icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and overridden as needed using the **Edit** icon.
WEP Shared Key Authentication	Select this option to require devices to use a WEP key to access the network using this profile. The controller or service platform uses the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

Client Identity Group	Select the client identity group to apply to this device profile. Client identity is a set of unique fingerprints used to identify a class of devices. A client identity group is a set of client attributes that identify devices and apply specific permissions and restrictions on them. The information is used to configure permissions and access rules for that device class and can assist administrators by applying permissions and rules to multiple devices simultaneously.
CMP Policy	Use the drop down-menu to assign a CMP policy to allow a device to 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.

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 resources on the internet.
7. Click **OK** to save the changes or overrides.

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

Overriding a 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.

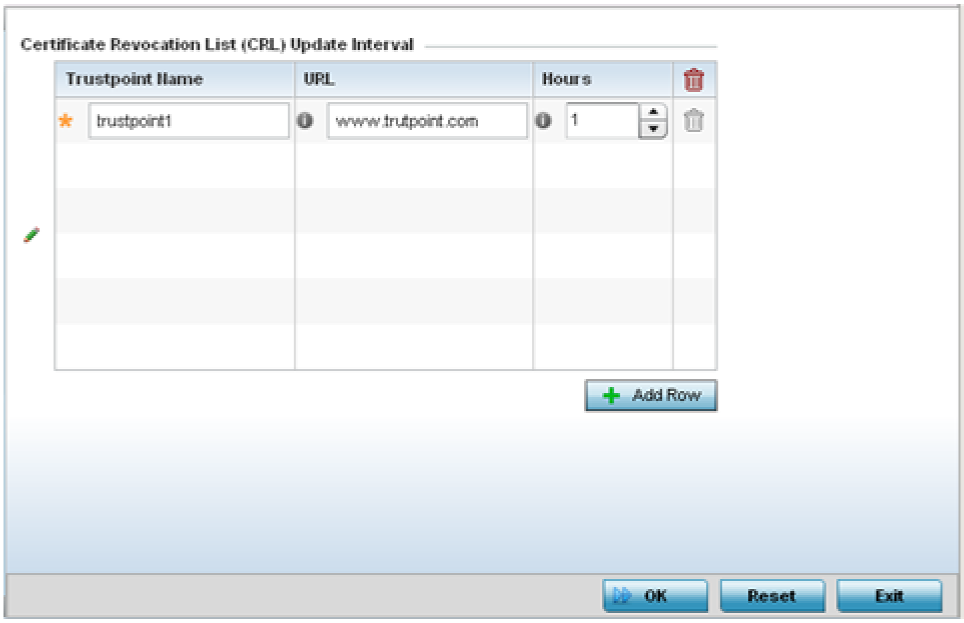
To define a certificate revocation configuration or override:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Select **Profile Overrides** → **Security**.

4 Select **Certificate Revocation**.



Certificate Revocation List (CRL) Update Interval

Trustpoint Name	URL	Hours
trustpoint1	www.trutpoint.com	1

Figure 120: Device Overrides - Certificate Revocation 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.

5 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.

6 Click **OK** to save the changes or overrides to the Certificate Revocation screen.

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

Overriding 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** from the web UI.

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Select **Profile Overrides** → **Security**.
4. Select **Trustpoints**.

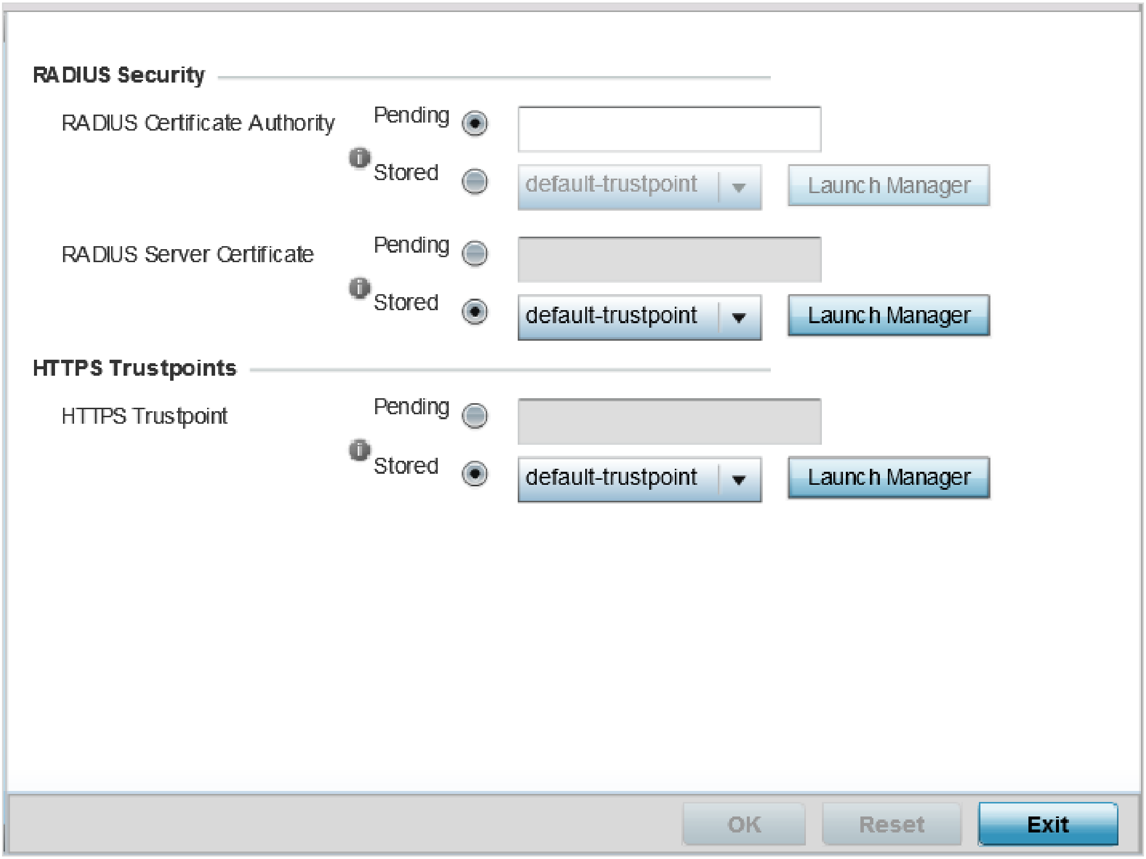


Figure 121: Profile Overrides - Trustpoints Screen

5. Set the following RADIUS Security certificate settings:

RADIUS Certificate Authority	Either use the **`default-trustpoint`** or click **Stored** to enable a drop-down menu where an existing certificate can be used. To make use of an existing certificate, click **Launch Manager**.
RADIUS Server Certificate	Either use the **`default-trustpoint`** or click **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To make use of an existing trustpoint, click **Launch Manager**.

6. 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 974.

7 Click **OK** to save the changes made in the RADIUS Trustpoints screen.

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

Overriding VPN Configuration

IPSec VPN provides a secure tunnel between two networked peer devices. Administrators can define which packets are sent within the tunnel, and how they're 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 SAs *(security associations)* 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).

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 pre-configuration.

To define a profile's VPN settings:

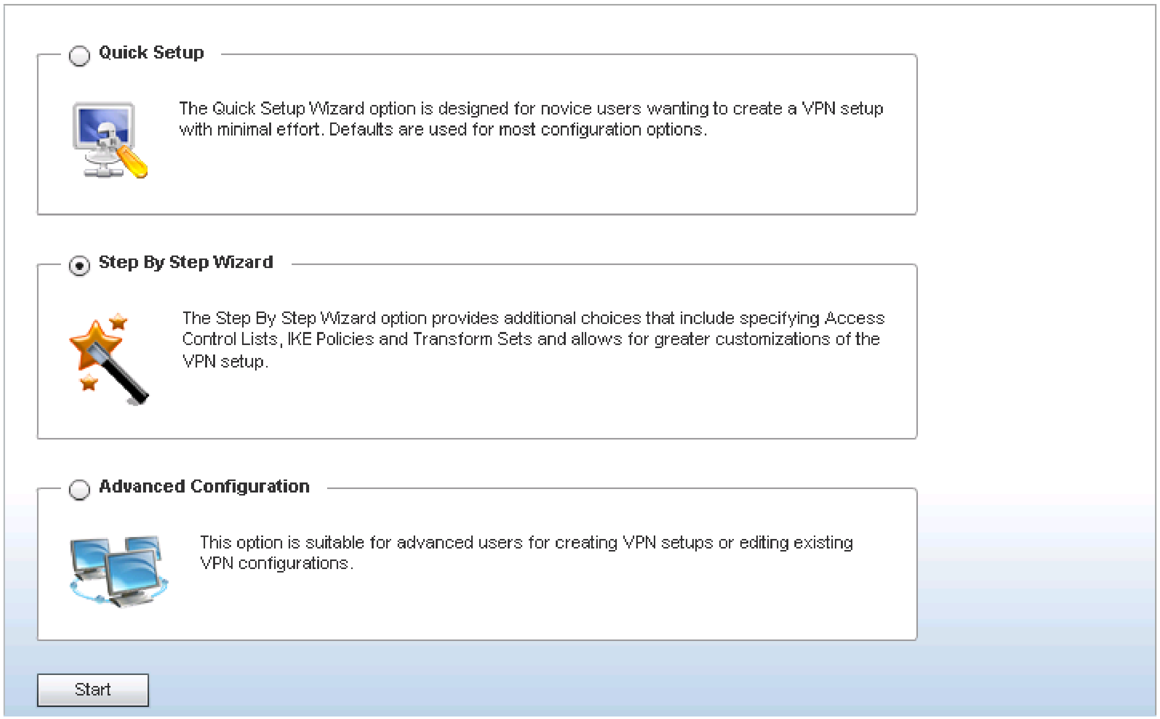
1 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

2 Select **Profile Overrides → Security**.

3 Select **VPN**.

The VPN configuration can be overridden either by using a built-in wizard 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 wizards that provide either basic or more thorough administration.



○ **Quick Setup**

The Quick Setup Wizard option is designed for novice users wanting to create a VPN setup with minimal effort. Defaults are used for most configuration options.

● **Step By Step Wizard**

The Step By Step Wizard option provides additional choices that include specifying Access Control Lists, IKE Policies and Transform Sets and allows for greater customizations of the VPN setup.

○ **Advanced Configuration**

This option is suitable for advanced users for creating VPN setups or editing existing VPN configurations.

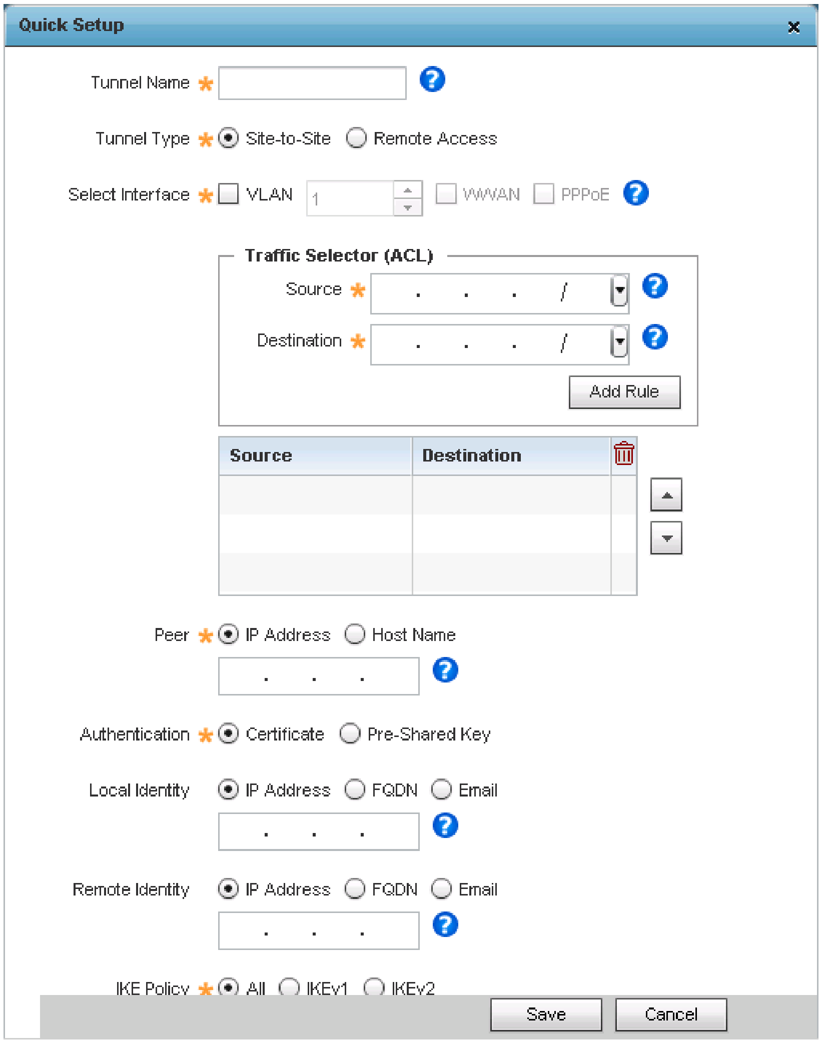
Figure 122: VPN Setup Wizard

- Quick Setup Wizard: Use this wizard to set a minimum number of basic VPN tunnel values. This wizard is designed for novice users, and enables them to setup a VPN configuration with minimum effort. This wizard uses default values for most parameters.
- Step By Step Wizard: Use this wizard to create a VPN tunnel using settings updated from their minimum default values. This wizard is designed for intermediate users who require the ability to customize some of the parameters.
- Advanced VPN Configuration: The advanced VPN configuration option does not utilize a setup wizard. Rather, it utilizes and its own screen flow where just about every facet of a VPN tunnel configuration can be set by a qualified network administrator. For more information, see Profile Security Configuration on page 676.

Overriding VPN Configuration: Quick Setup Wizard

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

1 In the **Security Configuration Wizard** screen, click **Quick Setup**.



Quick Setup

Tunnel Name *

Tunnel Type * ● Site-to-Site ○ Remote Access

Select Interface * ☐ VLAN 1 ☐ WWAN ☐ PPPoE

Traffic Selector (ACL)

Source * . . . /

Destination * . . . /

Peer * ● IP Address ○ Host Name

Authentication * ● Certificate ○ Pre-Shared Key

Local Identity ● IP Address ○ FQDN ○ Email

Remote Identity ● IP Address ○ FQDN ○ Email

IKE Policy * ● All ○ IKEv1 ○ IKEv2

Figure 123: VPN Quick Setup Wizard

2 Provide the following information to configure a VPN tunnel:

Tunnel Name	Provide a name for the tunnel. The name should identify the tunnel uniquely.
Tunnel Type	Configure the tunnel type as one of the following: • Site-to-Site – The tunnel provides a secured connection between two sites. This is the default setting. • Remote Access – The tunnel provides access to a network to remote devices.
Select Interface	Configure the interface to use for creating the tunnel. The following options are available: • VLAN – Configure the tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number. • WWAN – Configure the tunnel over the WAN interface. • PPPoE – Configure the tunnel over the PPPoE interface.

Traffic Selector (ACL)	Configure ACLs that manage the traffic passing through the VPN tunnel. The following options are available: • Source – Provide the source network along with its mask. • Destination – Provide the destination network along with its mask.
Peer	Configure the peer for this tunnel. The peer device can be specified either by its hostname or by its IP address.
Authentication	Set the authentication used to identify the peers on opposite ends of the VPN tunnel connection. The following can be configured: • Certificate – Use a certificate to authenticate. This is the default setting. • Pre-Shared Key – Use a pre-shared key to authenticate. Enter the secret key in the space provided.
Local Identity	Configure the local identity 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`**.
Remote Identity	Configure the access point 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	Configure the *Internet Key Exchange* (IKE) policy to use. IKE is used to exchange authentication keys. Select from one of the following: • All – Use any IKE policy. This is the default setting. • IKE1 – Use IKE 1 only. • IKE2 – Use IKE 2 only.
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 list.

3. Click **Save** to save the VPN tunnel configuration.

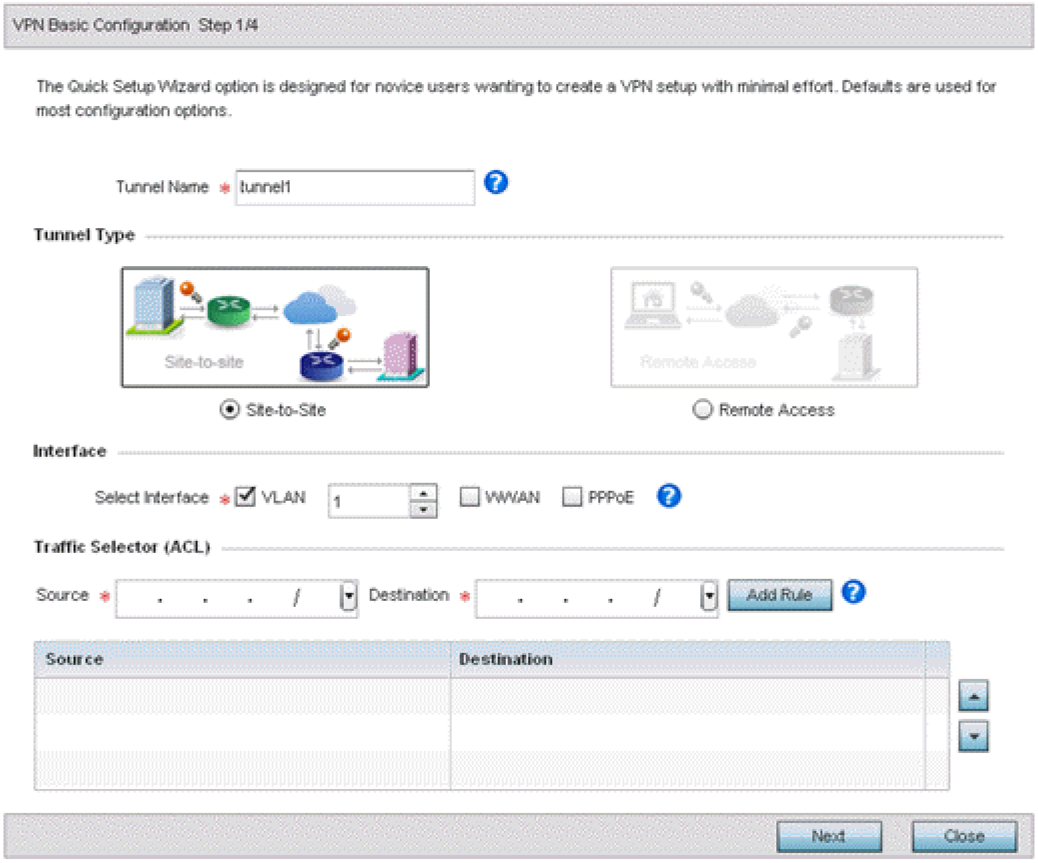
   To exit without saving, click **Cancel**.

Overriding VPN Configuration: Step By Step 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.

1. In the Security Configuration Wizard screen, click **Step-By-Step Wizard**.

2 Click **Start**



VPN Basic Configuration Step 1/4

The Quick Setup Wizard option is designed for novice users wanting to create a VPN setup with minimal effort. Defaults are used for most configuration options.

Tunnel Name * tunnel1

Tunnel Type

● Site-to-Site ○ Remote Access

Interface

Select Interface * ☑ VLAN 1 ☐ WWAN ☐ PPPoE

Traffic Selector (ACL)

Source * Destination *

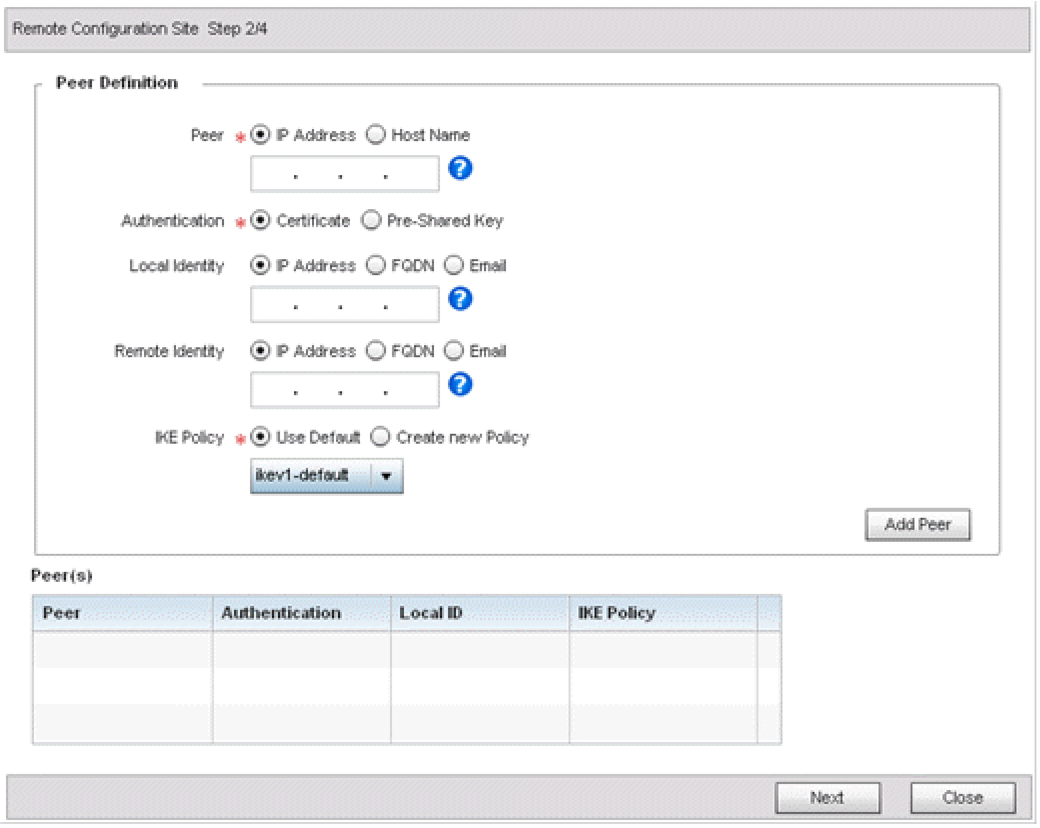
Source	Destination

Figure 124: VPN Step-By-Step Wizard - Step 1

3 Set the following VPN values in the Step 1 screen.

Tunnel Name	Provide a name for the tunnel.
Tunnel Type	Select the tunnel type being created. Two types of tunnels can be created. Use `Site to Site` to create a tunnel between two remote sites. Use `Remote Access` to create a tunnel between a user device and a network. `Site to Site` is the default setting.
Interface	Configure the interface to use for creating the tunnel – either Virtual LAN (`VLAN`), `WWAN`, or `PPPoE` depending on the interfaces available on the device.
Traffic Selector (ACL)	Creates the access control list (ACL) that is used to control who uses the network. Provide the Source and Destination IP address ranges with their net mask. Click **Add Rule** to add the rule into the ACL.

4 Click **Next**.



Remote Configuration Site Step 2/4

Peer Definition

Peer * ● IP Address ○ Host Name

Authentication * ● Certificate ○ Pre-Shared Key

Local Identity ● IP Address ○ FQDN ○ Email

Remote Identity ● IP Address ○ FQDN ○ Email

IKE Policy * ● Use Default ○ Create new Policy

ikev1-default

Figure 125: VPN Step-By-Step Wizard - Step 2

5 Set the following VPN values in the Step 2 screen.

If any of the required values in the Step 1 screen are not set properly, the Step 2 screen will not display until they are properly set.

Peer	Select the type of peer for this device when forming a tunnel. Peer information can be either an **`IP Address`** (default value) or **`Host Name`**. Provide the IP address or the host name of the peer device.
Authentication	Configure how devices authenticate on opposite ends of the tunnel connection. The following can be configured: • Certificate – The devices use a certificate to authenticate. This is the default setting. • Pre-Shared Key – The devices use a pre-shared key to authenticate.
Local Identity	Configure the local identity for the VPN tunnel. • P Address – The local identity is an IP address. This is the default setting. • FQDN – The local identity is a FQDN *(Fully Qualified Domain Name)* . • Email – The local identity is an E-mail address.

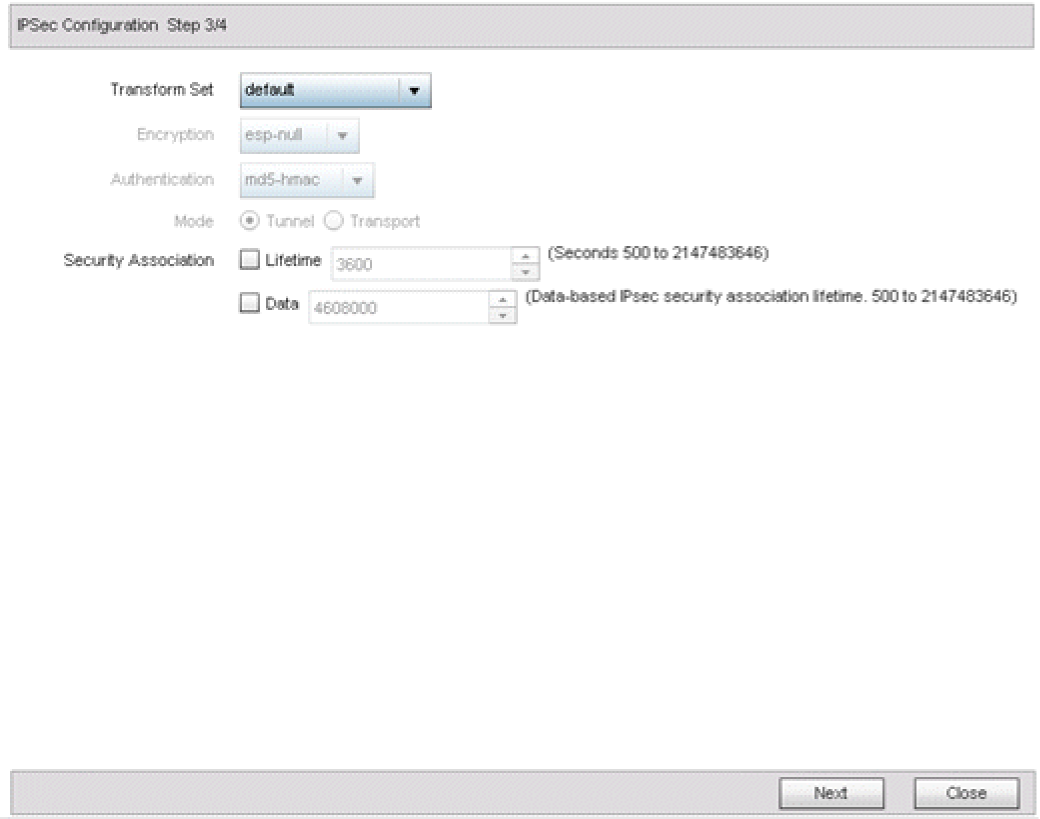
Remote Identity	Configure the remote identity for the VPN tunnel. • P Address – The remote identity is an IP address. This is the default setting. • FQDN – The remote identity is a FQDN. • Email – The remote identity is an E-mail address.
IKE Policy	Configure the *Internet Key Exchange* (IKE) policy to use when creating this VPN tunnel. The following options are available: • Use Default – Use the default IKE profiles. • Create new Policy – Create a new IKE policy.

6 Click **Add Peer** to add the tunnel peer information into the **Peer(s)** table.

This table lists all of the peers that are set for the VPN tunnel.

7 Click **Next** to proceed to the Step 3 screen.

Use the **Back** button to go to the previous step. If any of the required values in the Step 2 screen are not set properly, the Step 3 screen will not display until they are properly set.



IPSec Configuration Step 3/4

Transform Set: default

Encryption: esp-null

Authentication: md5-hmac

Mode: ● Tunnel ○ Transport

Security Association: ☐ Lifetime 3600 (Seconds 500 to 2147483646)

☐ Data 4608000 (Data-based IPsec security association lifetime. 500 to 2147483646)

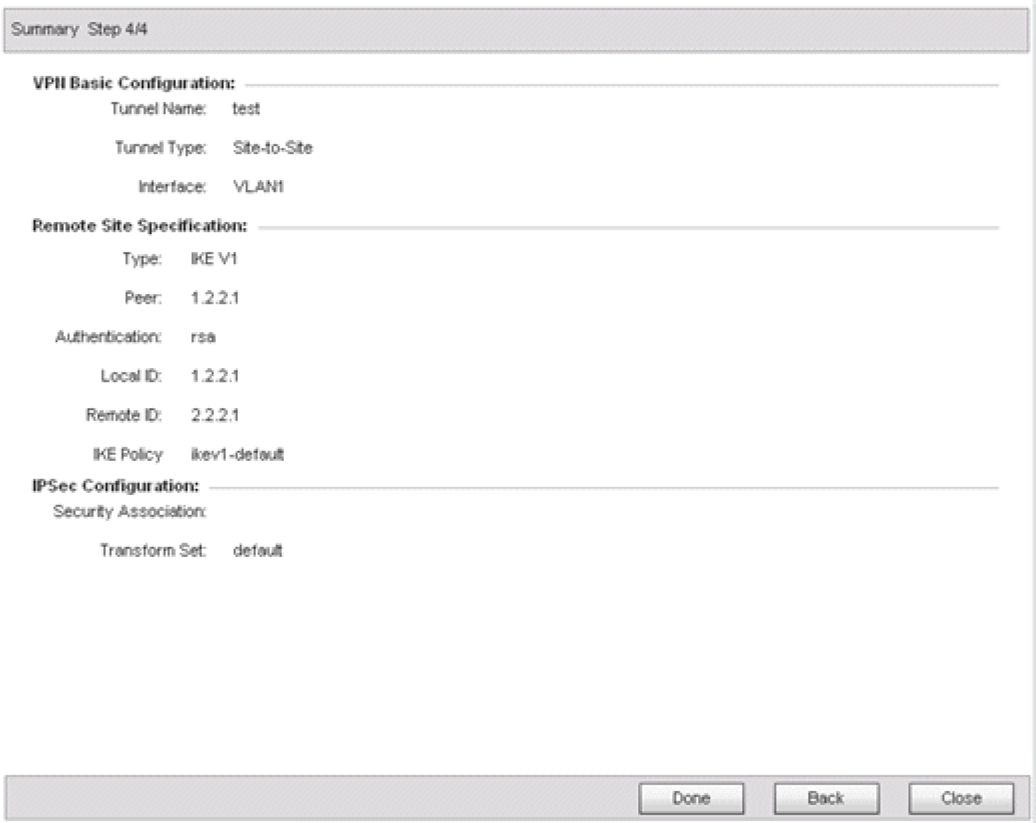
Figure 126: VPN Step-By-Step Wizard - Step 3

8 Set the following IPSec VPN values in the Step 3 screen.

Transform Set	Transform set is a set of configurations exchanged for creating the VPN tunnel and imposing a security policy.The transform set consists of the following: • Encryption – The encryption to use for creating the tunnel. • Authentication – The authentication used to identify tunnel. peers • Mode – The mode of the tunnel. This is how the tunnel will operate. From the drop-down list, select any pre-configured transform set, or click **Create New Policy** to create a new transform set.
Encryption	This field is enabled when **Create New Policy** is selected in the **Transform Set** field. This is the encryption that is used on data traversing through the tunnel. Select from the following algorithms: **`esp-null`**, **`des`**, **`3des`**, **`aes`**, **`aes-192`**, or **`aes-256`**.
Authentication	This field is enabled when **Create New Policy** is selected in the **Transform Set** field. This is the method peers authenticate as the source of the packet to other peers after a VPN tunnel has been created. Select from the following: **`MD5`**, **`SHA`**, **`SHA256`**, or **`AES-XCBC-HMAC-128`**.
Mode	This field is enabled when **Create New Policy** is selected in the **Transform Set** field. The mode indicates how packets are transported through the tunnel. • Tunnel – The tunnel is between two routers or servers. • Transport – The tunnel is between a client and a server.
Security Association	Configures the lifetime of a security association (SA). Keys and SAs should be renewed periodically to maintain the security of the tunnel. • Lifetime – Duration in seconds after which the keys should be changed. Set a value from 500 - 2,147,483,646 seconds. • Data – The key is changed after this quantity of data has been encrypted/ decrypted. Set a value from 500 - 2,147,483,646 KB.

9 Click **Next** to proceed to the Step 4 screen.

Use the **Back** button to go to the previous step. If any of the required values in the Step 3 screen are not set properly, the Step 4 screen will not display until they are properly set.



VPN Basic Configuration:
Tunnel Name: test
Tunnel Type: Site-to-Site
Interface: VLAN1

Remote Site Specification:
Type: IKE V1
Peer: 1.2.2.1
Authentication: rsa
Local ID: 1.2.2.1
Remote ID: 2.2.2.1
IKE Policy ikev1-default

IPSec Configuration:
Security Association:
Transform Set: default

Figure 127: VPN Step-By-Step Wizard - Step 4

10 Review the configuration and click **Done** to create the VPN tunnel.

Use the **Back** button to go back to a previous screen and modify the configuration. Click **Close** to close the wizard without creating a VPN tunnel.

Advanced VPN Configuration

The advanced VPN configuration option does not utilize a setup wizard. Rather, it utilizes its own screen flow where most facets of a VPN tunnel configuration can be set by a qualified network administrator.

For detailed information on creating a VPN tunnel configuration, refer to Setting the Profile's VPN Configuration on page 679.

Overriding Auto IPSec Tunnel Settings

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points which are within a range of valid IP addresses. 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 or associated access point.

Tunnels are sets of *security associations* (SAs) 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).

Internet Key Exchange (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 enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

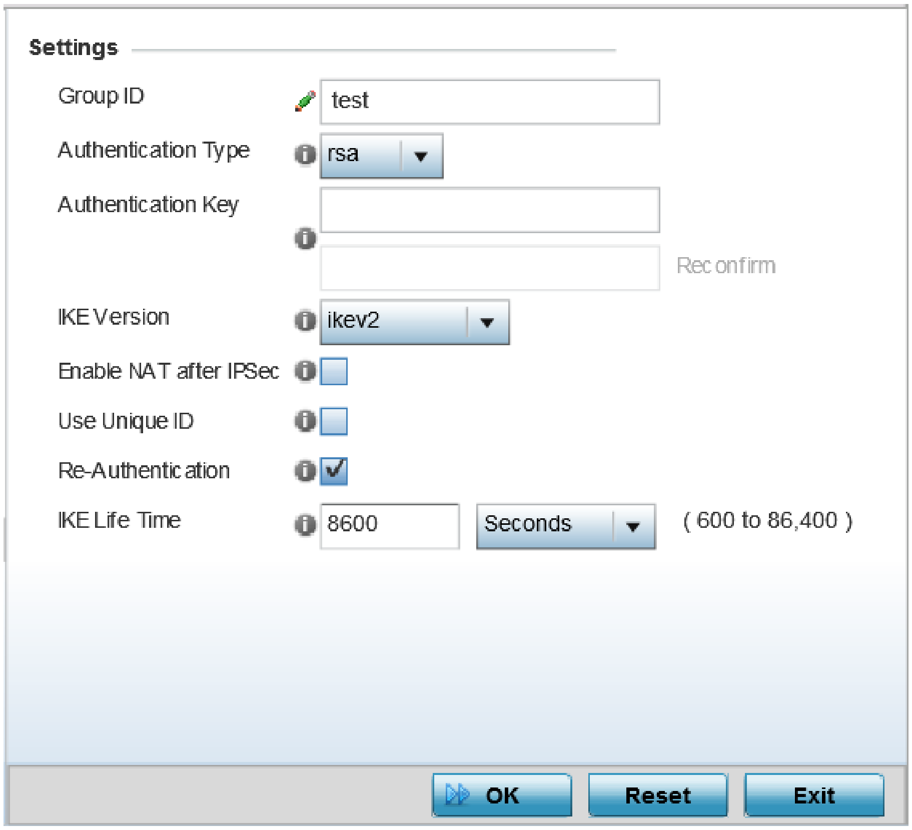
To define or override a profile's Auto IPSec tunnel configuration:

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

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Select **Profile Overrides** → **Security**.

4 Select **Auto IPSec Tunnel**.



Settings

Group ID: test

Authentication Type: rsa

Authentication Key:

Reconfirm

IKE Version: ikev2

Enable NAT after IPSec ☐

Use Unique ID ☐

Re-Authentication ☑

IKE Life Time: 8600 Seconds (600 to 86,400)

Figure 128: Device Overrides - Security – Auto IPSec Tunnel screen

The **Settings** field lists those Auto IPSec tunnel policies 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.

5 Refer to the following table to override the Auto IPSec tunnel settings:

Group ID	Define a 1 - 64 character identifier for an IKE exchange supporting auto IPSec tunnel secure peers.
Authentication Type	Select either **RSA** or **PSK** (Pre Shared Key) as the authentication type for secure peer authentication on the auto IPSec secure tunnel. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing, as well as encryption. The default setting is **RSA**.
Authentication Key	Enter the 8 - 21 character shared key (password) used for auto IPSec tunnel secure peer authentication.
IKE Version	Select the IKE version used for auto IPSec tunnel secure authentication with the IPSec gateway. **IKEv2** is the default setting.
Enable NAT after IPSec	Select this option to enable internal source port NAT on the auto IPSec secure tunnel.

Use Unique ID	Select this option to use a unique ID with auto IPSec secure authentication for the IPSec remote gateway (appending the MiNT ID). This setting is disabled by default.
Re-Authentication	Select this option to re-authenticate the key on a IKE rekey. This setting is enabled 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.

6 Click **OK** to save the changes made in the Auto IPSec Tunnel screen.

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

Overriding 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.

To define or override a NAT configuration that can be applied to a profile:

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

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Profile Overrides** → **Security**.

4 Select **NAT**.

The NAT Pool screen displays by default.

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.

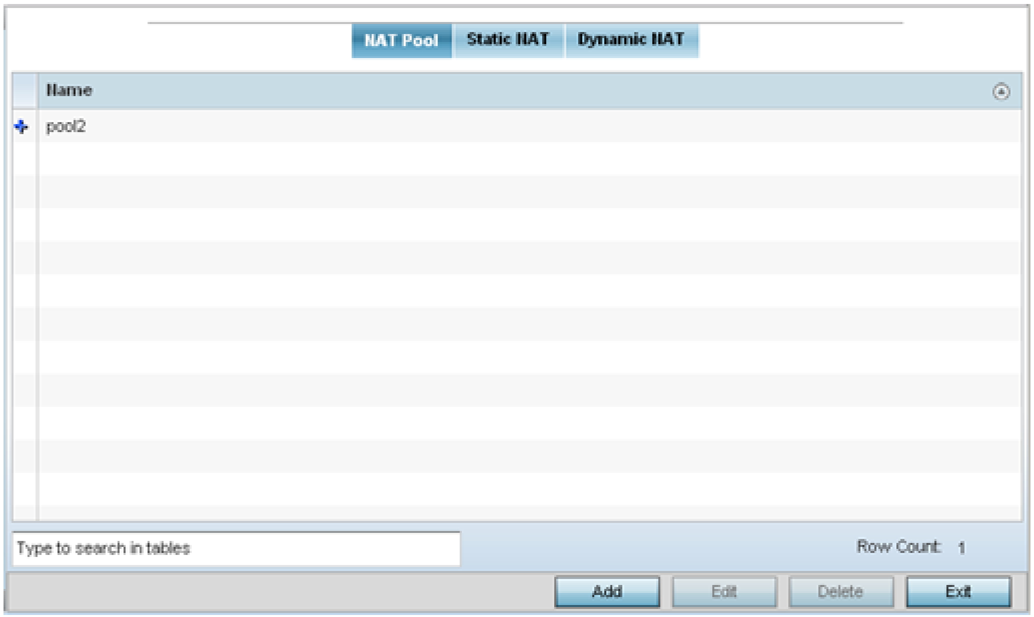


Figure 129: Device Overrides - NAT Pool Screen

5 Review existing NAT policies to determine if a new policy warrants creation or an existing policy warrants modification or deletion. You can select and apply any of these policies to a profile.

6 Click **Add** to create a new NAT policy that can be applied to a profile.

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.

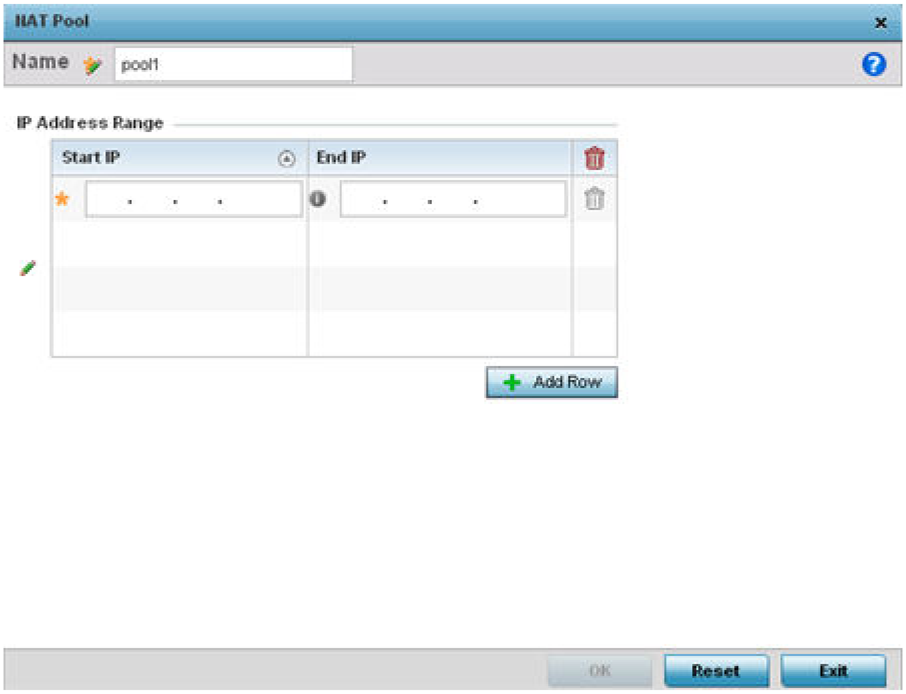


Figure 130: Device Overrides - Security - NAT Pool Screen

7 If you are adding a new NAT pool policy or editing the configuration of an existing policy, define the following parameters:

Name	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.
IP Address Range	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.

8 Click **+ Add Row**, in the IP Address Range table to append additional rows.

9 Click **OK** to save the changes made to the profile's NAT pool configuration.

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

Profile Overrides - Static NAT - Source

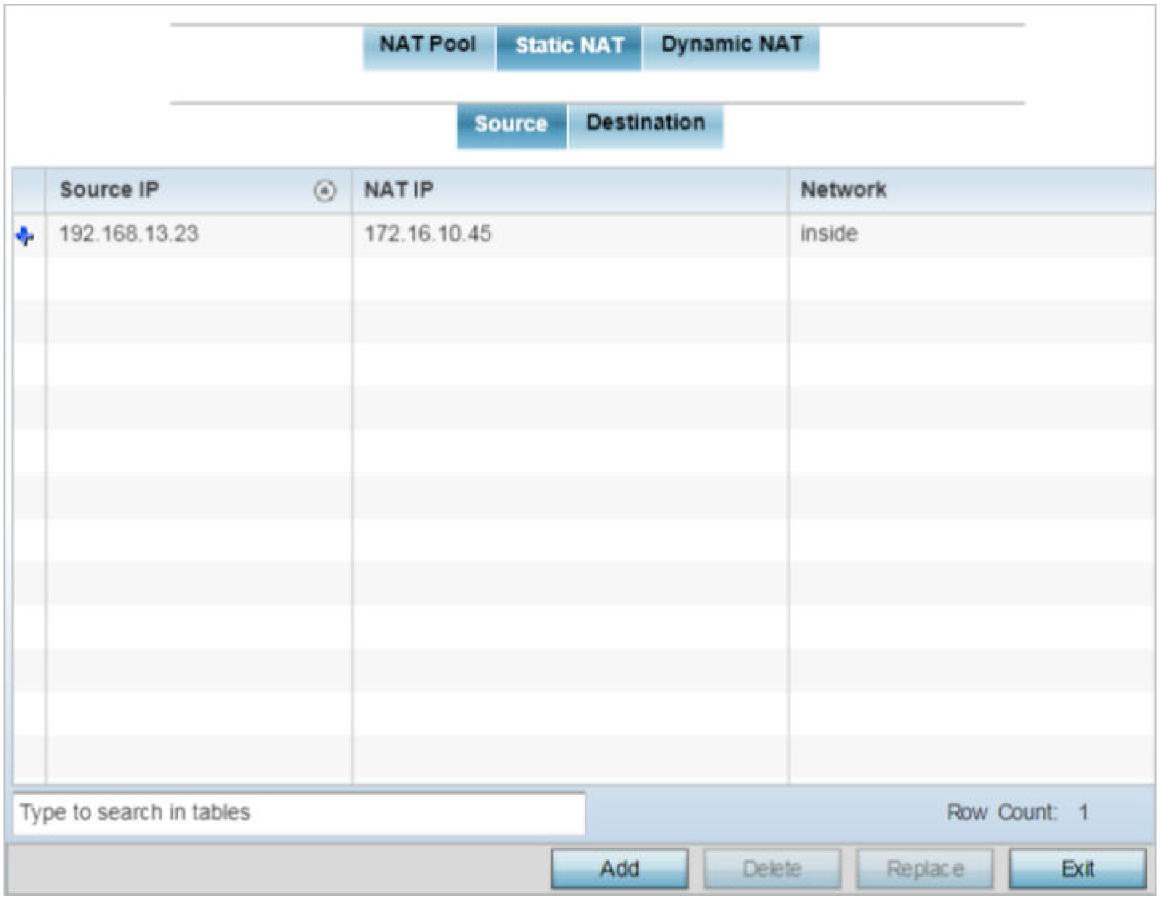
Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a web server on a perimeter interface with the internet, use static address translation to map the actual address to a registered IP address. Static address translation 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.



Source IP	NAT IP	Network
192.168.13.23	172.16.10.45	inside

Row Count: 1

Figure 131: 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.

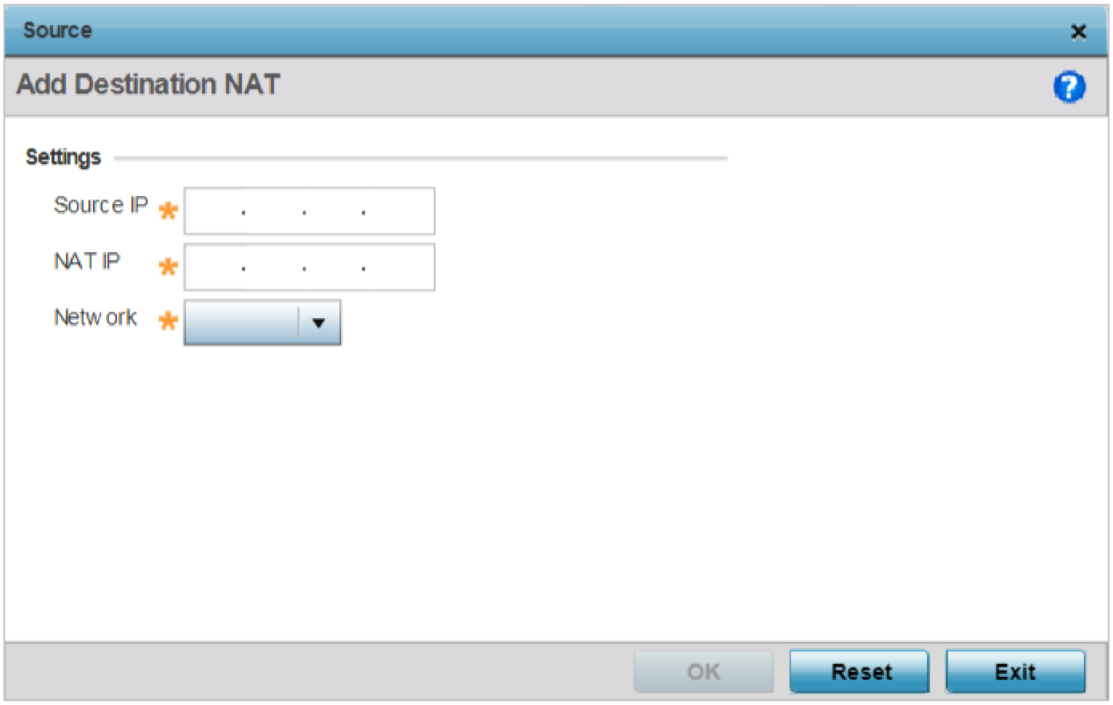


Figure 132: NAT Configuration - Add Static NAT Source IP Address Window

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. 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.

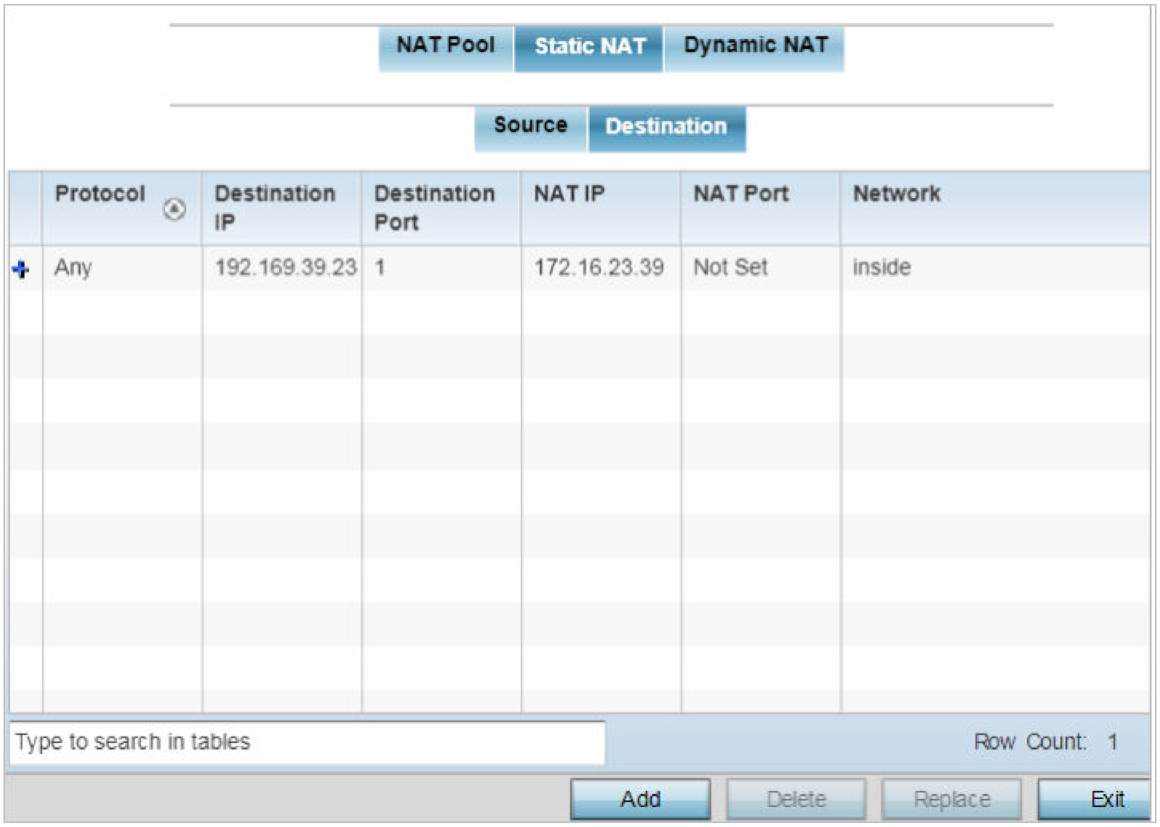
Click **Reset** to revert to the last saved configuration.

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.



	Protocol	Destination IP	Destination Port	NAT IP	NAT Port	Network
+	Any	192.169.39.23	1	172.16.23.39	Not Set	inside

Figure 133: 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.

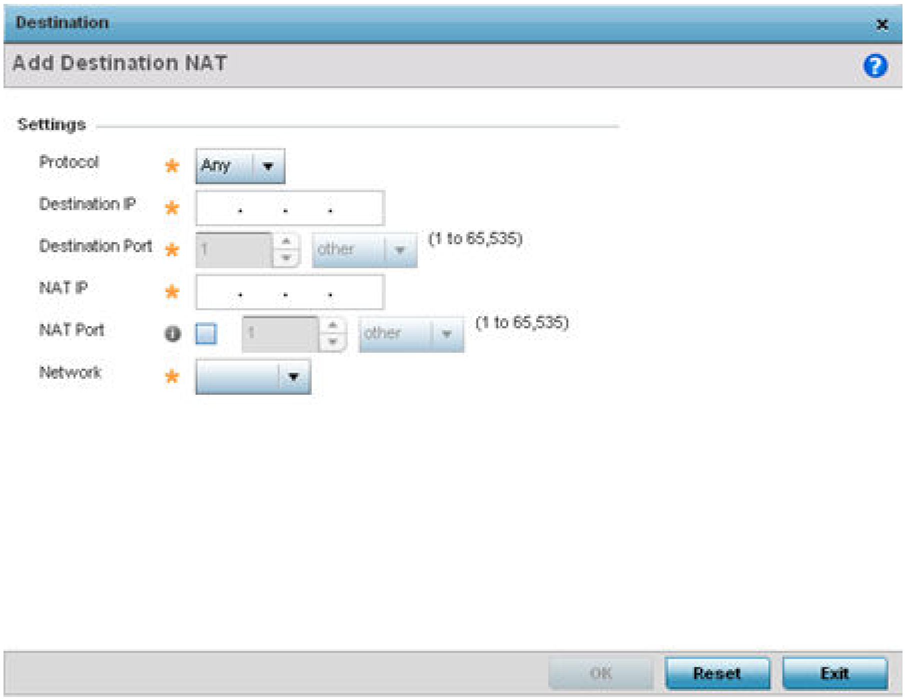


Figure 134: NAT Configuration - Add Static NAT Destination IP Address Window

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*. 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. 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. 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.

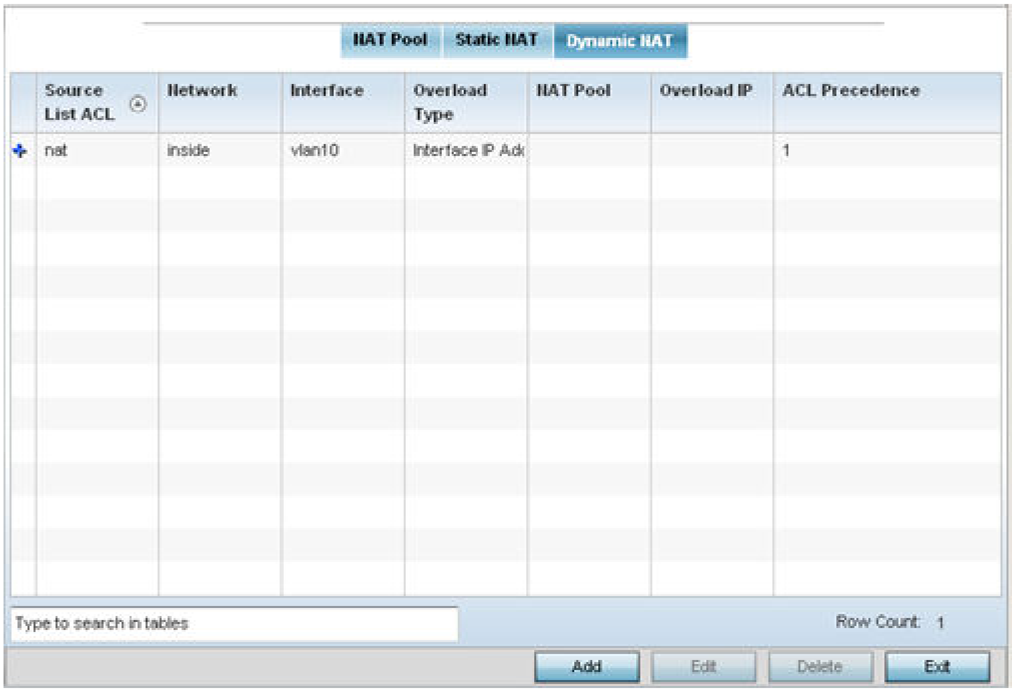
Profile Overrides - Dynamic NAT

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.



Source List ACL	Network	Interface	Overload Type	NAT Pool	Overload IP	ACL Precedence
nat	inside	vlan10	Interface IP Ad			1

Type to search in tables

Row Count: 1

Figure 135: 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.

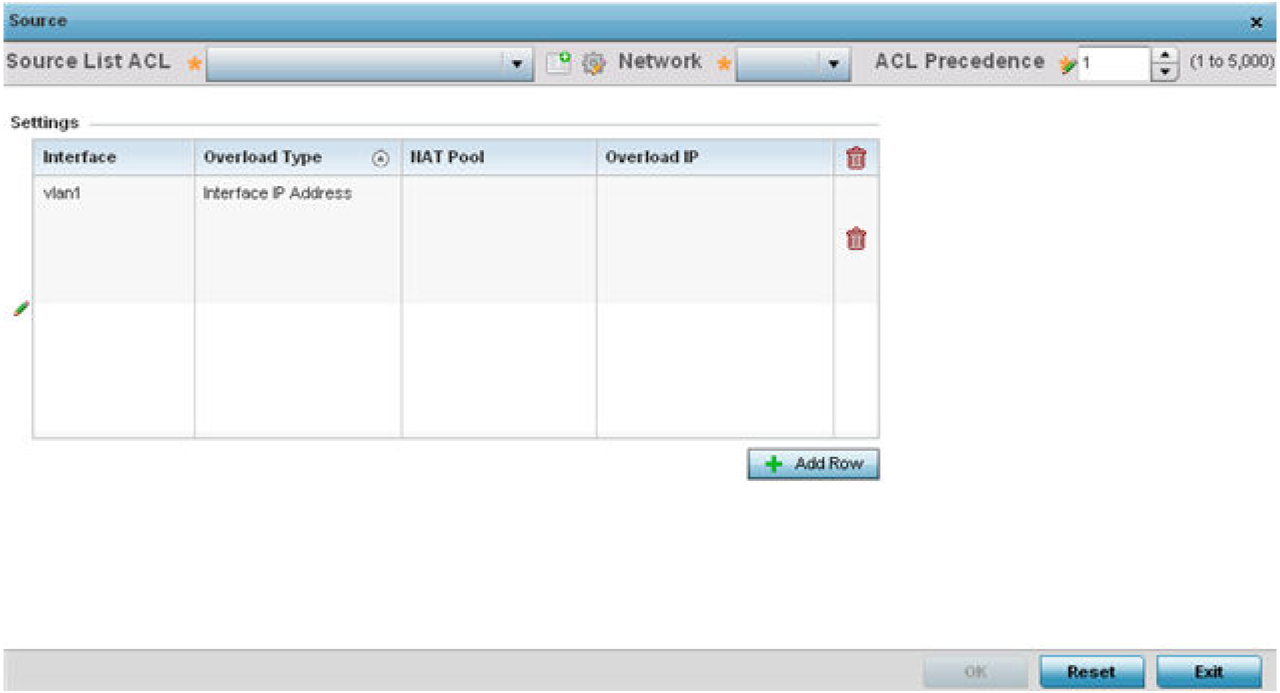


Figure 136: Profile Overrides - Security - NAT - Dynamic NAT - Source ACL List Screen

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. Note: 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.

Overriding a 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.

To define a NAT configuration or override that can be applied to a profile:

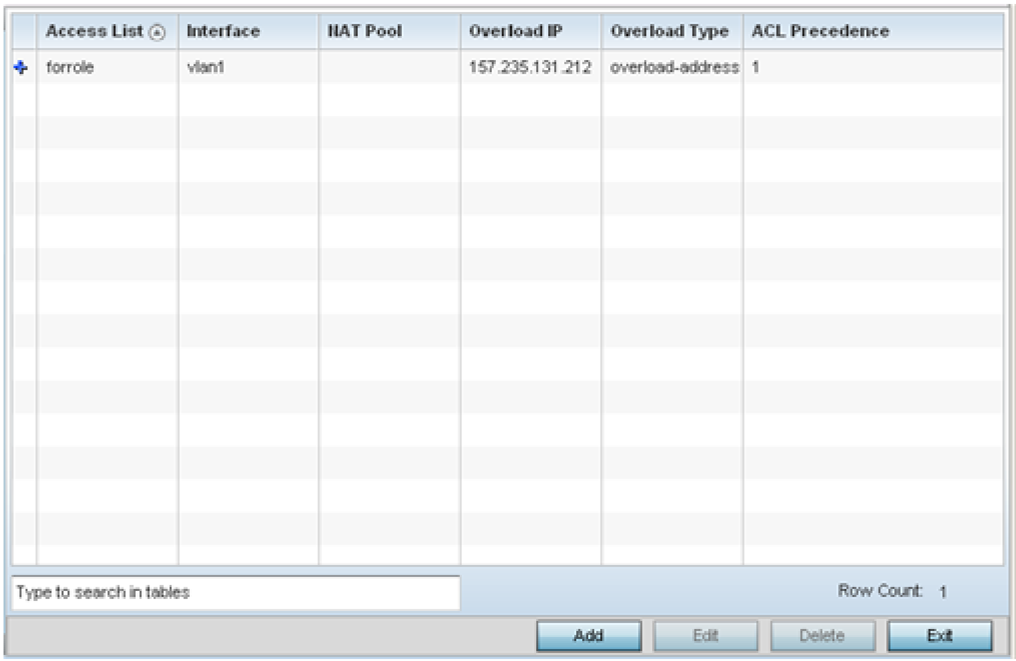
1. Select **Configuration** > **Devices** from the web UI.

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.
2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.
3. Select **Profile Overrides** > **Security**.

4 Select **Bridge NAT**.

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.



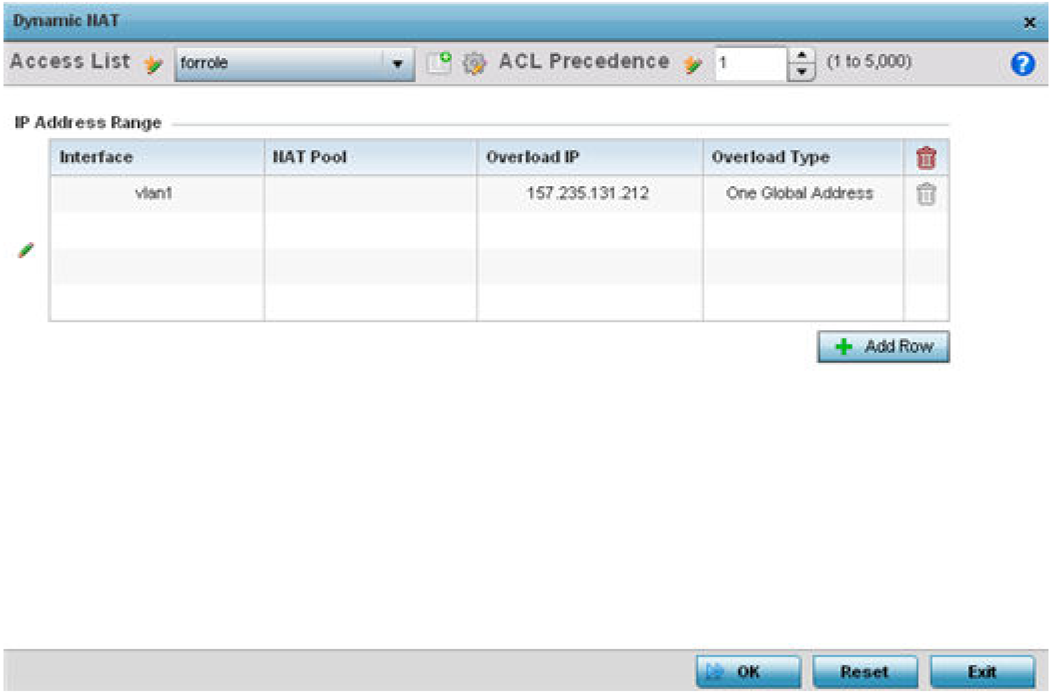
	Access List	Interface	NAT Pool	Overload IP	Overload Type	ACL Precedence
✚	forrole	vlan1		157.235.131.212	overload-address	1

Figure 137: Profile Overrides - Security - Bridge NAT Screen

5 Refer to the following **Bridge NAT** settings to determine whether a new bridge NAT configuration needs to be created, or whether an existing one can be edited or deleted:

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 to represent a large number of local addresses for this configuration.
Overload Type	Define the overload type utilized when several internal addresses are NATed to only one or a few external addresses. Select **`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.

6 Click **Add** to create a new bridge VLAN configuration, **Edit** to modify or override an existing configuration, or **Delete** to permanently remove a configuration.



Access List: forrole

ACL Precedence: 1 (1 to 5,000)

Interface	NAT Pool	Overload IP	Overload Type
vlan1		157.235.131.212	One Global Address

Figure 138: Profile Security - Dynamic NAT - Screen

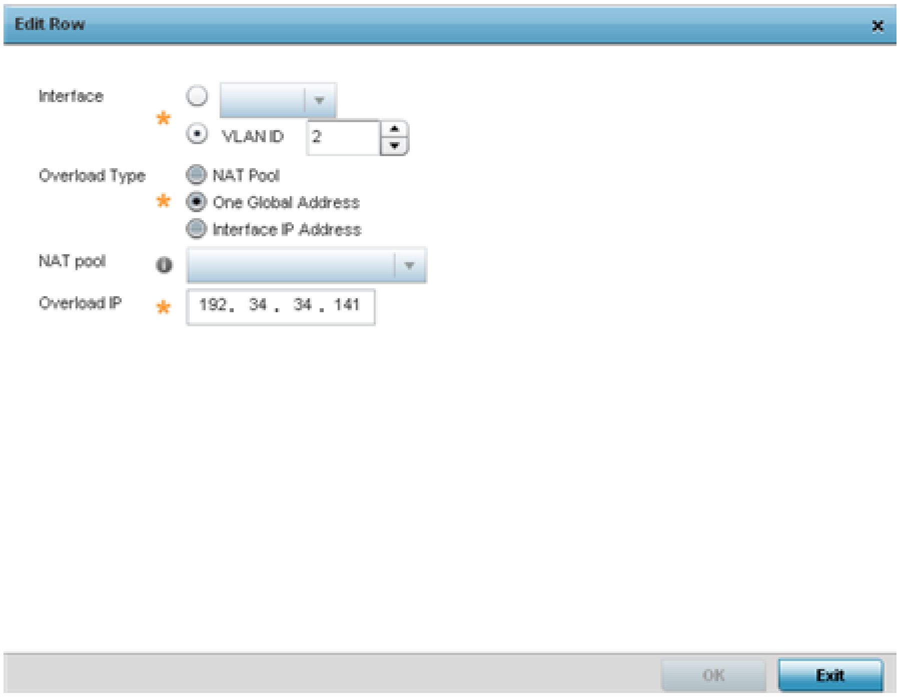
7 Select the **ACL** whose IP rules are applied to the policy based forwarding rule.

You can define a new ACL by clicking the **Create** icon, or you can modify an existing set of IP ACL rules by clicking the **Edit** icon.

8 Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the internet.

ACL Precedence	Set the priority (from 1 - 5000) for the ACL. The lower the value, the higher the priority assigned to these ACL rules.
Interface	Select the outgoing Layer 3 interface on which traffic is redirected. 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 of local addresses for this configuration.
Overload Type	Define the overload type utilized when several internal addresses are NATed to only one or a few external addresses. Select `NAT Pool`, `One Global Address`, or `Interface IP Address`. `Interface IP Address` is the default setting.

9 Click **+ Add Row** to set the interface, overload, and NAT pool settings for the bridge NAT configuration.



Interface: ○ (dropdown) ● VLAN ID 2

Overload Type: ○ NAT Pool ● One Global Address ○ Interface IP Address

NAT pool:

Overload IP: 192 . 34 . 34 . 141

Figure 139: Security Source Dynamic NAT Screen

10 Click **OK** to save the changes made in the **Add Row** and **Source Dynamic NAT** screens.

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

Overriding Application Visibility Settings

Deep packet inspection (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.

To configure a profile’s application visibility settings and overrides:

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

The Device Configuration screen displays in the right-hand side of the UI. This screen lists all devices within the managed network (peer controllers, service platforms and access points).

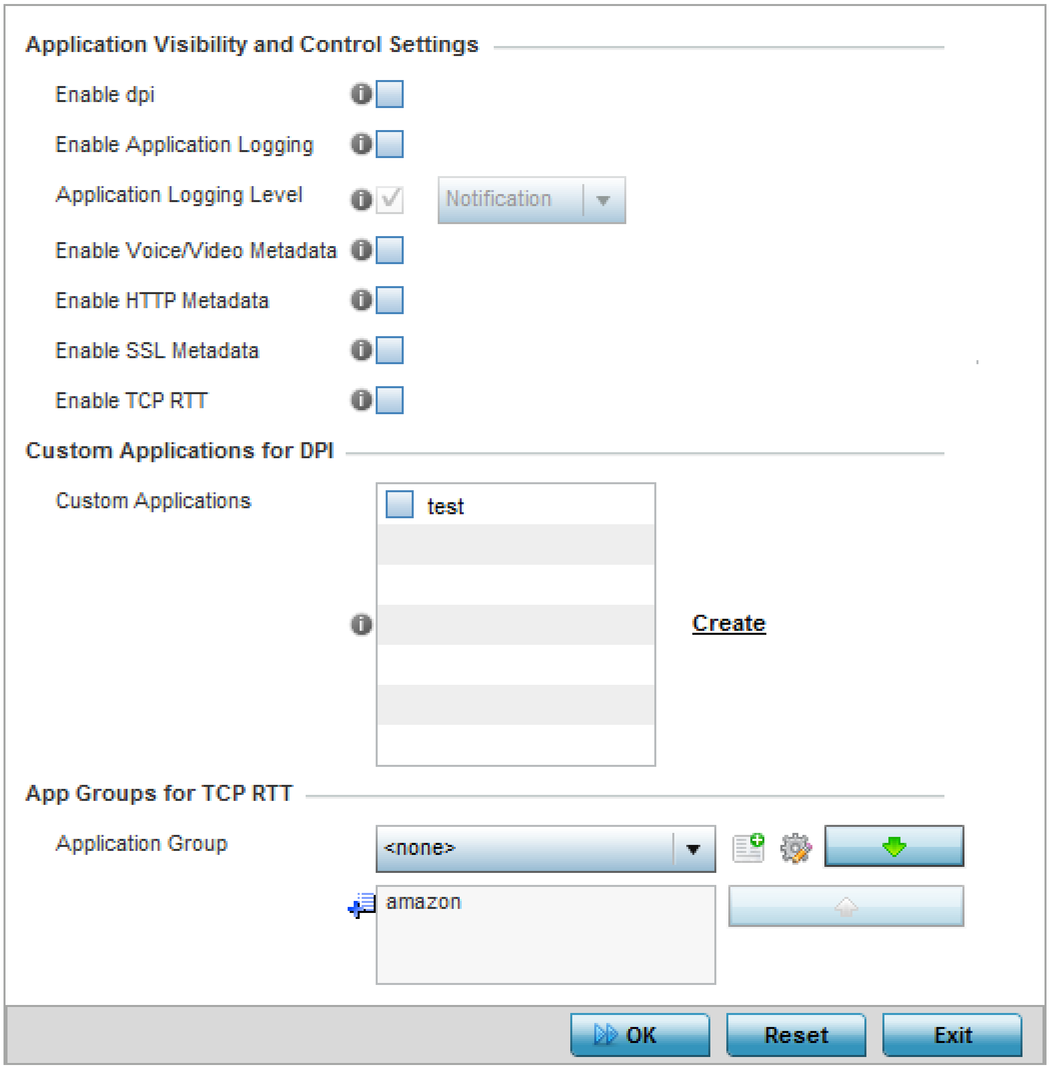
2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the Device Configuration screen.

The selected device's configuration menu displays in the right-hand UI.

3 Select **Profile Overrides** → **Security** → **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.


Application Visibility and Control Settings
Enable dpi ☐
Enable Application Logging ☐
Application Logging Level ☑ Notification
Enable Voice/Video Metadata ☐
Enable HTTP Metadata ☐
Enable SSL Metadata ☐
Enable TCP RTT ☐

Custom Applications for DPI
Custom Applications ☐ test

App Groups for TCP RTT
Application Group <none>
amazon

Figure 140: Profile Security - Application Visibility screen

4 Refer the following Application Visibility and Control settings:

Enable dpi	Enable this setting to provide deep-packet inspection. When enabled, network flows are inspected at a granular level to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.
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 509.
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 509.
7. Click **OK** to save the changes or overrides.

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

Overriding VRRP Configuration

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 **Configuration** → **Devices** from the web UI.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

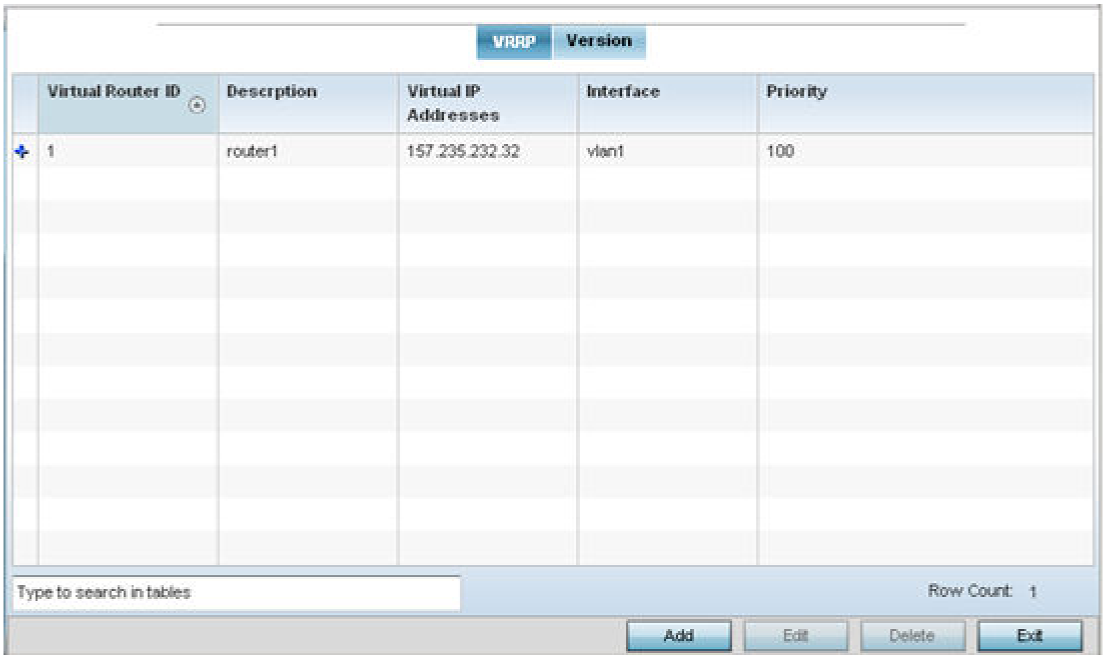
2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Profile Overrides**.

4 Select **VRRP**.

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.



	Virtual Router ID	Description	Virtual IP Addresses	Interface	Priority
✣	1	router1	157.235.232.32	vlan1	100

Row Count: 1

Figure 141: Device Overrides - VRRP Screen

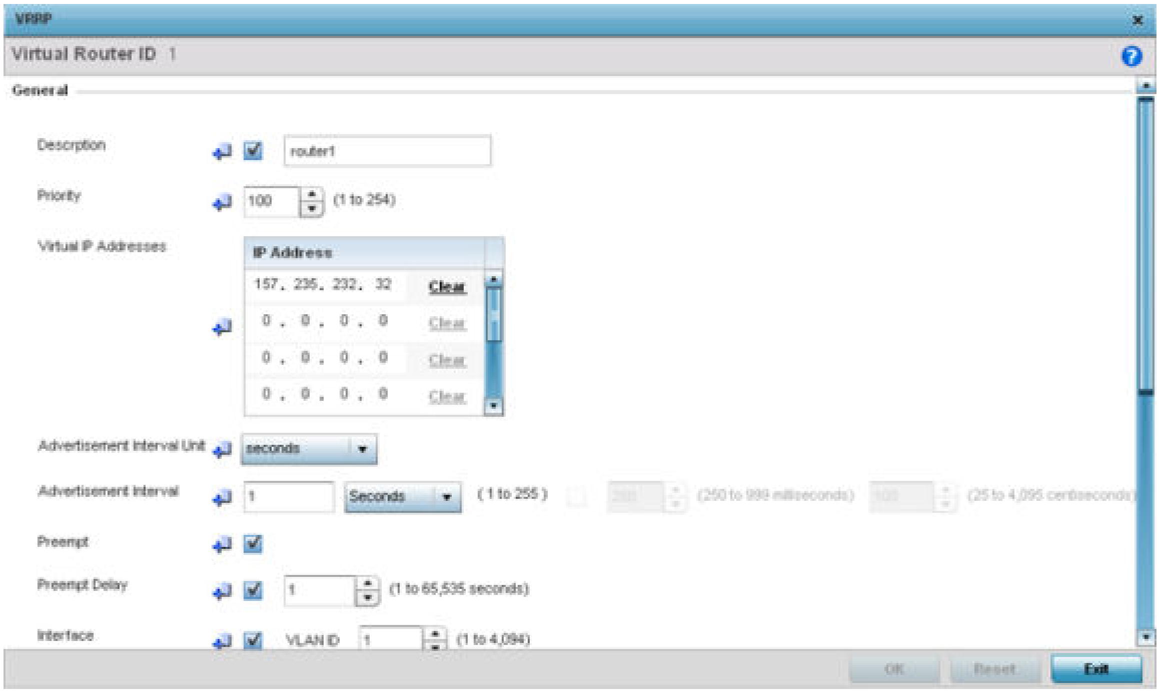
5 Review the following VRRP configuration data to assess whether a new VRRP configuration is required or whether an existing VRRP configuration can be modified or removed:

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.

6 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**.



Virtual Router ID 1

Description ☑ router1

Priority 100 (1 to 254)

Virtual IP Addresses

IP Address	
157. 235. 232. 32	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Advertisement Interval Unit seconds

Advertisement Interval 1 Seconds (1 to 255) ☐ 250 (250 to 999 milliseconds) 100 (25 to 4,095 centiseconds)

Preempt ☑

Preempt Delay ☑ 1 (1 to 65,535 seconds)

Interface ☑ VLAN ID 1 (1 to 4,094)

Figure 142: Device Overrides - VRRP - Virtual Router Screen

7 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.

8 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. 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.

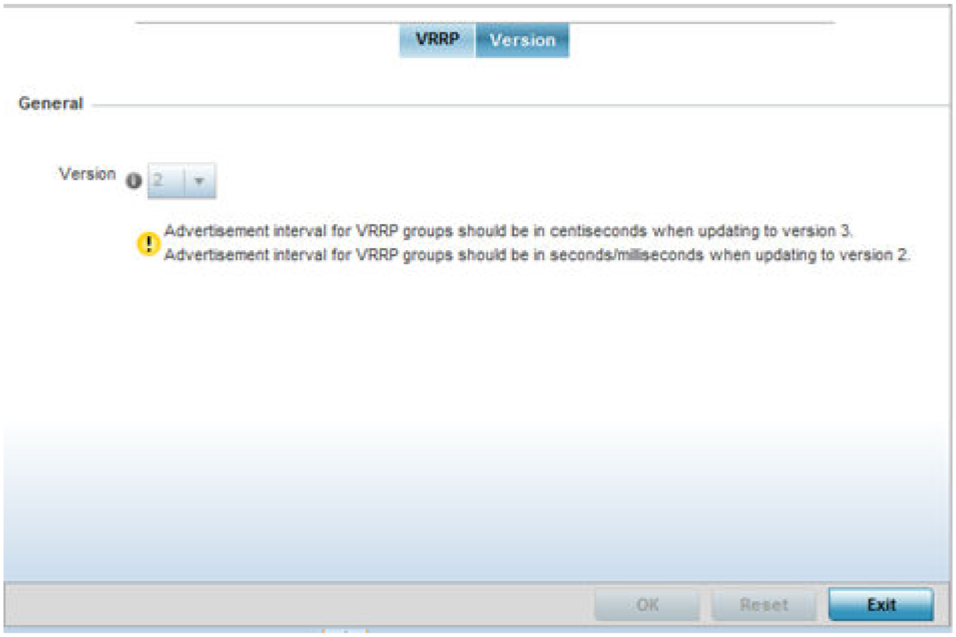
9 Refer to the Protocol Extension field to define the following:

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: Critical Resource Name	Select each critical resource needed for monitoring. The action specified in the **Critical Resource** drop-down menu is applied to each selected critical resource.
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.

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.



Advertisement interval for VRRP groups should be in centiseconds when updating to version 3.
Advertisement interval for VRRP groups should be in seconds/milliseconds when updating to version 2.

Figure 143: 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.

Overriding a Critical Resource Configuration

Critical resources are device IP addresses or interface destinations on the network interoperated 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** from the web UI.

   The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2. Select a target device in the lower left-hand side of the UI.

   You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3. Expand **Profile Overrides** and select **Critical Resources**.

   In the List of Critical Resources tab displays by default.

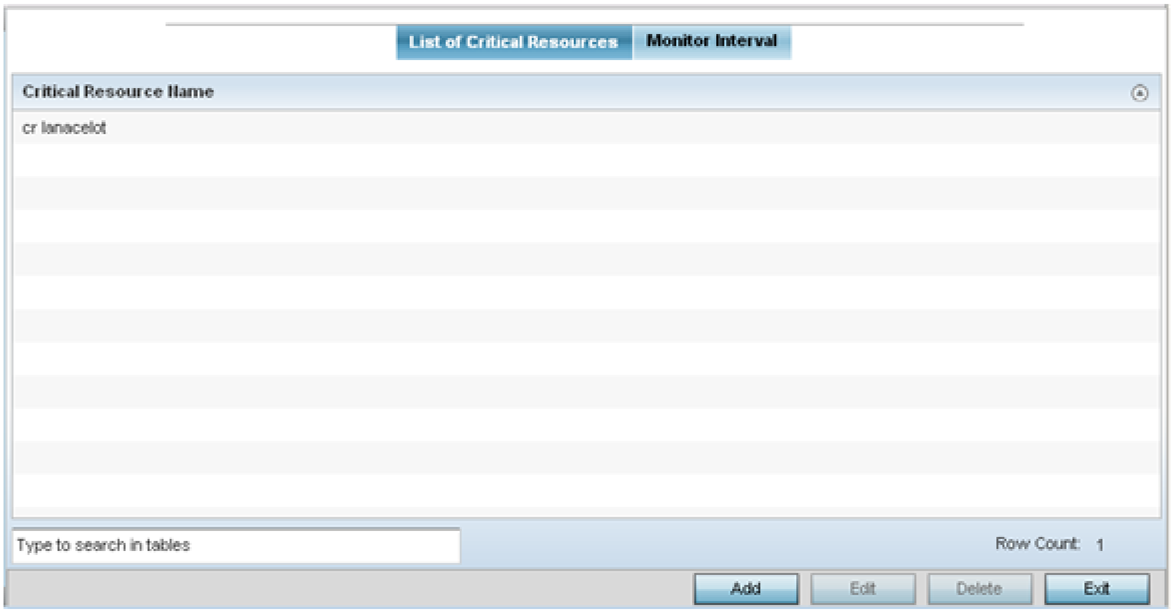


Figure 144: Device Overrides - Critical Resources Screen - List of Critical Resources Tab

   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 controller, service platform, or access point. However, a VLAN, WWAN, or PPPoE must be monitored behind an interface.

4. In the **Critical Resource Name** table, review the name of resources configured on this device.

5 Click **Add** to add a new critical resource and connection method.

Click **Edit** to modify or override the configuration for an existing critical resource.

If you are adding a new critical resource, assign it a name up to 32 characters.

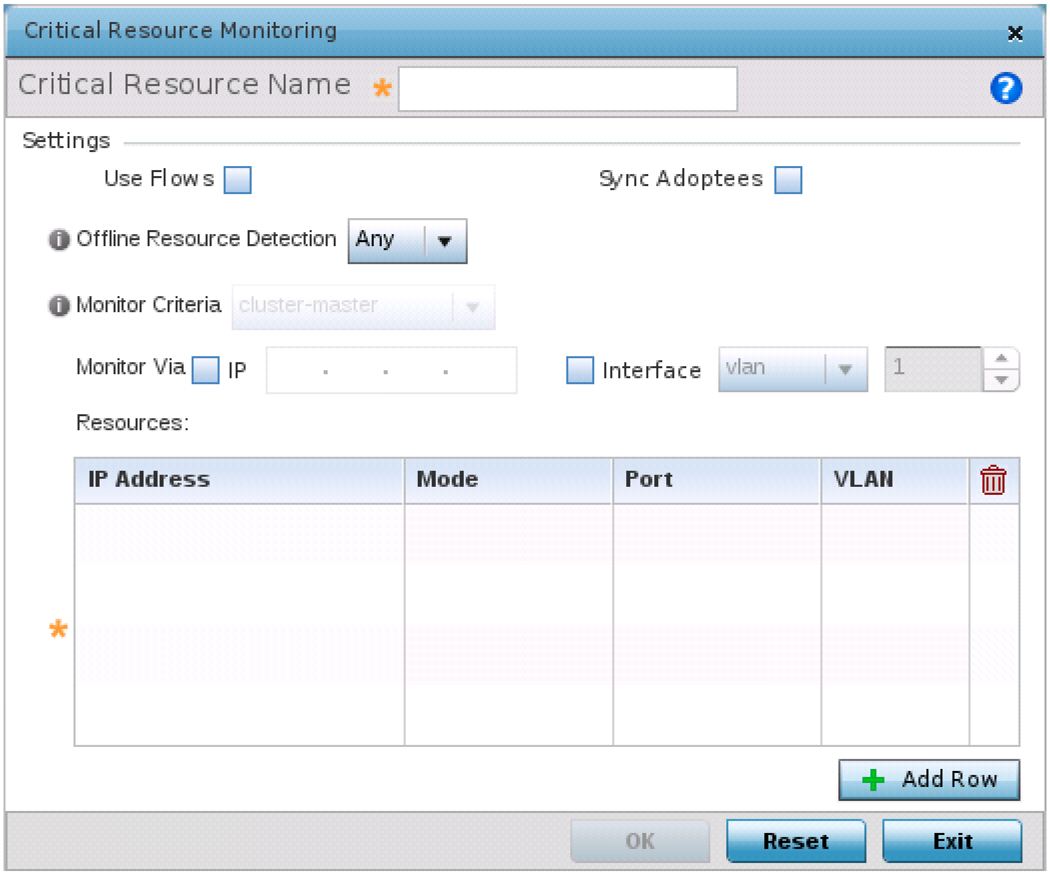


Figure 145: Critical Resources Screen - Adding a Critical Resource

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 at the top of the screen, 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 at the top of the screen, 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. Click **+ Add Row**, in the Resources table, to define the following critical resource configurations:

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. Select from: • **`arp-only`** – Use only the *Address Resolution Protocol* (ARP) for pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known. • **`arp-and-ping`** – Use both ARP and *Internet Control Message Protocol* (ICMP) for pinging the critical resource and sending control messages (for example, *device not reachable* or *requested service not available*).
Port	Define the interface on which to monitor critical resource. This field lists the available hardware interfaces. This option is available only when the selected mode is **`arp-only`**.
VLAN	Using the spinner control, define the VLAN on which the critical resource is available.

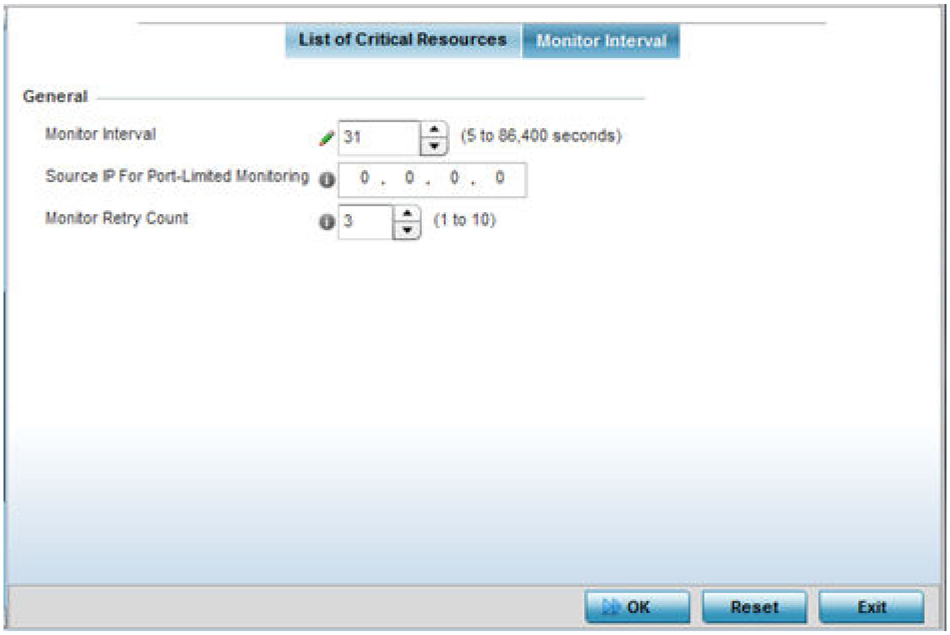
13. Click **OK** to save the changes to the critical resource configuration and monitor interval.

    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.



Monitor Interval 31 (5 to 86,400 seconds)

Source IP For Port-Limited Monitoring 0 . 0 . 0 . 0

Monitor Retry Count 3 (1 to 10)

Figure 146: 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.

Overriding a Services Configuration

A profile can contain specific guest access (captive portal), DHCP, server and RADIUS server configurations supported by the controller, service platform, or access point's own internal resources. These access, IP assignment, and user authorization resources can be defined uniquely as profile requirements dictate.

To define or override a profile's services configuration:

1 Select **Configuration** > **Devices** from the web UI.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

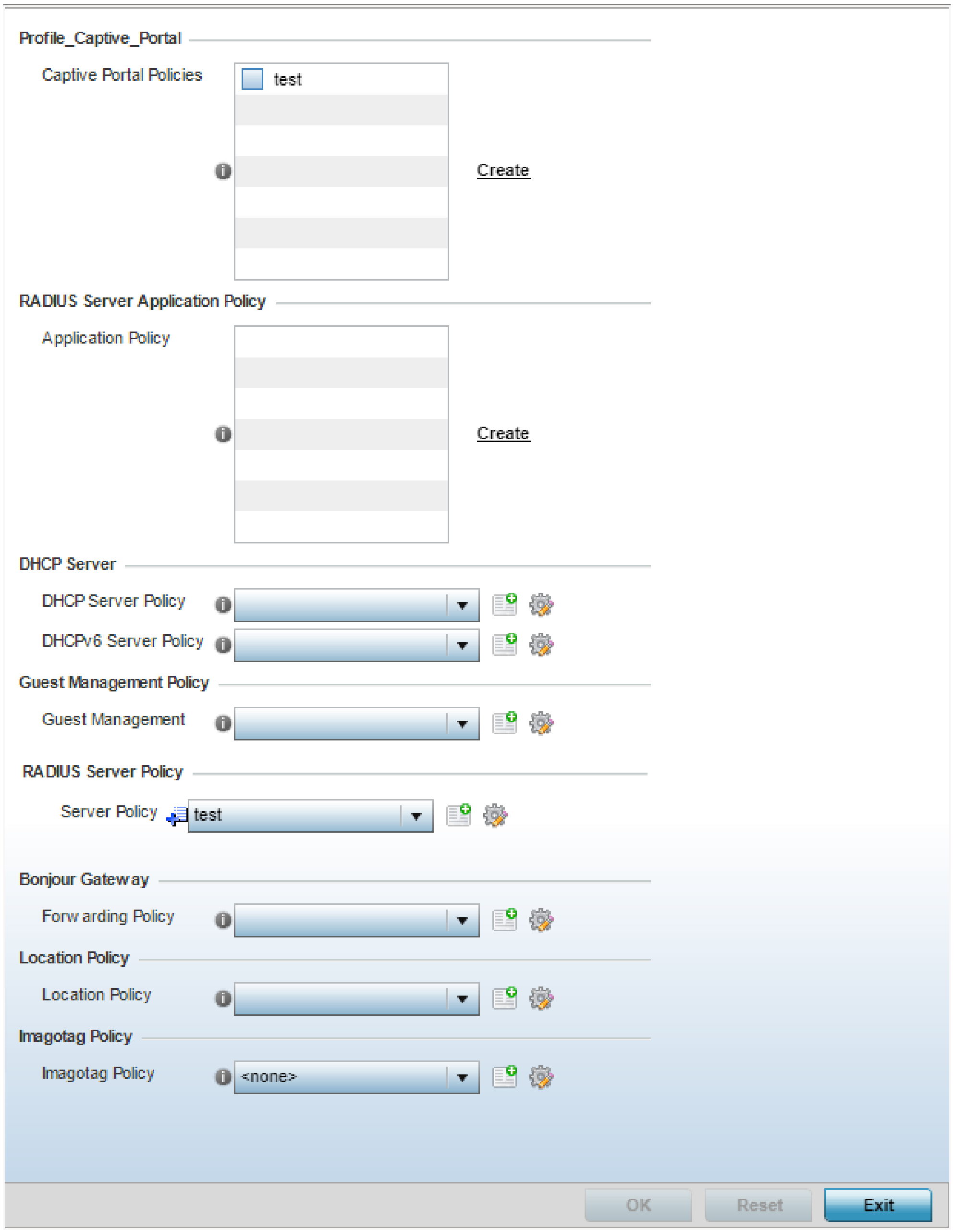
2 Select a target device in the lower left-hand side of the UI. The selected device's configuration menu displays.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Expand the **Profile Overrides** menu and select **Services**.

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.



Profile_Captive_Portal

Captive Portal Policies: ☐ test

RADIUS Server Application Policy

Application Policy

DHCP Server

DHCP Server Policy

DHCPv6 Server Policy

Guest Management Policy

Guest Management

RADIUS Server Policy

Server Policy: test

Bonjour Gateway

Forwarding Policy

Location Policy

Location Policy

Imagotag Policy

Imagotag Policy: <none>

Figure 147: Device Overrides - Services Screen

4. Refer to the **Captive Portal Hosting** field to set or override a guest access configuration (captive portal) for use with this profile.

   A *captive portal* is guest access policy for providing temporary and restrictive access to the wireless network.

   A captive portal configuration provides secure authenticated access using a standard Web browser. A captive portal provides authenticated access by capturing and re-directing a user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. After the administrator has logged into the captive portal, additional Agreement, Welcome, and Fail pages provide the administrator with several options for the captive portal's screen flow and user appearance.

   Select an existing captive portal policy, use the default captive portal policy, or click the **Create** link to create a new configuration that can be applied to this profile. For more information, see Captive Portal Policies on page 834.
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.

   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).
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.

   For more information, see Captive Portal Policy Basic Configuration on page 835.
8. Use the **Guest Management Policy** drop-down menu to select an existing Guest Management policy to use as a mechanism to manage guest users with this profile.

9 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. For more information, see RADIUS Server Policies on page 892.

10 Set **Bonjour Gateway** settings.

   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 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 only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

   From the **Forwarding Policy** drop-down menu, select the Bonjour Gateway forwarding policy.

11 Use the **Location Policy** drop-down menu to select and apply a location policy to the controller/ virtual controller. The location policy provides the ExtremeLocation server's hostname and ExtremeLocation tenant's location API key. This information is required by the controller to authenticate and authorize with the ExtremeLocation server. Use the **Create** or **Edit** icons to create a new policy or edit an existing policy.

   Note
   For information on creating location policies, see Location Policy on page 449.

12 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 or Edit icons to create a new policy or edit an existing policy. The Imagotag feature is supported only on the AP8432 model access point.

   For information on enabling support for SES-imagotag's ESL tags on WiNG APs with USB interfaces, seeSetting the Imagotag Policy on page 900.

13 Click **OK** to save the changes or overrides made to the profile's services configuration.

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

Overriding a Management Configuration

Controllers and service platforms have 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. In a clustered environment, these operations can be performed on one cluster member, then propagated to each member of the cluster and onwards to devices managed by each cluster member.

To define or override a profile's management configuration:

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

  The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.

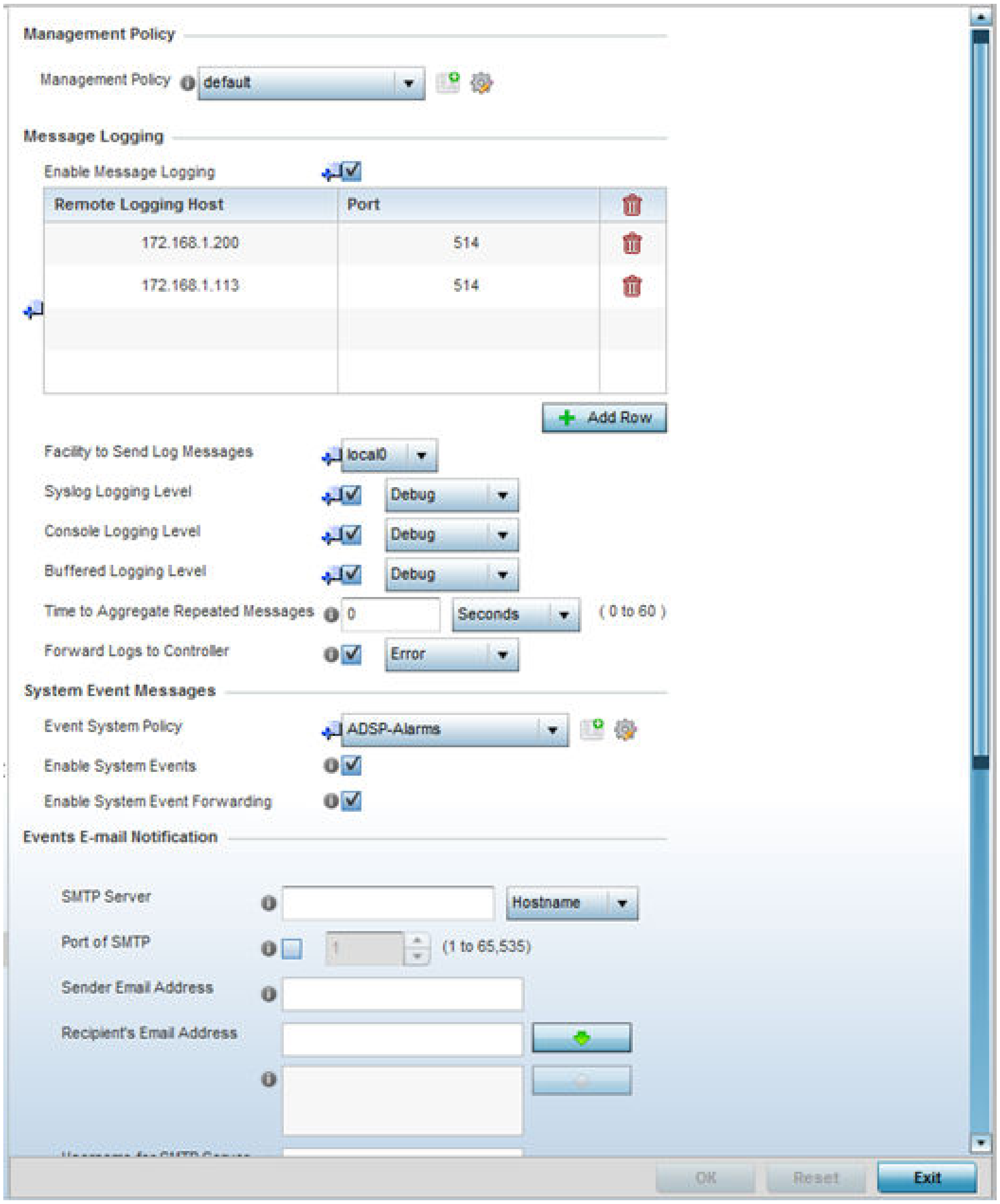
2 Select a target device in the lower left-hand side of the UI.

  You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

3 Go to **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.



Management Policy

Management Policy: default

Message Logging

Enable Message Logging ☑

Remote Logging Host	Port
172.168.1.200	514
172.168.1.113	514

Facility to Send Log Messages: local0

Syslog Logging Level ☑ Debug

Console Logging Level ☑ Debug

Buffered Logging Level ☑ Debug

Time to Aggregate Repeated Messages: 0 Seconds (0 to 60)

Forward Logs to Controller ☑ Error

System Event Messages

Event System Policy: ADSP-Alarms

Enable System Events ☑

Enable System Event Forwarding ☑

Events E-mail Notification

SMTP Server: Hostname

Port of SMTP ☐ 1 (1 to 65,535)

Sender Email Address

Recipient's Email Address

Figure 148: Device Overrides - Management Settings Screen

4 Refer to the **Management Policy** field to set or override a management configuration for this profile.

A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If there are no management policies that meet the data access requirements of this profile, click the **Create** icon to access screens used to define administration, access control, and SNMP configurations. Alternatively, select an existing policy and click the **Edit** icon to modify the configuration of an existing management policy. For more information, see Viewing Management Access Policies on page 904.

5 Refer to the Message Logging field to define how the profile logs system events.

It is important to log individual events to discern an overall pattern that might be negatively impacting performance.

Enable Message Logging	Select this option to enable the profile to log system events 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.
Remote Logging Host	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select the **Delete** icon as needed to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the local server (if used) for profile 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.
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.
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.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of the profile. 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.

6 Refer to the System Event Messages field to define or override how controller or service platform system messages are logged and forwarded on behalf of the profile.

   a Select an **Event System Policy** from the drop-down menu.

     If an appropriate policy does not exist, click **Create** to make a new policy.

   b 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 controller or service platform performance. This setting is enabled by default.

   c Select **Enable System Event Forwarding** to forward system events to another controller, service platform or cluster member.

     This setting is enabled by default.

7 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. Hostnames cannot include an underscore character.
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 up to 6 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.

8 In the **Persist Configuration Across Reloads** field, use the **Configure** drop-down menu to define whether configuration overrides should persist when the device configuration is reloaded.

  Options include **`Enabled`**, **`Disabled`**, and **`Secure`**.

9 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. This option is disabled by default.
Update Interval	Define an interval in either seconds (1 - 3,600), minutes (1 - 60), or hours (1) for pushing buffered packets. The default setting is 1 minute.

10 Refer to the External Analytics Engine section to define or override analytics engine login information for an external host.

  The Guest Access & Analytics software module is a site-wide Enterprise License available only on service platforms. When a customer visits a store, they connect to the Wireless LAN via guest access using a mobile device. The user needs to authenticate only on their first visit, and will automatically connect to the network for subsequent visits. The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors. The data can be exported for additional in-depth analysis.

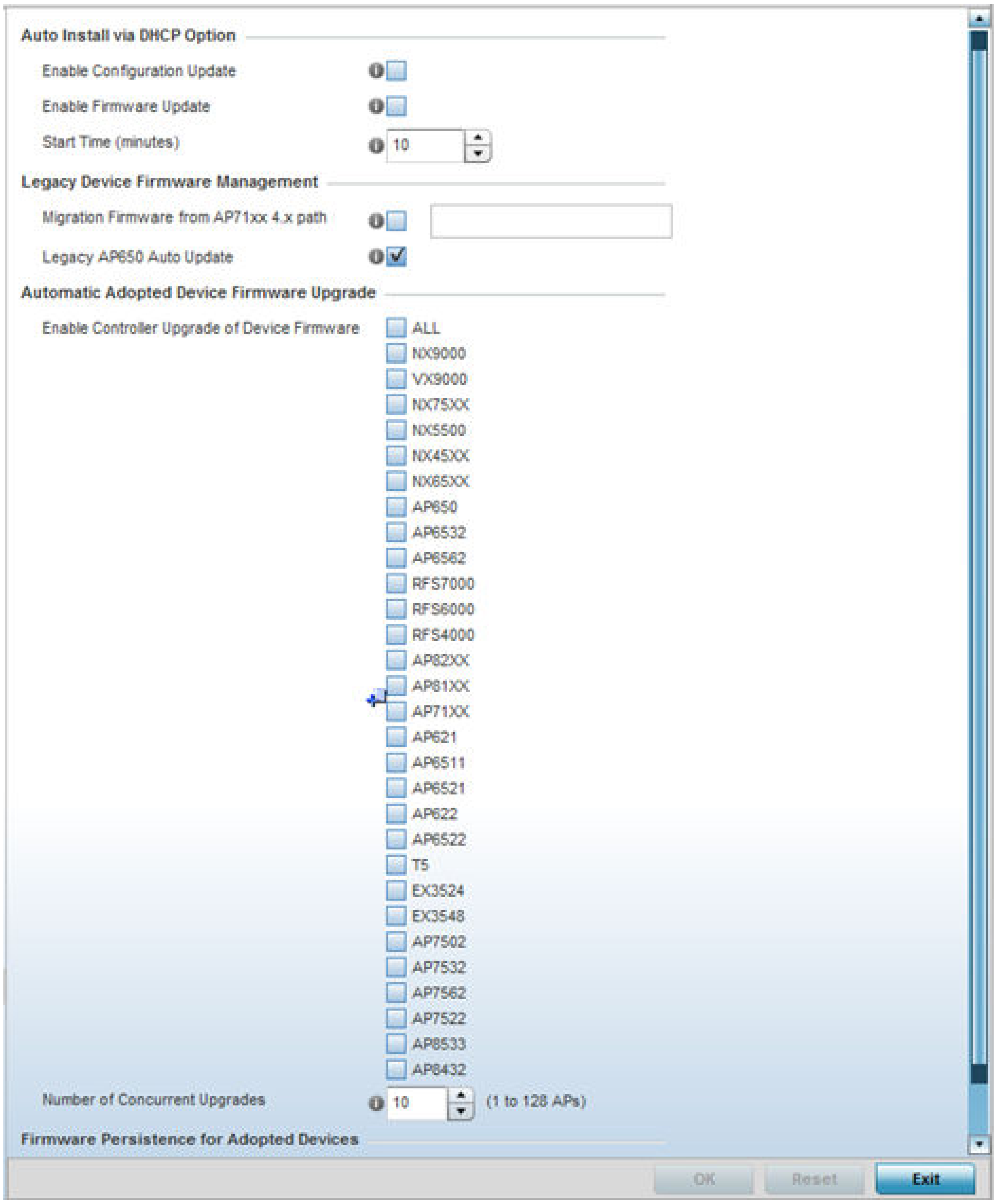
Controller	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
URL	When using an external analytics engine with an NX 9000 series service platform, enter the IP address or uniform resource locator (URL) for the system providing external analytics functions.
User Name	Enter the user name needed to access the external analytics engine.
Password	Enter the password associated with the username on the external analytics engine.
Update Interval	Set the interval in either seconds (1 - 3,600), minutes (1 - 60), or hours (1) to forward buffered information to an external server resource, even when the buffers are not full. The default setting is 1 minute.

11 Click **OK** to save the changes and overrides made to the profile’s management settings.

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

Firmware Configuration

1 Select the **Firmware** tab from the Management menu.



Auto Install via DHCP Option

Enable Configuration Update ☐

Enable Firmware Update ☐

Start Time (minutes) 10

Legacy Device Firmware Management

Migration Firmware from AP71xx 4.x path ☐

Legacy AP650 Auto Update ☑

Automatic Adopted Device Firmware Upgrade

Enable Controller Upgrade of Device Firmware
☐ ALL
☐ NX9000
☐ VX9000
☐ NX75XX
☐ NX5500
☐ NX45XX
☐ NX65XX
☐ AP650
☐ AP6532
☐ AP6562
☐ RFS7000
☐ RFS6000
☐ RFS4000
☐ AP82XX
☐ AP81XX
☐ AP71XX
☐ AP621
☐ AP6511
☐ AP6521
☐ AP622
☐ AP6522
☐ T5
☐ EX3524
☐ EX3548
☐ AP7502
☐ AP7532
☐ AP7562
☐ AP7522
☐ AP8533
☐ AP8432

Number of Concurrent Upgrades 10 (1 to 128 APs)

Figure 149: Profile Overrides - Management Firmware 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 from within the **Automatic Configuration Update** field to enable automatic profile configuration file updates from an external location. If this option is enabled (it is disabled by default), provide a complete path to the target configuration file used in the update.
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.
Start Time (minutes)	Set the number of minutes to delay the start of an auto upgrade operation. Stagger the start of an upgrade operation as needed in respect to allowing an access point to complete its current client support activity before being rendered offline during the update operation. The default setting is 10 minutes.

3 Refer to the parameters in the Legacy Device Firmware Management to set legacy access point firmware provisions:

Migration Firmware from AP71xx 4.x path	Provide a path to a firmware image used to provision AP71XX model access points currently using a 4.x version legacy firmware file. When a valid path is provided, the update is enabled to the version maintained locally for AP71XX models.
Legacy AP650 Auto Update	Select this option to provision AP650 model access points from their legacy firmware versions to the version maintained locally for that model. This setting is enabled by default, making updates to AP650 models automatic if a newer AP650 image is maintained locally.

4 Use the parameters in the Automatic Adopted AP Firmware Upgrade section to define an automatic firmware upgrade from a local file.

Enable Configuration Update of Device Firmware	Select the device model to upgrade using the most recent firmware file on the controller, service platform or Virtual Controller AP. This parameter is enabled by default. Select All to update all the listed device types.
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. The default value is 10. 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.

5. Select **Persist AP Images on Controller**, in the Firmware Persistence for Adopted Devices field, to enable the RF domain manager to retain and store the new image of an access point selected for a firmware update.

   The image is stored on the RF domain manager only when there is enough space to accommodate it. The upgrade sequence is different depending on whether the designated RF domain manager is a controller/service platform or an access point.

   - When the RF domain manager is an access point - The NOC uploads a provisions an access point model's firmware on to the access point RF domain manager. The NOC initiates an auto-update for access points using that model's firmware. If the **`Persist Image on Controller`** option is selected, the RF domain manager retains the image for that model. The NOC then provisions the firmware of the next access point type to the RF domain manager. The auto-update process is then repeated for that model. Once all the selected models have been updated, the RF domain manager's model is updated last.
   - When the RF domain manager is a controller or service platform - The NOC adopts controllers to the NOC's cluster within its RF domain. The NOC triggers an update on active controllers or service platforms and reboots them as soon as the update is complete. As soon as the active nodes come back u the NOC triggers an update on standby controllers or service platforms and reboots them as soon as the update is complete. When the standby controllers or service platforms come back up the following conditions apply:
     - If the reboot is not scheduled, the access points adopted to RF domain members are not updated. It is expected that the controllers and service platforms have auto-upgrade enabled which will update the access points when re-adopted.
     - If the reboot is scheduled, the NOC pushes the first access point model's firmware to the RF domain manager. The NOC initiates an access point upgrade on all access points on the RF domain manager for that model. If the **`Persist Image on Controller`** option is selected, the RF domain manager retains the image for that model. The NOC then provisions the firmware of the next access point type to the RF domain manager. This process is repeated until each selected access point model is updated.

   The Firmware Persistence feature is enabled for all controller and service platform RF domain managers with the flash memory capacity to store firmware images for the selected access point models they provision. This feature is disabled for access point RF Domain managers that do not typically have the flash memory capacity needed.

6. Click **OK** to save the changes and overrides made to the profile's management firmware configuration.

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

Heartbeat Configuration

1 Select **Heartbeat** from the Management menu.

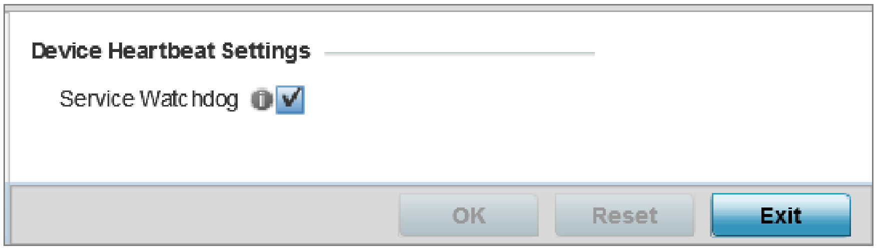


Figure 150: Device Overrides - Management Heartbeat Screen

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.

Mesh Point Configuration

Mesh points are access points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere, including moving vehicles.

To set or override a profile's mesh point configuration:

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

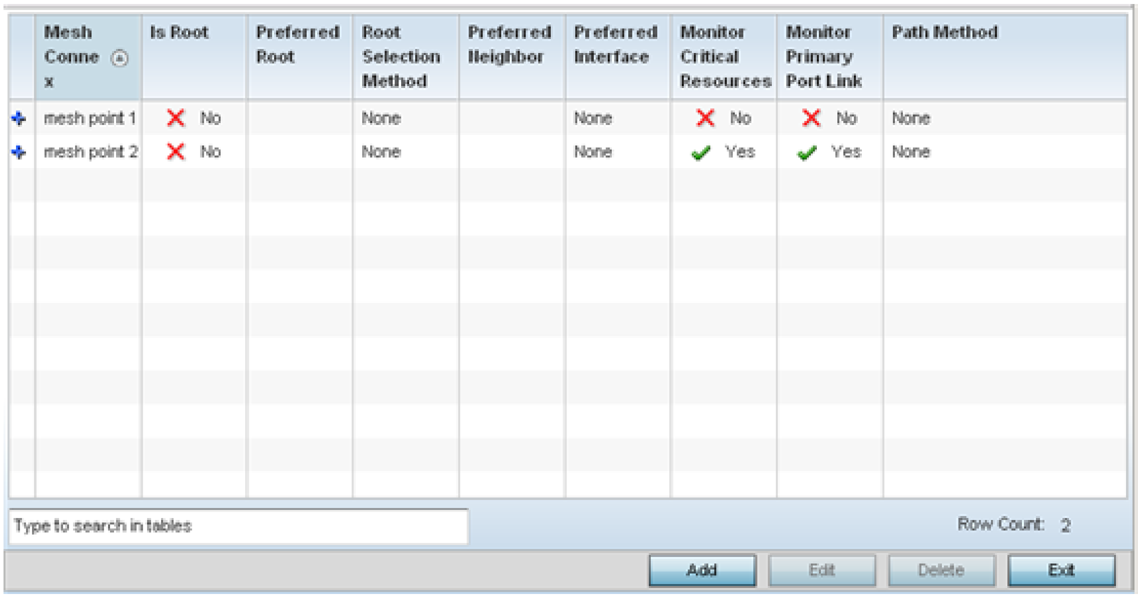
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms, or access points.

2 Select a device from those listed on the screen.

The selected Device's configuration menu displays.

3 Select **Mesh Point**.

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.



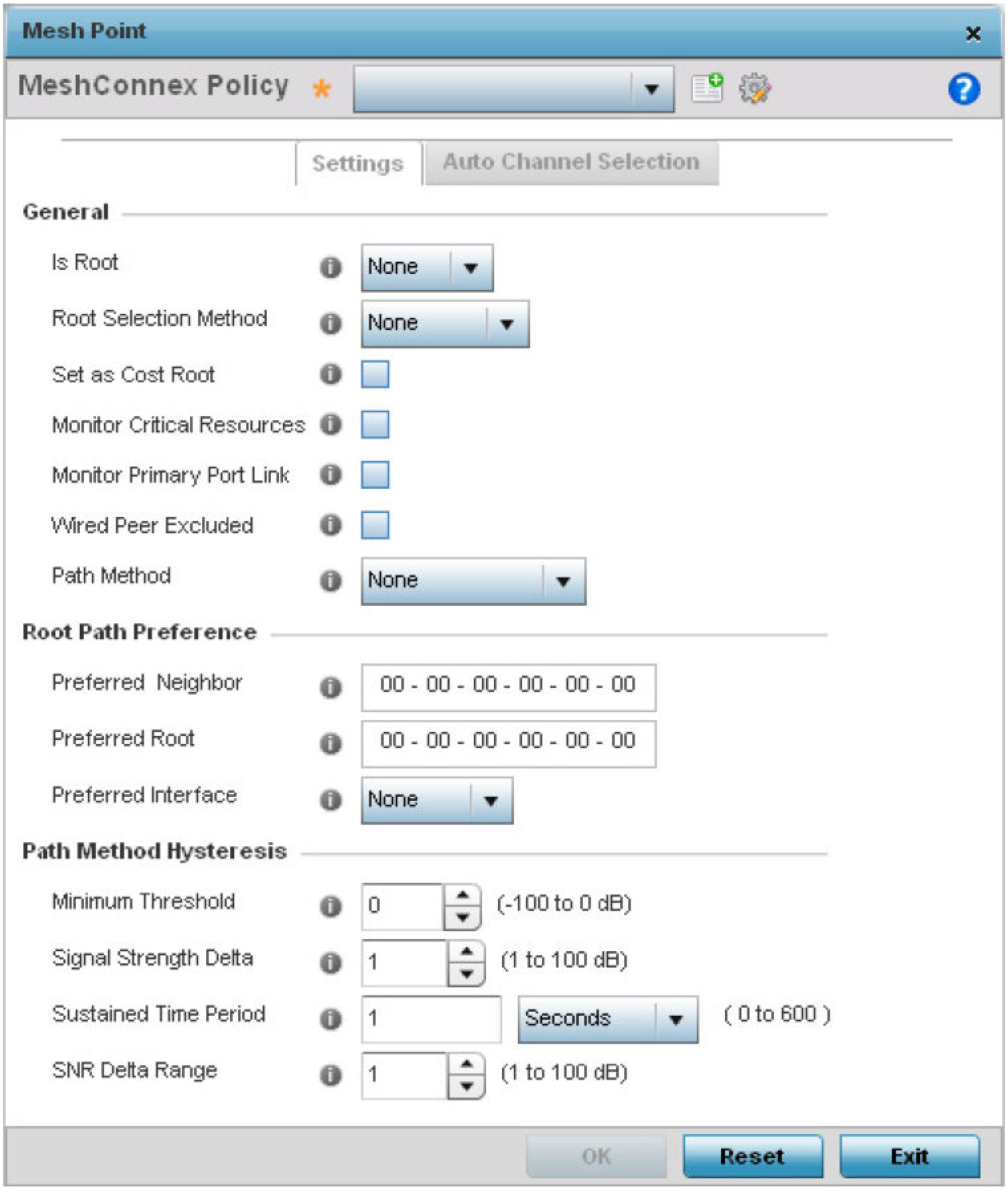
	Mesh Connex	Is Root	Preferred Root	Root Selection Method	Preferred Neighbor	Preferred Interface	Monitor Critical Resources	Monitor Primary Port Link	Path Method
✚	mesh point 1	✗ No		None		None	✗ No	✗ No	None
✚	mesh point 2	✗ No		None		None	✓ Yes	✓ Yes	None

Figure 151: Device Overrides - Mesh Point Screen

Refer to the Mesh Point screen to view existing Mesh Point overrides.

4 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**.



MeshConnex Policy *

General

Is Root: None
Root Selection Method: None
Set as Cost Root ☐
Monitor Critical Resources ☐
Monitor Primary Port Link ☐
Wired Peer Excluded ☐
Path Method: None

Root Path Preference

Preferred Neighbor: 00 - 00 - 00 - 00 - 00 - 00
Preferred Root: 00 - 00 - 00 - 00 - 00 - 00
Preferred Interface: None

Path Method Hysteresis

Minimum Threshold: 0 (-100 to 0 dB)
Signal Strength Delta: 1 (1 to 100 dB)
Sustained Time Period: 1 Seconds (0 to 600)
SNR Delta Range: 1 (1 to 100 dB)

Figure 152: Mesh Point Settings Screen

5 Define the following **General** mesh point settings:

MeshConnex Policy	If you are adding a new policy, specify a name for the MeshConnex Policy. The name cannot be edited later with other configuration parameters. Until a viable name is provided, the Settings tab cannot be enabled for configuration.
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.
Root Selection Method	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint. Select either **`None`**, **`auto-mint`** or **`auto-proximity`**. When *auto-mint* is selected, root selection is based on the total cost to the root. Cost to the root is measured as total cost through hops to the root node. Root selection occurs for the root with the least path cost. When *auto-proximity* is selected, root selection is based on signal strength of candidate roots. The option *None*, which is the default setting, indicates no preference in root selection.
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	Enable this feature to allow dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.
Monitor Primary Port Link	Enable this feature to allow dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.
Wired Peer Excluded	Select this option to exclude a mesh from forming a link with another mesh device that's a wired peer. This option is disabled by default.
Path Method	Select the method used for path selection in a mesh network. Available options include: • **`None`** – No criteria are used in root path selection. • **`uniform`** – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). • **`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 *Signal To Noise Ratio* (SNR) with the neighbor device. • **`snr-leaf`** – The path with the best signal to noise ratio is always selected. • **`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 312.

Note

When using 4.9GHz, the root preferences selection for the radio’s preferred interface still displays as 5GHz.

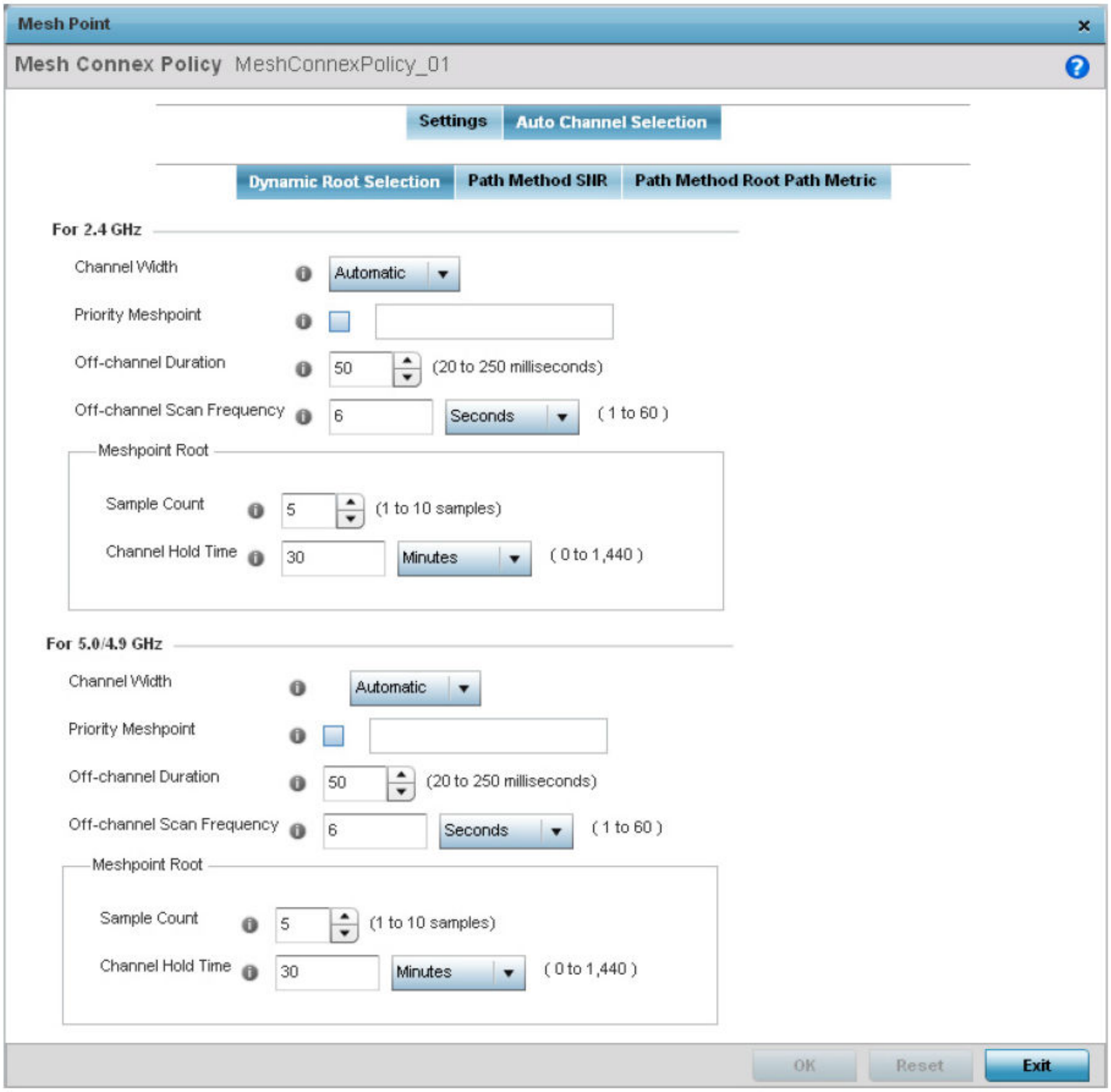
6 Set the following Root Path Preference values:

Preferred Neighbor	Specify the MAC address of a preferred neighbor to override mesh point settings.
Preferred Root	Specify the MAC address of a preferred root device to override mesh point settings.
Preferred Interface	Use the drop-down menu to override the preferred mesh point interface to 2.4GHz, 4.9 GHz or 5.0GHz. **None** defines the interface as open to any radio band.

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 the **Auto Channel Selection** tab to configure the parameters for the MeshConnex Auto Channel Selection policy.



Mesh Connex Policy MeshConnexPolicy_01

For 2.4 GHz
Channel Width: Automatic
Priority Meshpoint: ☐
Off-channel Duration: 50 (20 to 250 milliseconds)
Off-channel Scan Frequency: 6 Seconds (1 to 60)
Meshpoint Root
Sample Count: 5 (1 to 10 samples)
Channel Hold Time: 30 Minutes (0 to 1,440)

For 5.0/4.9 GHz
Channel Width: Automatic
Priority Meshpoint: ☐
Off-channel Duration: 50 (20 to 250 milliseconds)
Off-channel Scan Frequency: 6 Seconds (1 to 60)
Meshpoint Root
Sample Count: 5 (1 to 10 samples)
Channel Hold Time: 30 Minutes (0 to 1,440)

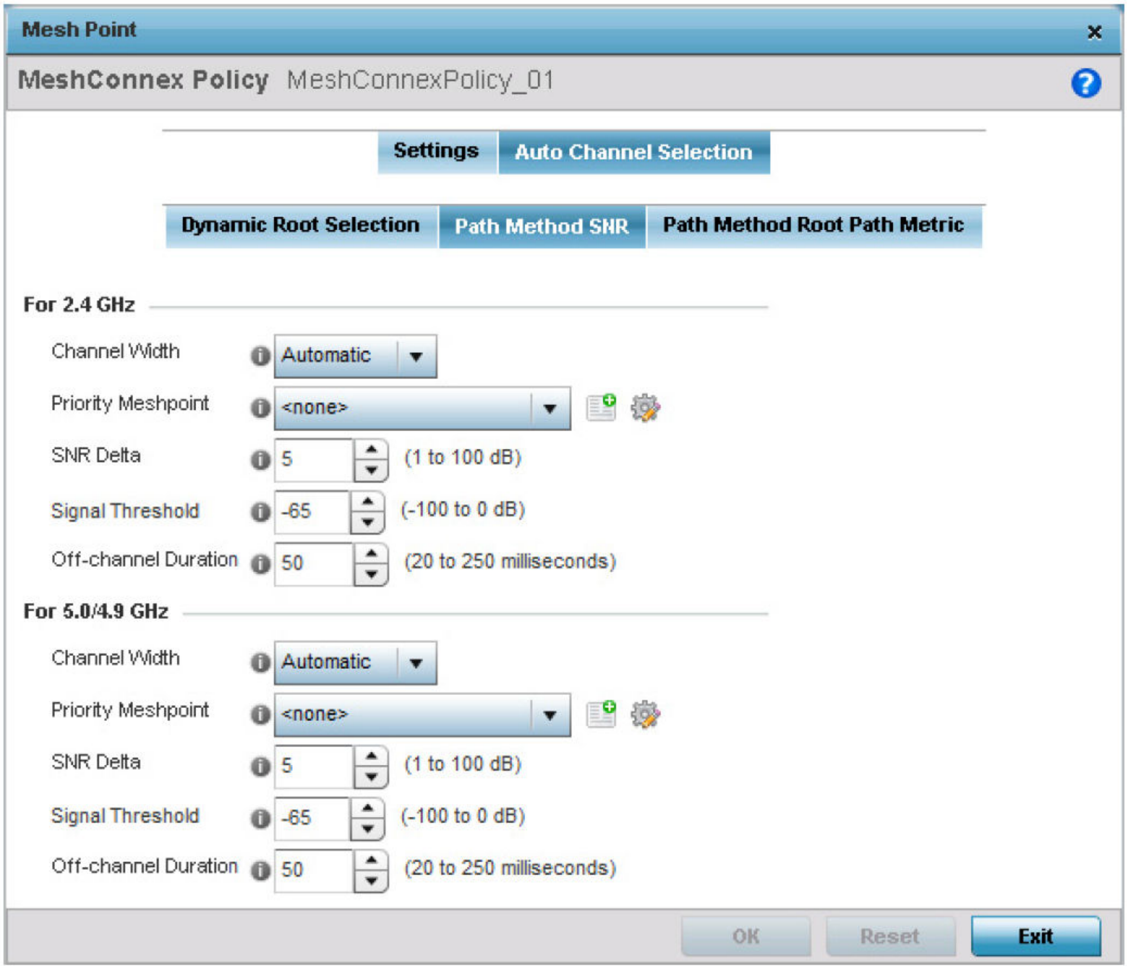
Figure 153: Mesh Point Auto Channel Selection Screen - Dynamic Root Selection Tab

The Dynamic Root Selection screen displays by default. This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies.

9 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: • **`Automatic`** – The channel width is calculated automatically. This is the default value. • **`20 MHz`** – Sets the width between adjacent channels as 20 MHz. • **`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.

10 Select the **Path Method SNR** tab to configure SNR ratio values when selecting the path to the meshpoint root.



For 2.4 GHz

Channel Width: Automatic
Priority Meshpoint: <none>
SNR Delta: 5 (1 to 100 dB)
Signal Threshold: -65 (-100 to 0 dB)
Off-channel Duration: 50 (20 to 250 milliseconds)

For 5.0/4.9 GHz

Channel Width: Automatic
Priority Meshpoint: <none>
SNR Delta: 5 (1 to 100 dB)
Signal Threshold: -65 (-100 to 0 dB)
Off-channel Duration: 50 (20 to 250 milliseconds)

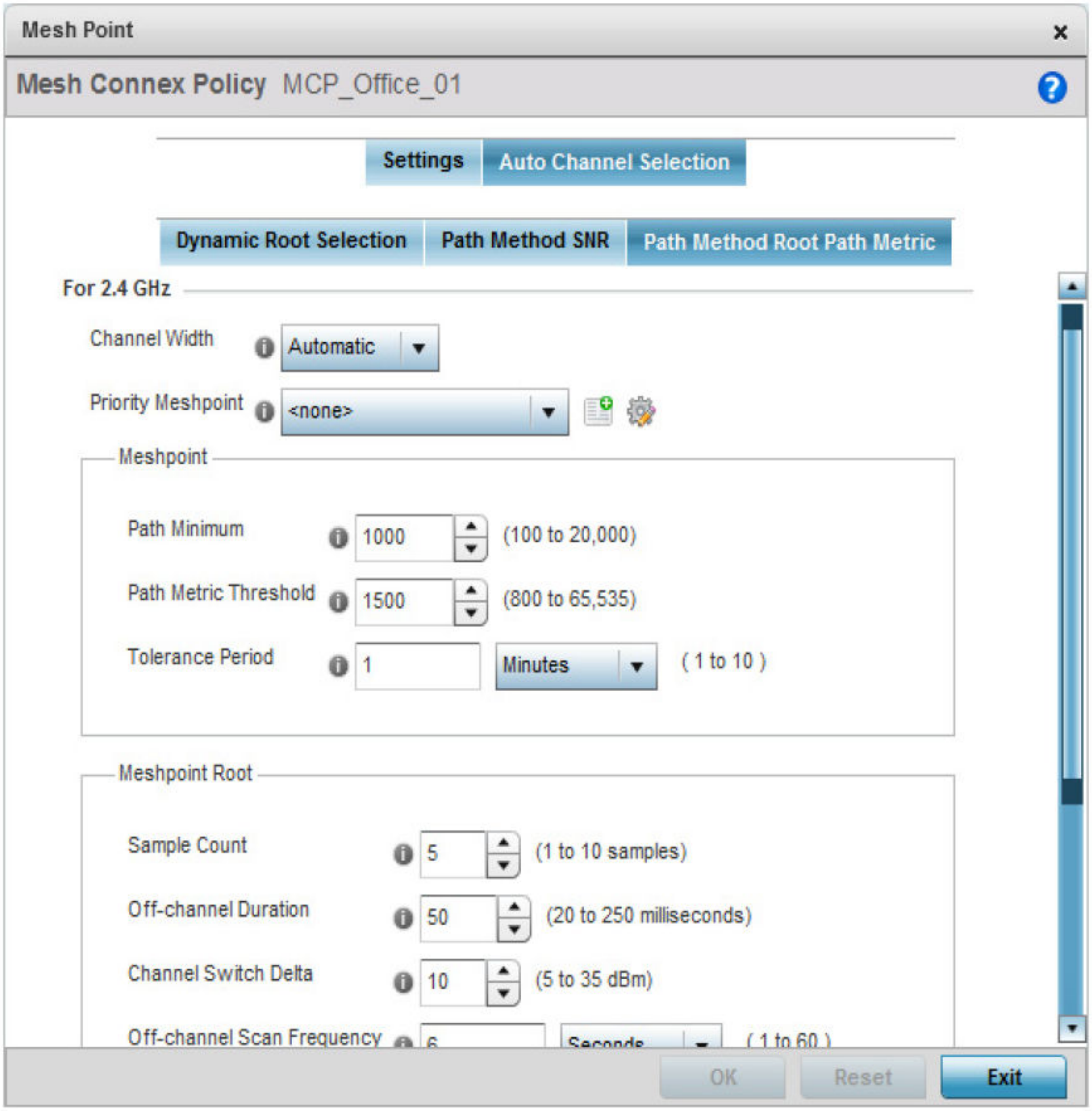
Figure 154: Mesh Point Auto Channel Selection Screen - Path Method SNR Tab

11 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: • `Automatic` – The channel width is calculated automatically. This is the default value. • `20 MHz` – Sets the width between adjacent channels as 20 MHz. • `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. 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). 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.

12 Select the **Path Method Root Path Metric** tab to calculate root path metrics.



For 2.4 GHz

Channel Width: Automatic

Priority Meshpoint: <none>

Meshpoint

Path Minimum: 1000 (100 to 20,000)

Path Metric Threshold: 1500 (800 to 65,535)

Tolerance Period: 1 Minutes (1 to 10)

Meshpoint Root

Sample Count: 5 (1 to 10 samples)

Off-channel Duration: 50 (20 to 250 milliseconds)

Channel Switch Delta: 10 (5 to 35 dBm)

Off-channel Scan Frequency: 6 Seconds (1 to 60)

Figure 155: Mesh Point Auto Channel Selection Screen - Path Method Root Path Metric Tab

13 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: • **`Automatic`** – The channel width is calculated automatically. This is the default value. • **`20 MHz`** – Sets the width between adjacent channels as 20 MHz. • **`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.

14 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 580.
- Use **`Opportunistic`** as the rate selection settings for the AP 7161 radio The default is **`Standard`**. For more information on defining this setting, see Radio Override Configuration on page 139.
- 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 Radio Override Configuration on page 139).

- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see Radio Override Configuration on page 139.
- Set a misconfiguration recovery time for the non-root AP profile. This configuration should delay the rejection of the newest configuration push from the controller, potentially causing adoption loss.

  The additional delay is to support cases when the new configuration from the controller causes the root AP to move from current channel to other channels, resulting in a mesh link going down, and in turn non-root APs losing adoption. This delay accommodates the time needed for the non-root AP to scan all channels and finding the best root node. The non-root AP can begin operating on the new channel, and establish the mesh link re-adopt to the controller. (For countries using DFS, the scan time is also factored in for the configured value). If the AP fails to find a suitable root node within this time, this new config is a misconfigured and the device would reject the latest config.

  For outdoor APs, it is recommended the misconfiguration-recovery-time be disabled. This can be accomplished by setting the value to 0. Update non root ap71xx profiles on the controller to include this change.

  Using an appropriate console terminal and or connection to your device log on to the CLI and follow these steps:

  ```
  rfs6000-xxxxxx>enable
  rfs6000-xxxxxx #configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  rfs6000-xxxxxx (config)#profile ap71xx Non-Root-AP71xx
  rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#misconfiguration-recovery-time 0
  rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#
  ```

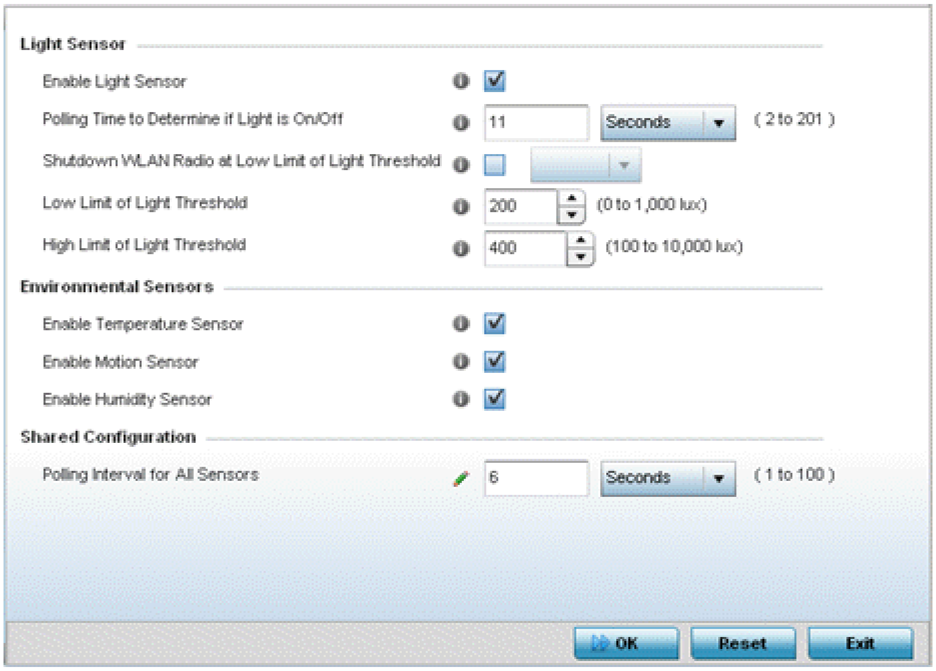
Overriding an Environmental Sensor Configuration (AP8132 Only)

A 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 access point's radio coverage area. The output of the sensor's detection mechanisms are viewable using the Environmental Sensor screen.

To set or override an environmental sensor configuration for an AP 8132 model access point:

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

2 Select **Environmental Sensor**.



Light Sensor

Enable Light Sensor ☑

Polling Time to Determine if Light is On/Off 11 Seconds (2 to 201)

Shutdown WLAN Radio at Low Limit of Light Threshold ☐

Low Limit of Light Threshold 200 (0 to 1,000 lux)

High Limit of Light Threshold 400 (100 to 10,000 lux)

Environmental Sensors

Enable Temperature Sensor ☑

Enable Motion Sensor ☑

Enable Humidity Sensor ☑

Shared Configuration

Polling Interval for All Sensors 6 Seconds (1 to 100)

Figure 156: Profile Overrides - Environmental Sensor Screen

3 Override or set the following **Light Sensor** settings for the AP 8132 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 access point'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 assess light intensity in its environment 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 access point's radios when the light intensity falls below the set threshold. 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 access point's location. In daytime, the light sensor's value is between 350-450. The default value for the low threshold is 200 – that is, the radios are turned off when the average reading value is lower than 200 lux.
High Limit of Light Threshold	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the access point's location. The default high threshold is 400 – that is, the radios are turned on when the average value is higher than 400 lux.

4 Enable or disable the following 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 (in 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 (in 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 (in the Statistics node). This setting is enabled by default.

5 In Shared Configuration, set the interval in either seconds (1 - 100) or minutes (1 - 2) between environmental polling transmissions (both light and environment).

The default setting is 5 seconds.

6 Click **OK** to save the changes made to the Environmental Sensor screen.

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.

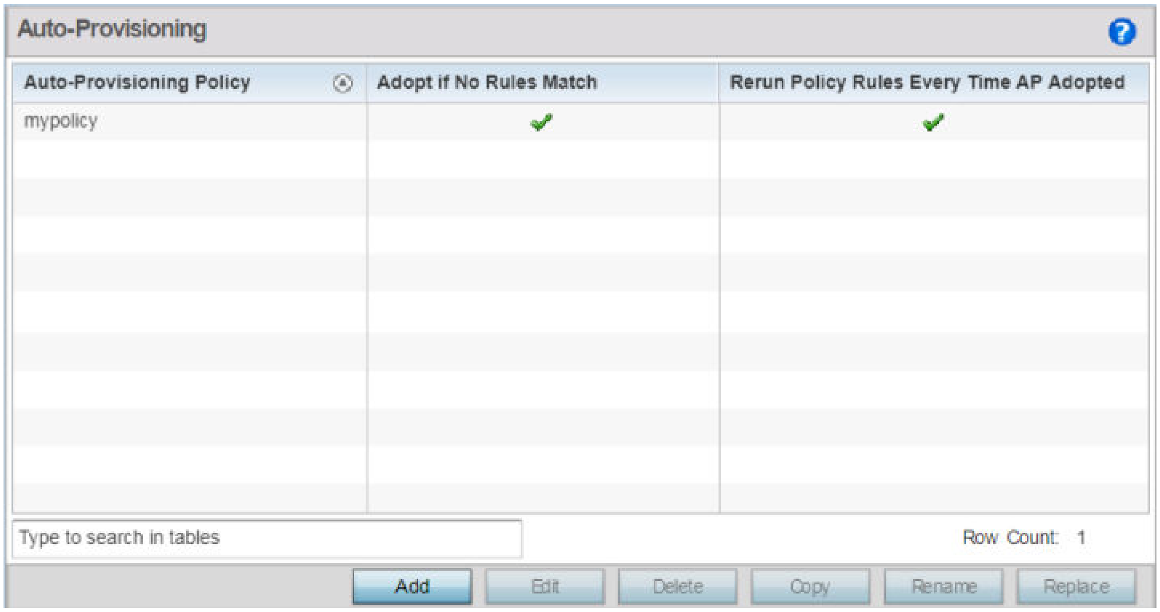


Figure 157: Auto-Provisioning Policy Screen

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.

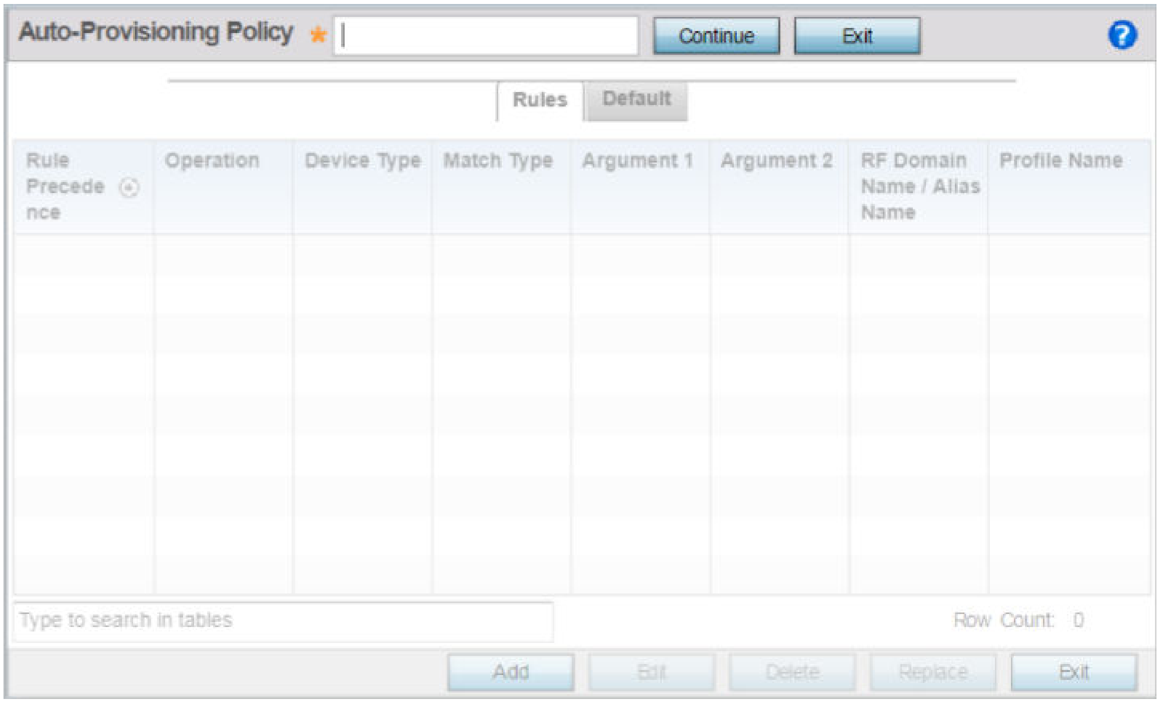


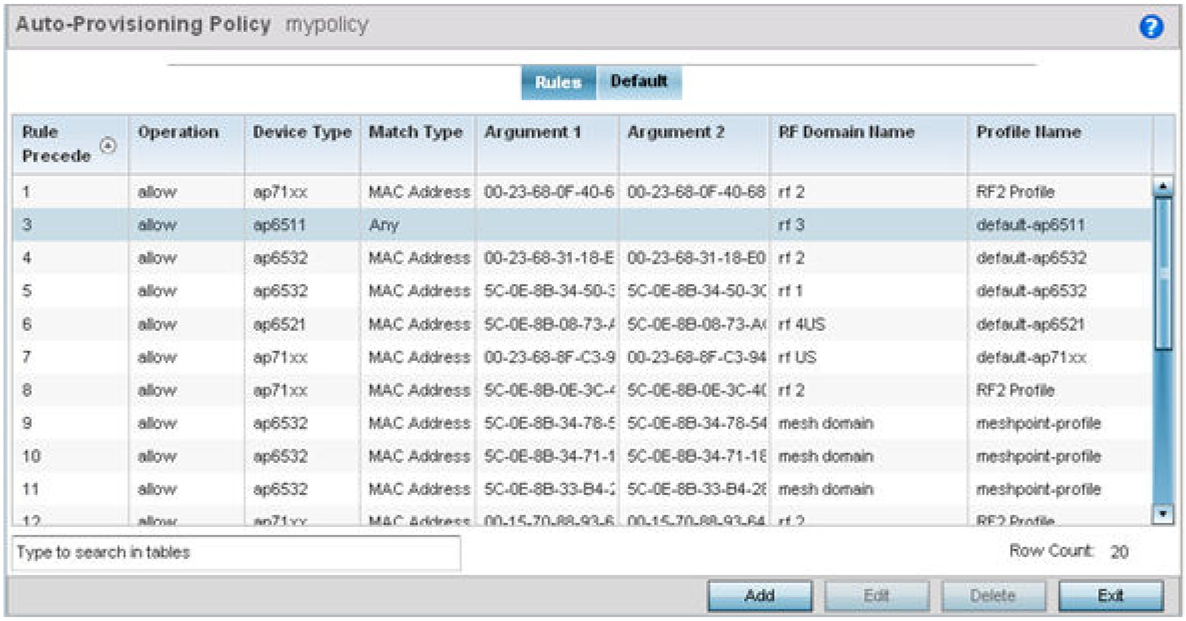
Figure 158: Auto-Provisioning Policy - Add New Policy Screen

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.



Rule Precede	Operation	Device Type	Match Type	Argument 1	Argument 2	RF Domain Name	Profile Name
1	allow	ap71xx	MAC Address	00-23-68-0F-40-6	00-23-68-0F-40-68	rf 2	RF2 Profile
3	allow	ap6511	Any			rf 3	default-ap6511
4	allow	ap6532	MAC Address	00-23-68-31-18-E	00-23-68-31-18-E0	rf 2	default-ap6532
5	allow	ap6532	MAC Address	5C-0E-8B-34-50-	5C-0E-8B-34-50-3	rf 1	default-ap6532
6	allow	ap6521	MAC Address	5C-0E-8B-08-73-	5C-0E-8B-08-73-A	rf 4US	default-ap6521
7	allow	ap71xx	MAC Address	00-23-68-8F-C3-9	00-23-68-8F-C3-94	rf US	default-ap71xx
8	allow	ap71xx	MAC Address	5C-0E-8B-0E-3C-	5C-0E-8B-0E-3C-4	rf 2	RF2 Profile
9	allow	ap6532	MAC Address	5C-0E-8B-34-78-	5C-0E-8B-34-78-54	mesh domain	meshpoint-profile
10	allow	ap6532	MAC Address	5C-0E-8B-34-71-1	5C-0E-8B-34-71-1	mesh domain	meshpoint-profile
11	allow	ap6532	MAC Address	5C-0E-8B-33-B4-	5C-0E-8B-33-B4-2	mesh domain	meshpoint-profile
12	allow	ap71xx	MAC Address	00-15-70-88-93-6	00-15-70-88-93-64	rf 2	RF2 Profile

Row Count: 20

Figure 159: 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: • allow – Allows the normal provisioning of connected access points upon request. • deny – Denies (prohibits) the provisioning of connected access point upon request. • 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. • 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: • MAC Address – The filter type is a MAC Address of the selected access point model. • IP Address – The filter type is the IP address of the selected access point model. • VLAN – The filter type is a VLAN. • Serial Number – The filter type is the serial number of the selected access point model. • Model Number – The filter type is the access point model number. • 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. For more information, see General Profile Configuration on page 531.

5 Click **Add** to add a new rule. The Rule screen displays.

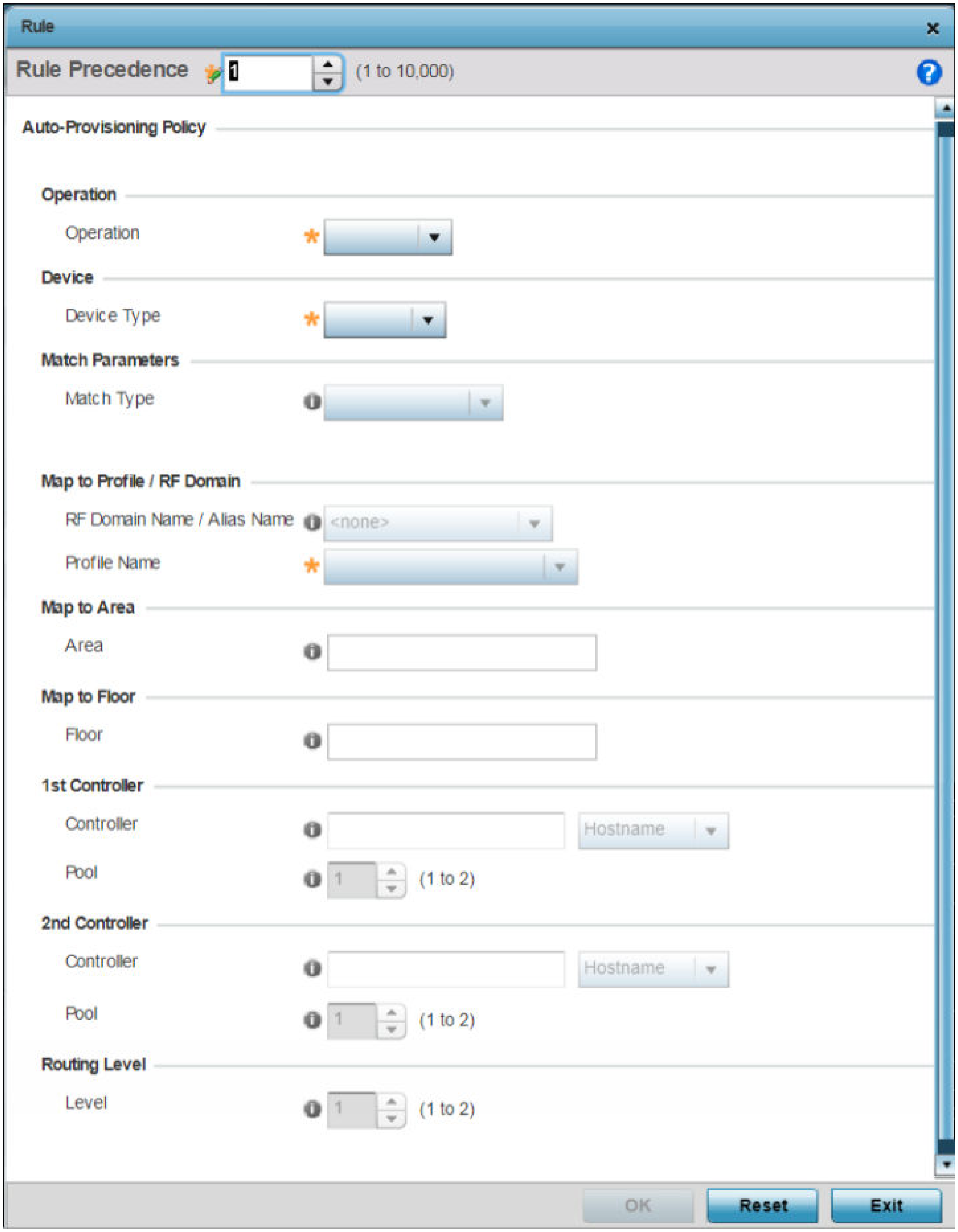


Figure 160: Auto Provisioning Policy - Add / Edit Rule Screen

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: • allow – Allows the normal provisioning of connected access points upon request. • deny – Denies (prohibits) the provisioning of connected access point upon request. • 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. • 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: • MAC Address – The filter type is a MAC Address of the selected access point model. • IP Address – The filter type is the IP address of the selected access point model. • VLAN – The filter type is a VLAN. • Serial Number – The filter type is the serial number of the selected access point model. • Model Number – The filter type is the access point model number. • 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 498. Select the **Create** icon to define a new RF Domain configuration or select the **Edit** icon to revise an existing configuration. For more information, see Managing RF Domains on page 748.
Profile Name	Define the profile used when an auto-provisioning policy is applied to a device. Select the **Create** icon to define a new Profile configuration or select the **Edit** icon to revise an existing configuration. For more information, see General Profile Configuration on page 531.
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.

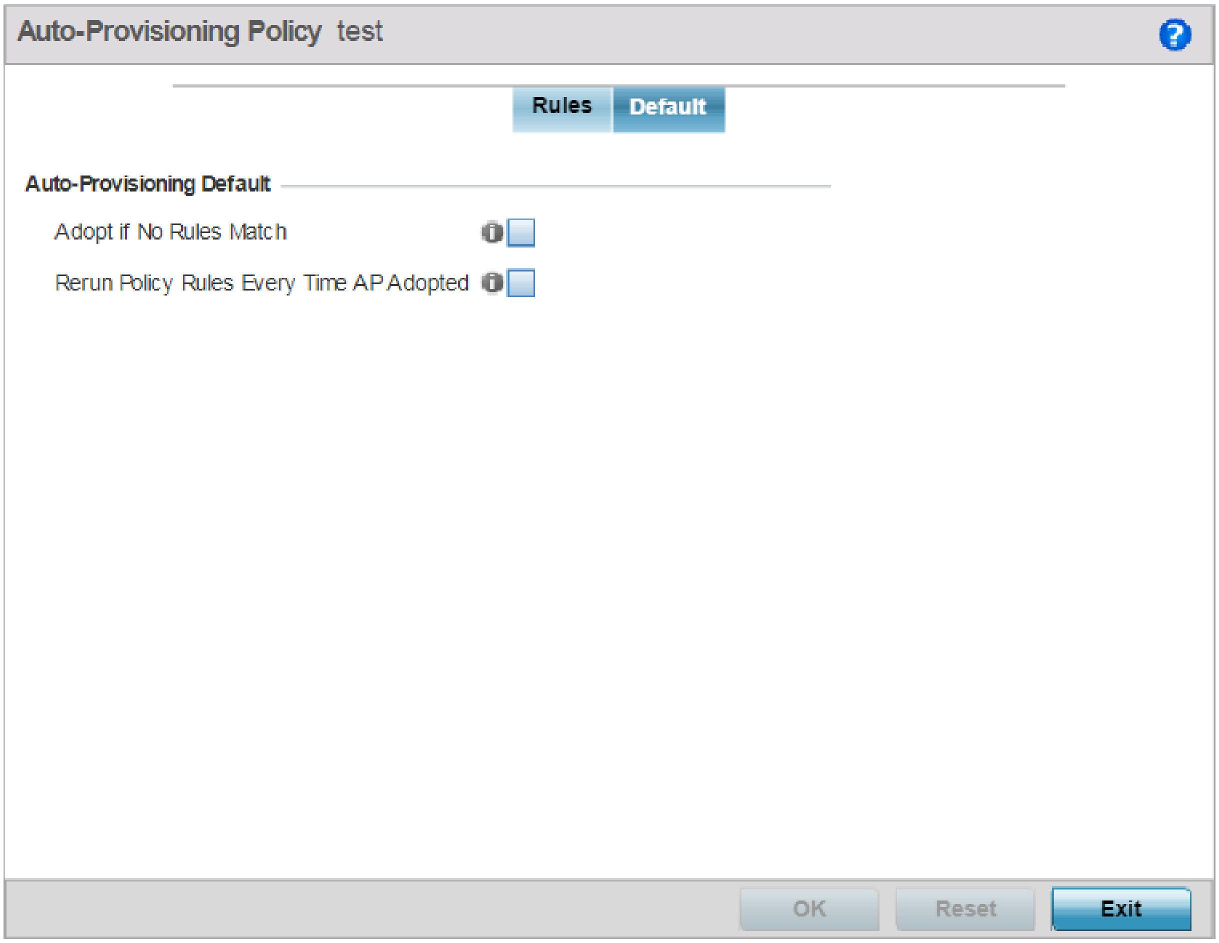

Auto-Provisioning Policy test
Rules
Default
Auto-Provisioning Default
Adopt if No Rules Match
Rerun Policy Rules Every Time AP Adopted
OK
Reset
Exit

Figure 161: 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

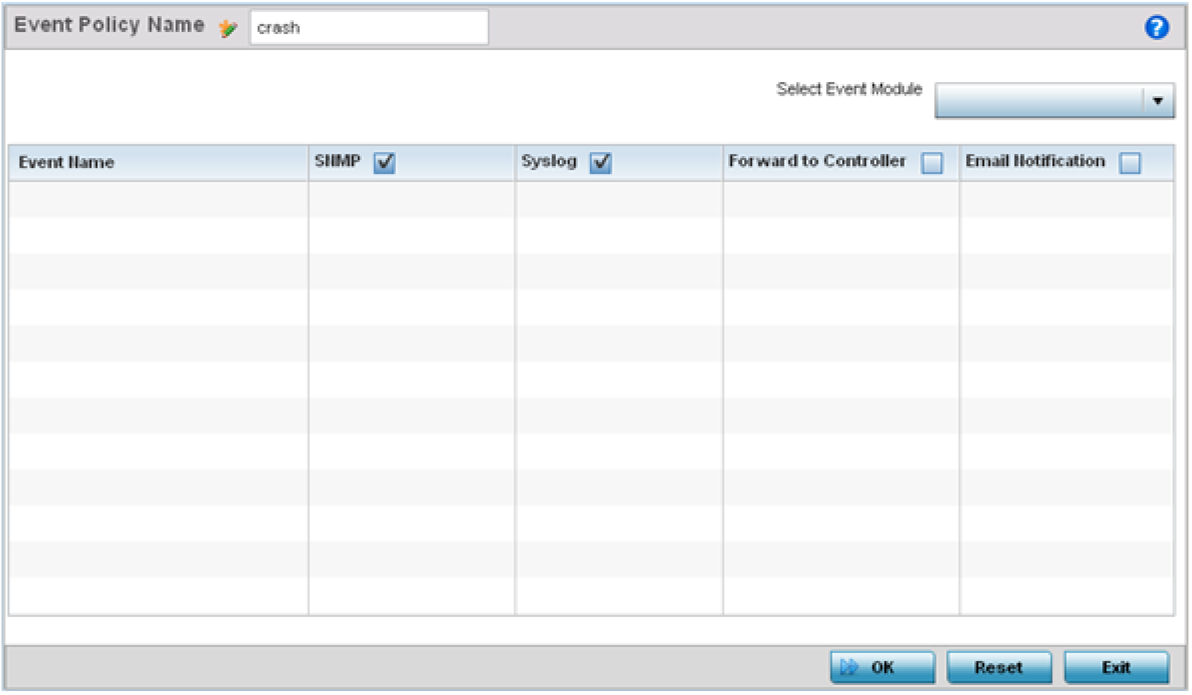
Event policies enable an administrator to create specific notification mechanisms using one, some or all of the SNMP, syslog, forwarding or e-mail notification options available. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can 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.



Event Policy Name: crash

SNMP ☑ Syslog ☑ Forward to Controller ☐ Email Notification ☐

Figure 162: 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.

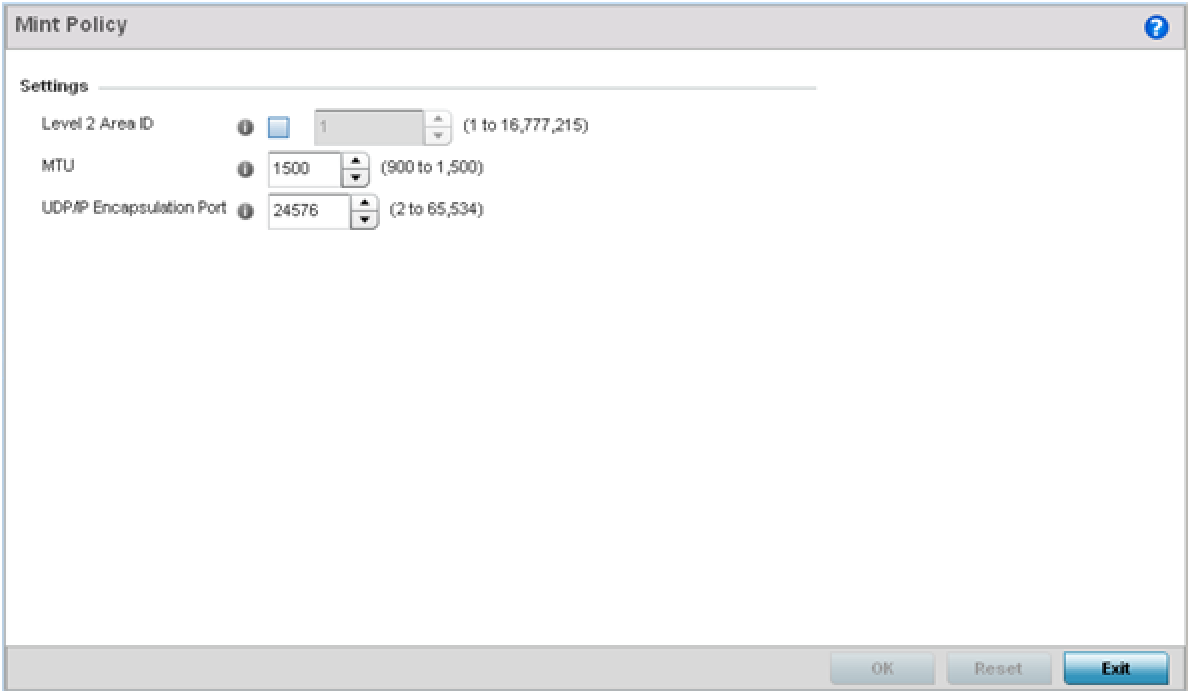
4 Review each event and select (or deselect) the **`SNMP`**, **`Syslog`**, **`Forward to Switch`** or **`Email Notification`** option as required for the event. Map an existing policy to a device profile as needed. Select Profile from the Map drop-down menu in the lower-left hand side of the screen. 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.

Managing MINT Policies

To add or modify a MINT Policy:

1 Select **Configuration** → **Devices** → **MINT Policy** to display the MINT Policy screen.



Mint Policy

Settings

Level 2 Area ID ☐ 1 (1 to 16,777,215)

MTU 1500 (900 to 1,500)

UDP/IP Encapsulation Port 24576 (2 to 65,534)

Figure 163: Configuration - Device - MiNT Policy Screen

2 Configure the following parameters:

Level 2 Area ID	Define a Level 2 Area ID for the Mint Policy. The Level 2 Area ID is 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.
MTU	Specify a MTU value for the mint policy between 900 and 1,500. The MTU setting specifies the maximum packet size used for mint packets. Larger packets will be fragmented so they fit within this packet size limit. The administrator may want to configure this parameter if the mint backhaul network requires or recommends smaller packet sizes. The default value is 1500.
UDP/IP Encapsulation Port	Specify the port to use for UDP/IP encapsulation between 2 and 65,534. This value specifies an alternate UDP port used by mint packets (and must be an even number). This port is used by mint control packets, and this port's value plus 1 is used to carry mint data packets. The default value is 24576.

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

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.

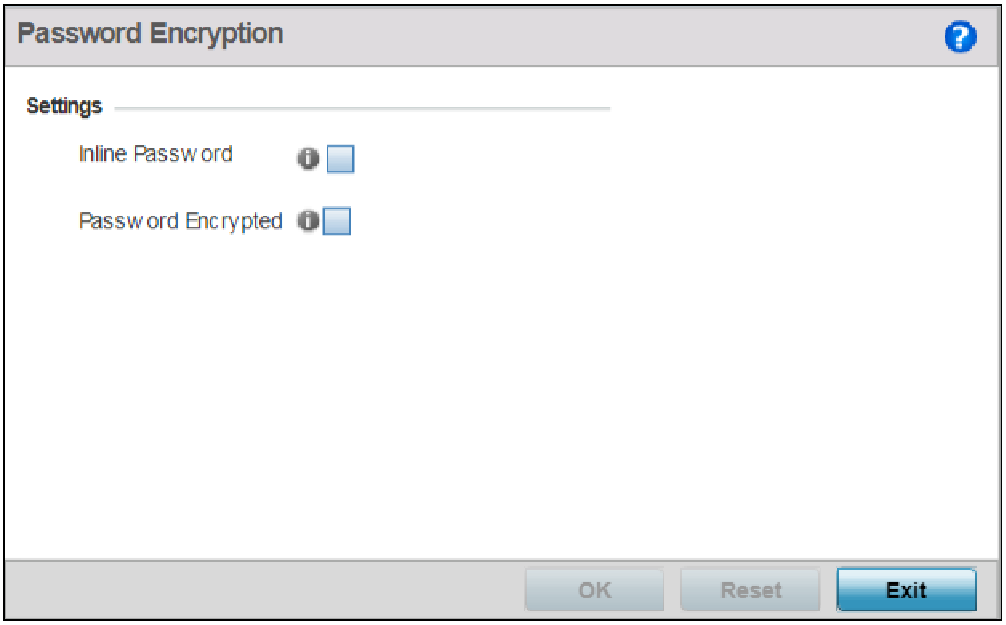


Figure 164: Configuration - Devices - Password Encryption Screen

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.

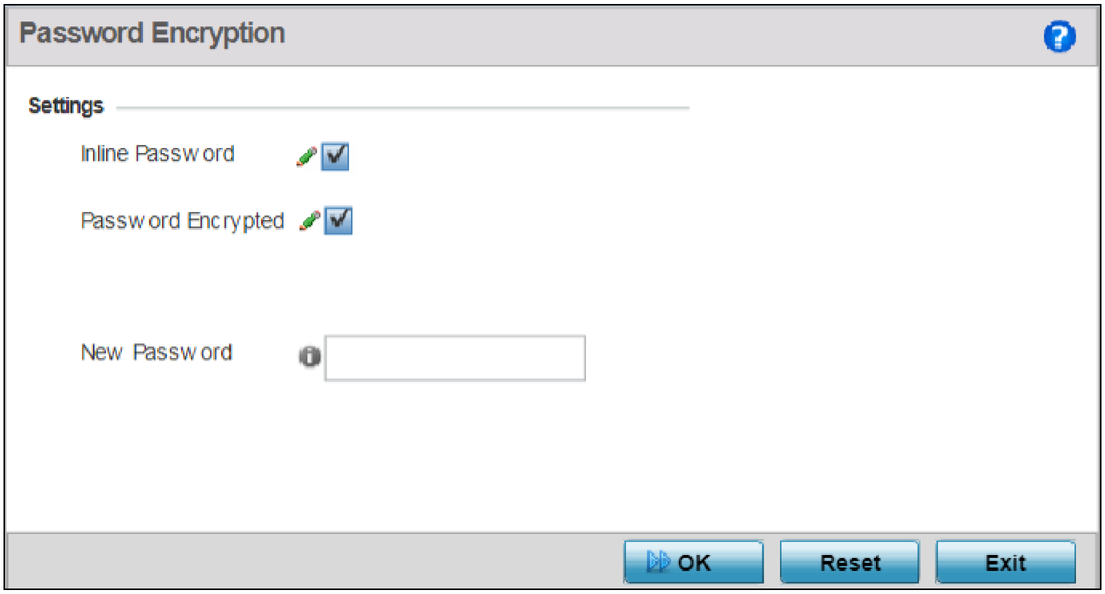


Figure 165: Configuration - Devices - Password Encryption - New Password Field

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.

6 Wireless Configuration

Wireless LAN Policies
WLAN QoS Policies
Radio QoS Policies
Association ACL
Smart RF Policies
MeshConnex Policies
Mesh QoS Policy
Passpoint Policy
Sensor Policy
Location Policy

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.

RFS 4000 model controllers support a maximum of 32 WLANs. NX 7500 model service platforms support up to 256 WLANs. An NX 95XX Series service platform supports up to 1000 WLANs. Access points can support a maximum of 16 WLANs per model.

The wireless configuration is comprised the following policies:

- Wireless LAN Policies on page 329
- WLAN QoS Policies on page 378
- Radio QoS Policies on page 392

- Association ACL on page 403
- Smart RF Policies on page 406
- MeshConnex Policies on page 421
- Mesh QoS Policy on page 428
- Passpoint Policy on page 435
- Sensor Policy on page 446
- Location Policy on page 449

WLAN policies can be separately selected and refined in the **Configuration** → **Wireless** pane located on the top left-hand side of the UI.

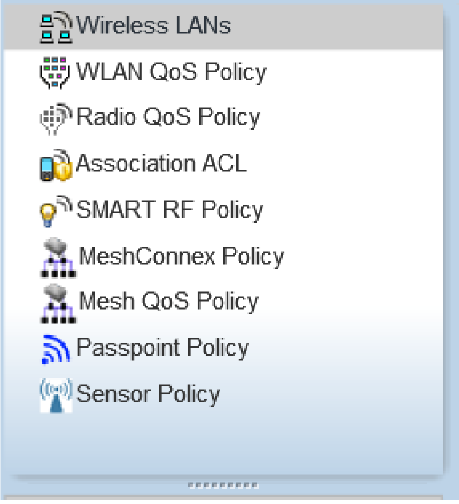
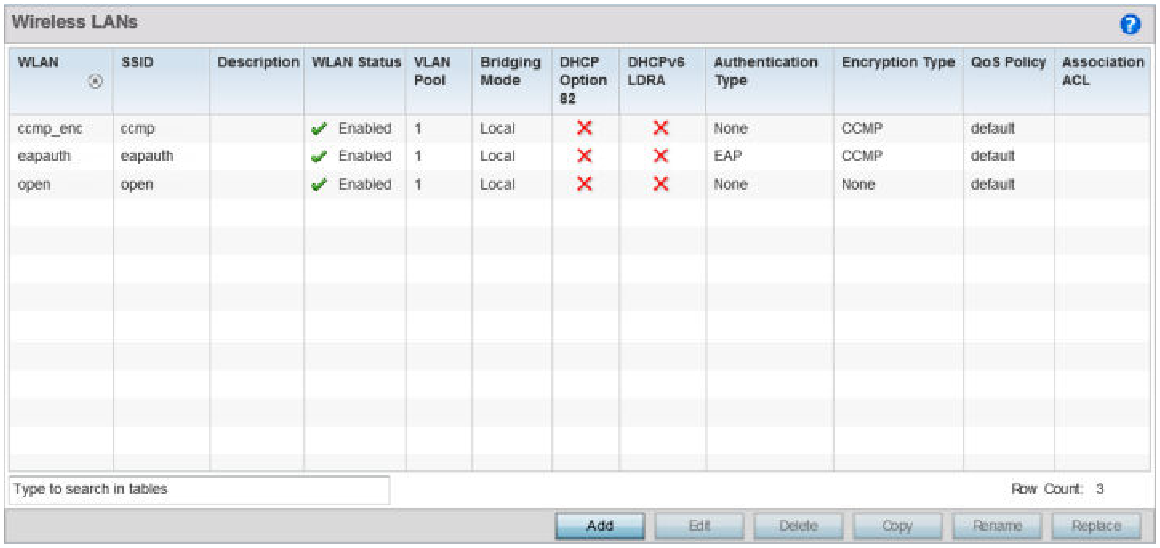


Figure 166: Configuration > Wireless Pane

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.



WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL
ccmp_enc	ccmp		✓ Enabled	1	Local	✗	✗	None	CCMP	default	
eapauth	eapauth		✓ Enabled	1	Local	✗	✗	EAP	CCMP	default	
open	open		✓ Enabled	1	Local	✗	✗	None	None	default	

Row Count: 3

Figure 167: 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. RFS 4000 series wireless controllers support a maximum of 32 WLANs. The NX 7500 service platforms support up to 256 WLANs.The NX 9500 series service platforms support up to 1000 WLANs.
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. 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. DHCP Option 82 is commonly used in large enterprise deployments to provide client physical attachment information. Option 82 is used in distributed DHCP server/relay environments, where relays insert additional information to identify the client's point of attachment. A red “X” defines DHCP option 82 as disabled, a green check means its enabled. **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 on page 331
- Configuring WLAN Security on page 334
- Configuring WLAN Firewall Settings on page 353
- Configuring WLAN Client Settings on page 361
- Configuring WLAN Accounting Settings on page 365
- Configuring WLAN Service Monitoring Settings on page 367
- Configuring Client Load Balancing Settings on page 369
- Configuring Advanced WLAN Settings on page 371
- Configuring Auto Shutdown Settings on page 377

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.

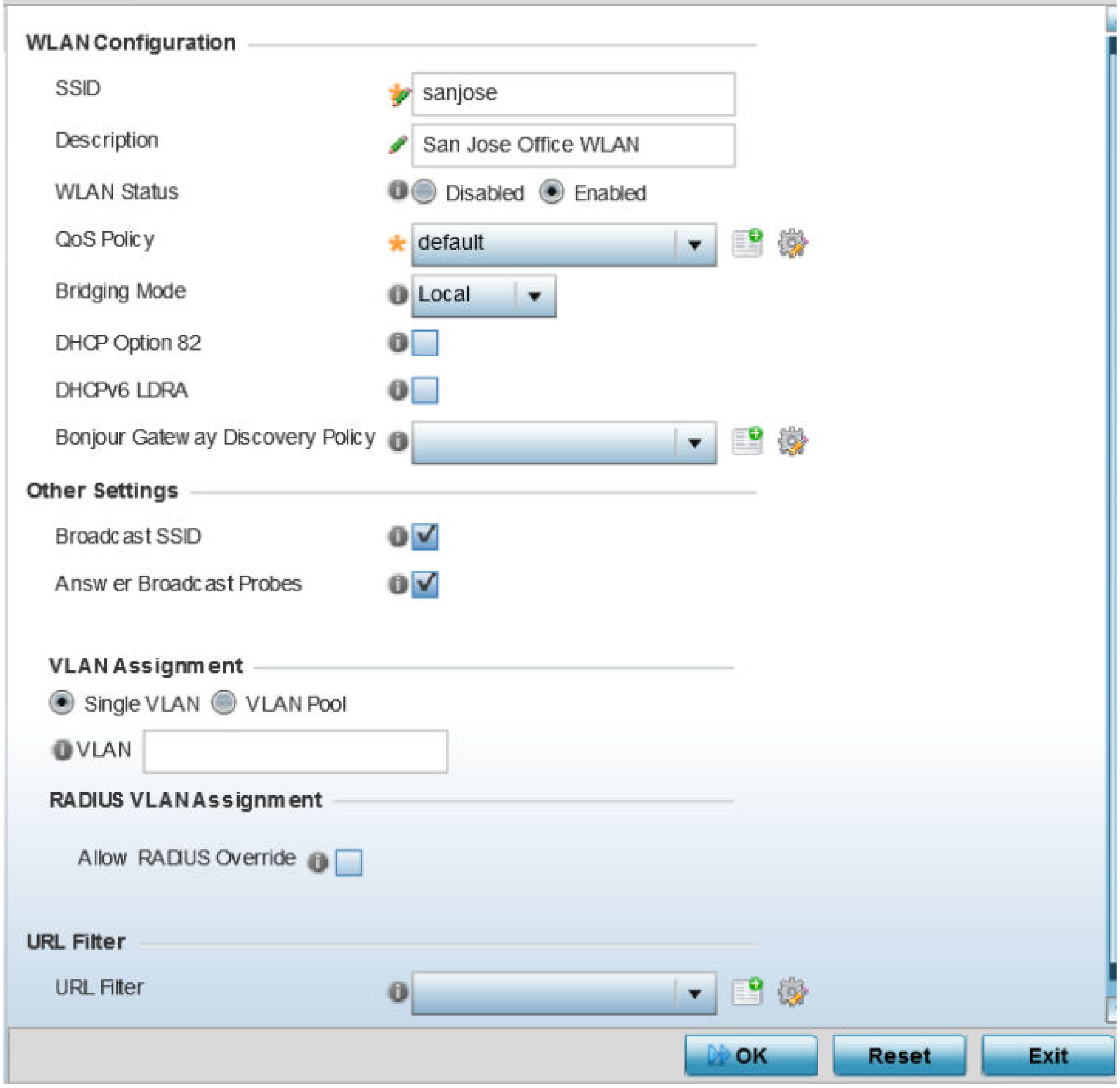
To define a WLAN's basic configuration:

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**.



WLAN Configuration

SSID: sanjose

Description: San Jose Office WLAN

WLAN Status: ○ Disabled ● Enabled

QoS Policy: default

Bridging Mode: Local

DHCP Option 82: ☐

DHCPv6 LDRA: ☐

Bonjour Gateway Discovery Policy:

Other Settings

Broadcast SSID: ☑

Answer Broadcast Probes: ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN:

RADIUS VLAN Assignment

Allow RADIUS Override: ☐

URL Filter

URL Filter:

Figure 168: 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 378.
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. 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. 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. Note: This setting is disabled by default.
Bonjour Gateway Discovery Policy	Select an existing Bonjour configuration to apply to the WLAN configuration. Bonjour provides a method to discover services on a WLAN. 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. 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 wireless controller to broadcast SSIDs within beacons. If a hacker tries to isolate and hack a client SSID via a client, the ESSID will display since the ESSID is in the beacon. 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). 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. When selected, a table is displayed. display a table with VLAN and wireless client columns (representing configurable options). Use this table to define the VLANs available to this WLAN. Additionally, define the number of wireless clients supported by each VLAN. Select the **+ Add Row** button to add additional VLANs to the WLAN.

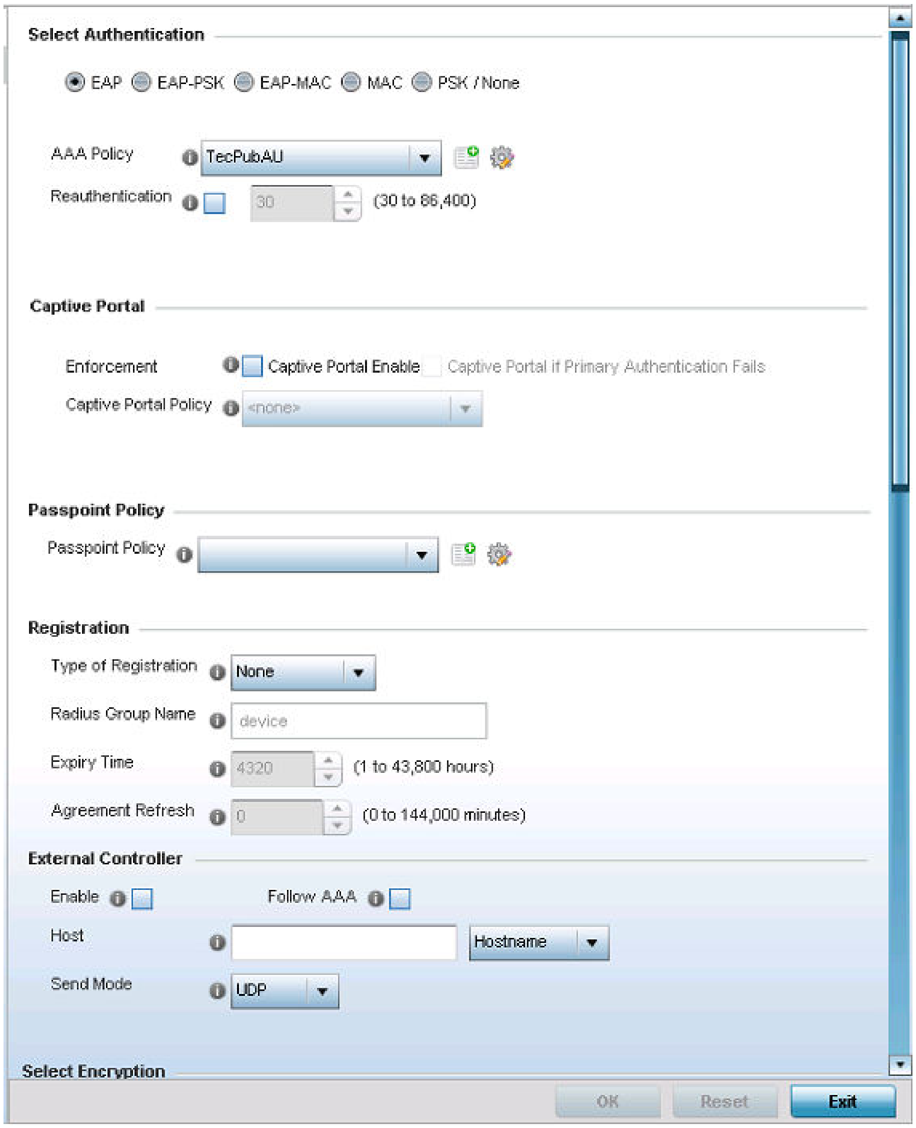
6 Select **Allow Radius Override**, in the RADIUS VLAN Assignment field, to allow an override to the WLAN configuration. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in the RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN configuration (defined earlier) is used. In other words,

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.

Configuring WLAN Security

A WLAN can be assigned a security policy supporting authentication, captive portal or encryption schemes.



Select Authentication

● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None

AAA Policy: TecPubAU

Reauthentication ☐ 30 (30 to 86,400)

Captive Portal

Enforcement ☐ Captive Portal Enable ☐ Captive Portal if Primary Authentication Fails

Captive Portal Policy: <none>

Passpoint Policy

Passpoint Policy:

Registration

Type of Registration: None

Radius Group Name: device

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

External Controller

Enable ☐ Follow AAA ☐

Host: Hostname

Send Mode: UDP

Select Encryption

Figure 169: 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 336
- MAC Authentication on page 338
- PSK / None on page 339

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 339 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 340.

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 342
- WPA2-CCMP on page 344
- WEP 64 on page 346
- WEP 128 on page 348
- Keyguard on page 350
- T5 Controller Security on page 351

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:

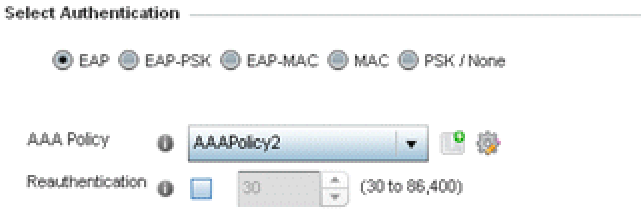
1 Select **Configuration** → **Wireless** → **Wireless LANs** to display available WLANs.

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.



Select Authentication

● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None

AAA Policy: AAAPolicy2

Reauthentication: ☐ 30 (30 to 86,400)

Figure 170: 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.

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.

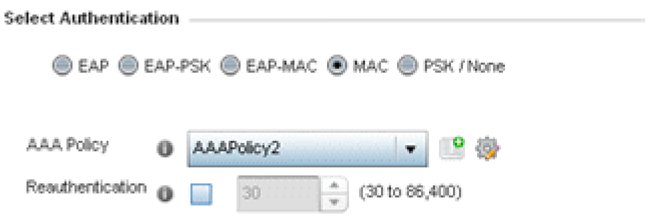
MAC authentication can only validate devices, not users. MAC authentication only references a client's wireless interface card MAC address when authenticating the device, it does not distinguish the device's user credentials. MAC authentication is somewhat poor as a standalone data protection technique, 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.



Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ● MAC ○ PSK / None

AAA Policy: AAAPolicy2

Reauthentication ☐ 30 (30 to 86,400)

Figure 171: 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.

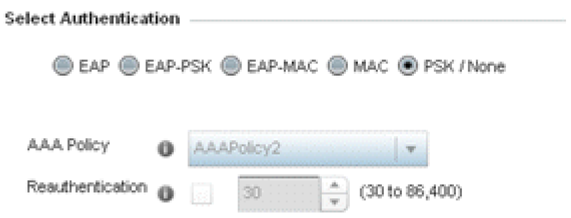
   Use the spinner control set the number of seconds (between 30 - 86,400) that, when exceeded, forces the EAP supported client to reauthenticate to use the WLAN.
4. Select **OK** when completed to update the WLAN's MAC configuration.

   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.



Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ● PSK / None

AAA Policy: AAAPolicy2

Reauthentication: ☐ 30 (30 to 86,400)

Figure 172: 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).

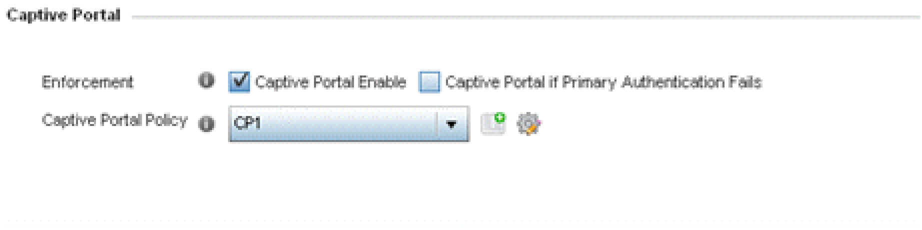
Captive Portal

A *captive portal* is guest access policy for providing guests temporary and restrictive access to the network. For an overview of the captive portal process and information on how to define a captive portal policy, see Captive Portal Policies on page 834.

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.



Captive Portal

Enforcement ☑ Captive Portal Enable ☐ Captive Portal if Primary Authentication Fails

Captive Portal Policy: CP1

Figure 173: 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 834.

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.

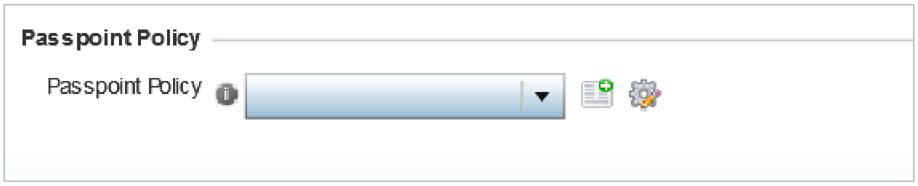
To assign a passpoint policy to a WLAN:

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.



Passpoint Policy

Passpoint Policy

Figure 174: 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 435.

6 Select **OK** when completed to update the WLAN's passpoint policy configuration.

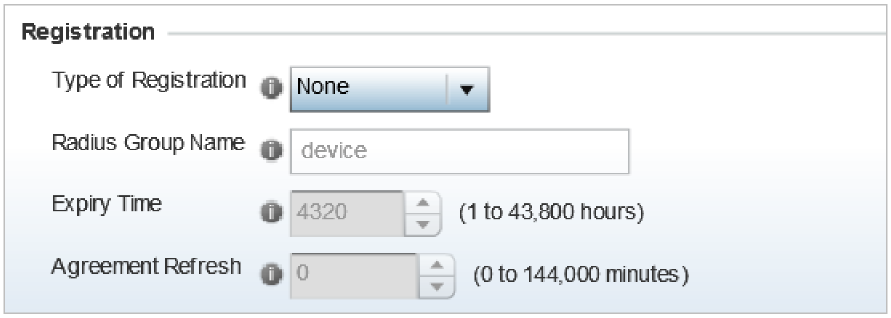
Select **Reset** to revert to the last saved configuration.

Registration

Registration requires the validation of devices by address to continue the authentication process.

To assign Registration to a WLAN:

1 Select **Configuration** → **Wireless** → **Wireless LAN Policy** 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.



Registration

Type of Registration: None

Radius Group Name: device

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

Figure 175: WLAN Policy Security Screen - MAC Registration

5 Use the **Type of Registration** drop-down menu to set the self-registration type for the selected WLAN.

Options include **`None`**, **`device`**, **`user`**, and **`device-OTP`**.

When captive portal guest users are authenticating using their User ID (Email Address/Mobile Number/ Member ID) and the received pass code in order to complete the registration process. The WLAN authentication type should be **`MAC-Authentication`** and the WLAN registration type should be configured as **`device-OTP`**.

When captive portal device registration is through social media, the WLAN registration type should be set as device registration, and the captive portal needs to be configured for guest user social authentication.

6 Enter a 64 character maximum RADIUS Group Name to which the registering user associates.

When left blank, devices are not associated with a RADIUS group.

7 Use the **Expiry Time** spinner control to set the amount of time (from 1 - 43,800 hours) before registration addresses expire and must be re-entered.

8 Set the **Agreement Refresh** as the amount of time (from 0 - 144,000 minutes) before the agreement page is displayed if the user has not been logged during the specified period.

The default setting is 0 days.

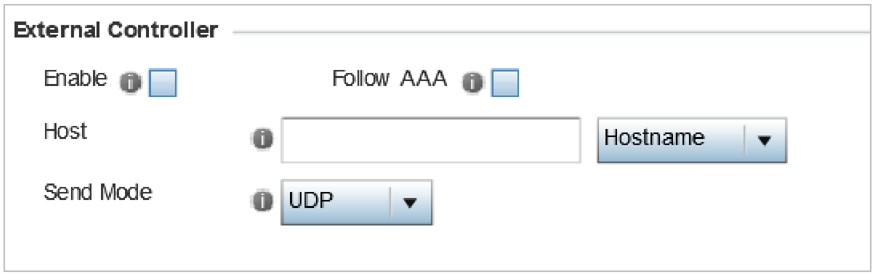
9 Select **OK** when completed to update the WLAN's registration settings.

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

External Controller

To set the WLAN’s external controller or service platform security configuration:

1. Select **Configuration** → **Wireless** → **Wireless LAN Policy** 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.



External Controller

Enable ☐ Follow AAA ☐

Host Hostname

Send Mode UDP

Figure 176: WLAN Policy Security Screen - External Controller Field

5. Select the **Enable** option if WLAN authentication is to be handled using an external resource.

   This feature is disabled by default.
6. Select the **Follow AAA** option if the resource handling WLAN authentication and accounting is an external RADIUS server specified within an AAA policy.

   However, ensure that an AAA policy identifying the authentication and accounting server exists and is associated with the WLAN.

   Note
   For ExtremeGuest deployment, the authenticating and accounting server specified in the AAA policy should point to the EGuest server host.

   ---
7. If using an external resource, use the drop-down menu to select either **Hostname** or **IP Address**, and enter the server information in the **Host** field.

   Hostnames cannot include the underscore character.
8. Select the Send Mode as either **`UDP`**, **`HTTP`** or **`HTTPS`**.

   The default setting is **`UDP`**.
9. 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:

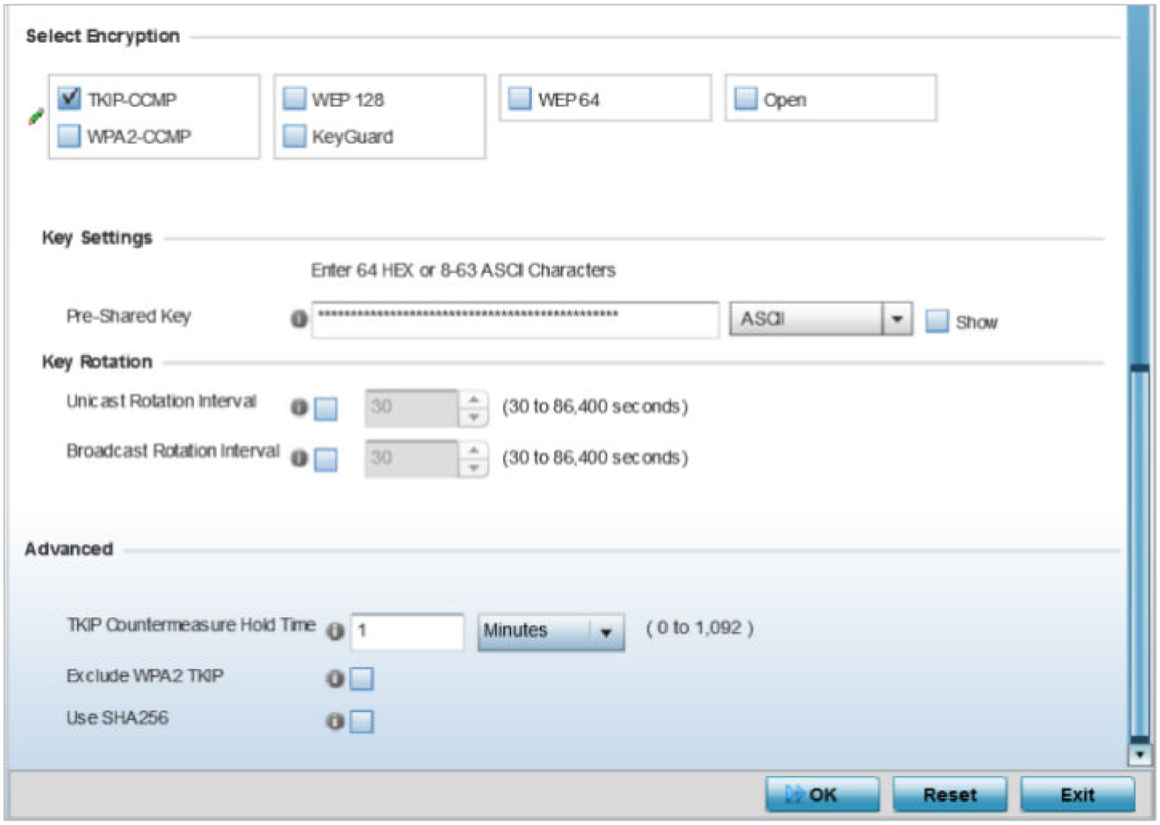
1 Select **Configuration** → **Wireless** → **Wireless LAN Policy** to display available WLANs.

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.



☑ TKIP-CCMP
☐ WPA2-CCMP
☐ WEP 128
☐ KeyGuard
☐ WEP 64
☐ Open

Pre-Shared Key ** ASCII ☐ Show

Unicast Rotation Interval ☐ 30 (30 to 86,400 seconds)

Broadcast Rotation Interval ☐ 30 (30 to 86,400 seconds)

TKIP Countermeasure Hold Time 1 Minutes (0 to 1,092)

Exclude WPA2 TKIP ☐

Use SHA256 ☐

Figure 177: 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 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 to enable use of the SHA-256 hash algorithms with WPA2. This is optional when using WPA2 without 802.11w Protected Management Frames (PMF) enabled. This is mandatory when PMF is enabled.

8 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:

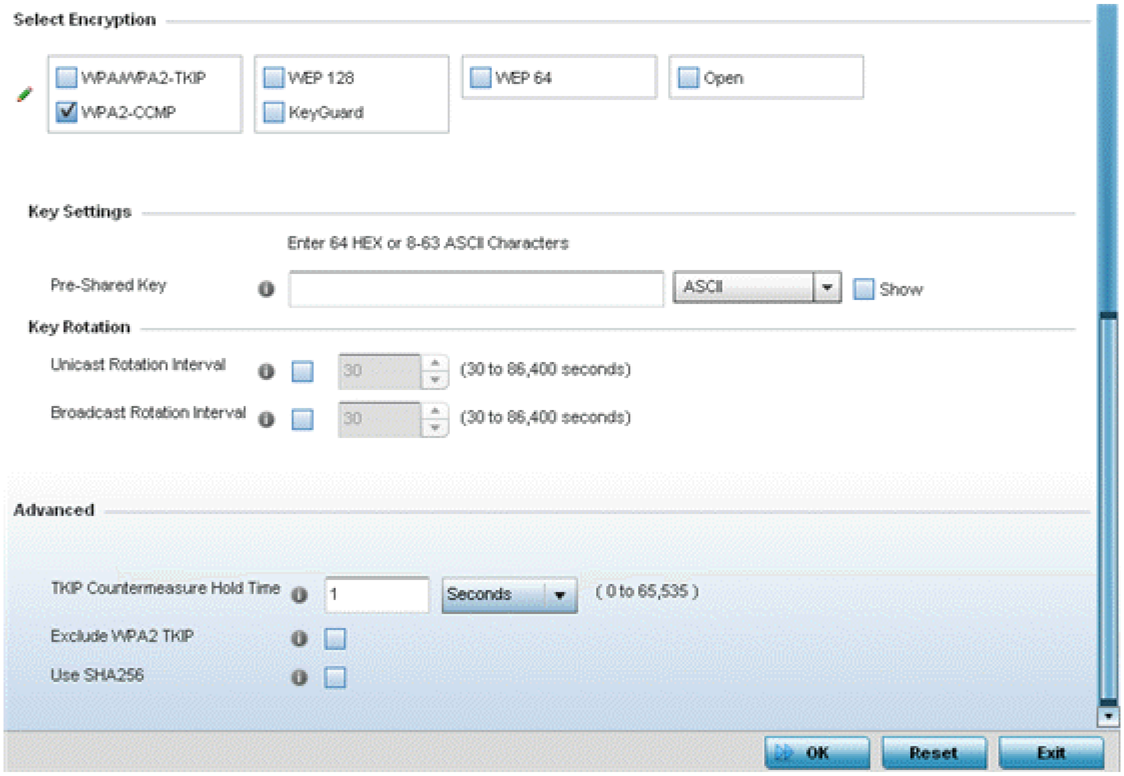
1 Select **Configuration** → **Wireless** → **Wireless LAN Policy** to display available WLANs.

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.



Select Encryption

☐ WPA/WPA2-TKIP
☑ WPA2-CCMP
☐ WEP 128
☐ KeyGuard
☐ WEP 64
☐ Open

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key: ASCII ☐ Show

Key Rotation

Unicast Rotation Interval ☐ 30 (30 to 86,400 seconds)

Broadcast Rotation Interval ☐ 30 (30 to 86,400 seconds)

Advanced

TKIP Countermeasure Hold Time: 1 Seconds (0 to 65,535)

Exclude WPA2 TKIP ☐

Use SHA256 ☐

Figure 178: 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 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 for an Access Point to advertise and enable support for only WPA-TKIP. Select this option if certain older clients are not compatible with the 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. Consider enabling 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.

8 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 LAN Policy** 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.

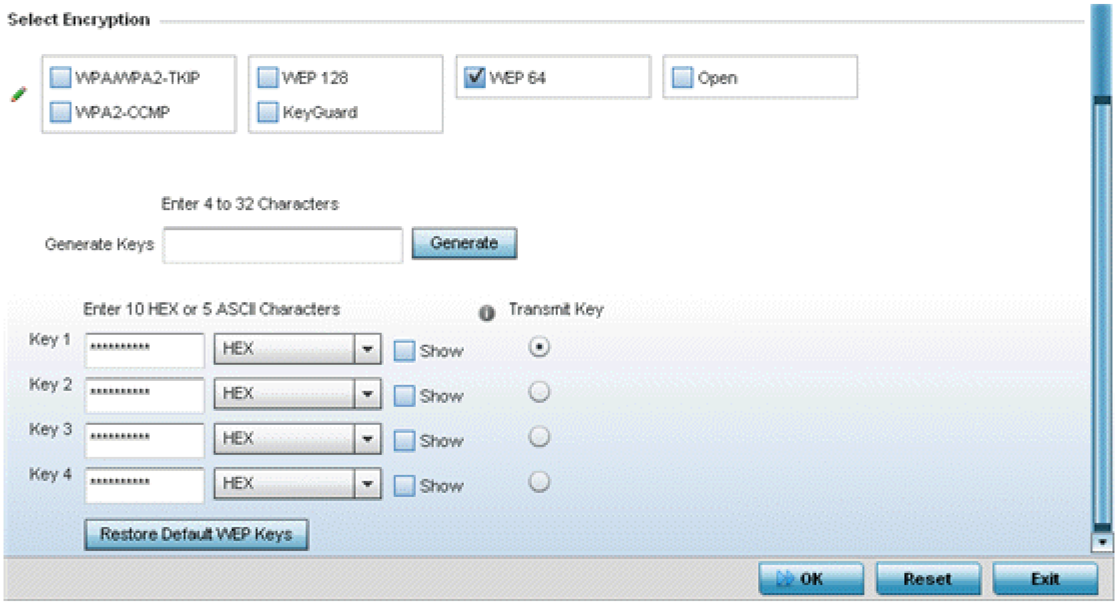


Figure 179: WLAN Security - WEP 64 Screen

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. Wireless devices 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 LAN Policy** 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.

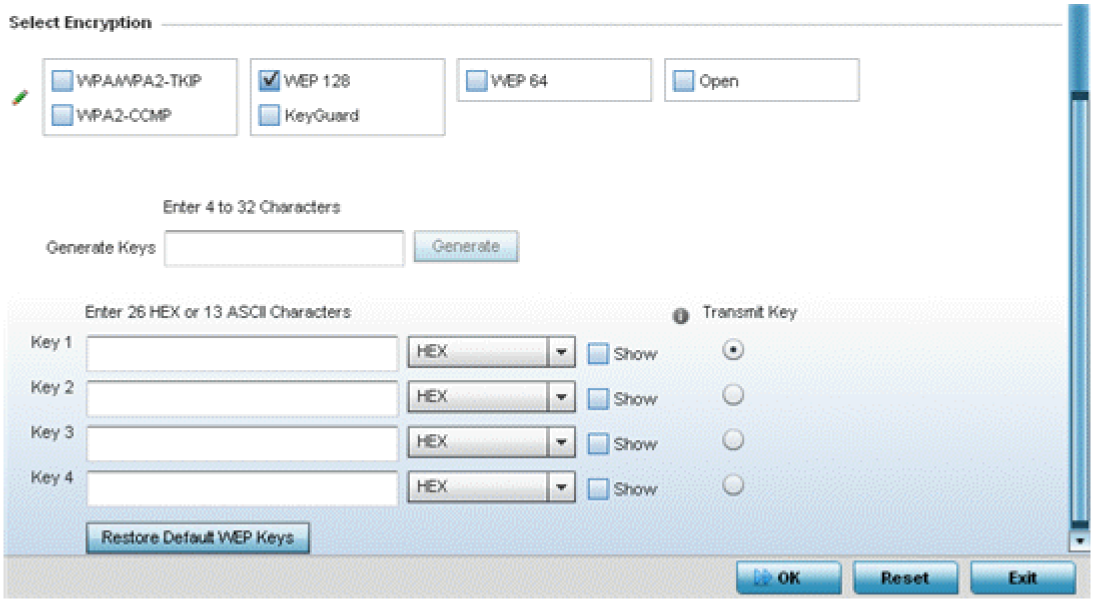


Figure 180: WLAN Security - WEP 128 Screen

5 Configure the following WEP 128 settings:

Generate Keys	Specify a 4- to 32-character pass key and click **Generate**. The pass key can be any alphanumeric string. Wireless devices 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 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 101112131415161718191A1B1C
- Key 2 202122232425262728292A2B2C
- Key 3 303132333435363738393A3B3C
- Key 4 404142434445464748494A4B4C

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 LAN Policy** 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.

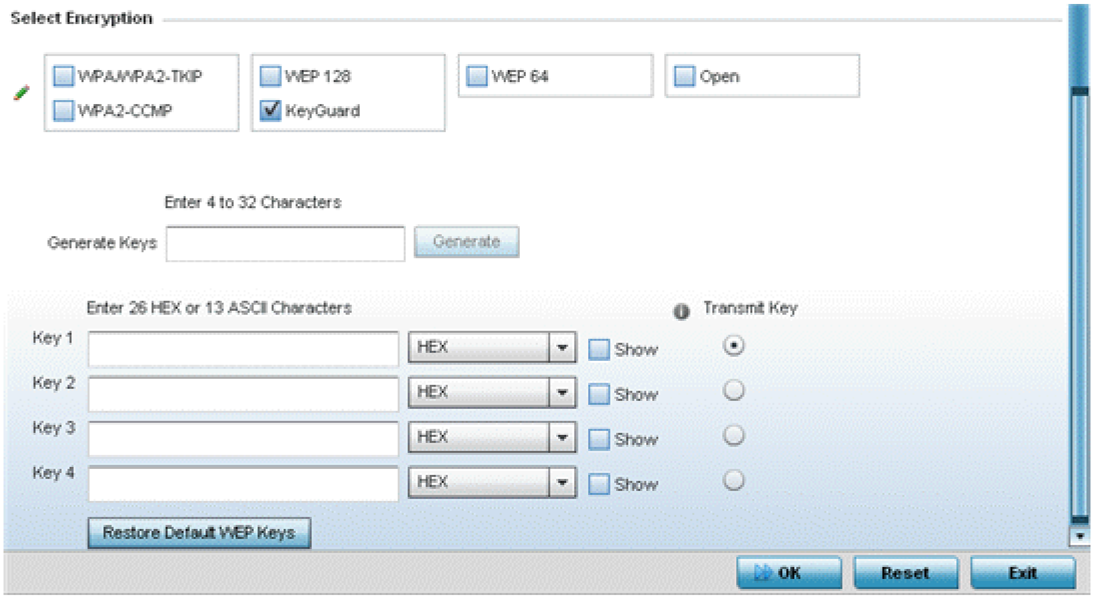


Figure 181: WLAN Security - Keyguard Screen

5 Configure the following keyguard settings:

Generate Keys	Specify a 4- to 32-character pass key and click **Generate**. The pass key can be any alphanumeric string. Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without 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:

- Authentication techniques can also be enabled on WLANs supporting other 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.

T5 Controller Security

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs *(Customer Premises Equipments)* are the T5 controller managed radio devices. These CPEs use DSL *(Digital Subscriber Line)* as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

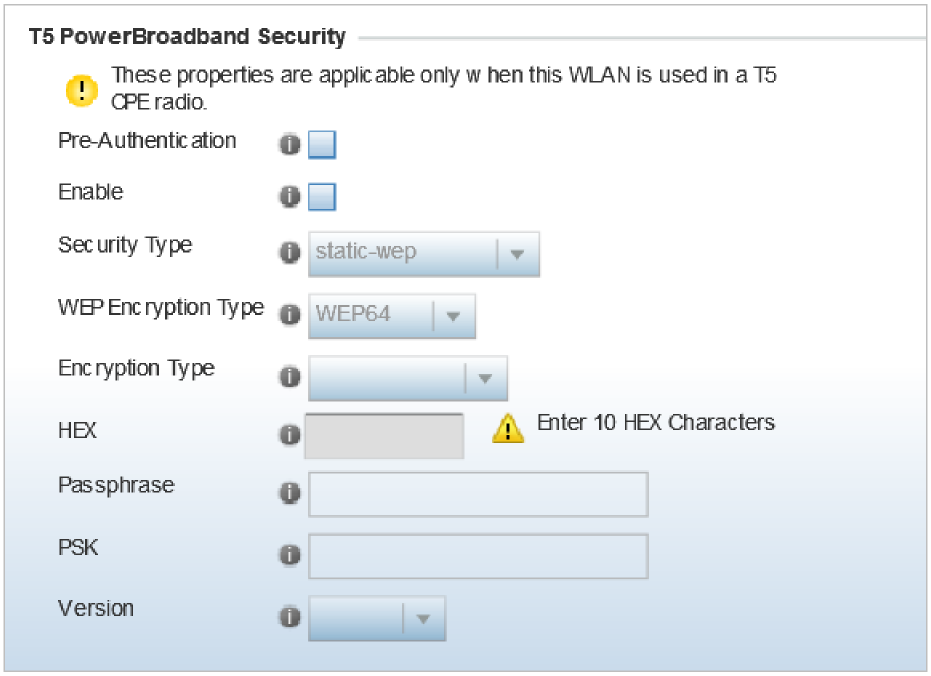
To configure WLAN security settings for a T5 controller and its connected CPEs:

1 Select **Configuration** → **Wireless** → **Wireless LAN Policy** 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 **T5 PowerBroadband Security** field at the bottom of the screen.



T5 PowerBroadband Security

These properties are applicable only when this WLAN is used in a T5 CPE radio.

Pre-Authentication ☐

Enable ☐

Security Type: static-wep

WEP Encryption Type: WEP64

Encryption Type:

HEX: Enter 10 HEX Characters

Passphrase:

PSK:

Version:

Figure 182: WLAN Security - T5 PowerBroadband Security Screen

5 Configure the following **T5 PowerBroadband Security** settings (available only when the WLAN supports T5 controllers and their connected CPEs radio devices):

Pre-Authentication	Select this option to invoke the use of pre-authentication 802.11i fast roaming. This setting is disabled by default.
Enable	Select this option to enable the **Security Type and WEP Encryptions Type** drop-down menus used to define and apply different encryption and authentication settings to the T5 WLAN security configuration.
Security Type	Use the drop-down menu to select the security type to apply to the WLAN. Options include **`static-wep`** (default), **`wpa-enterprise`**, and **`wpapersonal`**.
WEP Encryption Type	If **`static-wep`** is selected as the **Encryption Type**, use this setting to apply either a WEP 64 or WEP 128 encryption algorithm to the T5 support WLAN configuration.
Encryption Type	If **`wpa-enterprise`** or **`wpa-personal`** is selected as the **Encryption Type**, use this setting to apply either a CCMP, TKIP or TKIP-CCMP encryption algorithm to the T5 controller WLAN security configuration.
HEX	If you are using **`static-wep`**, provide the 10-26 character Hex password used to derive the security key.
Passphrase	If you are using **`static-wep`**, 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 converted into a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

PSK	Enter either an alphanumeric string as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted into a numeric value. This passphrase saves the administrator from entering the 256- bit key each time keys are generated.
Verison	If **`wpa-enterprise`** or **`wpa-personal`** is selected as the **Encryption Type**, use this setting to apply a WPA or WPA2 encryption scheme to the T5 support WLAN configuration.

6 Select **OK** when completed to update the T5 PowerBroadband Security configuration.

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

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 771.

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.

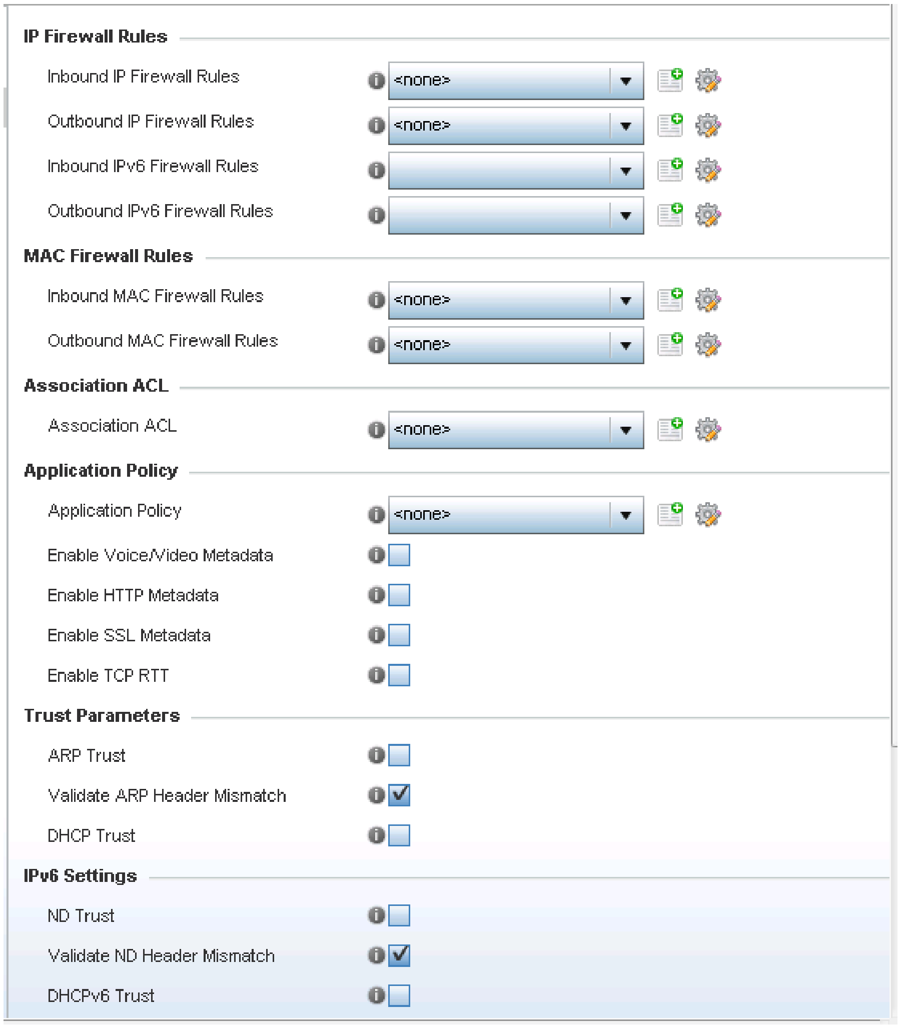
Keep in mind that IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

To review access policies, create a new policy or edit the properties of an existing policy:

1 Select **Configuration** → **Wireless LANs** → **Wireless LANs** Policy 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..



IP Firewall Rules

Inbound IP Firewall Rules <none>

Outbound IP Firewall Rules <none>

Inbound IPv6 Firewall Rules

Outbound IPv6 Firewall Rules

MAC Firewall Rules

Inbound MAC Firewall Rules <none>

Outbound MAC Firewall Rules <none>

Association ACL

Association ACL <none>

Application Policy

Application Policy <none>

Enable Voice/Video Metadata ☐

Enable HTTP Metadata ☐

Enable SSL Metadata ☐

Enable TCP RTT ☐

Trust Parameters

ARP Trust ☐

Validate ARP Header Mismatch ☑

DHCP Trust ☐

IPv6 Settings

ND Trust ☐

Validate ND Header Mismatch ☑

DHCPv6 Trust ☐

Figure 183: WLAN Policy Firewall Screen

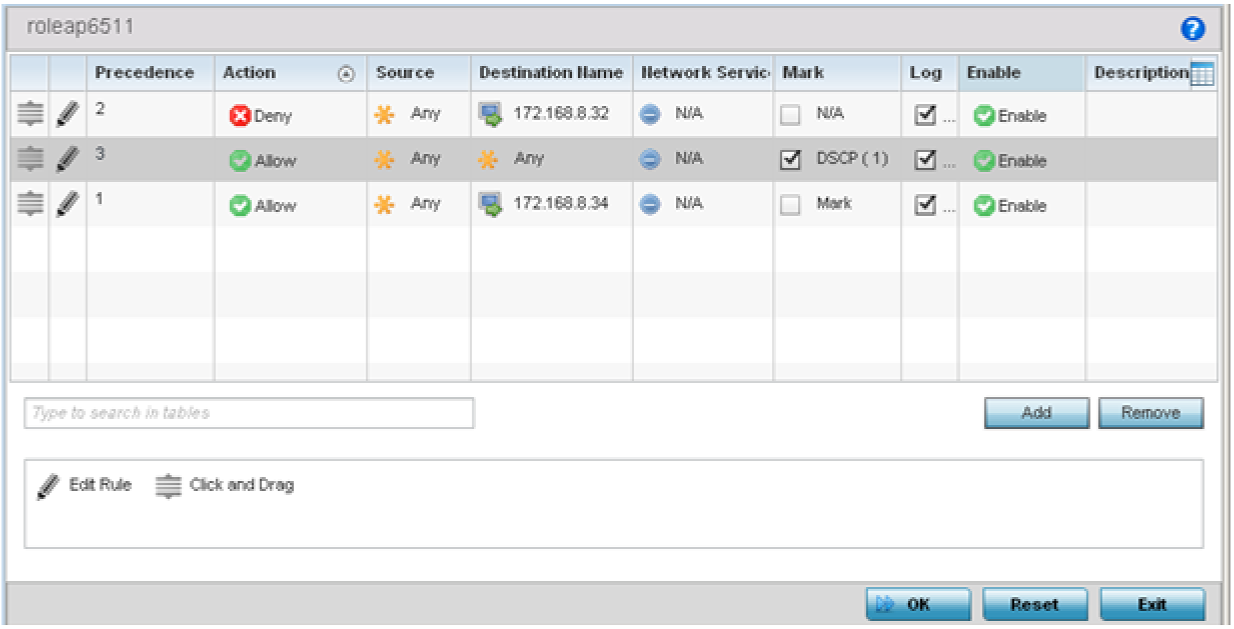
The screen displays editable fields for IP Firewall Rules, MAC Firewall Rules, Trust Parameters, and Client Deny Limits.

4 Select an existing **Inbound IP Firewall Rule** and **Outbound IP Firewall Rule** using the drop-down menu.

If no rules exist, select the **Create** icon to display a screen where Firewall rules can be created. Select the **Edit** icon to modify the configuration of a selected Firewall policy configuration.

If you are creating a new IP firewall rule, provide a name up to 32 characters.

5 Click **Add**.



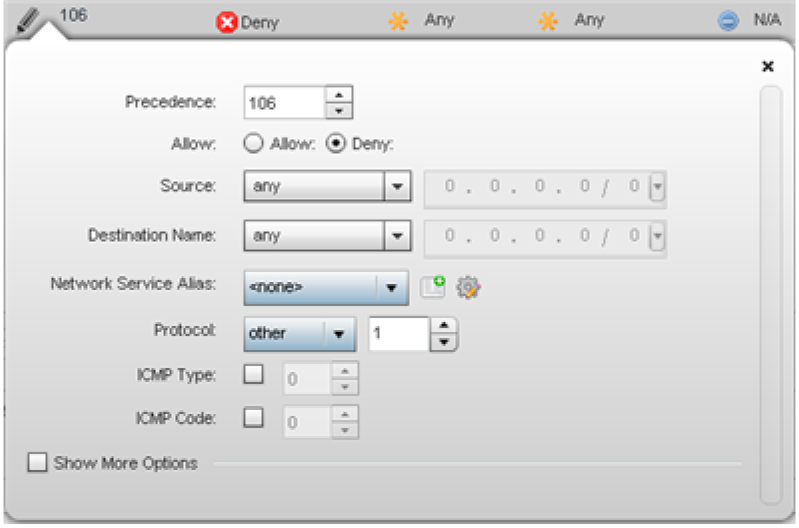
roleap6511

		Precedence	Action	Source	Destination Name	Network Servic	Mark	Log	Enable	Description
		2	Deny	Any	172.168.8.32	N/A	☐ N/A	☑ ...	Enable	
		3	Allow	Any	Any	N/A	☑ DSCP (1)	☑ ...	Enable	
		1	Allow	Any	172.168.8.34	N/A	☐ Mark	☑ ...	Enable	

Figure 184: 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.

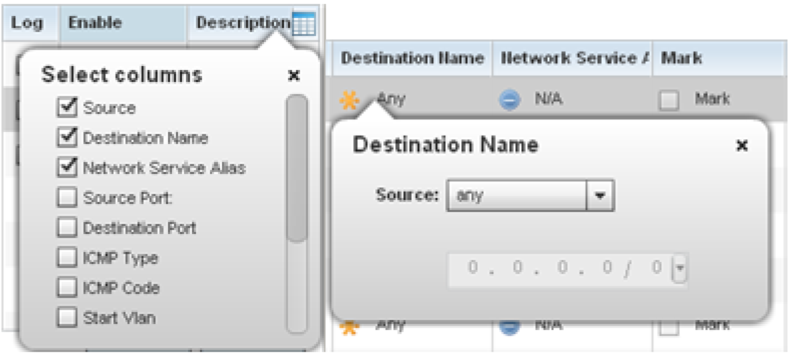


106 Deny Any Any N/A

Precedence: 106
Allow: ○ Allow: ● Deny:
Source: any 0 . 0 . 0 . 0 / 0
Destination Name: any 0 . 0 . 0 . 0 / 0
Network Service Alias: <none>
Protocol: other 1
ICMP Type: ☐ 0
ICMP Code: ☐ 0
☐ Show More Options

Figure 185: IP Firewall Rules Add Criteria 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.



Select columns

- ☑ Source
- ☑ Destination Name
- ☑ Network Service Alias
- ☐ Source Port
- ☐ Destination Port
- ☐ ICMP Type
- ☐ ICMP Code
- ☐ Start Vlan

Destination Name

Source: any

0 . 0 . 0 . 0 / 0

Figure 186: IP Firewall Rules Add Criteria Screen

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 IP firewall rule settings as required:

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: Deny Instructs the Firewall to prohibit a packet from proceeding to its destination Permit 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.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (**`any`**), are designated as a set of configurations consisting of protocol and port mappings (an **`alias`**), set as a numeric IP address (**`host`**) or defined as **`network IP and mask`**. Selecting **`alias`** requires that a destination network group alias be available or created.

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. 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 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. 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.
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, 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 an IP Firewall rule's **Mark** checkbox to enable or disable event marking and set the rule's 8021p or dscp level (from 0 - 7).
Log	Select an IP Firewall rule's **Log** checkbox to enable or disable event logging for this rule's usage.
Enable	Select an IP Firewall rule's **Enable** or **Disable** icon to determine this rule's inclusion with the IP firewall policy.
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 Select existing inbound and 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. MAC firewall rules can also be applied to an EX3500 Ethernet PoE switch connected and utilized by a WiNG managed device.

9 Select the **+ Add Row** button.

10 Select the added row to expand it into configurable parameters.

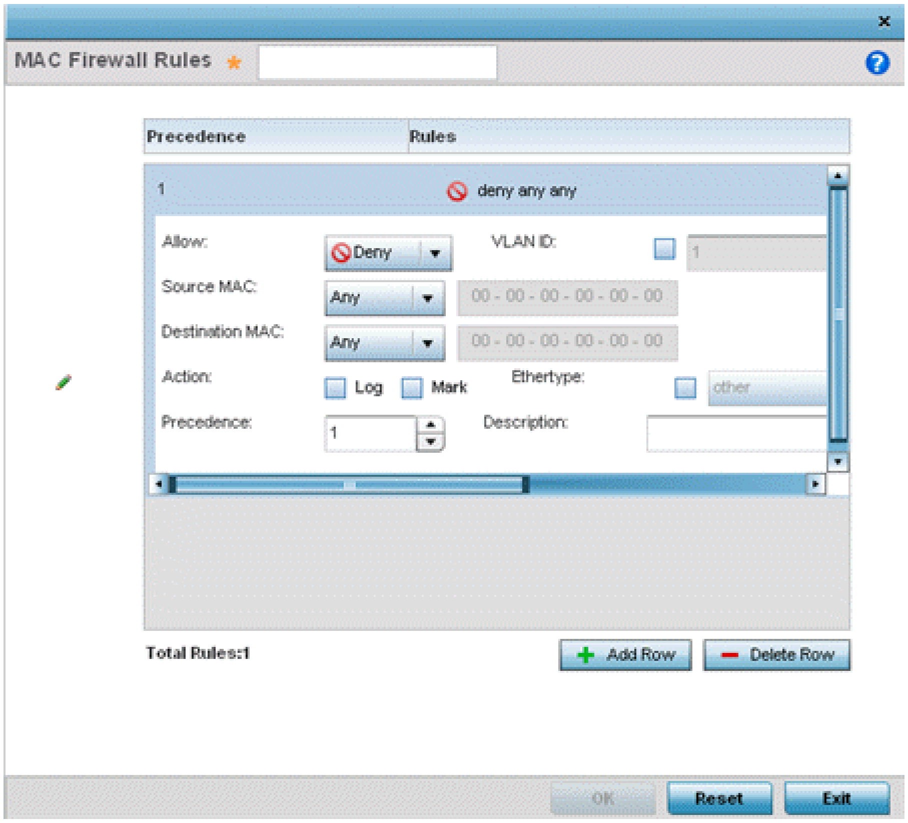


Figure 187: MAC Firewall Rules Screen

11 Define the following parameters for either the inbound or outbound MAC Firewall Rules for either a WiNG managed device or an EX3500 switch connected to a WiNG managed device:

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: Deny — Instructs the Firewall to prohibit a packet from proceeding to its destination Permit — Instructs the Firewall to allow a packet to proceed to its destination
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 between 1 - 4094. EX3500 PoE switches utilize a VLAN Mask option (from 0 - 4095) to mask the exposure of the VLAN ID.
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.
Source and Destination MAC	Enter both **Source** and **Destination** MAC addresses. The wireless controller uses 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: Log — Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted. Mark — Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. 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.
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. EX3500 PoE switches utilize an Ether Mask option (from 0 - 65535) to mask the exposure of the Ethertype.
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.
Description	Provide an ACL setting description (up to 64 characters) for the rule to help differentiate it from others with similar configurations.

12. If you are creating a new **Association ACL**, provide a name specific to its function.

    Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.
13. 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 specific 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 dashboard (starting with WiNG 5.9.3, Extreme NSight is a separate target) 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.
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 dashboard. This setting is disabled by default.

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 dashboard. This setting is disabled by default.
Enable TCP RTT	Select this option to enable the extraction of RTT *(Round Trip Time)* from TCP *(Transmission Control Protocol)* flows. When enabled, the RTT information from TCP flows detected on the VLAN interface associated with the WLAN is extracted and forwarded to the Extreme NSight appliance by access points. However, this TCP-RTT metadata is viewable only on the Extreme NSight dashboard. This setting is disabled by default. Note: Extreme NSight is a licensed feature. For more information on Extreme NSight, please refer to the Extreme NSight™ User Guide, available at https://extremenetworks.com/documentation.

14 Set the following **Trust Parameters**:

ARP Trust	Select the check box to enable ARP Trust on this WLAN. ARP packets received on this WLAN are considered trusted, and is used to identify rogue devices within the network. This setting is disabled by default.
Validate ARP Header Mismatch	Select this option to verify the mismatch for source MAC in the ARP and Ethernet headers. By default, mismatch verification is enabled.
DHCP Trust	Select the check box to enable DHCP trust on this WLAN. This setting is disabled by default.

15 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.

16 Set the following **Wireless Client Deny** configuration:

Wireless Client Denied Traffic Threshold	If enabled, any associated client that exceeds the thresholds configured for storm traffic is either deauthenticated or blacklisted depending on the selected action. The threshold range is 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 the check box and define a setting between 0 - 86,400 seconds. After the blacklist duration has been exceeded, offending clients can reauthenticate once again.

17 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.

18 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

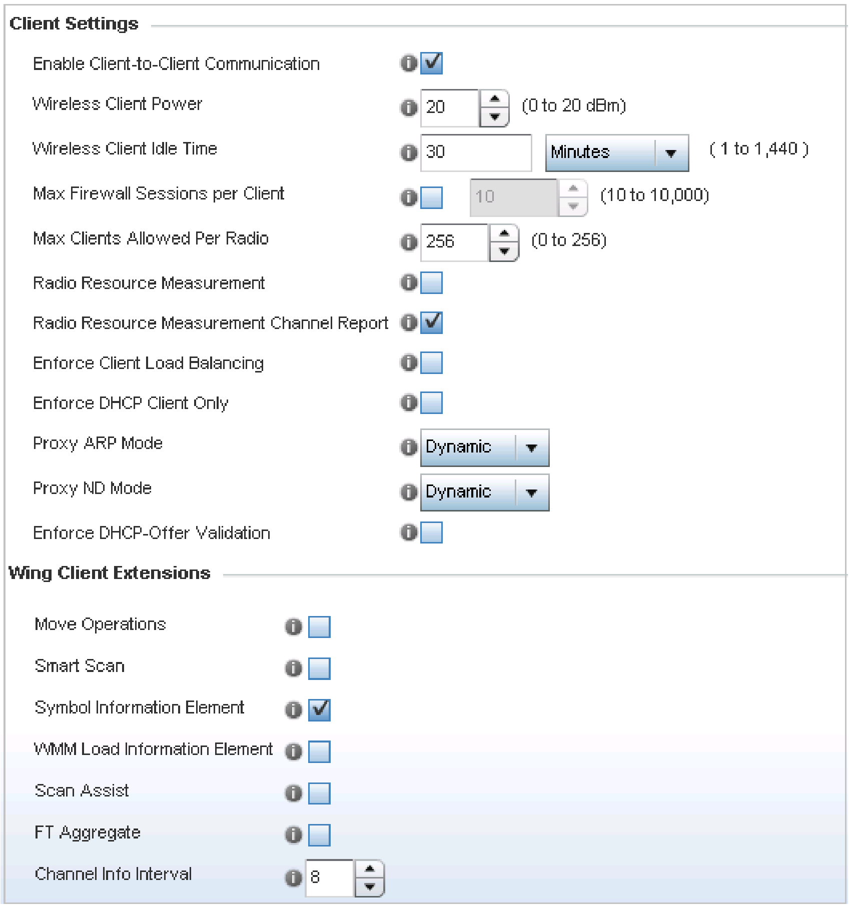
Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations.

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.



Client Settings

Enable Client-to-Client Communication ☑
Wireless Client Power 20 (0 to 20 dBm)
Wireless Client Idle Time 30 Minutes (1 to 1,440)
Max Firewall Sessions per Client ☐ 10 (10 to 10,000)
Max Clients Allowed Per Radio 256 (0 to 256)
Radio Resource Measurement ☐
Radio Resource Measurement Channel Report ☑
Enforce Client Load Balancing ☐
Enforce DHCP Client Only ☐
Proxy ARP Mode Dynamic
Proxy ND Mode Dynamic
Enforce DHCP-Offer Validation ☐

Wing Client Extensions

Move Operations ☐
Smart Scan ☐
Symbol Information Element ☑
WMM Load Information Element ☐
Scan Assist ☐
FT Aggregate ☐
Channel Info Interval 8

Figure 188: 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	Use the spinner control to set the maximum number of clients (from 0 - 256) allowed to associate to each radio within this WLAN. The default setting is 256.
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. 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 the check box to distribute clients evenly amongst associated access point radios. This feature is disabled by default. 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.

Proxy ND Mode	Use the drop-down menu to define the proxy ND *(neighbor discovery)* mode for WLAN member clients as either **`Strict`** or **`Dynamic`**. ND Proxy is used in IPv6 to provide reachability by allowing the a client to act as proxy. Proxy certificate signing can be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network topology is defined. 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 Select **Client Isolation**, in the **T5 PowerBroadband Client Settings** field, to disallow clients connecting to the WLAN to communicate with one another. This setting applies exclusively to CPE devices managed by a T5 controller and is disabled by default.

Use the **Inactivity Time Out** field to define the inactivity timeout specific to T5 clients. Set the maximum amount of time T5 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.

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The CPEs *(Customer Premises Equipments)* are the T5 controller managed radio devices. These CPEs use a DSL *(Digital Subscriber Line)* as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

12 Click **OK** when completed to update the WLAN's client settings. Click **Reset** to revert the screen to the last saved configuration.

WLAN Client Setting Deployment Considerations

Before defining client support settings for a controller, service platform, or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Clients on the same WLAN associated to an AP can communicate locally at the AP Level without going through the controller or service platform. If this is undesirable, an access point's **Client-to-Client Communication** option should be disabled.
- When the wireless client idle time setting is exceeded, the client is no longer able to access WLAN resources and must re-authenticate. The default value is 1,800 seconds.
- Access points can support up to 256 clients per access point or radio.

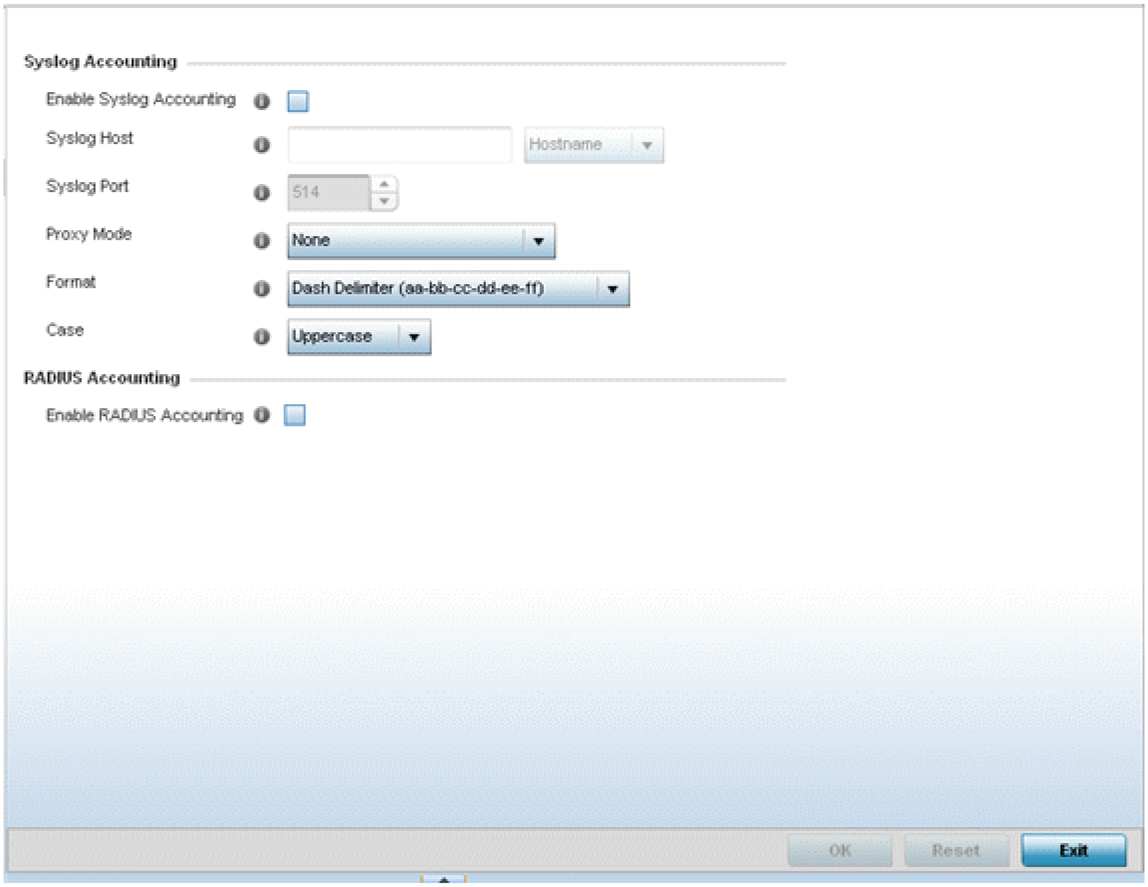
Configuring WLAN Accounting Settings

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**.



Syslog Accounting

Enable Syslog Accounting ☐

Syslog Host Hostname

Syslog Port 514

Proxy Mode None

Format Dash Delimiter (aa-bb-cc-dd-ee-ff)

Case Uppercase

RADIUS Accounting

Enable RADIUS Accounting ☐

Figure 189: 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. Note: 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.
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.

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:

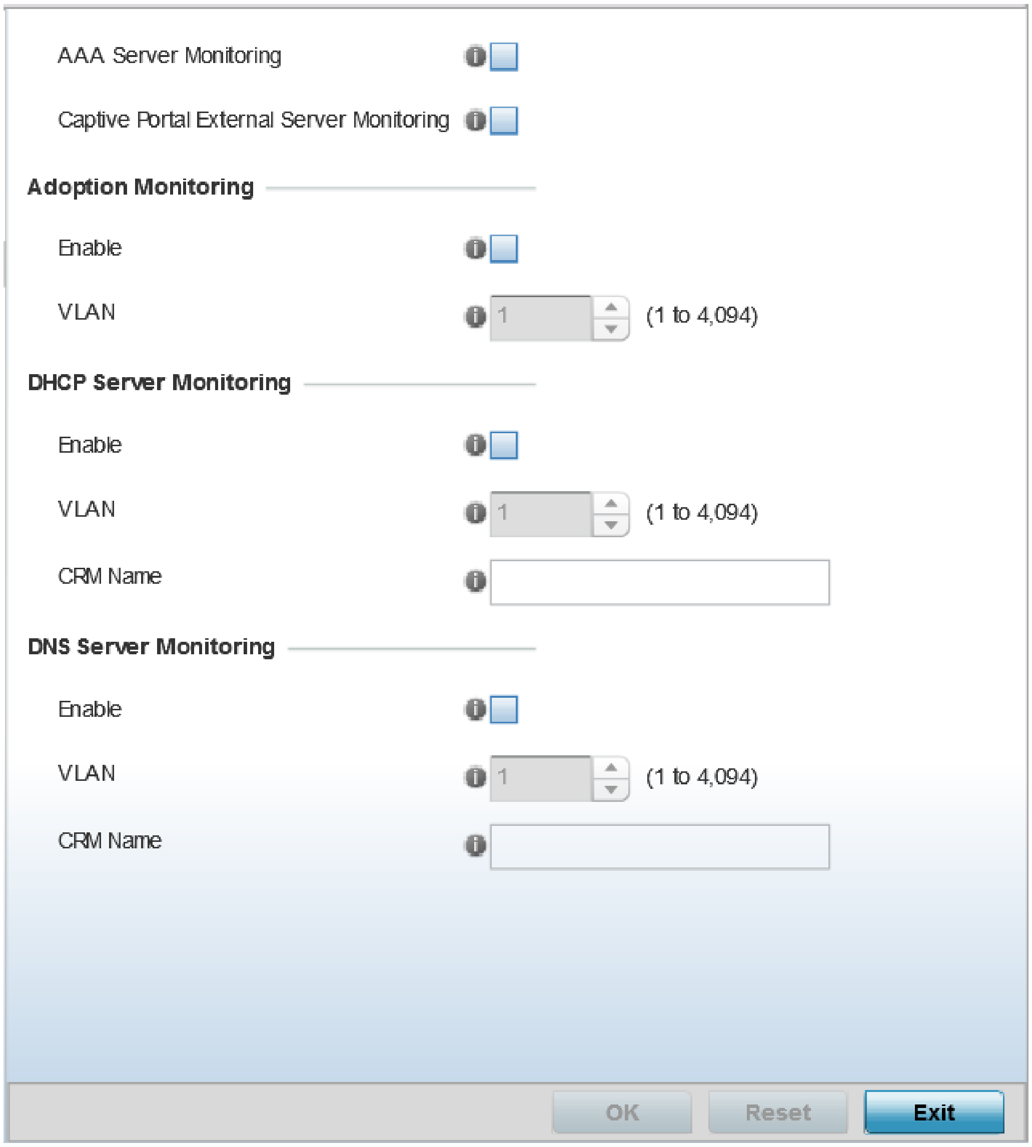
- When the RADIUS authentication server becomes unavailable. The RADIUS server could be local or external to the controller, service platform or access point.
- When an externally hosted captive portal is unavailable (for any reason)
- If an access point’s connected controller or service platform becomes 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**.



AAA Server Monitoring ☐

Captive Portal External Server Monitoring ☐

Adoption Monitoring

Enable ☐

VLAN 1 (1 to 4,094)

DHCP Server Monitoring

Enable ☐

VLAN 1 (1 to 4,094)

CRM Name

DNS Server Monitoring

Enable ☐

VLAN 1 (1 to 4,094)

CRM Name

Figure 190: 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. Note: 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.

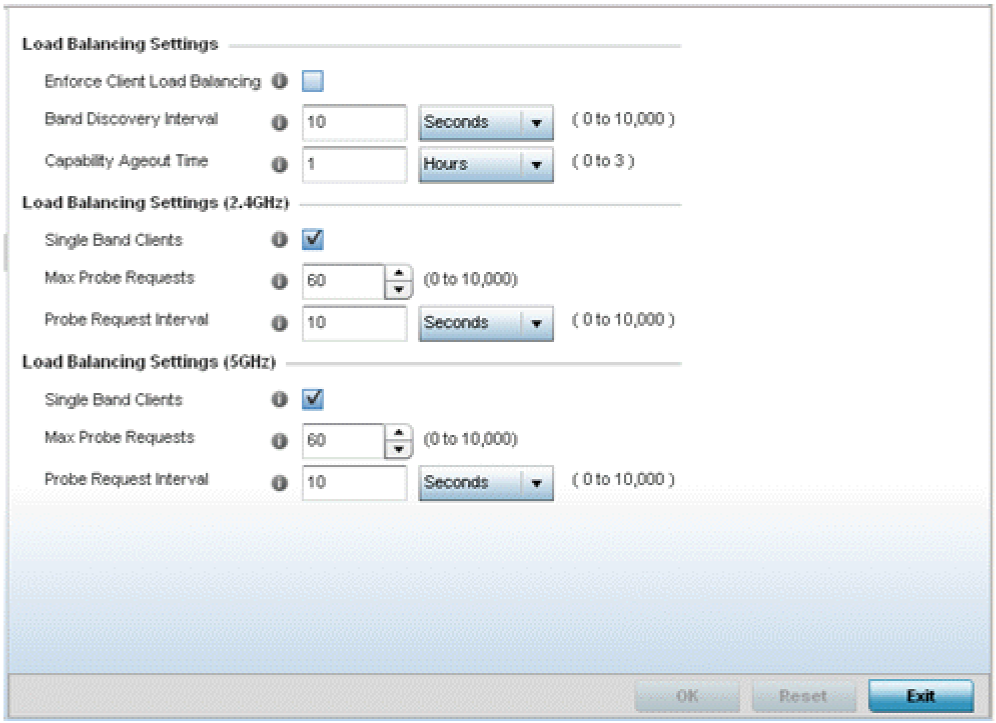
Configuring Client Load Balancing Settings

To configure WLAN client load balance 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 Select **Client Load Balancing**.



Load Balancing Settings

Enforce Client Load Balancing ☐

Band Discovery Interval 10 Seconds (0 to 10,000)

Capability Ageout Time 1 Hours (0 to 3)

Load Balancing Settings (2.4GHz)

Single Band Clients ☑

Max Probe Requests 60 (0 to 10,000)

Probe Request Interval 10 Seconds (0 to 10,000)

Load Balancing Settings (5GHz)

Single Band Clients ☑

Max Probe Requests 60 (0 to 10,000)

Probe Request Interval 10 Seconds (0 to 10,000)

Figure 191: 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. The following models can support 256 clients per access point: AP 6522, AP 6532, AP 6562, AP 7161, AP 7602, AP 7622, AP 81XX. The following models can support 512 clients per access point: AP-7612, AP7632, AP7662. 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	Enter a value (from 0 - 10,000 seconds) to set the interval dedicated to discover a client's radio band capability before its access point radio association. The default setting is 24 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. 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.

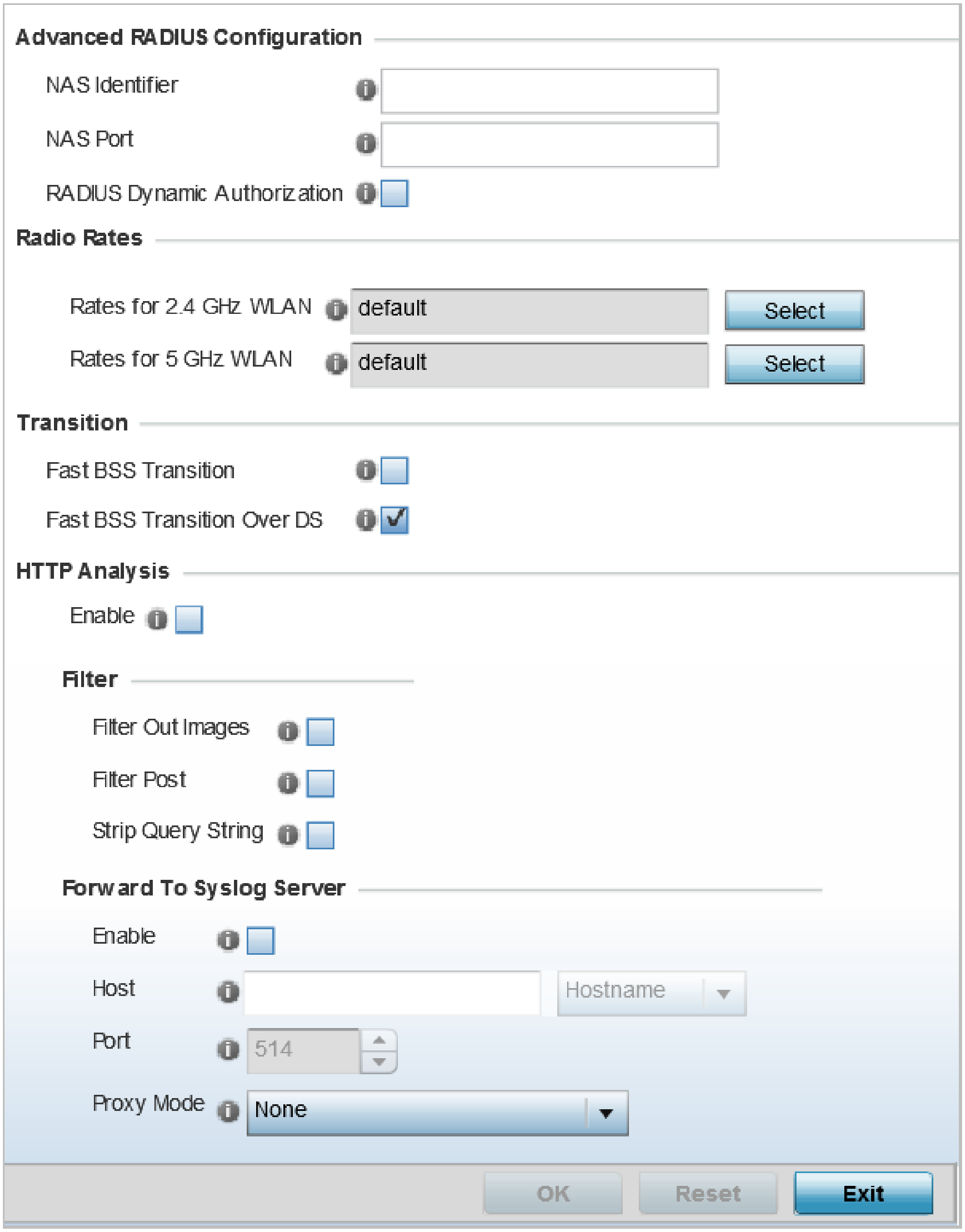
Click **Reset** to revert the screen to its last saved configuration.

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**.



Advanced RADIUS Configuration

NAS Identifier

NAS Port

RADIUS Dynamic Authorization ☐

Radio Rates

Rates for 2.4 GHz WLAN: default

Rates for 5 GHz WLAN: default

Transition

Fast BSS Transition ☐

Fast BSS Transition Over DS ☑

HTTP Analysis

Enable ☐

Filter

Filter Out Images ☐

Filter Post ☐

Strip Query String ☐

Forward To Syslog Server

Enable ☐

Host: Hostname

Port: 514

Proxy Mode: None

Figure 192: WLAN - Advanced Configuration Screen

4 Refer to the **Protected Management Frames (802.11w)** field to set a frame protection mode and security association for the WLAN's advanced configuration.

Mode	Select a radio button for the mode (either `Disabled`, `Optional` or `Mandatory`). `Disabled` is the default setting.
SA Query Attempts	Use the spinner control to set the number of security association query attempts, between 1 and 10. The default value is 5.
SA Query Retry Timeout	Set the timeout (from 100-1,000 milliseconds) for waiting for a response to a SA query before resending it. The default is 201 milliseconds.

5 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. Set the numeric port value between 0 and 4,294,967,295.
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.

6 Refer to the **Radio Rates** field to define selected data rates for both the 2.4 GHz and 5.0 GHz bands.

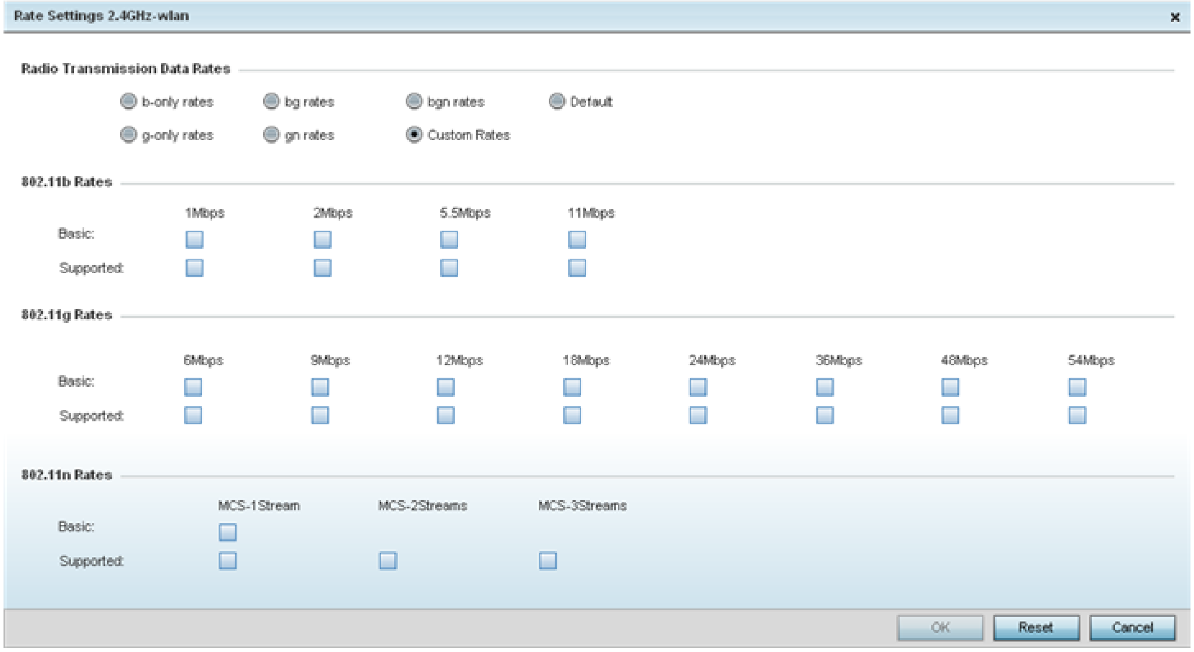
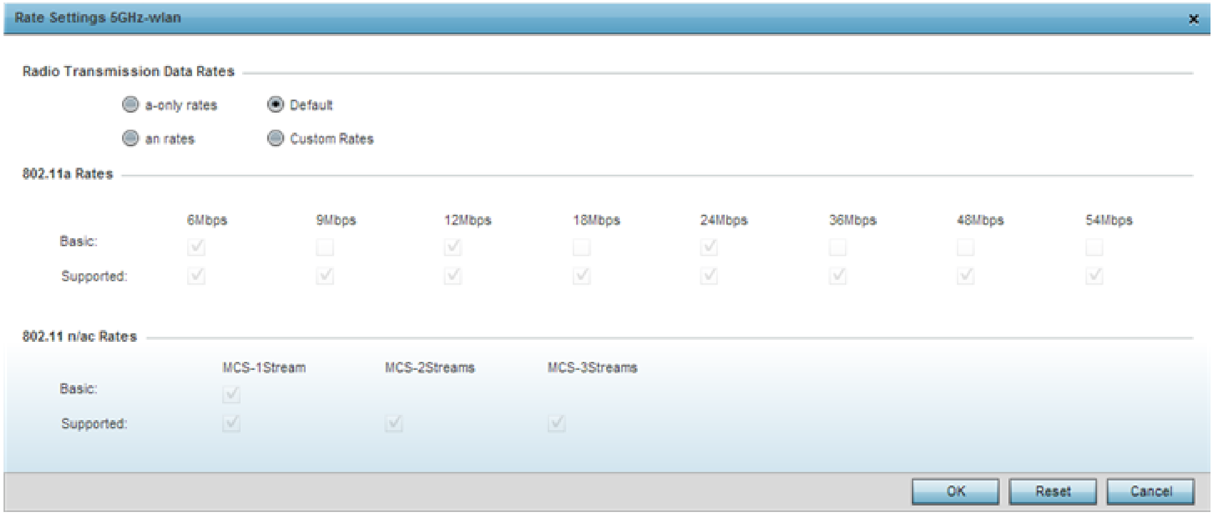


Figure 193: Advanced WLAN Rate Settings 2.4 GHz Screen



Radio Transmission Data Rates

○ a-only rates ● Default
○ an rates ○ Custom Rates

802.11a Rates

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	☑	☐	☑	☐	☑	☐	☐	☐
Supported:	☑	☑	☑	☑	☑	☑	☑	☑

802.11 n/ac Rates

	MCS-1Stream	MCS-2Streams	MCS-3Streams
Basic:	☑		
Supported:	☑	☑	☑

Figure 194: Advanced WLAN Rate Settings 5 GHz Screen

Define both minimum Basic and optimal Supported rates as required for the 802.11b rates, 802.11g rates and 802.11n supported by the 2.4 GHz band and the 802.11a and 802.11n rates supported by the 5.0 GHz band. These are the supported client rates within this WLAN.

802.11n MCS rates are defined as follows, both with and without short guard intervals (SGI):

Table 9: 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 10: 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

Table 10: MCS-2 Stream (continued)

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI
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 11: 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 12: 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
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260

Table 12: 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
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

7 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.

8 Enable **HTTP Analysis** for log file analysis on this WLAN.

This setting is disabled by default.

9 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.

10 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	Enter a **`Hostname`** or **`IP Address`** for the syslog server to forward HTTP analytics. Hostnames cannot include an underscore character.
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`**.

11 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

The Auto Shutdown feature causes the WLAN to shut down when certain criteria are met. It also allows administrators to set the operating days and hours of certain WLANs for security or bandwidth purposes.

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**.

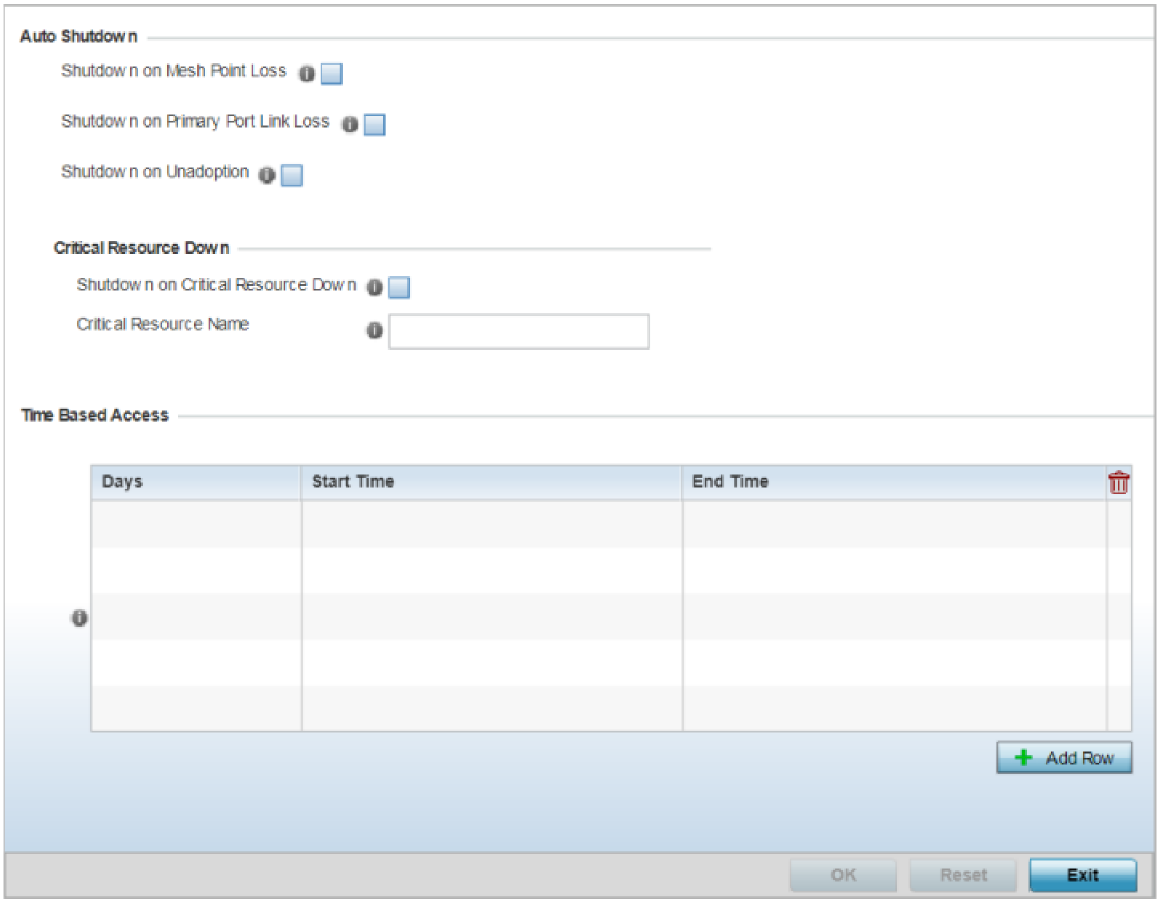


Figure 195: WLAN - Auto Shutdown Screen

4 Refer to the **Auto Shutdown** field to set the WLAN's shutdown criteria.

Shutdown on Mesh Point Loss	Select this option to automatically disable the WLAN when its associated mesh point (mesh dedicated access point) is unreachable. This setting is disabled by default.
Shutdown on Primary Port Link Loss	Select this option to automatically disable the WLAN when its primary port link is unreachable. This setting is disabled by default.
Shutdown on Unadoption	Select this option to automatically disable the WLAN when associated accesspoints are unadopted. 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.

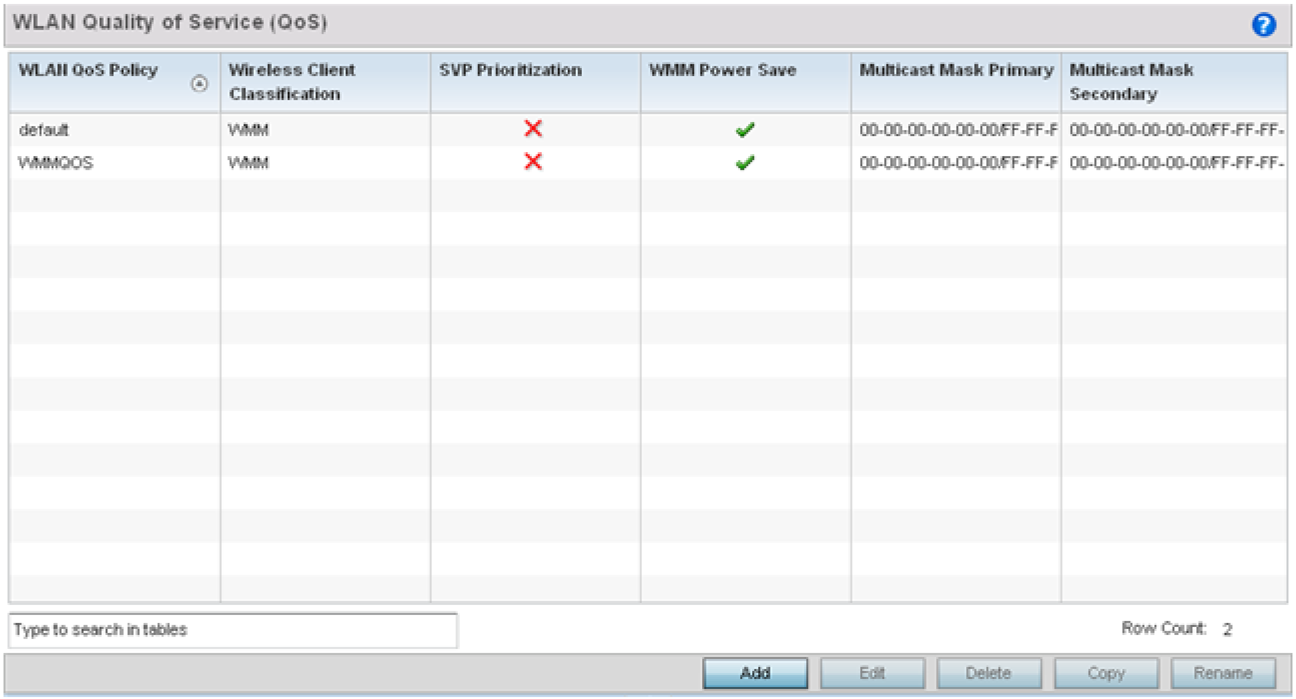
Use the WLAN Quality of Service (QoS) Policy screen to add a new QoS policy or edit the attributes of an existing policy.

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.



WLAN QoS Policy	Wireless Client Classification	SVP Prioritization	WMM Power Save	Multicast Mask Primary	Multicast Mask Secondary
default	WMM	✗	✓	00-00-00-00-00-00/FF-FF-F	00-00-00-00-00-00/FF-FF-FF-
WMMQOS	WMM	✗	✓	00-00-00-00-00-00/FF-FF-F	00-00-00-00-00-00/FF-FF-FF-

Figure 196: 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: • `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. • `Voice`– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • `Video` – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • `Normal` – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • `Low` – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio. • `Non-Unicast` – Optimized for non-Unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multicast.
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 381
- Configuring a WLAN's QoS Rate Limit Settings on page 385
- Configuring Multimedia Optimizations on page 390

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

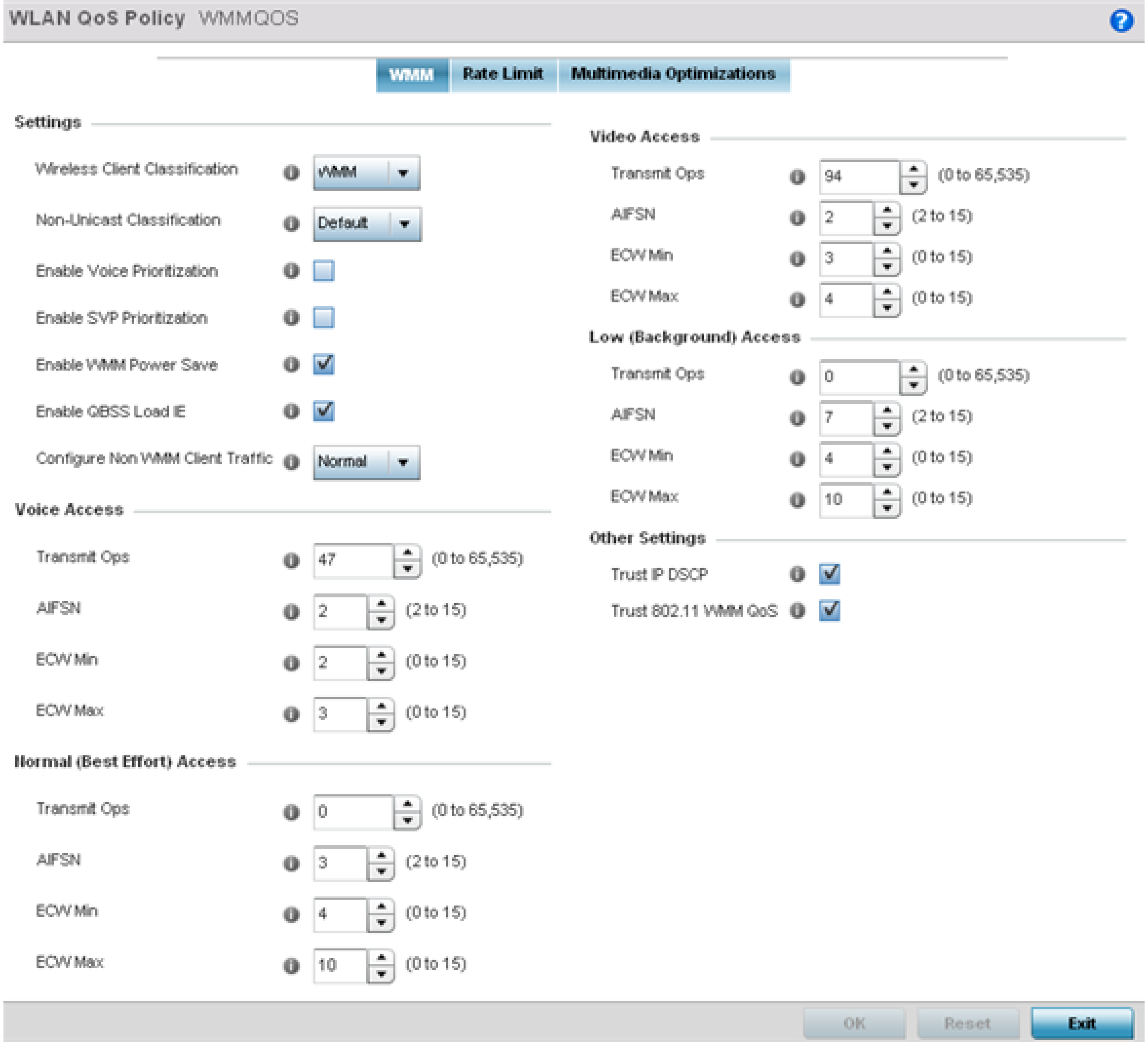
Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

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.



Settings

Wireless Client Classification: WMM
Non-Unicast Classification: Default
Enable Voice Prioritization ☐
Enable SVP Prioritization ☐
Enable WMM Power Save ☑
Enable QBSS Load IE ☑
Configure Non WMM Client Traffic: Normal

Voice Access

Transmit Ops: 47 (0 to 65,535)
AIFSN: 2 (2 to 15)
ECW Min: 2 (0 to 15)
ECW Max: 3 (0 to 15)

Normal (Best Effort) Access

Transmit Ops: 0 (0 to 65,535)
AIFSN: 3 (2 to 15)
ECW Min: 4 (0 to 15)
ECW Max: 10 (0 to 15)

Video Access

Transmit Ops: 94 (0 to 65,535)
AIFSN: 2 (2 to 15)
ECW Min: 3 (0 to 15)
ECW Max: 4 (0 to 15)

Low (Background) Access

Transmit Ops: 0 (0 to 65,535)
AIFSN: 7 (2 to 15)
ECW Min: 4 (0 to 15)
ECW Max: 10 (0 to 15)

Other Settings

Trust IP DSCP ☑
Trust 802.11 WMM QoS ☑

Figure 197: 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: • **`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. • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
Non-Unicast Classification	Use the drop-down menu to select the Non-Unicast Classification for this WLAN's intended traffic. Non-unicast classification types include: • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
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 select the Non-WMM client traffic Classification. brNon-WMM classification types include: • **`Voice`**– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. • **`Video`** – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. • **`Normal`** – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. • **`Low`** – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.

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

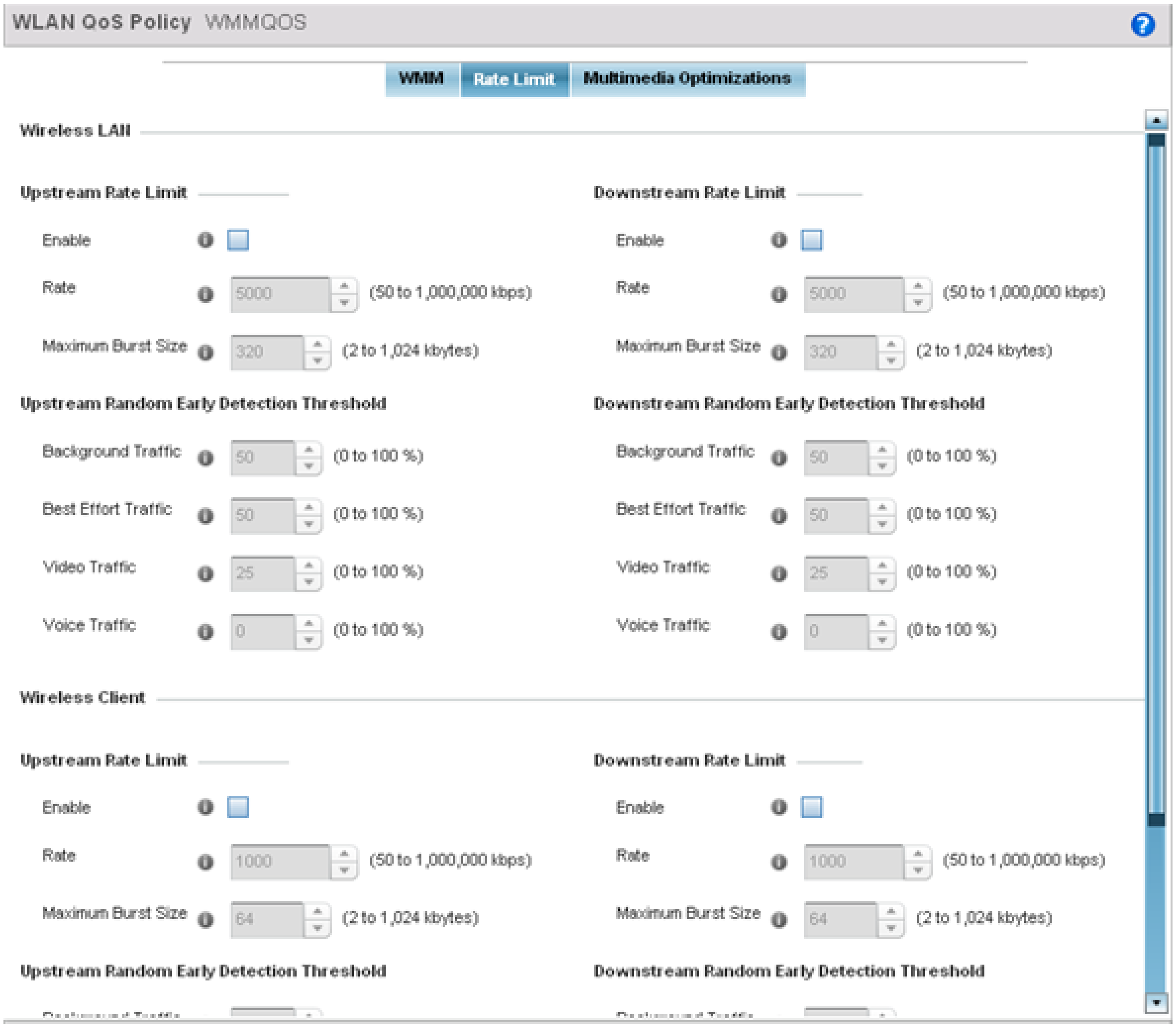
Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the 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.

Connected wireless clients can also have QoS rate limit settings defined in both the *upstream* and *downstream* direction.

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 Rate Limit tab.



WLAN QoS Policy WMMQOS

Wireless LAN

Upstream Rate Limit
Enable ☐
Rate 5000 (50 to 1,000,000 kbps)
Maximum Burst Size 320 (2 to 1,024 kbytes)

Downstream Rate Limit
Enable ☐
Rate 5000 (50 to 1,000,000 kbps)
Maximum Burst Size 320 (2 to 1,024 kbytes)

Upstream Random Early Detection Threshold
Background Traffic 50 (0 to 100 %)
Best Effort Traffic 50 (0 to 100 %)
Video Traffic 25 (0 to 100 %)
Voice Traffic 0 (0 to 100 %)

Downstream Random Early Detection Threshold
Background Traffic 50 (0 to 100 %)
Best Effort Traffic 50 (0 to 100 %)
Video Traffic 25 (0 to 100 %)
Voice Traffic 0 (0 to 100 %)

Wireless Client

Upstream Rate Limit
Enable ☐
Rate 1000 (50 to 1,000,000 kbps)
Maximum Burst Size 64 (2 to 1,024 kbytes)

Downstream Rate Limit
Enable ☐
Rate 1000 (50 to 1,000,000 kbps)
Maximum Burst Size 64 (2 to 1,024 kbytes)

Upstream Random Early Detection Threshold

Downstream Random Early Detection Threshold

Figure 198: WLAN QoS Policy Screen - Rate Limit Tab

4 Configure the following parameters to define the **WLAN Upstream Rate Limit**. These values apply to traffic from the controller to associated access point radios and connected wireless clients.

Enable	Select this option to enable rate limiting for data transmitted from the controller to associated access point radios and connected wireless 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 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 and the controller or service platform.

Enable	Select this option to enable rate limiting for data transmitted from the controller or service platform to its associated access point radios and 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 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 the client to its associated access point radio and connected wireless controller. Enabling this option does not invoke client 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. The default burst size is 64 kbytes.

9 Set the following **Upstream Random Early Detection Threshold** settings for each access category.

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. 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. 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. 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. 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 traffic from a controller or service platform to associated access point radios and the wireless client.

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 between 2 - 64 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

11 Set the following **Downstream Random Early Detection Threshold** settings.

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. 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. 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. 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. The default threshold is 0%.0% means no early random drops will occur.

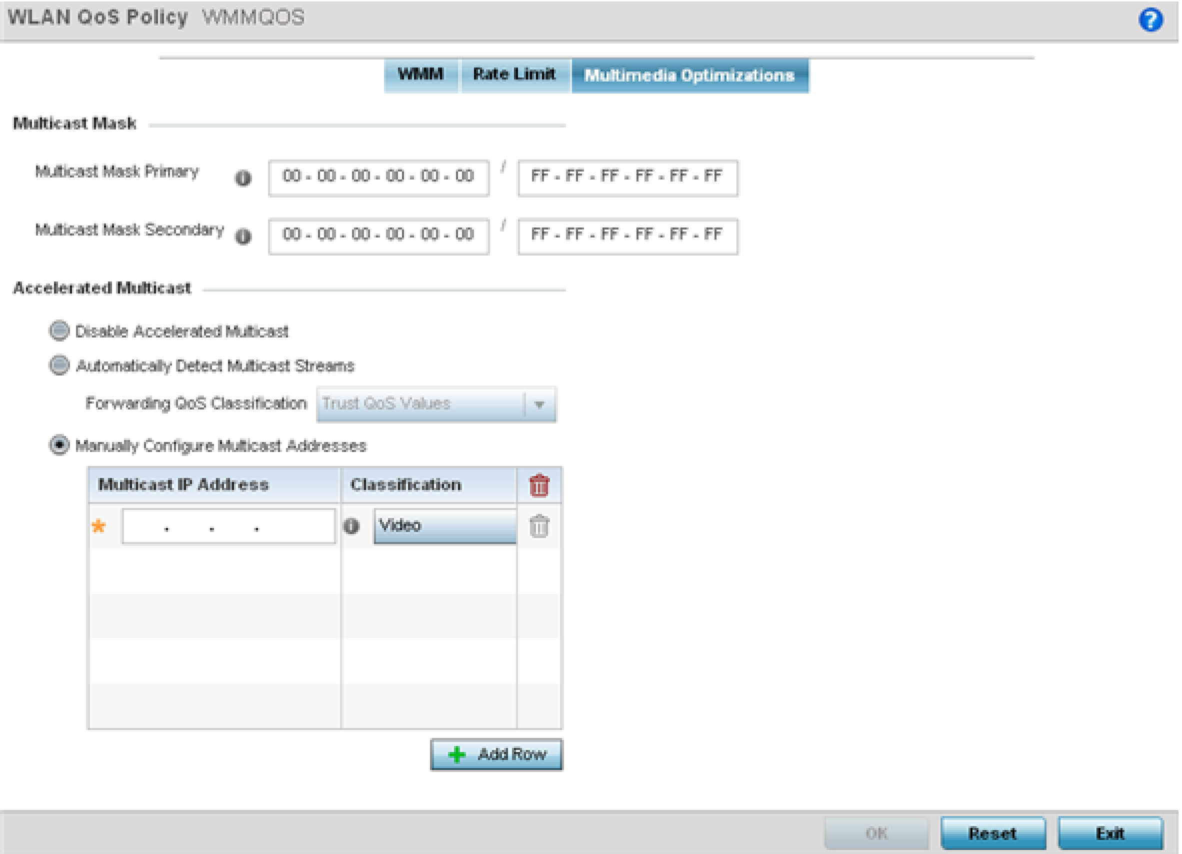
12 Click **OK** when completed to update this WLAN's QoS rate limit settings. Click **Reset** to revert the screen to its last saved configuration.

Configuring Multimedia Optimizations

Multimedia optimizations customize the size and speed of multimedia content (voice, video etc.) to deliver WLAN traffic strategically to the WLAN's managed clients and their defined QoS requirements.

To configure a QoS rate limit configuration for a controller, service platform or access point managed 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.



WLAN QoS Policy WMMQOS

Multicast Mask

Multicast Mask Primary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

Multicast Mask Secondary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

Accelerated Multicast

○ Disable Accelerated Multicast

○ Automatically Detect Multicast Streams

Forwarding QoS Classification Trust QoS Values

● Manually Configure Multicast Addresses

Multicast IP Address	Classification
. . .	Video

Figure 199: 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 in case the primary becomes unavailable.

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.
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. A WiNG 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.

WiNG managed controllers, service platforms and access points include *Session Initiation Protocol* (SIP), *Skinny Call Control Protocol* (SCCP), and *Application Layer Gateways* (ALGs) that enable devices to identify voice streams and dynamically set voice call bandwidth. Controllers use the data to provide prioritization and admission control to these devices without requiring TSPEC or WMM client support.

WiNG managed controllers, service platforms, and access points support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

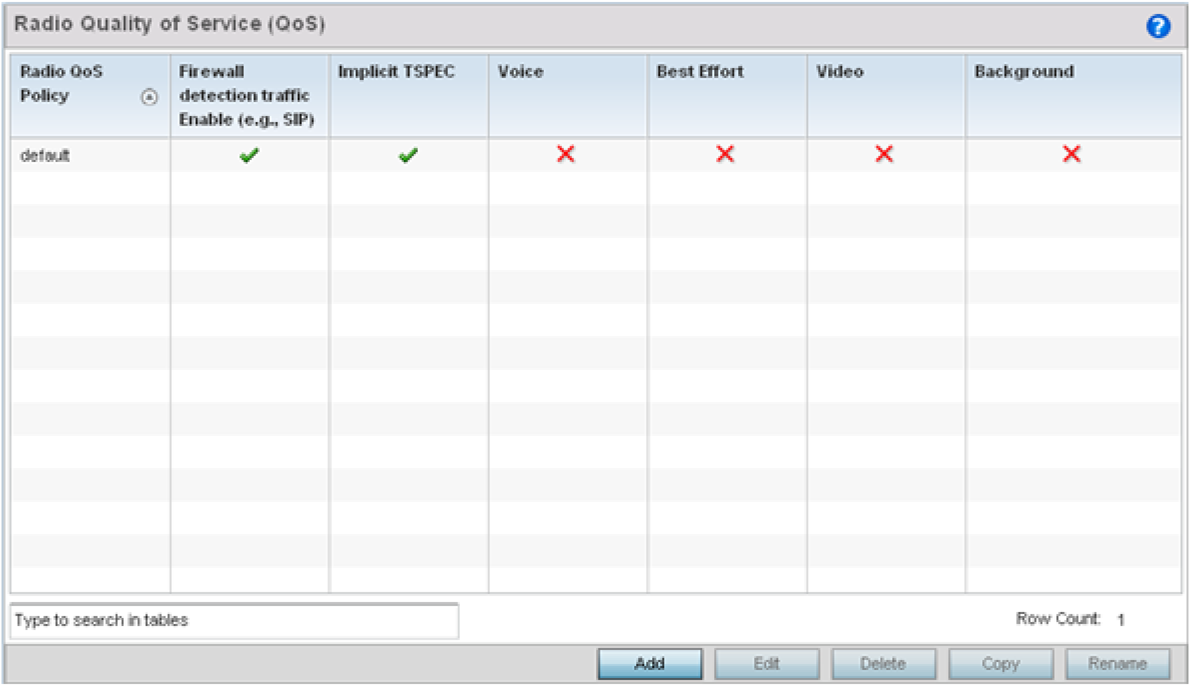
Note
Statically setting a WLAN WMM access category value prioritizes traffic to the client, but does not prioritize traffic from the client.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using *Vendor Specific Attributes* (VSAs). Rate limits can be applied to authenticating users using 802.1X, captive portal authentication and 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.



Radio QoS Policy	Firewall detection traffic Enable (e.g., SIP)	Implicit TSPEC	Voice	Best Effort	Video	Background
default	✓	✓	✗	✗	✗	✗

Row Count: 1

Figure 200: Radio QoS Policy Screen

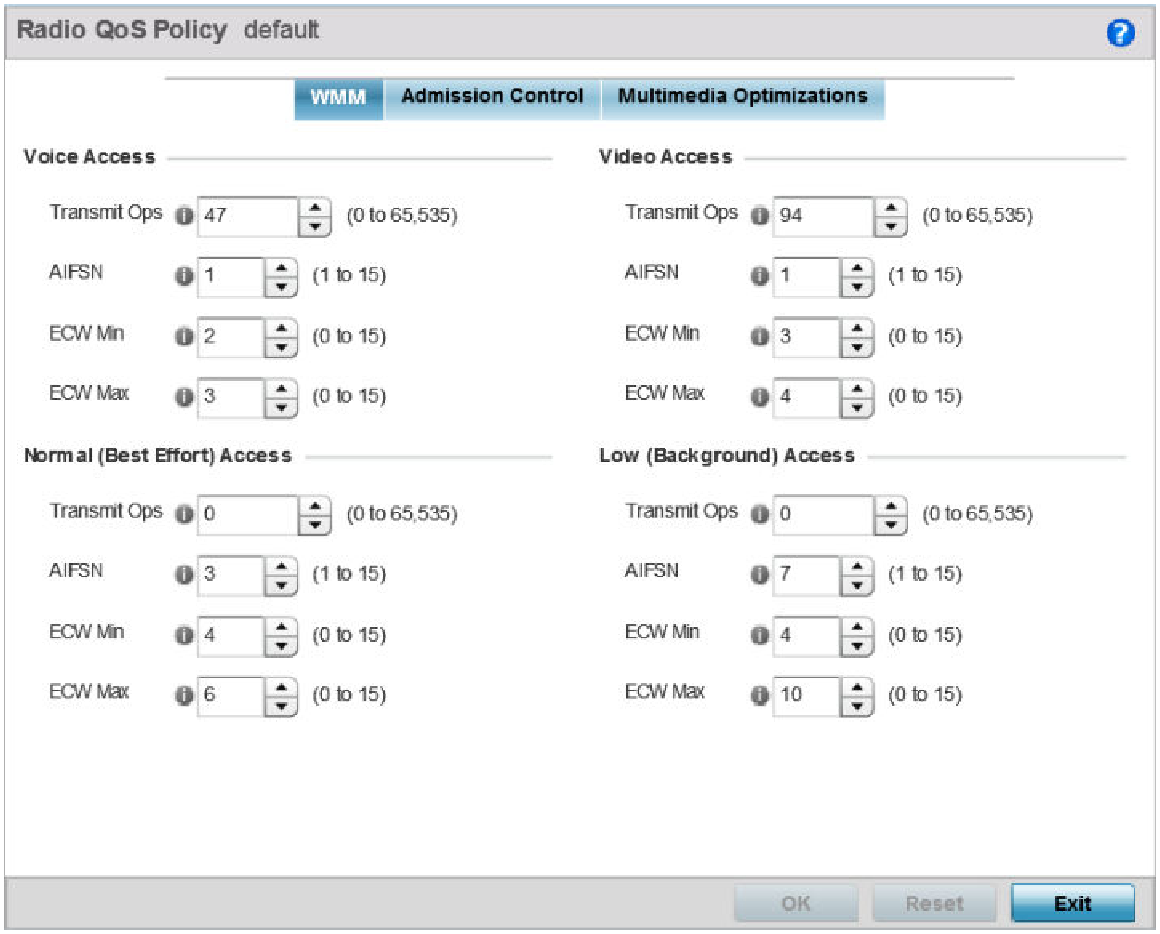
The Radio QoS Policy screen lists those radio QoS policies created thus far. Any of these policies can be selected and applied.

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.

Optionally, **Copy** or **Rename** QoS policies as needed.



Radio QoS Policy default

Voice Access

Transmit Ops 47 (0 to 65,535)
AIFSN 1 (1 to 15)
ECW Min 2 (0 to 15)
ECW Max 3 (0 to 15)

Video Access

Transmit Ops 94 (0 to 65,535)
AIFSN 1 (1 to 15)
ECW Min 3 (0 to 15)
ECW Max 4 (0 to 15)

Normal (Best Effort) Access

Transmit Ops 0 (0 to 65,535)
AIFSN 3 (1 to 15)
ECW Min 4 (0 to 15)
ECW Max 6 (0 to 15)

Low (Background) Access

Transmit Ops 0 (0 to 65,535)
AIFSN 7 (1 to 15)
ECW Min 4 (0 to 15)
ECW Max 10 (0 to 15)

Figure 201: 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.

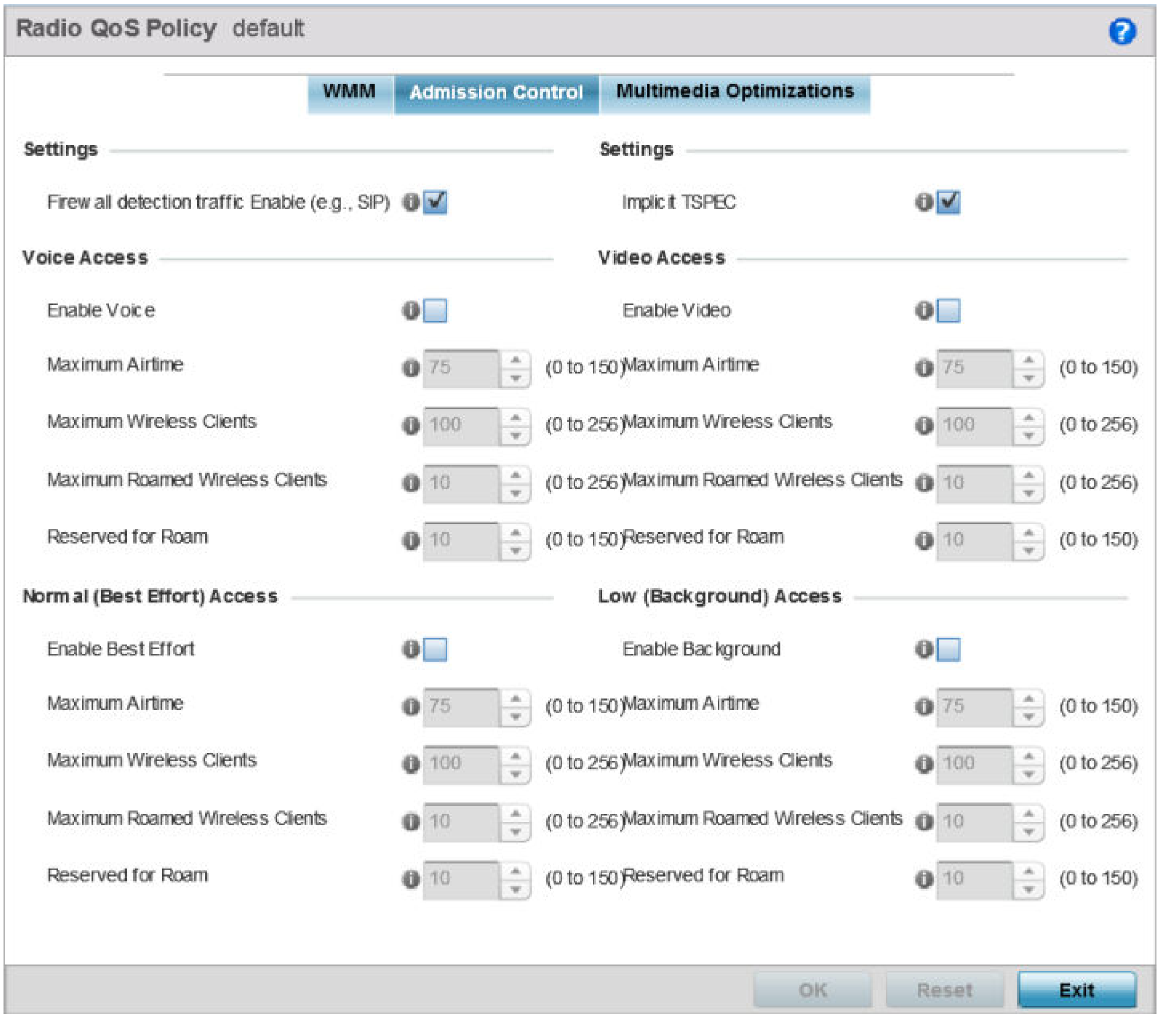
ECW Min	The **ECW Min** is combined with the **ECW Max** to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 4.
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.



Radio QoS Policy default

Settings

Firewall detection traffic Enable (e.g., SIP) ☑

Settings

Implicit TSPEC ☑

Voice Access

Enable Voice ☐
Maximum Airtime 75 (0 to 150)
Maximum Wireless Clients 100 (0 to 256)
Maximum Roamed Wireless Clients 10 (0 to 256)
Reserved for Roam 10 (0 to 150)

Video Access

Enable Video ☐
Maximum Airtime 75 (0 to 150)
Maximum Wireless Clients 100 (0 to 256)
Maximum Roamed Wireless Clients 10 (0 to 256)
Reserved for Roam 10 (0 to 150)

Normal (Best Effort) Access

Enable Best Effort ☐
Maximum Airtime 75 (0 to 150)
Maximum Wireless Clients 100 (0 to 256)
Maximum Roamed Wireless Clients 10 (0 to 256)
Reserved for Roam 10 (0 to 150)

Low (Background) Access

Enable Background ☐
Maximum Airtime 75 (0 to 150)
Maximum Wireless Clients 100 (0 to 256)
Maximum Roamed Wireless Clients 10 (0 to 256)
Reserved for Roam 10 (0 to 150)

Figure 202: 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:

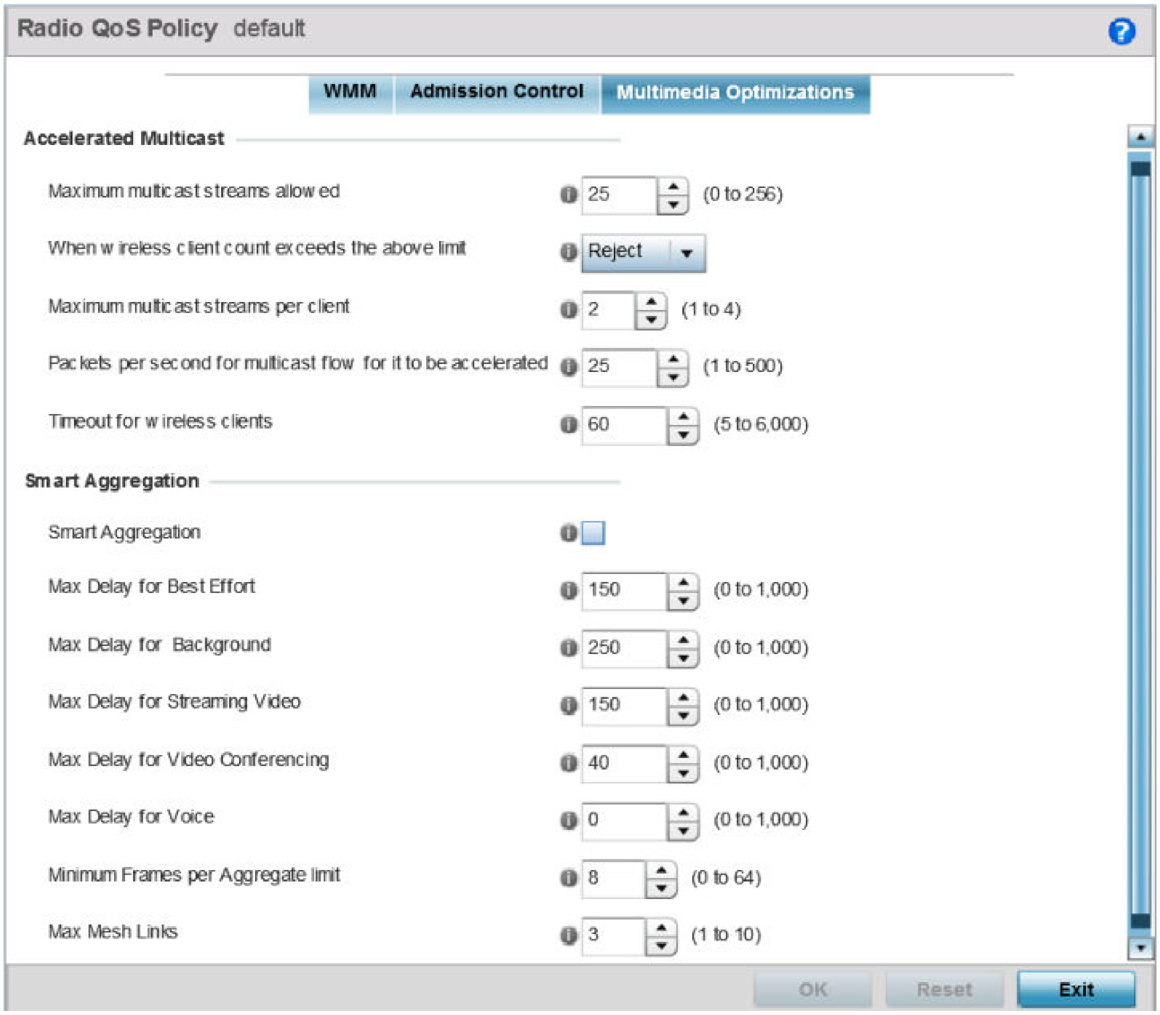
Enable Video	Select the check box to enable admission control for this policy's video traffic. Only video traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
Maximum Airtime	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.



Accelerated Multicast

Maximum multicast streams allowed: 25 (0 to 256)
When wireless client count exceeds the above limit: Reject
Maximum multicast streams per client: 2 (1 to 4)
Packets per second for multicast flow for it to be accelerated: 25 (1 to 500)
Timeout for wireless clients: 60 (5 to 6,000)

Smart Aggregation

Smart Aggregation: ☐
Max Delay for Best Effort: 150 (0 to 1,000)
Max Delay for Background: 250 (0 to 1,000)
Max Delay for Streaming Video: 150 (0 to 1,000)
Max Delay for Video Conferencing: 40 (0 to 1,000)
Max Delay for Voice: 0 (0 to 1,000)
Minimum Frames per Aggregate limit: 8 (0 to 64)
Max Mesh Links: 3 (1 to 10)

Figure 203: 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 371.

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.

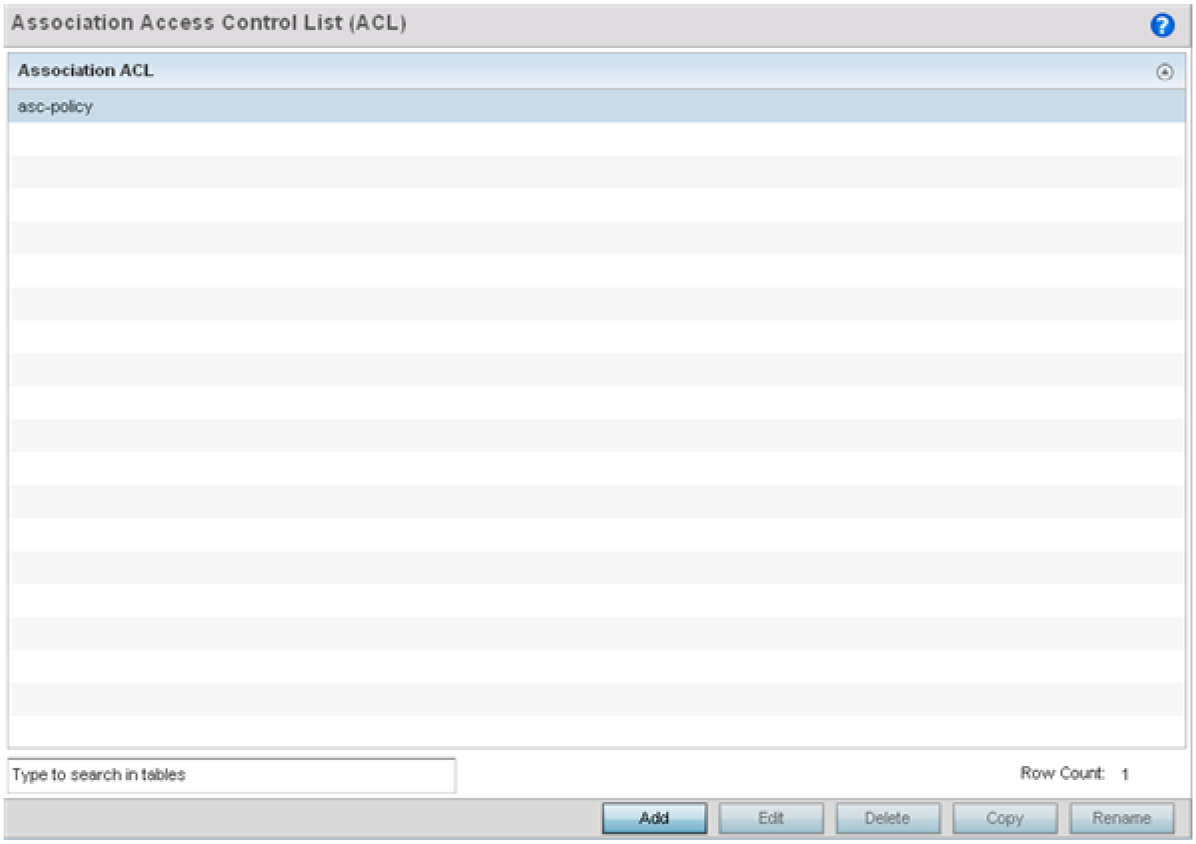
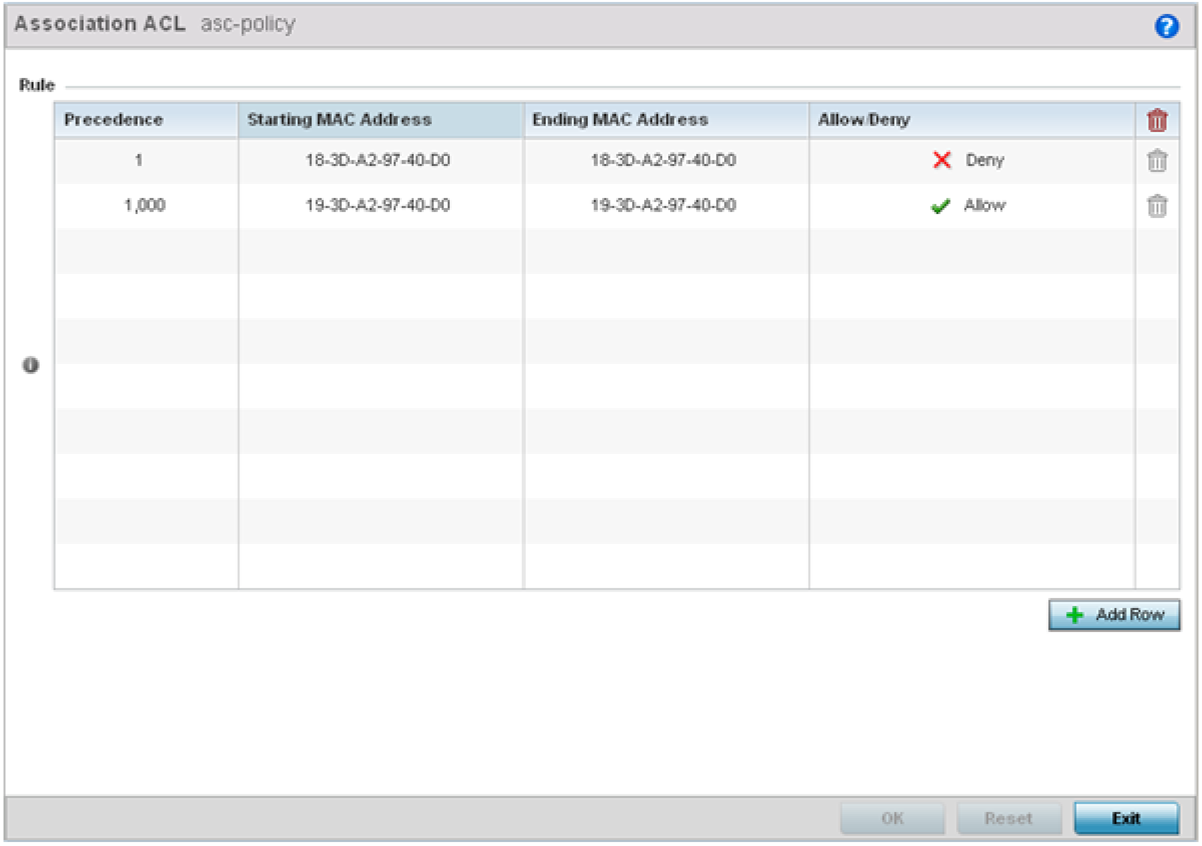


Figure 204: Association Access Control List (ACL) Screen

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.



Precedence	Starting MAC Address	Ending MAC Address	Allow/Deny
1	18-3D-A2-97-40-D0	18-3D-A2-97-40-D0	✗ Deny
1,000	19-3D-A2-97-40-D0	19-3D-A2-97-40-D0	✓ Allow

Figure 205: 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 MAC address for clients requesting association.
Ending MAC Address	Provide an ending MAC address for clients requesting association.
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 radio. Smart RF policies can be added to specific RF Domains to apply site specific deployment configurations and self-healing values to device groups.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using data obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the network for external WiFi interference, neighbor WiFi interference, non-WiFi interference and client connectivity. Smart RF then intelligently applies various algorithms to arrive at the optimal channel and power selection for all access points in the network and constantly reacts to changes in the RF environment.

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.

Smart RF is supported on any RF Domain manager. In standalone environments, an individual controller, service platform or access point manages the calibration and monitoring phases. In clustered environments, a single device is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

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.

Configuring Smart RF Basic Settings

To define a Smart RF policy:

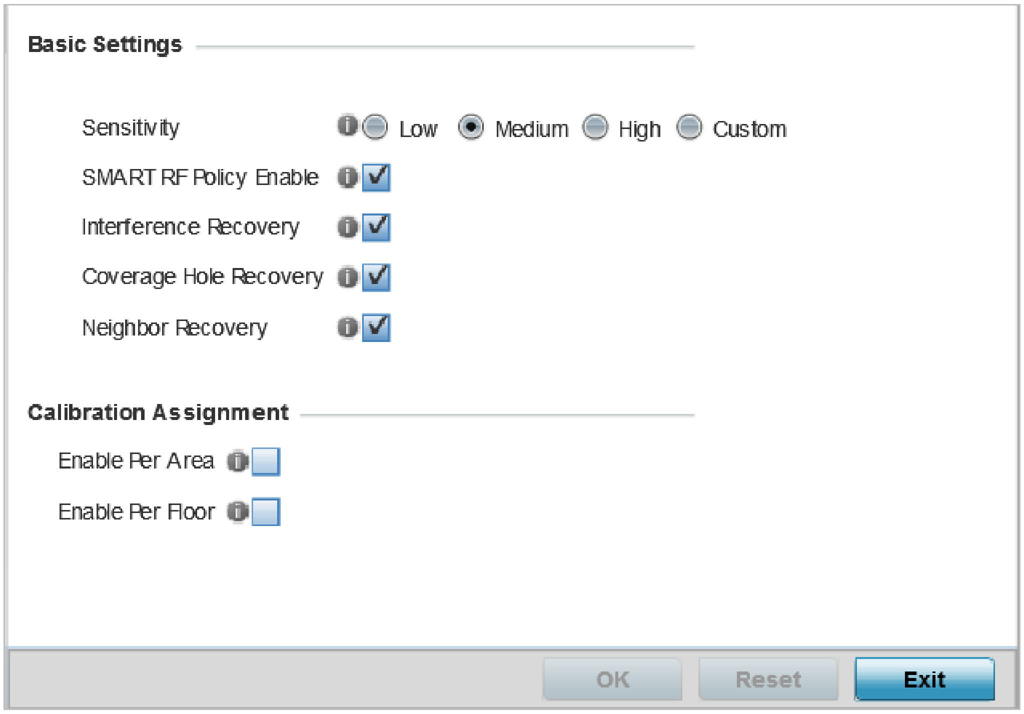
1 Refer to the following configuration data for existing Smart RF policies:

Smart RF Policy	Displays the name assigned to the Smart RF policy when it was initially created. The name cannot be modified as part of the edit process.
Smart RF Policy Enable	Displays a green check mark if Smart RF has been enabled for the listed policy. A red “X” designates the policy as being disabled.
Interference Recovery	Displays a green check mark if interference recovery has been enabled for the listed policy. A red “X” designates interference recovery being disabled.
Coverage Hole Recovery	Displays a green check mark if coverage hole recovery has been enabled for the listed policy. A red “X” designates coverage hole recovery being disabled.
Neighbor Recovery	Displays a green check mark if neighbor recovery has been enabled for the listed policy. A red “X” designates neighbor recovery being disabled.

2 Click **Add** to create a new Smart RF 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** Smart RF policies as needed.

The Basic Configuration screen displays by default for new or modified Smart RF policies.



Basic Settings

Sensitivity ○ Low ● Medium ○ High ○ Custom

SMART RF Policy Enable ☑

Interference Recovery ☑

Coverage Hole Recovery ☑

Neighbor Recovery ☑

Calibration Assignment

Enable Per Area ☐

Enable Per Floor ☐

Figure 206: 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. The **Custom** option allows an administrator to adjust the parameters and thresholds for **Interference Recovery**, **Coverage Hole Recovery**, and **Neighbor Recovery**. Using the **Low**, **Medium** (recommended), and **High** settings still allows these features to be utilized.
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 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.
Neighbor Recovery	Select this option to enable Neighbor Recovery when a failed radio is detected within the Smart RF supported radio coverage area. Smart RF can provide automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor Recovery is enabled by default when the sensitivity setting is **`Medium`**.

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.

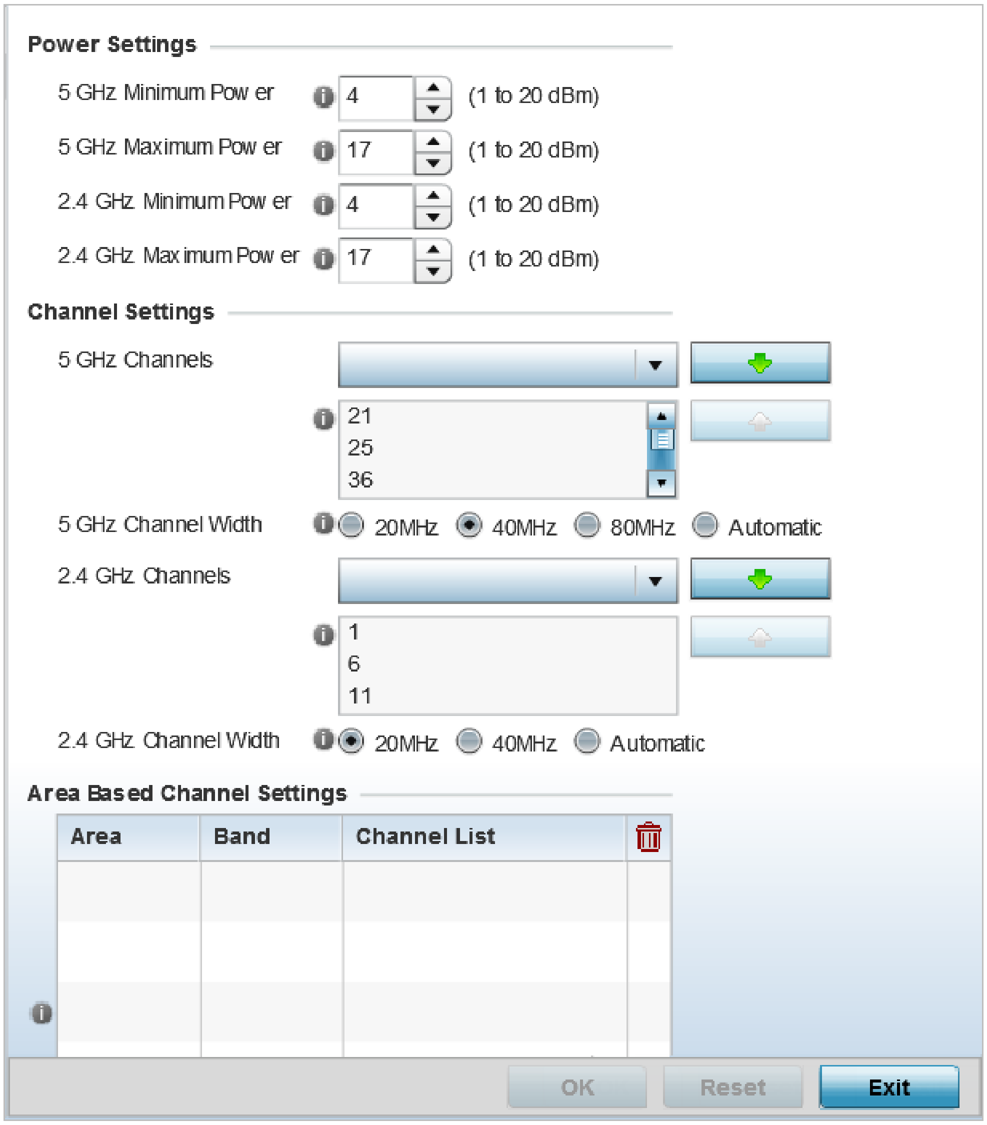
Configuring Smart RF Channel & Power Settings

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 5 and 2.4 GHz radios and select channel settings in respect to the device channel usage.

Note
The **Power Settings** and **Channel Settings** parameters are enabled only when **`Custom`** or **`Medium`** is selected as the **Sensitivity** setting from the Basic Configuration screen.



Power Settings

5 GHz Minimum Power: 4 (1 to 20 dBm)
5 GHz Maximum Power: 17 (1 to 20 dBm)
2.4 GHz Minimum Power: 4 (1 to 20 dBm)
2.4 GHz Maximum Power: 17 (1 to 20 dBm)

Channel Settings

5 GHz Channels: 21, 25, 36
5 GHz Channel Width: ○ 20MHz ● 40MHz ○ 80MHz ○ Automatic
2.4 GHz Channels: 1, 6, 11
2.4 GHz Channel Width: ● 20MHz ○ 40MHz ○ Automatic

Area Based Channel Settings

Area	Band	Channel List

Figure 207: 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. If you are deploying an 802.11ac supported Access Point, 80MHz channel width options are available as well.
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	Specify the deployment area assigned to the listed policy when deployed a means of identifying the devices physical locations.
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.

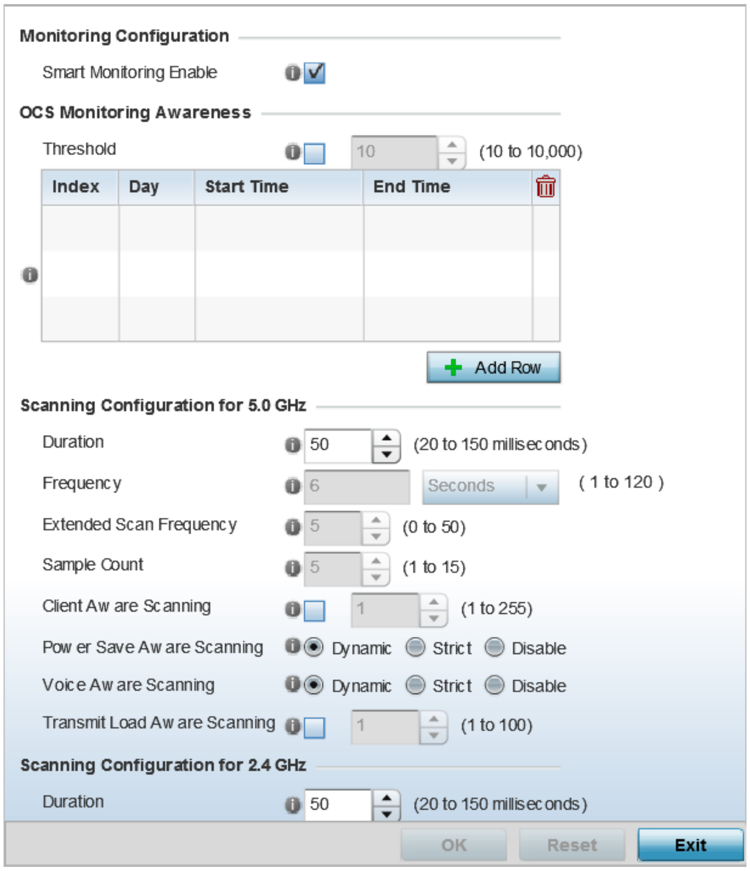
5 Click **OK** to update the Smart RF and Power settings for this policy.

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

Configuring Smart RF Scanning Configuration

To configure the Smart RF scanning configuration:

1 Select **Scanning Configuration**.



Monitoring Configuration

Smart Monitoring Enable ☑

OCS Monitoring Awareness

Threshold ☐ 10 (10 to 10,000)

Index	Day	Start Time	End Time

Add Row

Scanning Configuration for 5.0 GHz

Duration 50 (20 to 150 milliseconds)

Frequency 6 Seconds (1 to 120)

Extended Scan Frequency 5 (0 to 50)

Sample Count 5 (1 to 15)

Client Aware Scanning ☐ 1 (1 to 255)

Power Save Aware Scanning ● Dynamic ○ Strict ○ Disable

Voice Aware Scanning ● Dynamic ○ Strict ○ Disable

Transmit Load Aware Scanning ☐ 1 (1 to 100)

Scanning Configuration for 2.4 GHz

Duration 50 (20 to 150 milliseconds)

Figure 208: 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.
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:

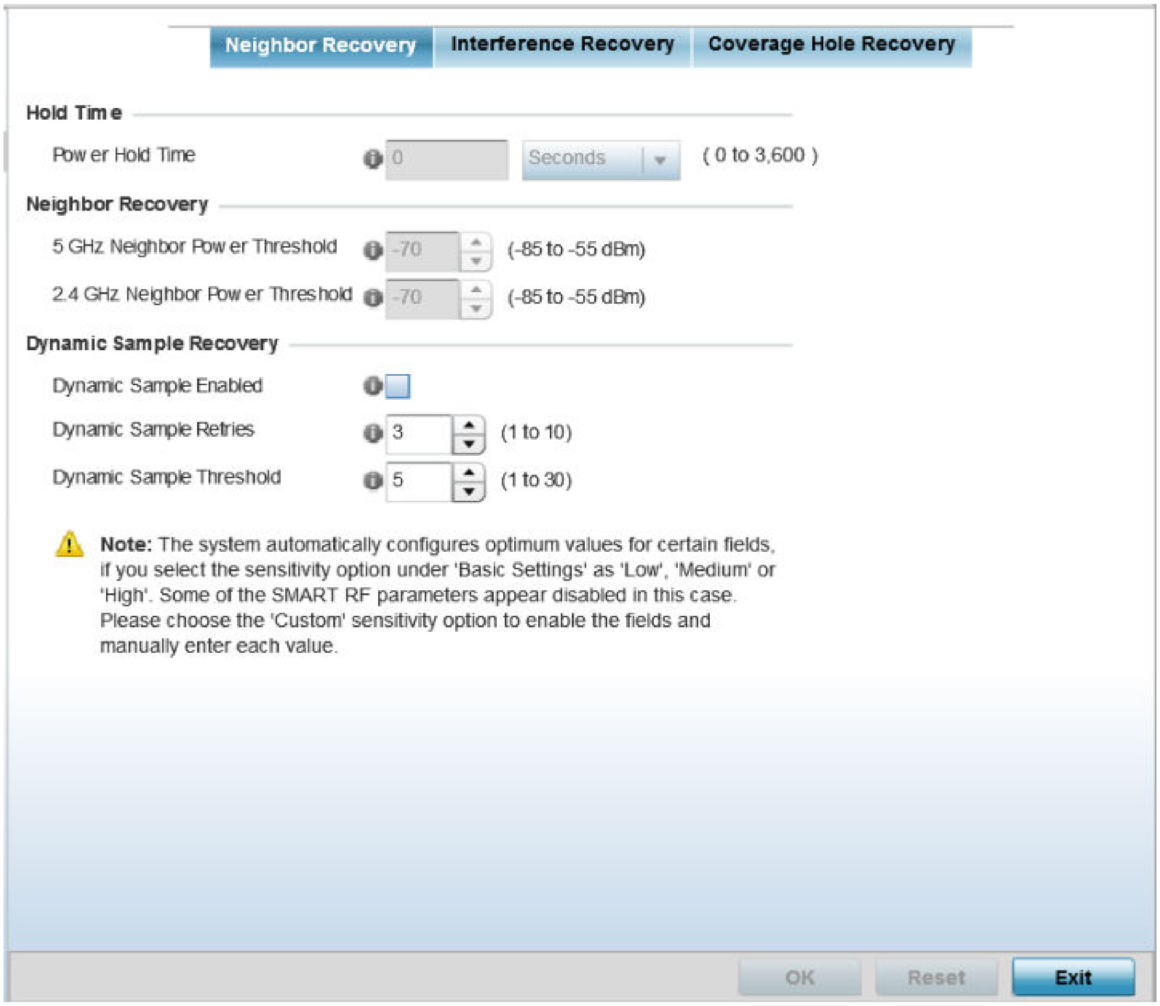
1 Select **Recovery**.

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 Basic Configuration screen.

The Neighbor Recovery tab displays by default. Use the Neighbor, Interference and Coverage Hole recovery tabs to define how 5 and 2.4 GHz radios compensate for failed neighbor radios, interference that affects the Smart RF supported network, and detected coverage holes that require 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.



Hold Time

Power Hold Time: 0 Seconds (0 to 3,600)

Neighbor Recovery

5 GHz Neighbor Power Threshold: -70 (-85 to -55 dBm)

2.4 GHz Neighbor Power Threshold: -70 (-85 to -55 dBm)

Dynamic Sample Recovery

Dynamic Sample Enabled: ☐

Dynamic Sample Retries: 3 (1 to 10)

Dynamic Sample Threshold: 5 (1 to 30)

Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.

Figure 209: 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 5.0 GHz radio uses if it is required to increase its output power to compensate for a failed radio within its wireless 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 2.4 GHz radio uses if it is required to increase its output power to compensate for a failed radio within its wireless 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 minimum number of sample reports (from 1- 30) used before a Smart RF power compensation requires dynamic sampling. The default setting is 5.

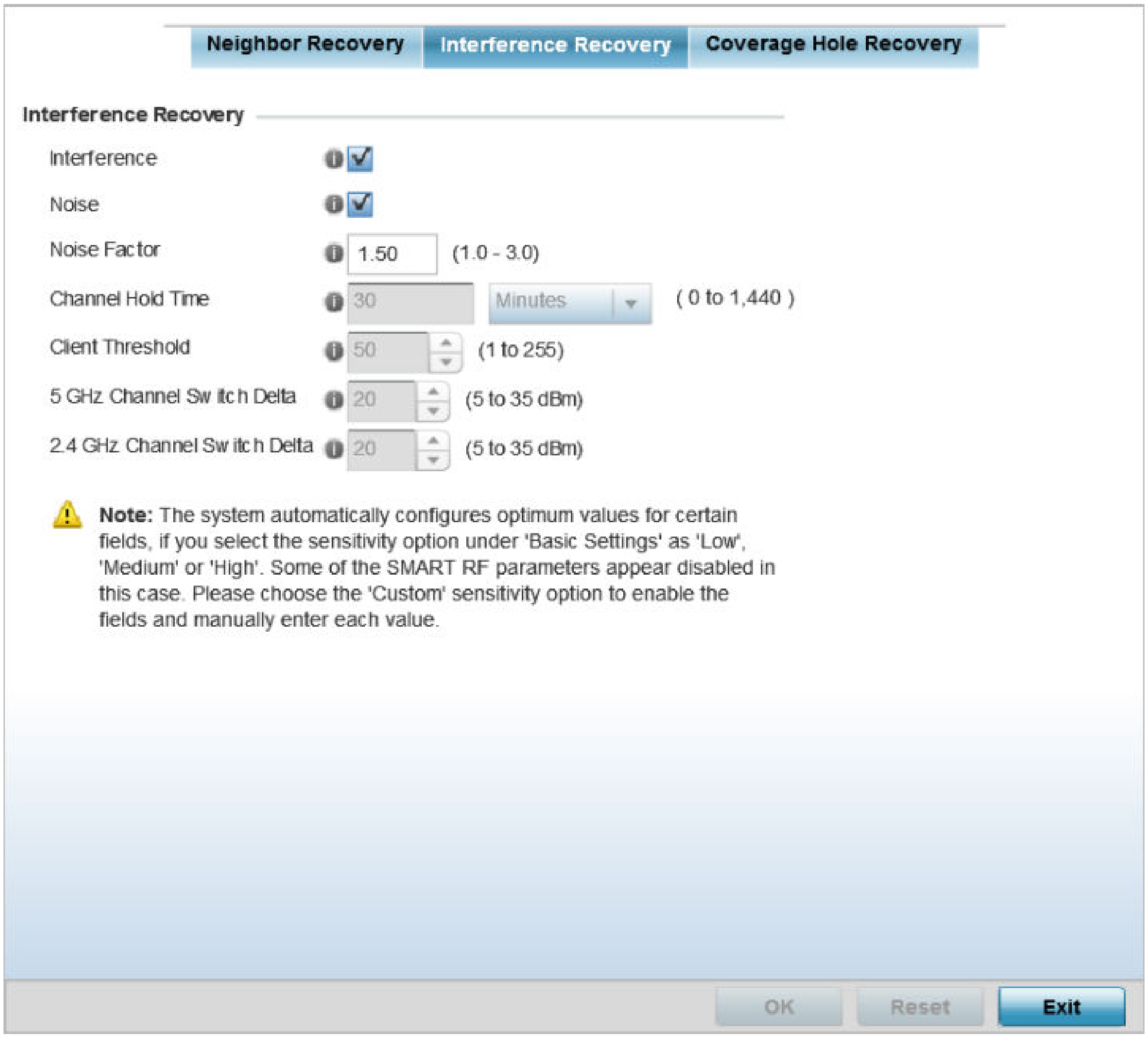
5 Click **OK** to update the Smart RF Neighbor Recovery settings for this policy.

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**.



Interference Recovery

Interference ☑

Noise ☑

Noise Factor 1.50 (1.0 - 3.0)

Channel Hold Time 30 Minutes (0 to 1,440)

Client Threshold 50 (1 to 255)

5 GHz Channel Switch Delta 20 (5 to 35 dBm)

2.4 GHz Channel Switch Delta 20 (5 to 35 dBm)

Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.

Figure 210: 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 devices 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. The default setting is 1.50.
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.

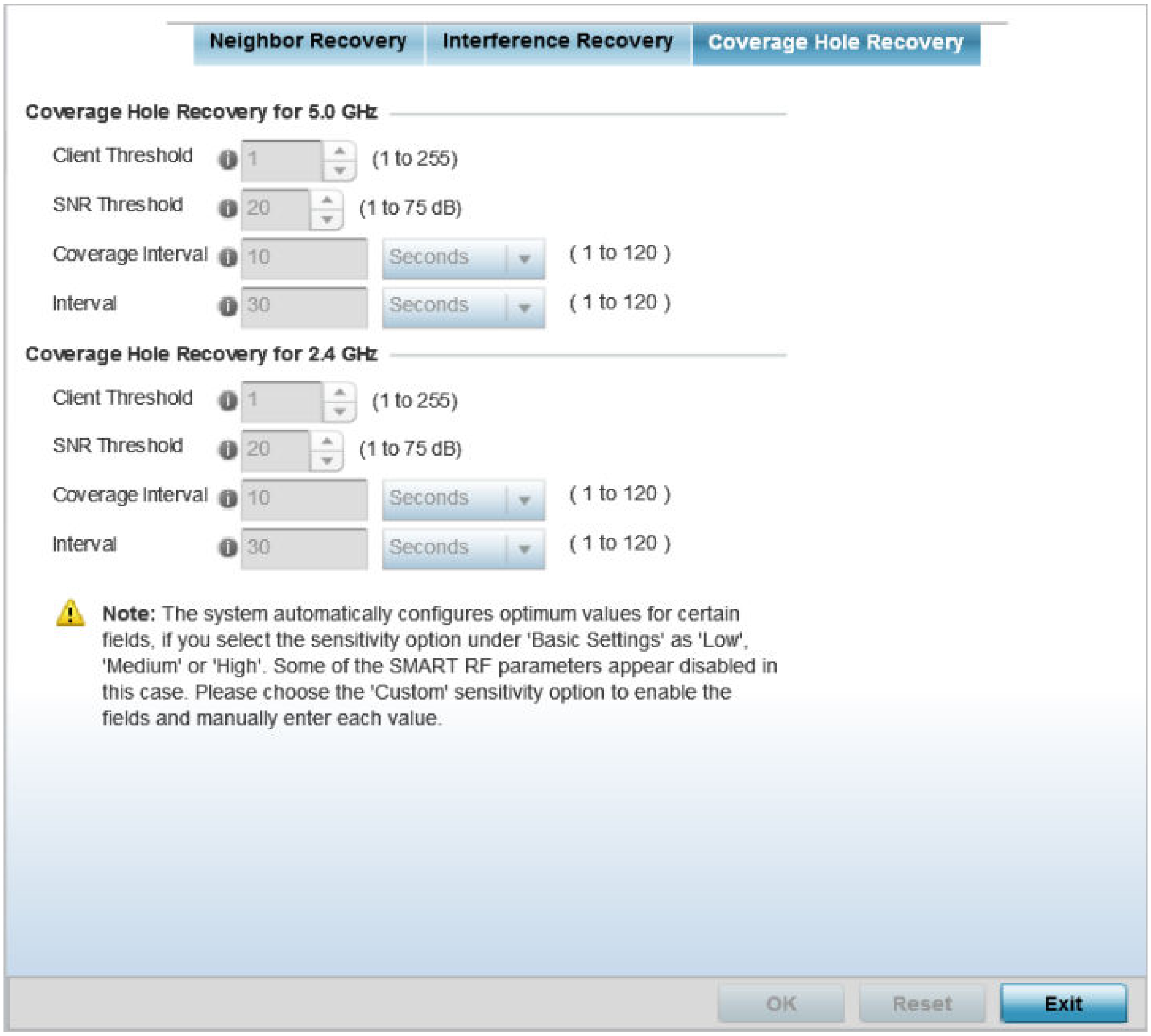
Client Threshold	Set a client threshold for the Smart RF policy between 1 - 255. If the set threshold number of clients are connected to a radio, the radio does not change its channel, even though required, based on the interference recovery determination made by the smart master. The default setting 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**.



Coverage Hole Recovery for 5.0 GHz

Client Threshold 1 (1 to 255)
SNR Threshold 20 (1 to 75 dB)
Coverage Interval 10 Seconds (1 to 120)
Interval 30 Seconds (1 to 120)

Coverage Hole Recovery for 2.4 GHz

Client Threshold 1 (1 to 255)
SNR Threshold 20 (1 to 75 dB)
Coverage Interval 10 Seconds (1 to 120)
Interval 30 Seconds (1 to 120)

Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.

Figure 211: 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. 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.

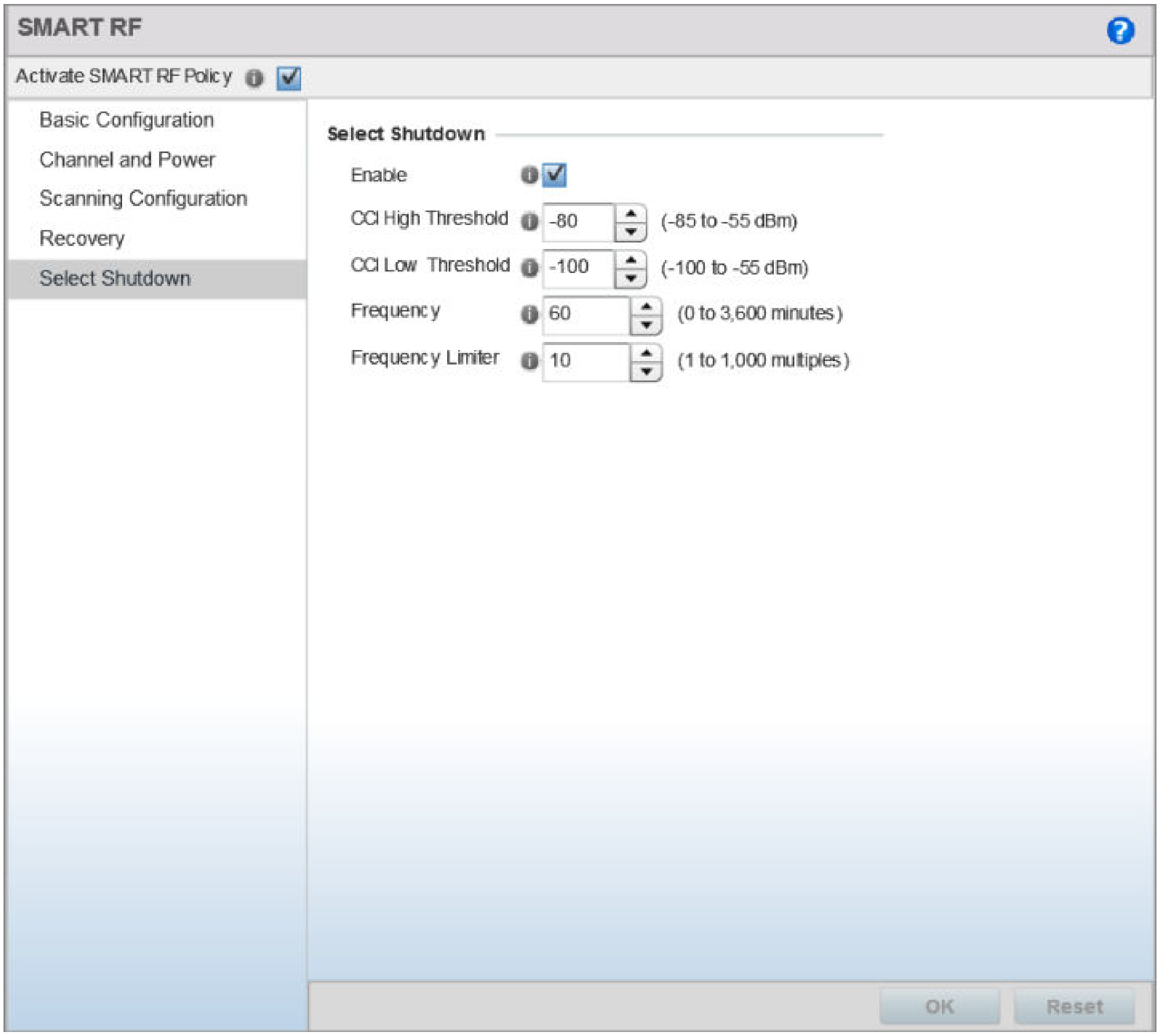
3 Click **OK** to update the Smart RF Coverage Hole Recovery settings for this policy.

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**,



SMART RF

Activate SMART RF Policy ☑

Select Shutdown

Enable ☑

CCI High Threshold -80 (-85 to -55 dBm)

CCI Low Threshold -100 (-100 to -55 dBm)

Frequency 60 (0 to 3,600 minutes)

Frequency Limiter 10 (1 to 1,000 multiples)

Figure 212: 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. 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. 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. 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. 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. 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. 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:

- 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.

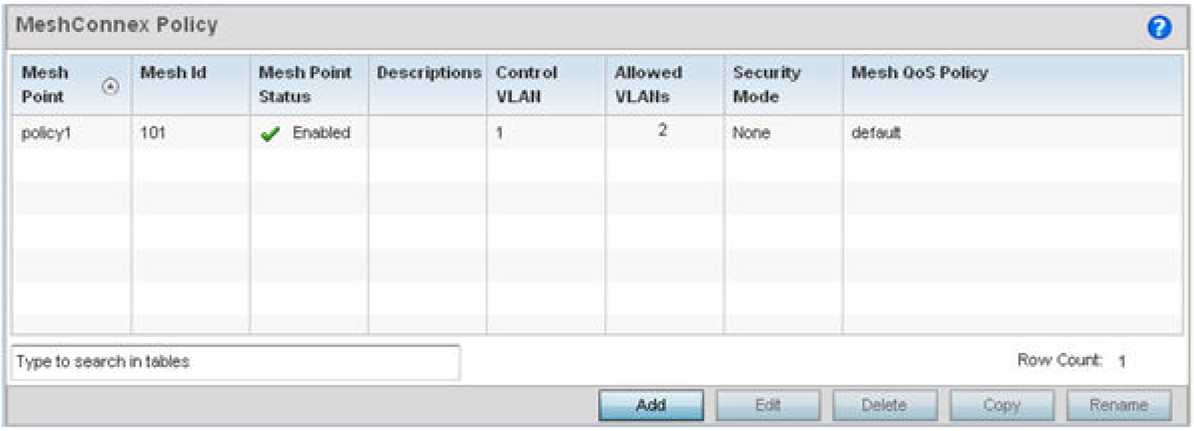
MeshConnex is designed for large-scale, high-mobility outdoor mesh deployments. MeshConnex continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MeshConnex uses this data to dynamically form and continually maintain paths for 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.

Configuring a MeshConnex Policy

To define a MeshConnex policy:

1 Select **Configuration** > **Wireless** > **MeshConnex Policy** tto display existing MeshConnex policies.



Mesh Point	Mesh Id	Mesh Point Status	Descriptions	Control VLAN	Allowed VLANs	Security Mode	Mesh QoS Policy
policy1	101	✓ Enabled		1	2	None	default

Figure 213: MeshConnex Policy Screen

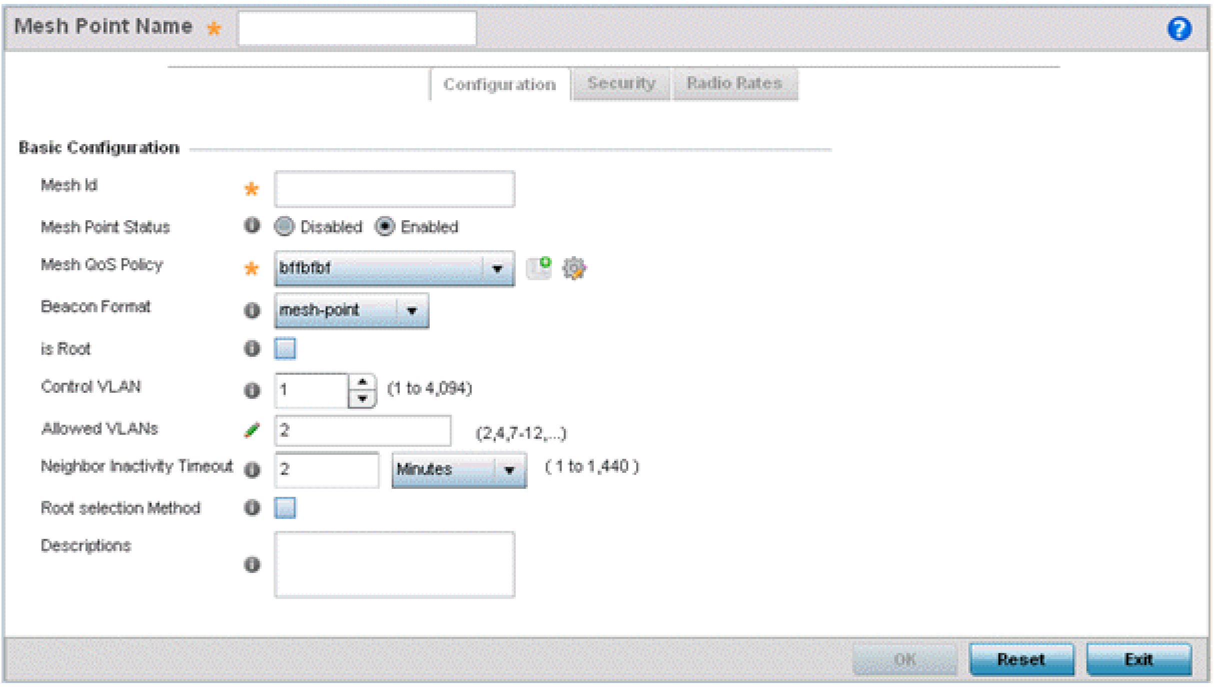
2 Refer to the following configuration data for existing MeshConnex policies:

Mesh Point Name	The administrator assigned name of each listed mesh point.
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.



Mesh Point Name *

Basic Configuration

Mesh Id *

Mesh Point Status ○ Disabled ● Enabled

Mesh QoS Policy * bffbfbf

Beacon Format mesh-point

is Root ☐

Control VLAN 1 (1 to 4,094)

Allowed VLANs 2 (2,4,7-12,...)

Neighbor Inactivity Timeout 2 Minutes (1 to 1,440)

Root selection Method ☐

Descriptions

Figure 214: 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.

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**.

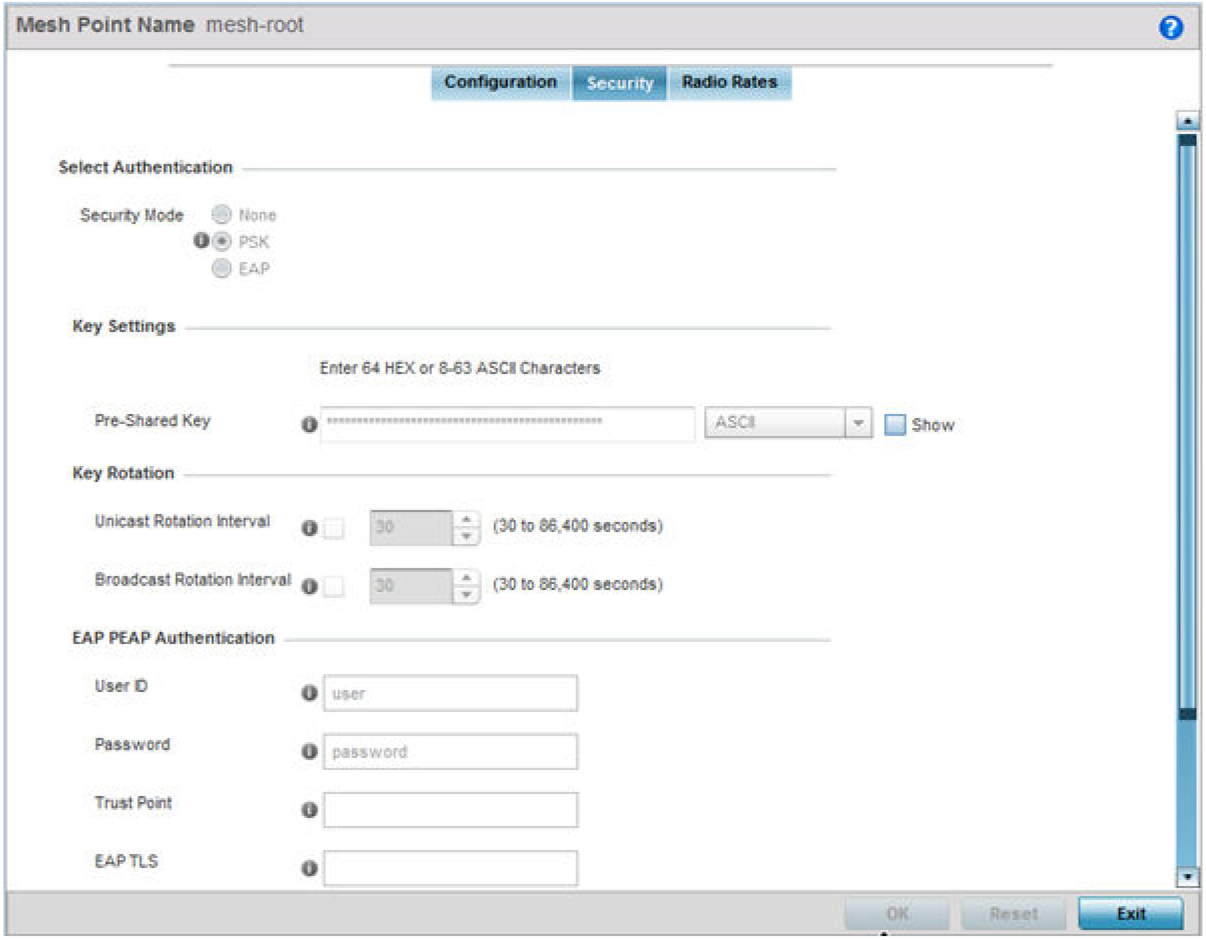


Figure 215: MeshConnex Security Screen

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 **EAP** to use a secured credential exchange, dynamic keying and strong encryption. If selecting **EAP**, refer to the **EAP PEAP** Authentication field at the bottom of the screen and define the credentials of an EAP user and trustpoint. 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.

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).
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.

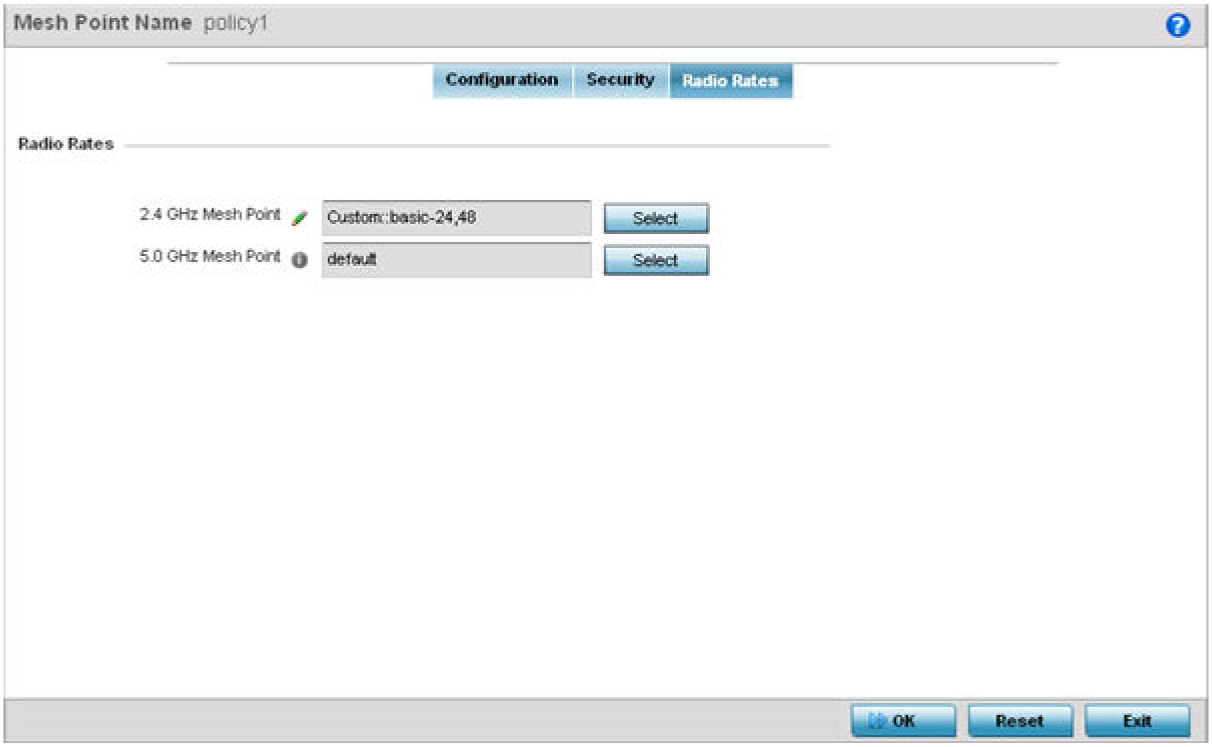
10 If you are using EAP to secure the mesh point, set the following **EAP PEAP Authentication** settings.

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 the supplicant. The default EAP type is **`PEAP-MS-CHAPv2`**.
EAP Identity	Enter the 32-character maximum identity string used during phase 1 authentication. This string does not need to represent the identity of the user, rather an anonymous identity string.
AAA Policy	Select an existing AAA Policy from the drop-down menu to apply to this user's mesh point EAP configuration. *Authentication, authorization, and accounting* (AAA) 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.

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

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

12 Select **Radio Rates**.



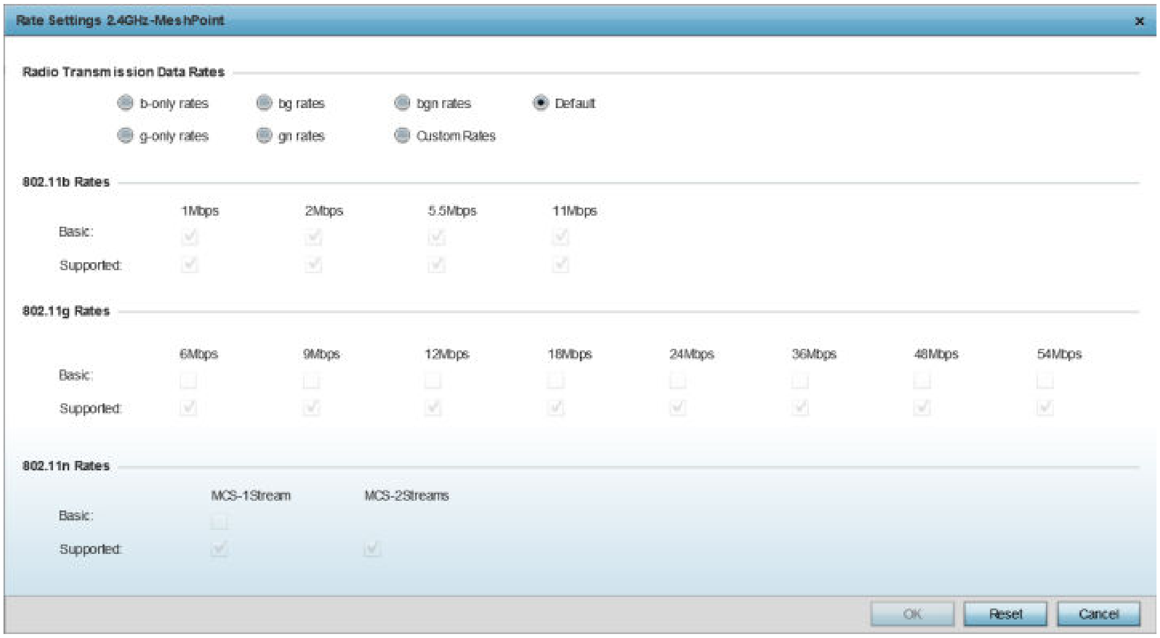
2.4 GHz Mesh Point: Custom::basic-24,48

5.0 GHz Mesh Point: default

Figure 216: Radio Rate Settings

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. 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. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). 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. 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. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.



● Default

802.11b Rates

	1Mbps	2Mbps	5.5Mbps	11Mbps
Basic:	☑	☑	☑	☑
Supported:	☑	☑	☑	☑

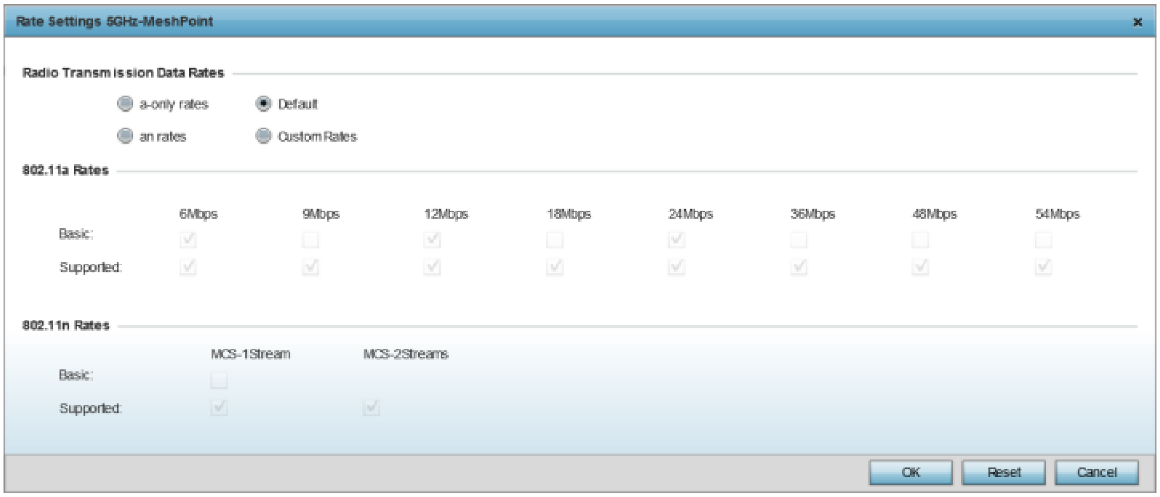
802.11g Rates

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	☐	☐	☐	☐	☐	☐	☐	☐
Supported:	☑	☑	☑	☑	☑	☑	☑	☑

802.11n Rates

	MCS-1Stream	MCS-2Streams
Basic:	☐	
Supported:	☑	☑

Figure 217: Advanced Rate Settings 2.4 GHz Screen



● Default

802.11a Rates

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	☑	☐	☑	☐	☑	☐	☐	☐
Supported:	☑	☑	☑	☑	☑	☑	☑	☑

802.11n Rates

	MCS-1Stream	MCS-2Streams
Basic:	☐	
Supported:	☑	☑

Figure 218: 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.

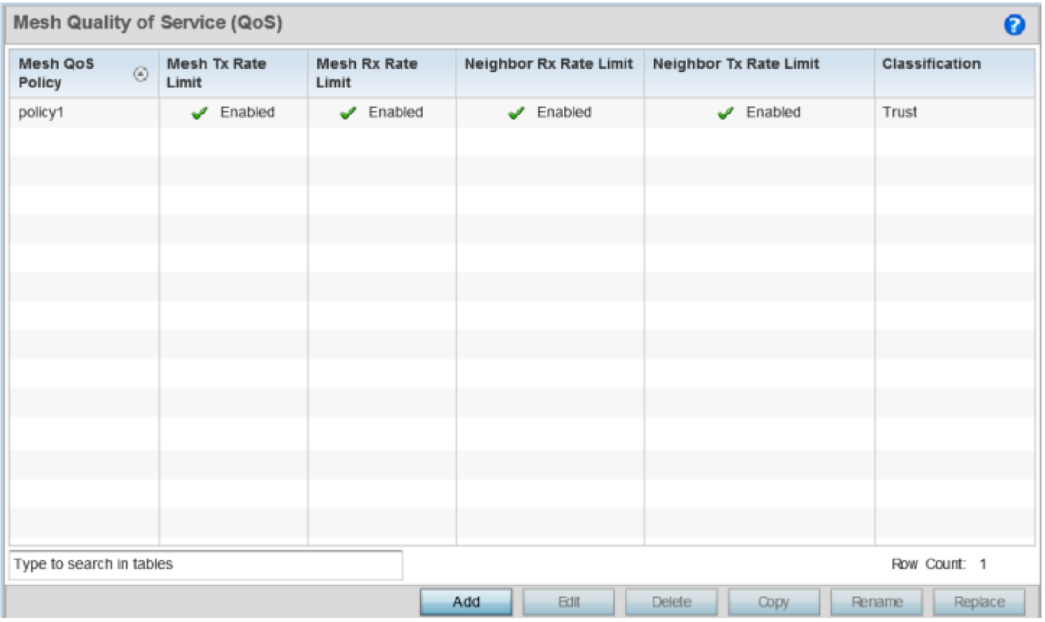
The Quality of Service screen displays a list of mesh QoS policies available to mesh points. Each mesh QoS policy can be selected to edit its properties. If none of the exiting Mesh QoS policies supports an ideal QoS configuration for the intended data traffic of this mesh point, click **Add** to create a new policy. Select an existing mesh QoS policy and select **Edit** to change the properties of the mesh QoS policy.

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.



Mesh Quality of Service (QoS)

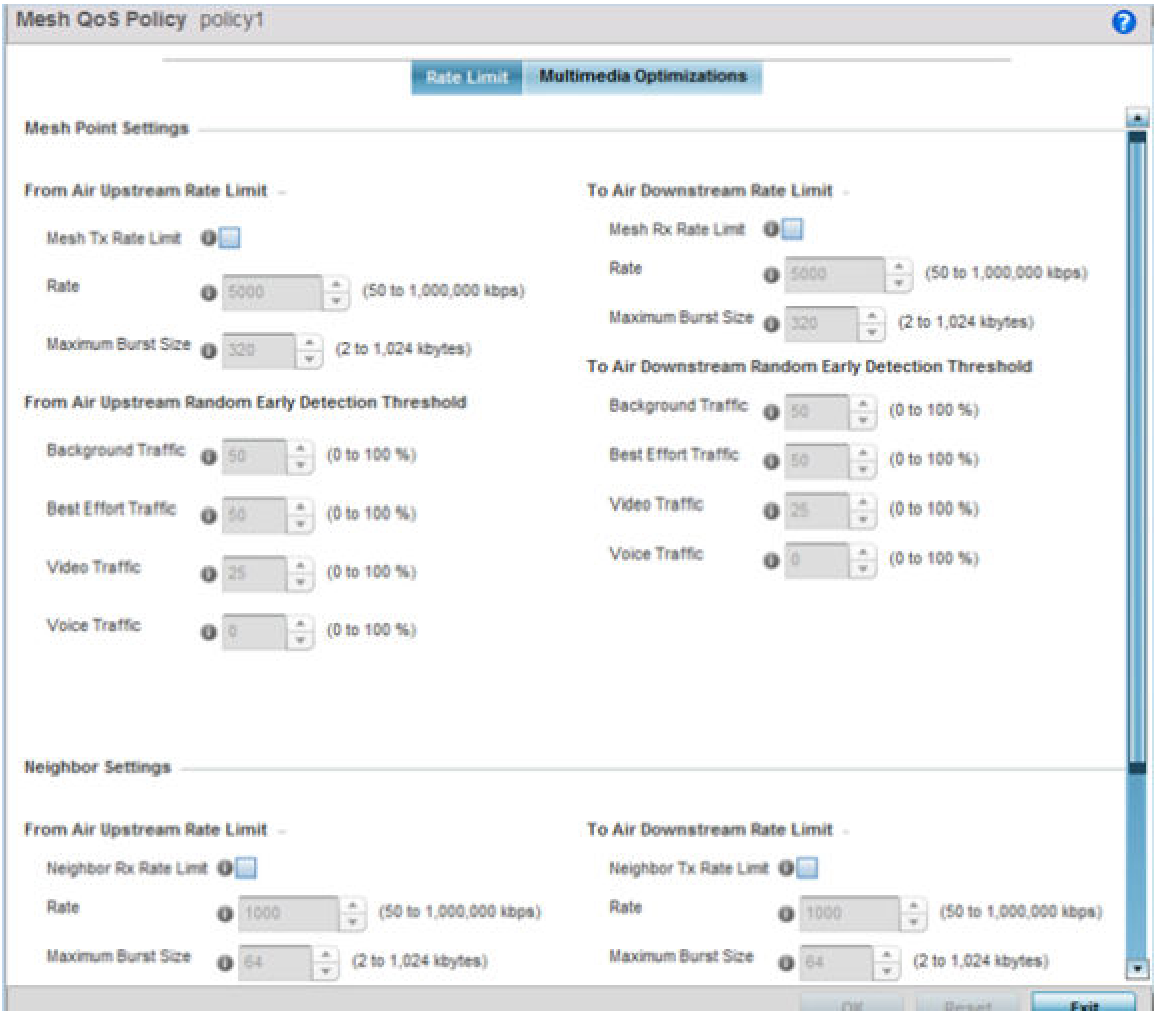
Mesh QoS Policy	Mesh Tx Rate Limit	Mesh Rx Rate Limit	Neighbor Rx Rate Limit	Neighbor Tx Rate Limit	Classification
policy1	✓ Enabled	✓ Enabled	✓ Enabled	✓ Enabled	Trust

Figure 219: Mesh QoS Policy Screen

2 Refer to the following configuration data for existing mesh QoS policies:

Mesh QoS Policy	The administrator assigned name of each mesh QoS policy.
Mesh Tx Rate Limit	Whether a **Mesh Tx Rate Limit** is enabled for each mesh QoS policy. 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. 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. 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. 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. Classification types are **`Trust`**, **`Voice`**, **`Video`**, **`Best Effort`**, and **`Background`**.

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.



Mesh QoS Policy policy1

Mesh Point Settings

From Air Upstream Rate Limit

Mesh Tx Rate Limit ☐
Rate 5000 (50 to 1,000,000 kbps)
Maximum Burst Size 320 (2 to 1,024 kbytes)

From Air Upstream Random Early Detection Threshold

Background Traffic 50 (0 to 100 %)
Best Effort Traffic 50 (0 to 100 %)
Video Traffic 25 (0 to 100 %)
Voice Traffic 0 (0 to 100 %)

To Air Downstream Rate Limit

Mesh Rx Rate Limit ☐
Rate 5000 (50 to 1,000,000 kbps)
Maximum Burst Size 320 (2 to 1,024 kbytes)

To Air Downstream Random Early Detection Threshold

Background Traffic 50 (0 to 100 %)
Best Effort Traffic 50 (0 to 100 %)
Video Traffic 25 (0 to 100 %)
Voice Traffic 0 (0 to 100 %)

Neighbor Settings

From Air Upstream Rate Limit

Neighbor Rx Rate Limit ☐
Rate 1000 (50 to 1,000,000 kbps)
Maximum Burst Size 64 (2 to 1,024 kbytes)

To Air Downstream Rate Limit

Neighbor Tx Rate Limit ☐
Rate 1000 (50 to 1,000,000 kbps)
Maximum Burst Size 64 (2 to 1,024 kbytes)

Figure 220: 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**.

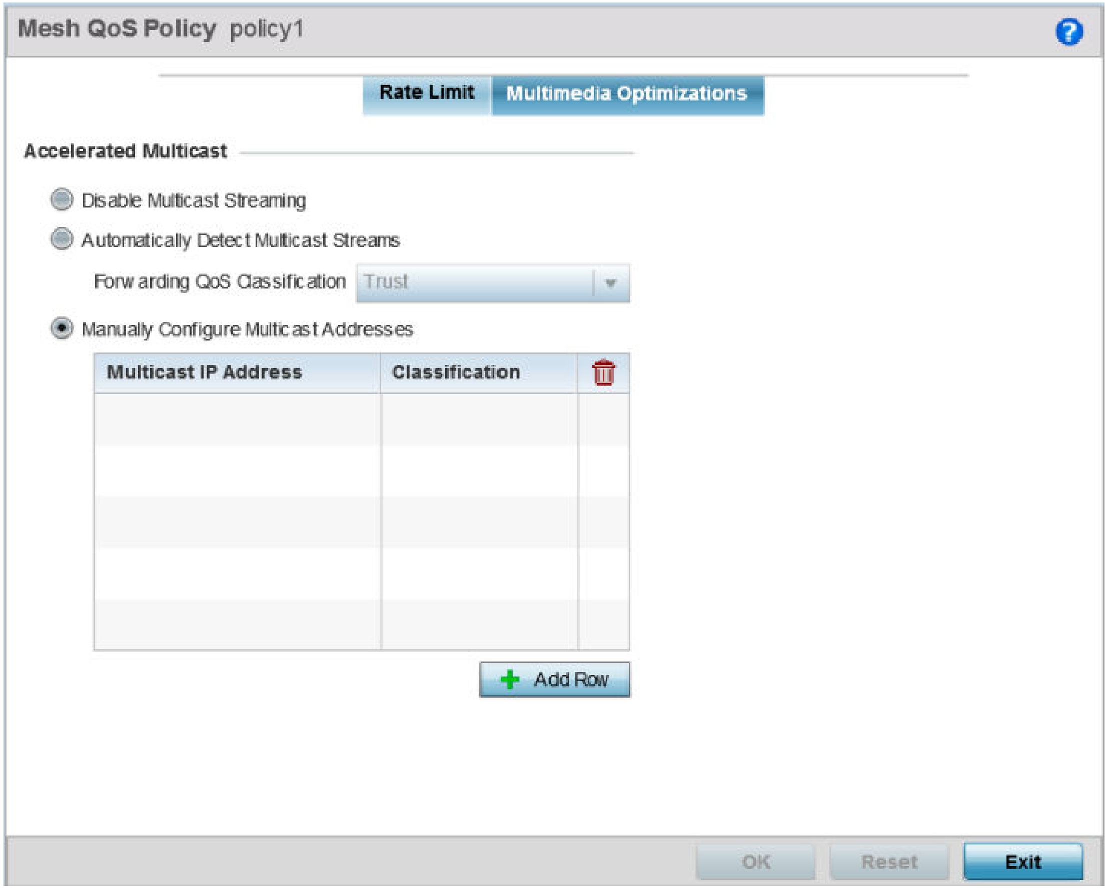

Mesh QoS Policy policy1
Rate Limit
Multimedia Optimizations
Accelerated Multicast
○ Disable Multicast Streaming
○ Automatically Detect Multicast Streams
Forwarding QoS Classification
Trust
● Manually Configure Multicast Addresses
Multicast IP Address
Classification
Add Row
OK
Reset
Exit

Figure 221: 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 **+ Add Row** 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 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.

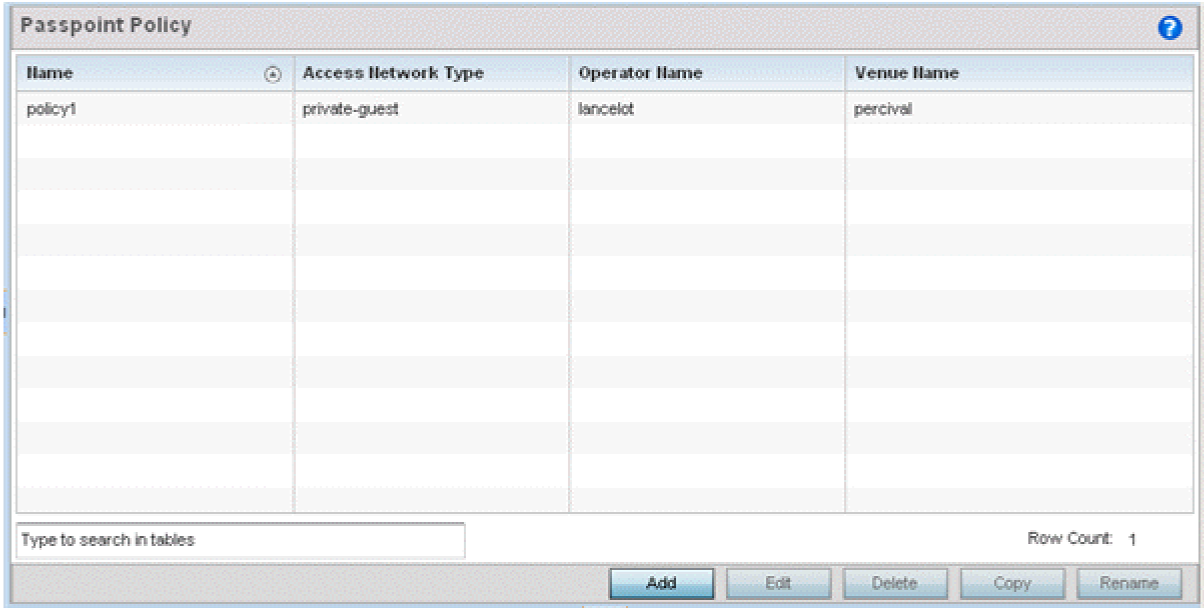
Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

The Passpoint Policy screen displays a list of passpoint polices for network hotspots. Each passpoint policy can be selected to edit its properties. If no exiting passpoint policies supports the required deployment, select Add to create a new policy.

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.



Passpoint Policy

Name	Access Network Type	Operator Name	Venue Name
policy1	private-guest	lancelot	percival

Type to search in tables

Row Count: 1

3 Refer to the following configuration data for existing passpoint policies:

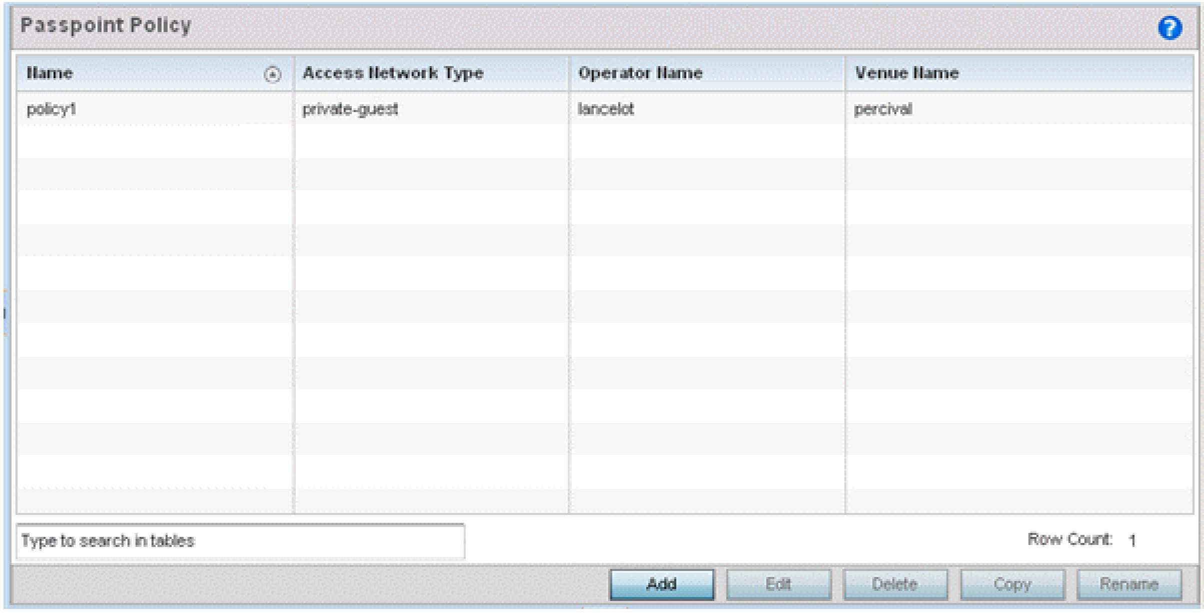
Name	Displays the administrator assigned name of each passpoint policy.
Access Network Type	Displays the network access permissions the administrator has set for the passpoint policy.
Operator Name	Displays the unique name assigned to the administrator or operator responsible for the configuration and 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.



Name	Access Network Type	Operator Name	Venue Name
policy1	private-guest	lancelot	percival

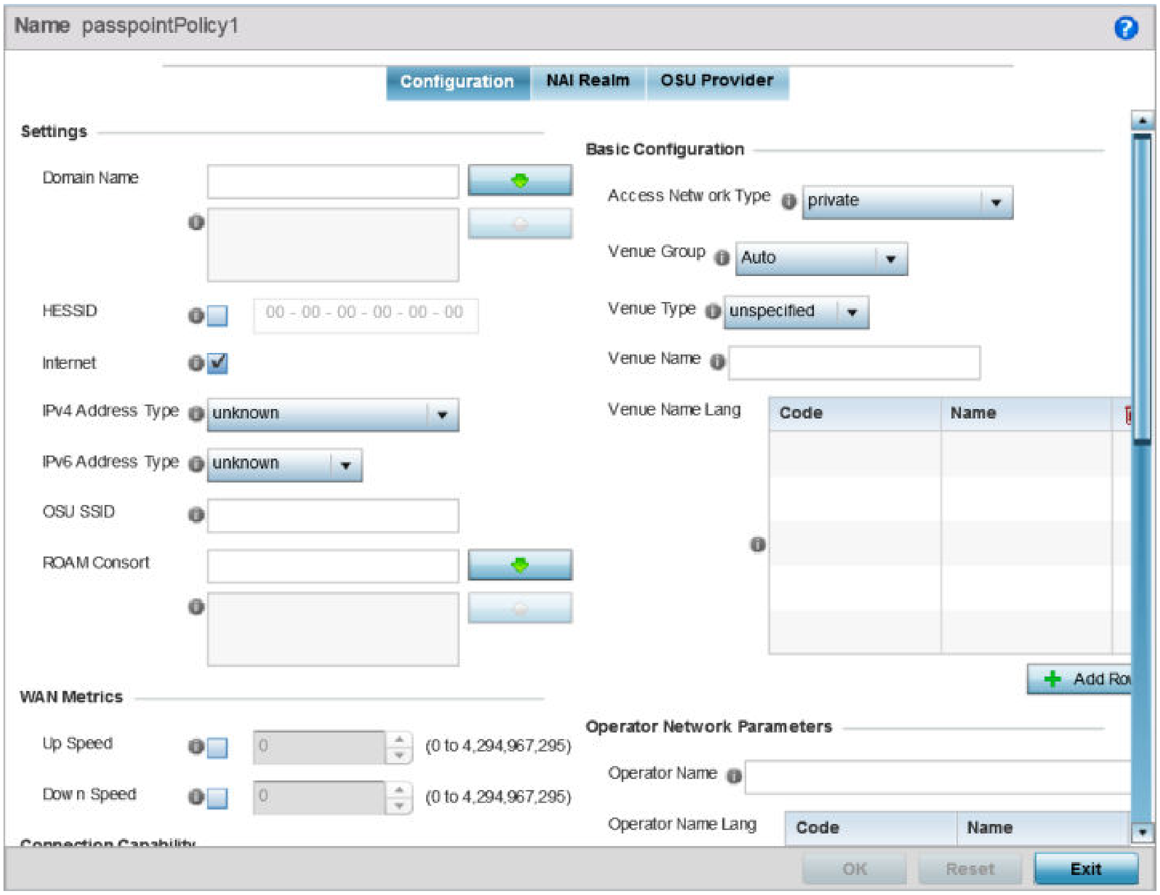
Figure 222: Passpoint Policy Screen

2 Refer to the following configuration data for existing passpoint policies:

Name	The administrator assigned name of each passpoint policy.
Access Network Type	The network access permissions the administrator has set for the passpoint policy.
Operator Name	The unique name assigned to the administrator or operator responsible for the configuration and operation of the access point managed hotspot.
Venue Name	The administrator assigned name of the venue (or physical location) of the deployed access point 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.



Name passpointPolicy1

HESSID ☐ 00 - 00 - 00 - 00 - 00 - 00

Internet ☑

IPv4 Address Type unknown

IPv6 Address Type unknown

Up Speed ☐ 0 (0 to 4,294,967,295)

Down Speed ☐ 0 (0 to 4,294,967,295)

Access Network Type private

Venue Group Auto

Venue Type unspecified

Figure 223: 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. 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.

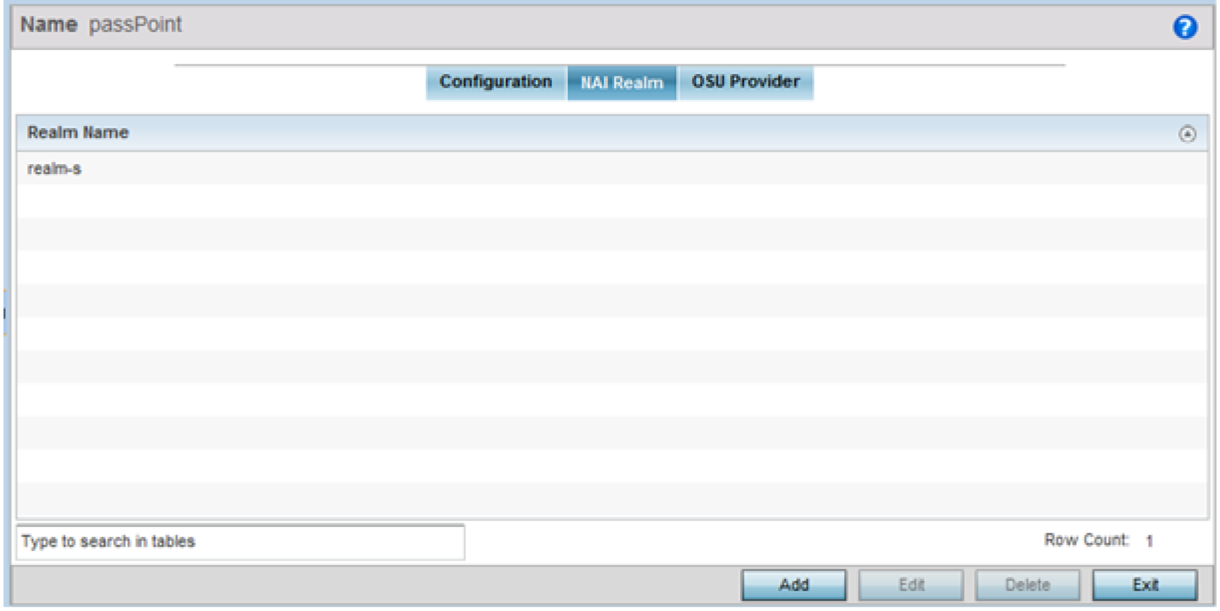
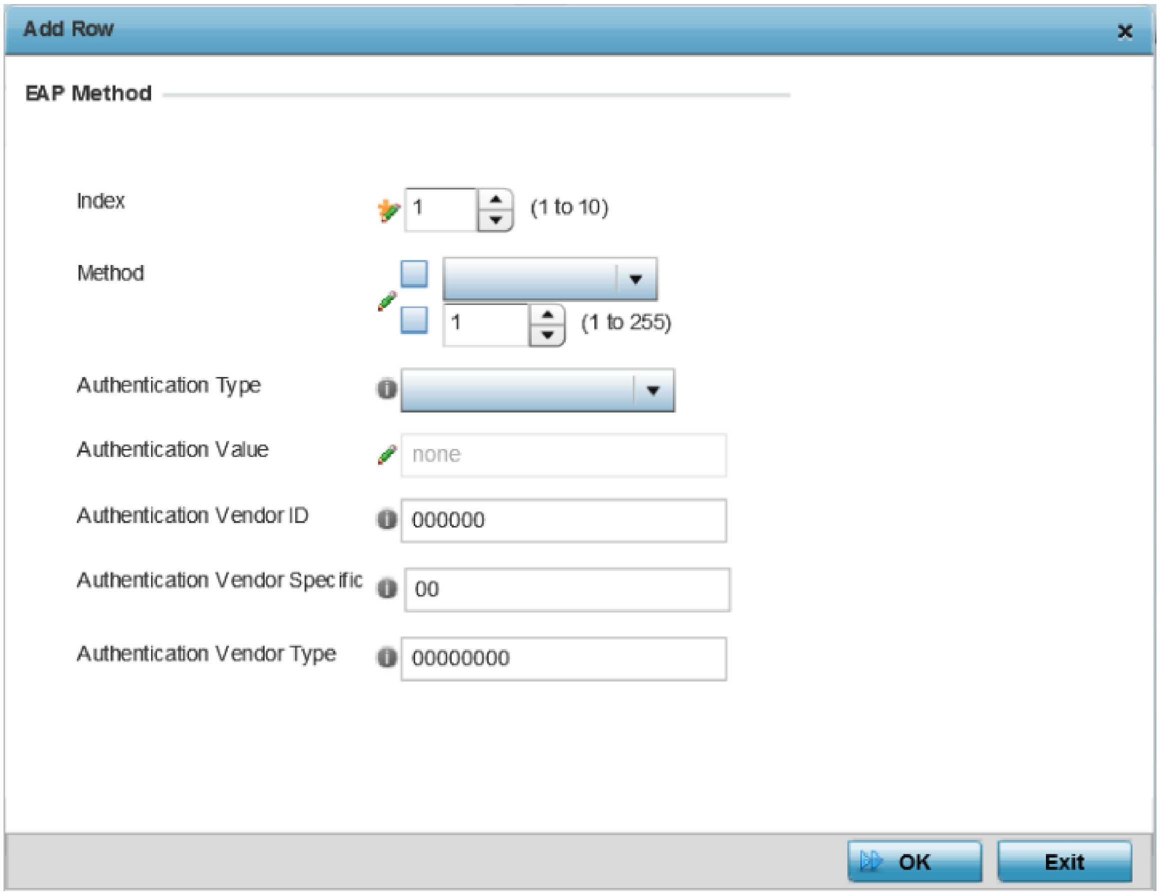


Figure 224: Passpoint Policy - NAI Realm Screen

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.



Index 1 (1 to 10)

Method ☐ ☐ 1 (1 to 255)

Authentication Type

Authentication Value none

Authentication Vendor ID 000000

Authentication Vendor Specific 00

Authentication Vendor Type 00000000

Figure 225: 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.

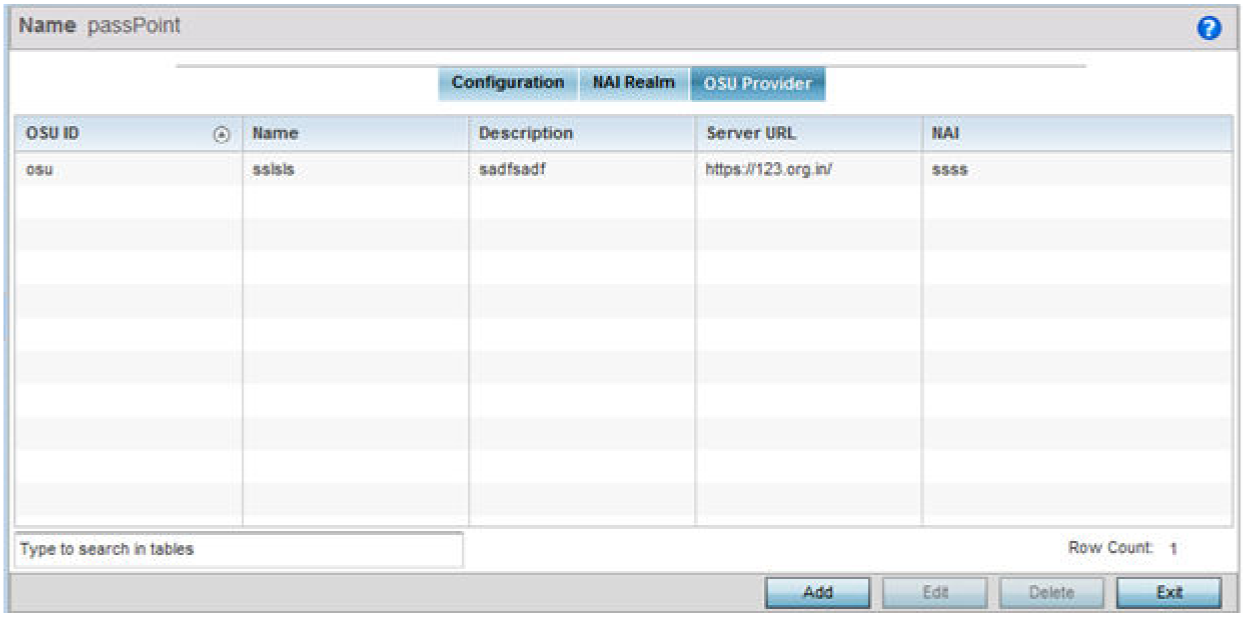
16 Select **OSU Provider**.

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.



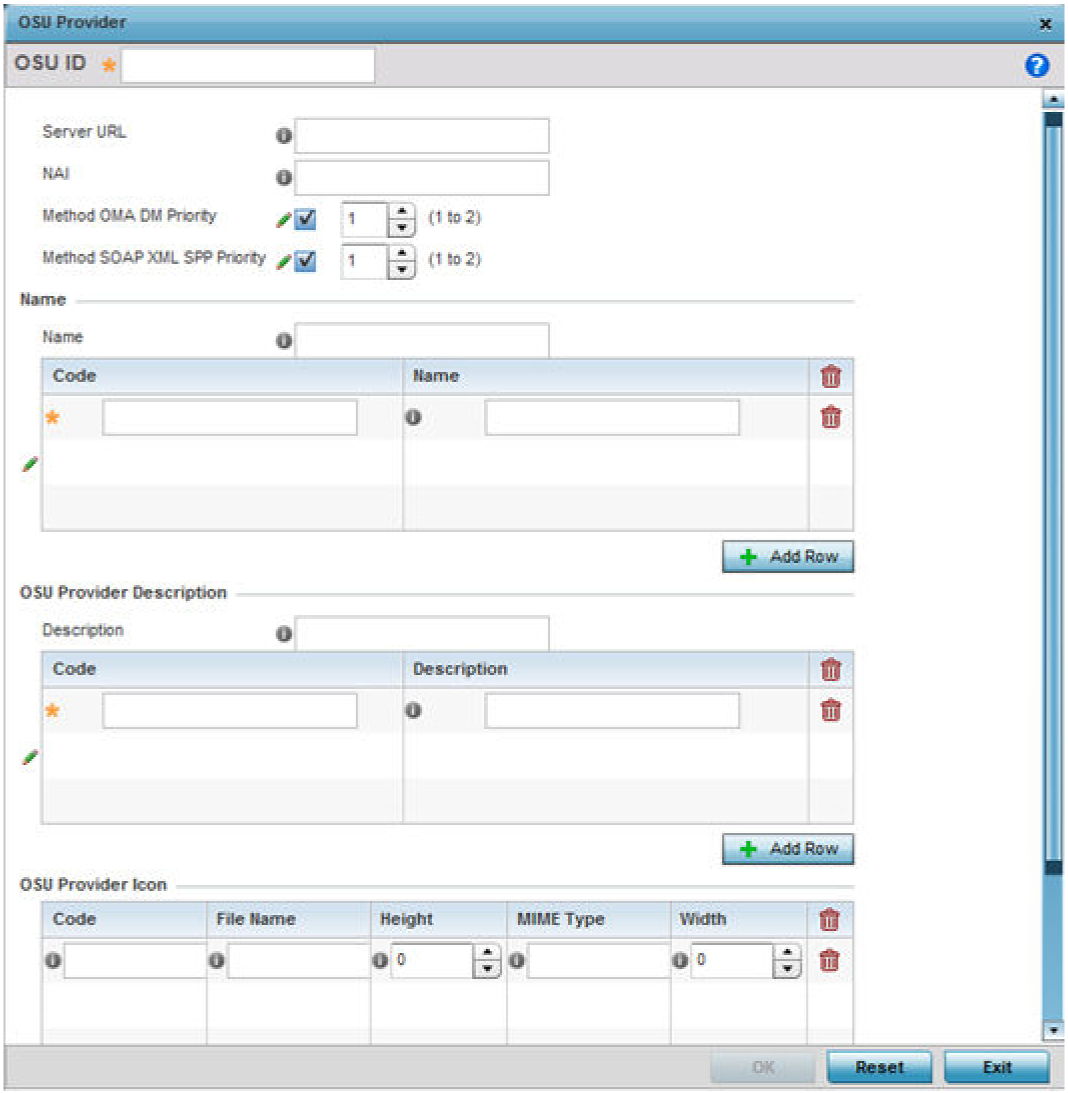
Name passPoint

OSU ID	Name	Description	Server URL	NAI
osu	sslsls	sadfsadf	https://123.org.in/	ssss

Row Count: 1

Figure 226: 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.



Method OMA DM Priority ☑ 1 (1 to 2)

Method SOAP XML SPP Priority ☑ 1 (1 to 2)

Figure 227: 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

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 administer and manage existing sensor policies:

1 Select **Configuration** → **Wireless** → **Sensor Policy** to display existing sensor policies.

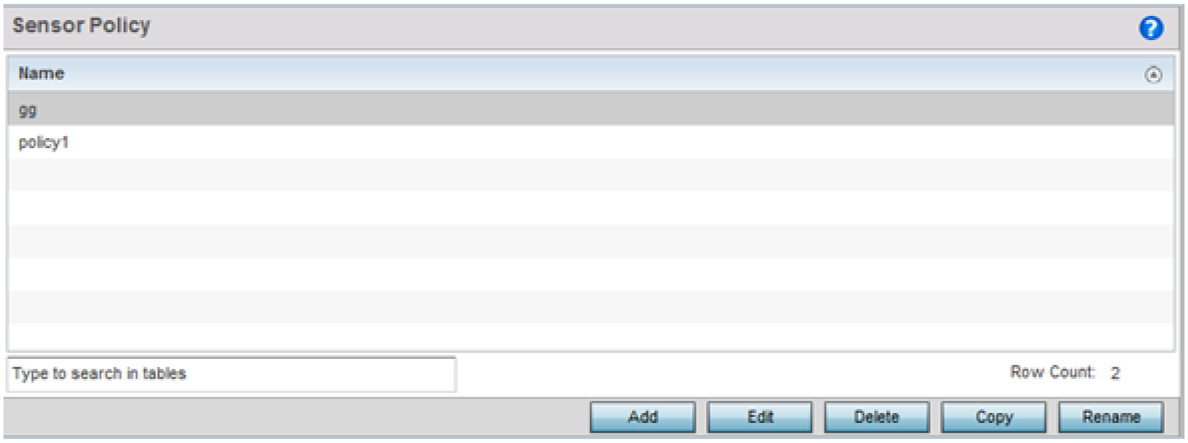
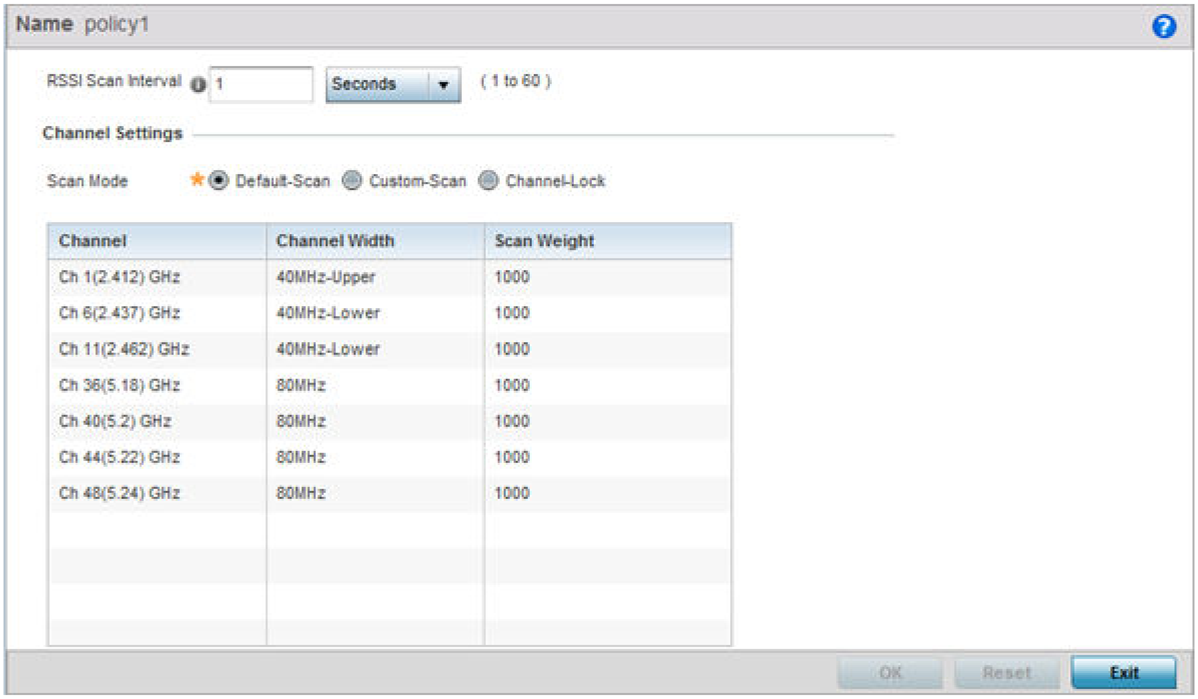


Figure 228: Sensor Policy Screen

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.

   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, not the WiNG interface, to configure the sensor.



Name policy1

RSSI Scan Interval: 1 Seconds (1 to 60)

Channel Settings

Scan Mode ★ ● Default-Scan ○ Custom-Scan ○ Channel-Lock

Channel	Channel Width	Scan Weight
Ch 1(2.412) GHz	40MHz-Upper	1000
Ch 6(2.437) GHz	40MHz-Lower	1000
Ch 11(2.462) GHz	40MHz-Lower	1000
Ch 36(5.18) GHz	80MHz	1000
Ch 40(5.2) GHz	80MHz	1000
Ch 44(5.22) GHz	80MHz	1000
Ch 48(5.24) GHz	80MHz	1000

Figure 229: 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. Define a name unique to the policy’s channel and scan mode configuration to help differentiate it from other policies.
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. 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. 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). 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. 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. 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. 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.

Location Policy

ExtremeLocation is a scalable, enterprise grade, cloud-based location and analytics solution. It is a licensed product. WiNG customers having ExtremeLocation entitlement, can view sites (RF Domains) within the ExtremeLocation user interface. The site hierarchy details is propagated to the ExtremeLocation server by the WiNG, controllers.

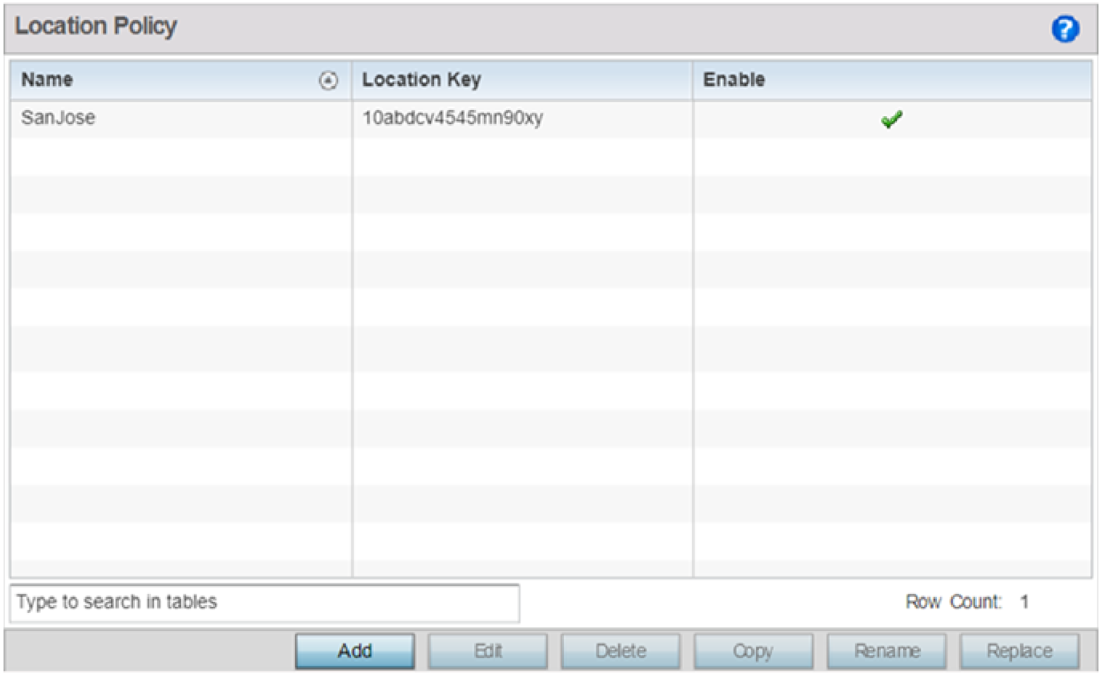
The location policy provides the ExtremeLocation server hostname and the ExtremeLocation tenant's API key. Configure a location policy and apply on the site controller's self. When applied, the controller authenticates and authorizes with the ExtremeLocation server and exports tenant site hierarchy details to the server.

Note
For information on applying location policy to the controller's self, see Overriding a Services Configuration on page 291.

Note
For information on ExtremeLocation, refer to the ExtremeLocation user guide, available at https://extremenetworks.com/documentation.

To configure a location policy:

1 Go to **Configuration** → **Wireless** → **Location Policy**.



Name	Location Key	Enable
SanJose	10abdcv4545mn90xy	✓

Figure 230: Configuration → Wireless → Location Policy

2 Review existing policies, to determine if a new policy warrants creation or an existing policy warrants modification.

Name	Displays the Location policy name.
Location Key	Displays the ExtremeLocation tenant's API key.
Enable	Displays whether the location policy is enabled or not.

Adding Location Policy

You can add a location policy or manage existing policies to match your requirements.

1 Click **Add** to create a new policy.

Note
To *edit*, *copy*, *rename*, or *replace* an existing policy, select the policy and click **Edit**, **Copy**, **Rename** or **Replace** respectively.

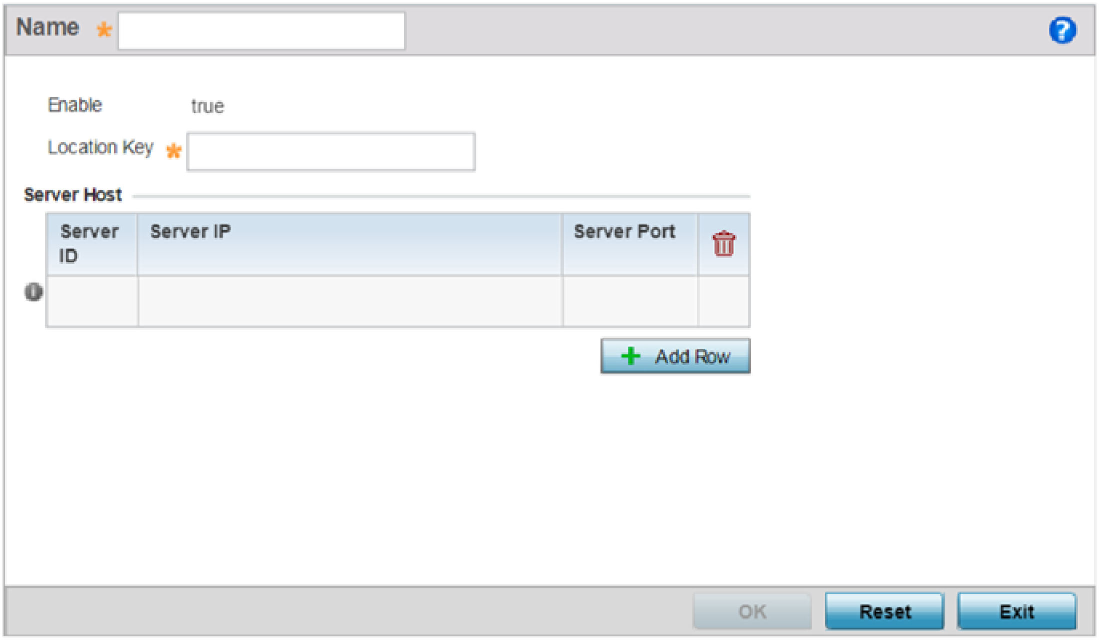


Figure 231: Configuration → Wireless → Add Location Policy Screen

2 If creating a new policy, enter a `name` in the Name field. The policy name should not exceed 32 characters in length and should uniquely identify it from other existing location policies.

3 Configure the following parameters:

Enable	By default the policy is enabled and the value displays as true.
Location Key	Enter your 64-bit ExtremeLocation tenant API key. This is the key the controller/virtual controller uses to authenticate with the ExtremeLocation server. Note: You can generate the API-Key from the ExtremeLocation UI. For more information, refer to the ExtremeLocation user guide, available at https://extremenetworks.com/documentation.

4 Click **Add Row**, in the Server Host table, and configure the following parameters:

Server ID	Set the server host ID number. Currently only one ExtremeLocation server can be configured.
Server IP	Configure the ExtremeLocation server's hostname of IP address.

Note
Specify the server 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.

Server Port	Set the port on which the ExtremeLocation server is reachable. Select the port from 1 - 65535. Note By default the ExtremeLocation server is reachable on port 443.

5 Click **OK** to save your location policy configuration.

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

7 Network Configuration

Policy Based Routing (PBR)
L2TP V3 Configuration
Crypto CMP Policy
AAA Policy
AAA TACACS Policy
IPv6 Router Advertisment Policy
Border Gateway Protocol (BGP)
Alias
Application Policy
Application
Application Group
Schedule Policy
URL Filtering
Web Filtering
Configuring EX3500 QoS Class
Configuring EX3500 QoS Policy Map
Network Deployment Considerations

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) on page 454
- L2TP V3 Configuration on page 458
- Crypto CMP Policy on page 462
- AAA Policy on page 465
- AAA TACACS Policy on page 476
- IPv6 Router Advertisment Policy on page 481
- Border Gateway Protocol (BGP) on page 485
- Alias on page 498
- Application Policy on page 506
- Application on page 509
- Application Group on page 511
- Schedule Policy on page 513
- URL Filtering on page 514
- Web Filtering on page 518
- Configuring EX3500 QoS Class on page 519

- Configuring EX3500 QoS Policy Map on page 523
- Network Deployment Considerations on page 527

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.

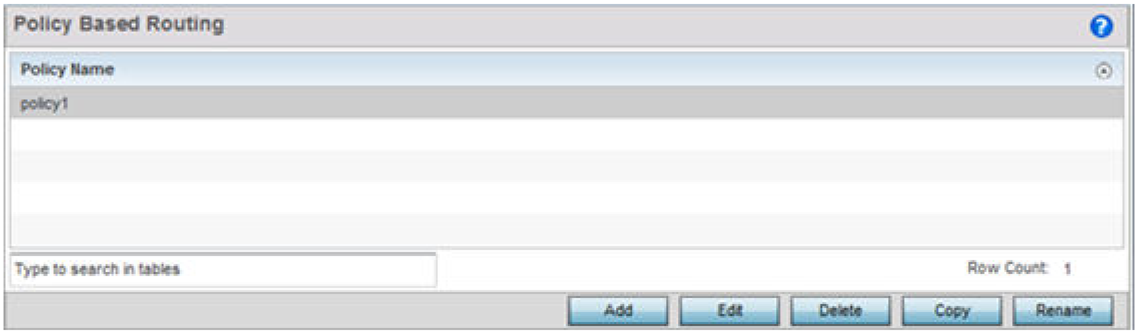
Note

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:

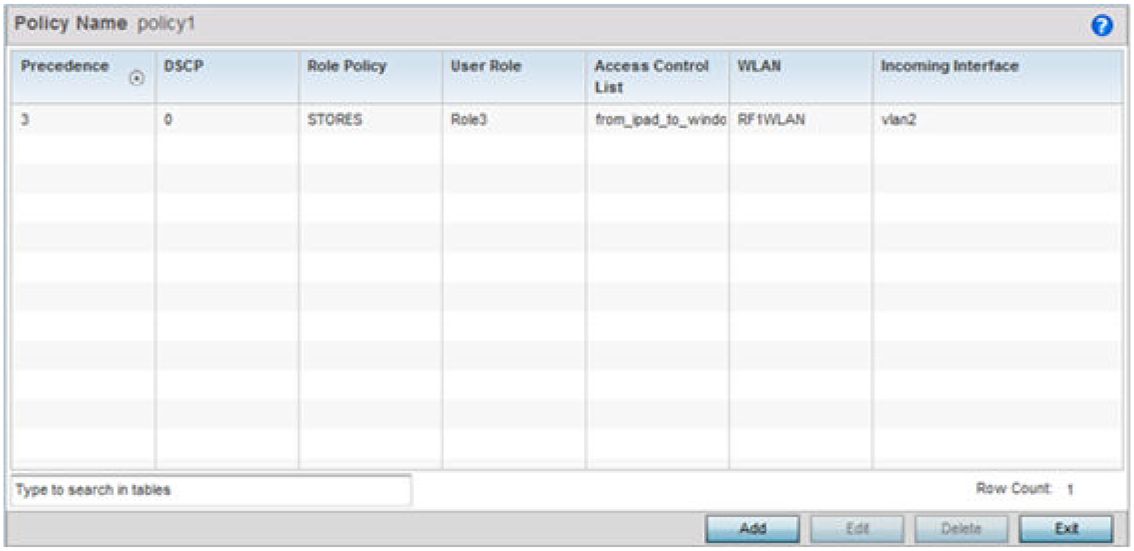
1 Select **Configuration** → **Network** → **Policy Based Routing**.

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.



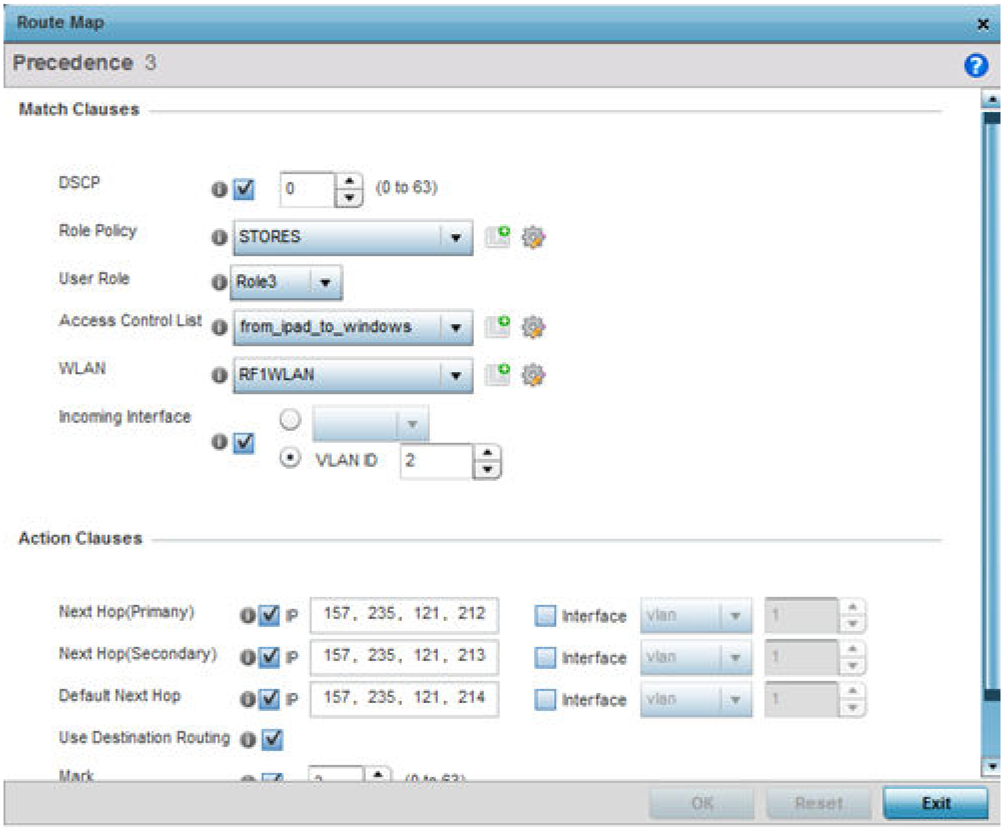
Policy Name policy1

Precedence	DSCP	Role Policy	User Role	Access Control List	WLAN	Incoming Interface
3	0	STORES	Role3	from_ipad_to_windo	RF1WLAN	vlan2

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**.



DSCP ☑ 0 (0 to 63)
Role Policy STORES
User Role Role3
Access Control List from_ipad_to_windows
WLAN RF1WLAN
Incoming Interface ☑ ○ ● VLAN ID 2
Next Hop(Primary) ☑ IP 157.235.121.212 ☐ Interface vlan 1
Next Hop(Secondary) ☑ IP 157.235.121.213 ☐ Interface vlan 1
Default Next Hop ☑ IP 157.235.121.214 ☐ Interface vlan 1
Use Destination Routing ☑

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.

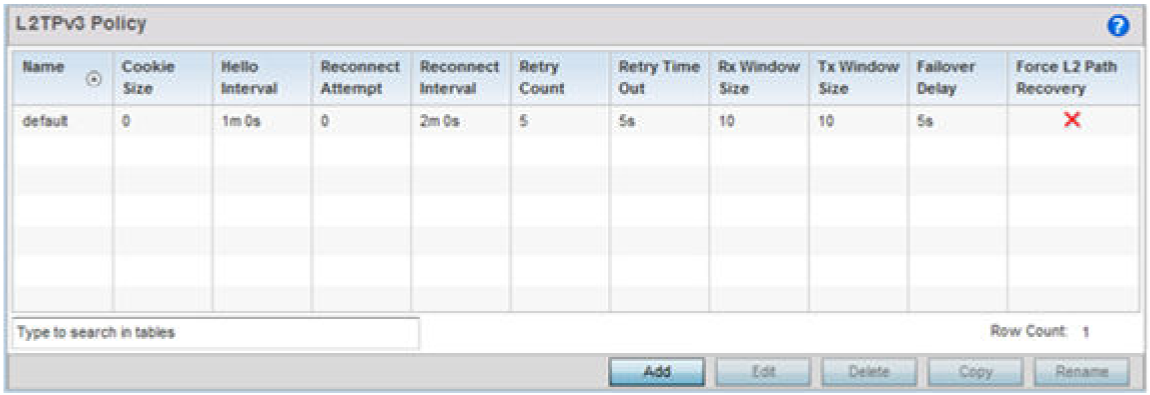
The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control 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.



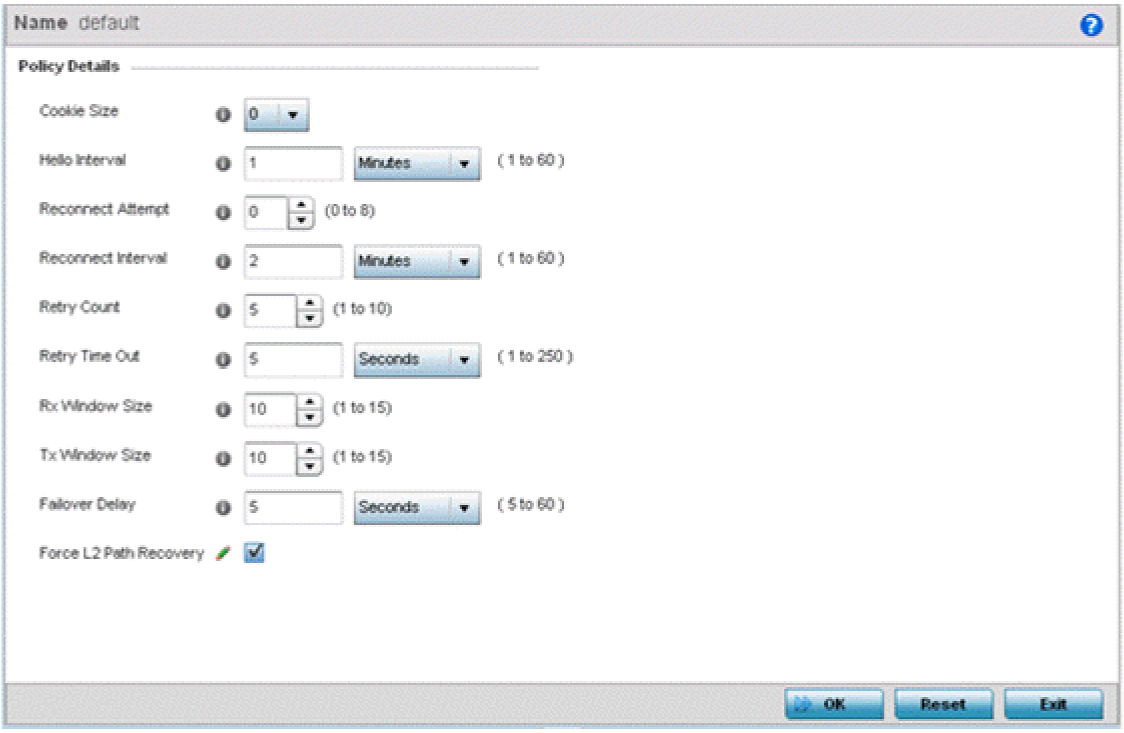
L2TPv3 Policy

Name	Cookie Size	Hello Interval	Reconnect Attempt	Reconnect Interval	Retry Count	Retry Time Out	Rx Window Size	Tx Window Size	Failover Delay	Force L2 Path Recovery
default	0	1m 0s	0	2m 0s	5	5s	10	10	5s	✗

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.



Name default

Policy Details

Cookie Size 0
Hello Interval 1 Minutes (1 to 60)
Reconnect Attempt 0 (0 to 8)
Reconnect Interval 2 Minutes (1 to 60)
Retry Count 5 (1 to 10)
Retry Time Out 5 Seconds (1 to 250)
Rx Window Size 10 (1 to 15)
Tx Window Size 10 (1 to 15)
Failover Delay 5 Seconds (5 to 60)
Force L2 Path Recovery ☑

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.

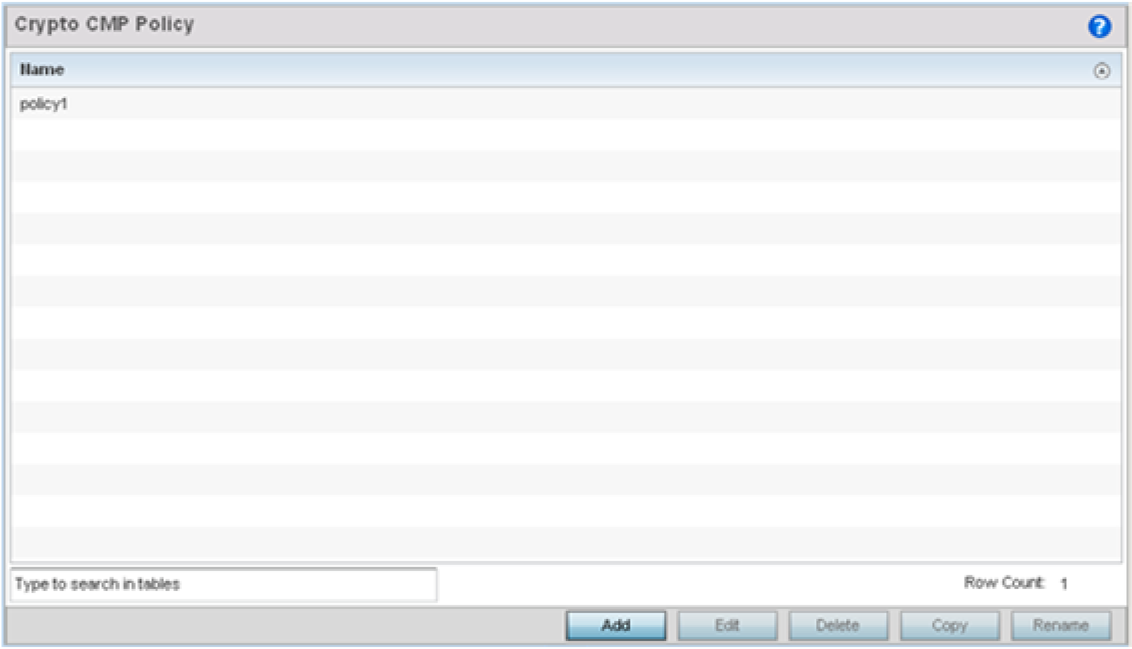
Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting 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.

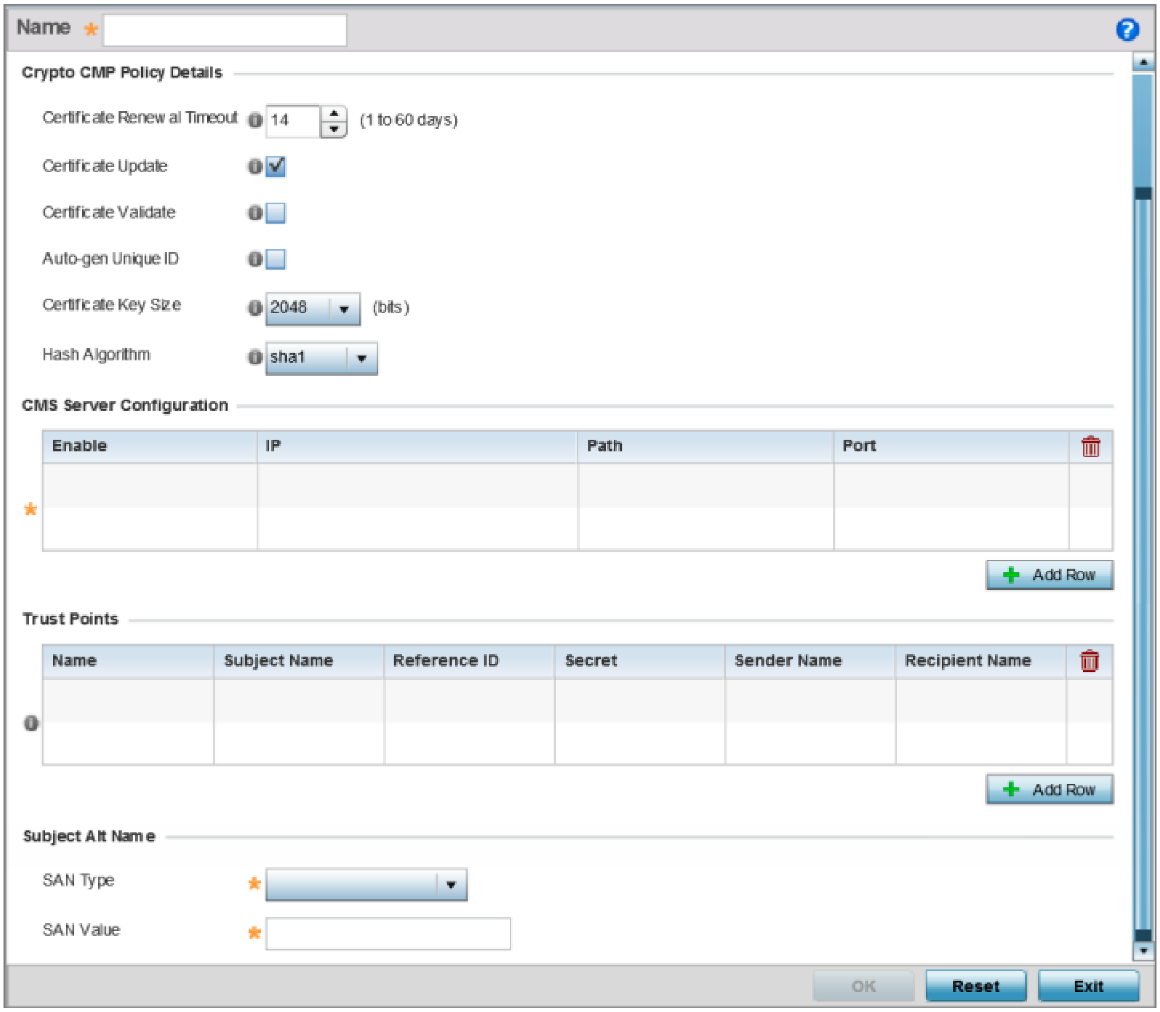
To review, create or edit a Crypto CMP policy:

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.



Name *

Crypto CMP Policy Details

Certificate Renewal Timeout: 14 (1 to 60 days)

Certificate Update: ☑

Certificate Validate: ☐

Auto-gen Unique ID: ☐

Certificate Key Size: 2048 (bits)

Hash Algorithm: sha1

CMS Server Configuration

Enable	IP	Path	Port

Trust Points

Name	Subject Name	Reference ID	Secret	Sender Name	Recipient Name

Subject Alt Name

SAN Type *

SAN Value *

Figure 232: 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.

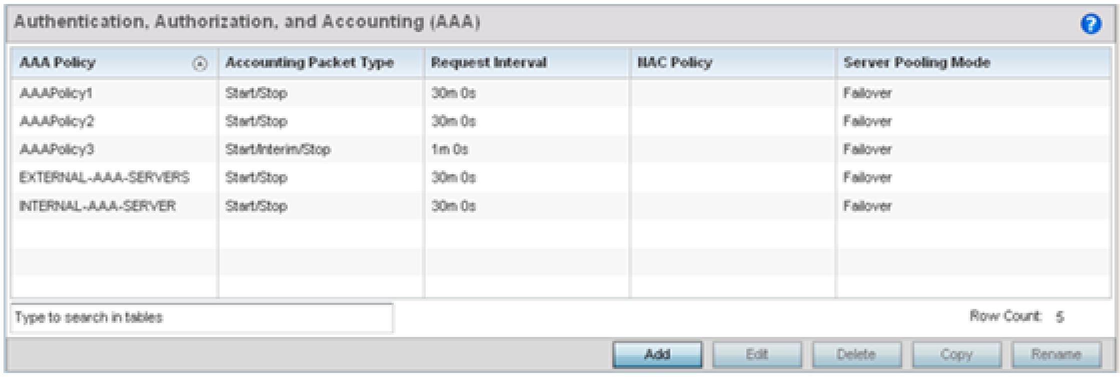
Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized 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.



Authentication, Authorization, and Accounting (AAA)

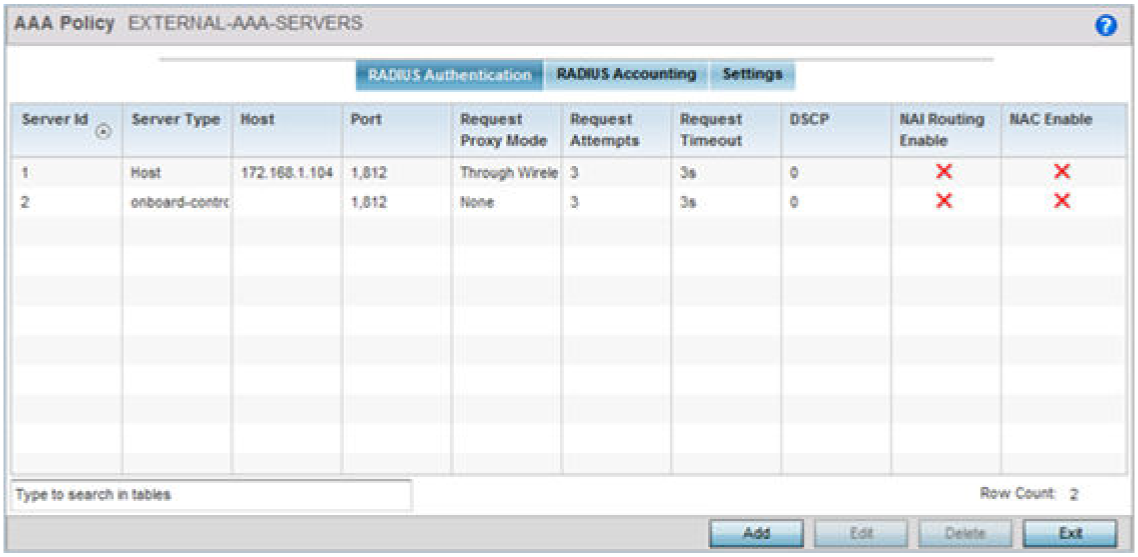
AAA Policy	Accounting Packet Type	Request Interval	NAC Policy	Server Pooling Mode
AAAPolicy1	Start/Stop	30m 0s		Failover
AAAPolicy2	Start/Stop	30m 0s		Failover
AAAPolicy3	Start/Interim/Stop	1m 0s		Failover
EXTERNAL-AAA-SERVERS	Start/Stop	30m 0s		Failover
INTERNAL-AAA-SERVER	Start/Stop	30m 0s		Failover

Row Count: 5

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: • *Start Only* — Sends a start accounting notice to initiate user accounting. • *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.



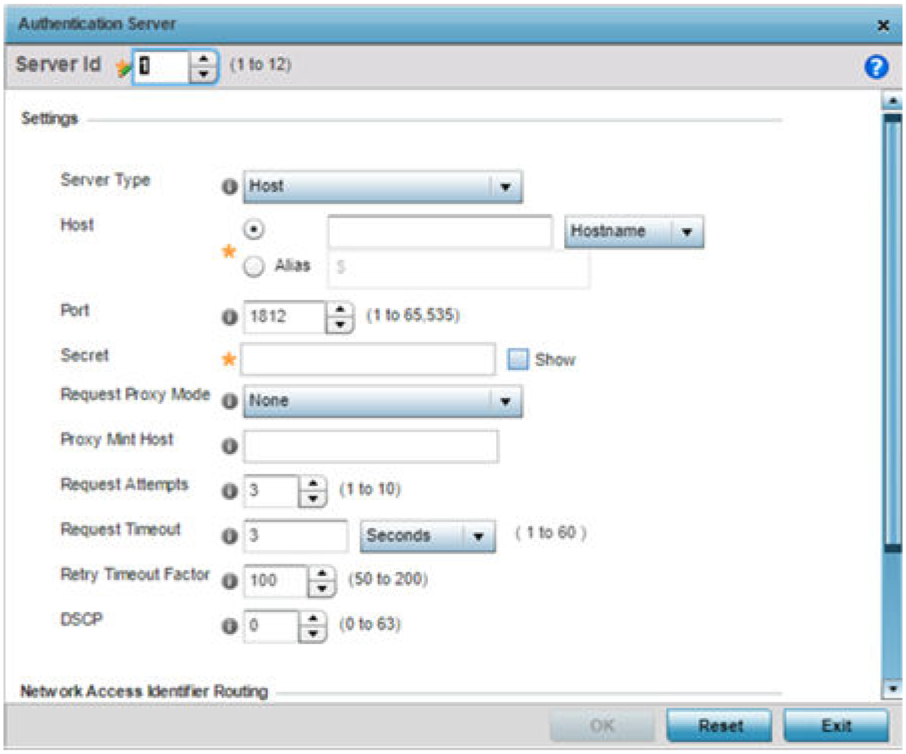
Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1	Host	172.168.1.104	1,812	Through Wirele	3	3s	0	✗	✗
2	onboard-contrc		1,812	None	3	3s	0	✗	✗

4. Refer to the following RADIUS Authentication details:

Server Id	Displays the numerical server index (1-12) 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.



Authentication Server

Server Id: 1 (1 to 12)

Settings

Server Type: Host

Host: ● ○ Alias; Hostname

Port: 1812 (1 to 65,535)

Secret: ☐ Show

Request Proxy Mode: None

Proxy Mint Host:

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

Network Access Identifier Routing

6 Define the following settings to add or modify AAA RADIUS authentication server configuration:

Server Id	Define the numerical server index (1-12) 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`**.
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.

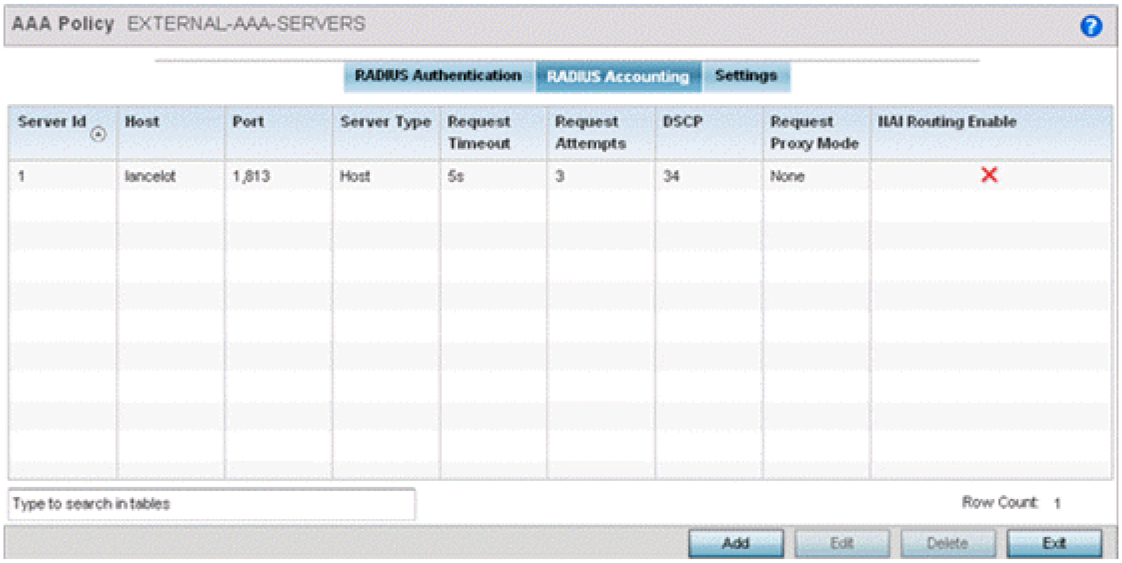
Request Attempts	Specify the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
Request Timeout	Specify the time from 1 - 60 seconds for the access point’s re-transmission 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.



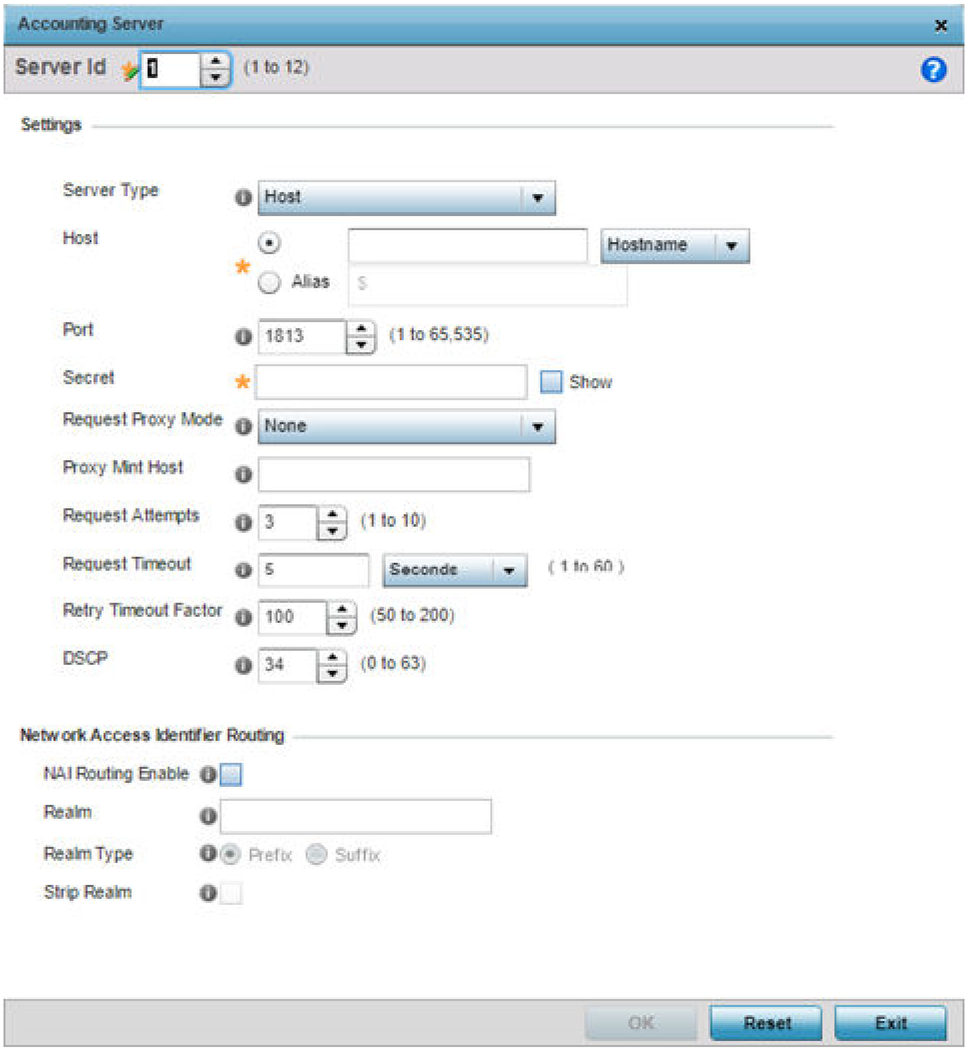
AAA Policy EXTERNAL-AAA-SERVERS

Server Id	Host	Port	Server Type	Request Timeout	Request Attempts	DSCP	Request Proxy Mode	NAI Routing Enable
1	lancelot	1,813	Host	5s	3	34	None	✗

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 (1-12) 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.



Server Id 1 (1 to 12)

Settings

Server Type: Host
Host: ● Hostname
○ Alias $
Port: 1813 (1 to 65,535)
Secret: ☐ Show
Request Proxy Mode: None
Proxy Mint Host:
Request Attempts: 3 (1 to 10)
Request Timeout: 5 Seconds (1 to 60)
Retry Timeout Factor: 100 (50 to 200)
DSCP: 34 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable: ☐
Realm:
Realm Type: ● Prefix ○ Suffix
Strip Realm: ☐

12 Define the following settings to add or modify AAA RADIUS accounting server configuration:

Server Id	Displays the numerical server index (1-12) 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.

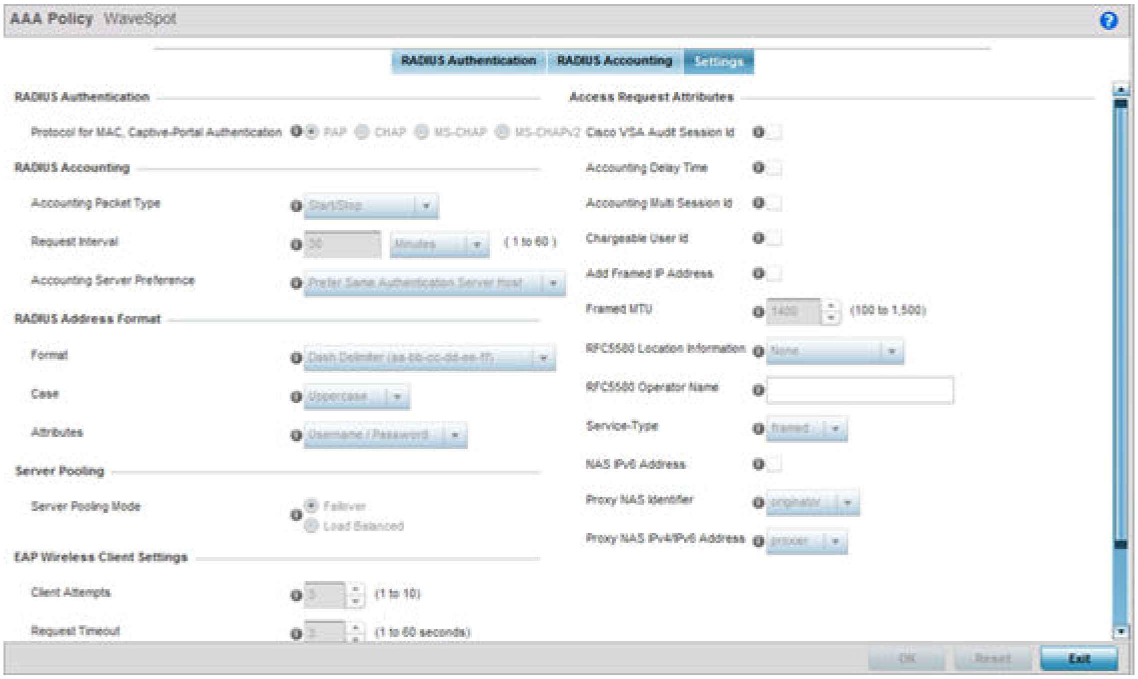
Request Proxy Mode	Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be **`None`**, **`Through Wireless Controller`** , **`Through RF Domain Manager`** ot **`Through Mint Host`**.
Proxy Mint Host	Specify a 64 character maximum hostname or 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.



RADIUS Authentication

Protocol for MAC, Captive-Portal Authentication: ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPv2

RADIUS Accounting

Accounting Packet Type: Start/Stop

Request Interval: 30 Minutes (1 to 60)

Accounting Server Preference: Prefer Same Authentication Server Host

RADIUS Address Format

Format: Dash Delimiter (aa-bb-cc-dd-ee-ff)

Case: Uppercase

Attributes: Username / Password

Server Pooling

Server Pooling Mode: ● Failover ○ Load Balanced

EAP Wireless Client Settings

Client Attempts: 3 (1 to 10)

Request Timeout: 3 (1 to 60 seconds)

Access Request Attributes

Cisco VSA Audit Session Id: ☐

Accounting Delay Time: ☐

Accounting Multi Session Id: ☐

Chargeable User Id: ☐

Add Framed IP Address: ☐

Framed MTU: 1400 (100 to 1,500)

RFC5580 Location Information: None

RFC5580 Operator Name:

Service-Type: framed

NAS IPv6 Address: ☐

Proxy NAS Identifier: originator

Proxy NAS IPv4/IPv6 Address: proxier

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: • **`Prefer Same Authentication Server Host`** – Uses the authentication server host name as the host used for RADIUS accounting. This is the default setting. • **`Prefer Same Authentication Server Index`** – Uses the same index as the authentication server for RADIUS accounting. • **`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.

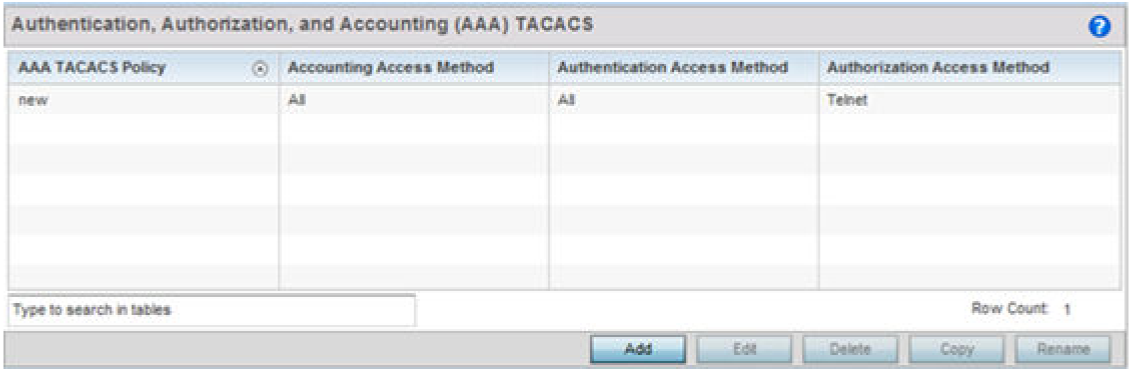
TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS are:

- 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.



AAA TACACS Policy	Accounting Access Method	Authentication Access Method	Authorization Access Method
new	All	All	Telnet

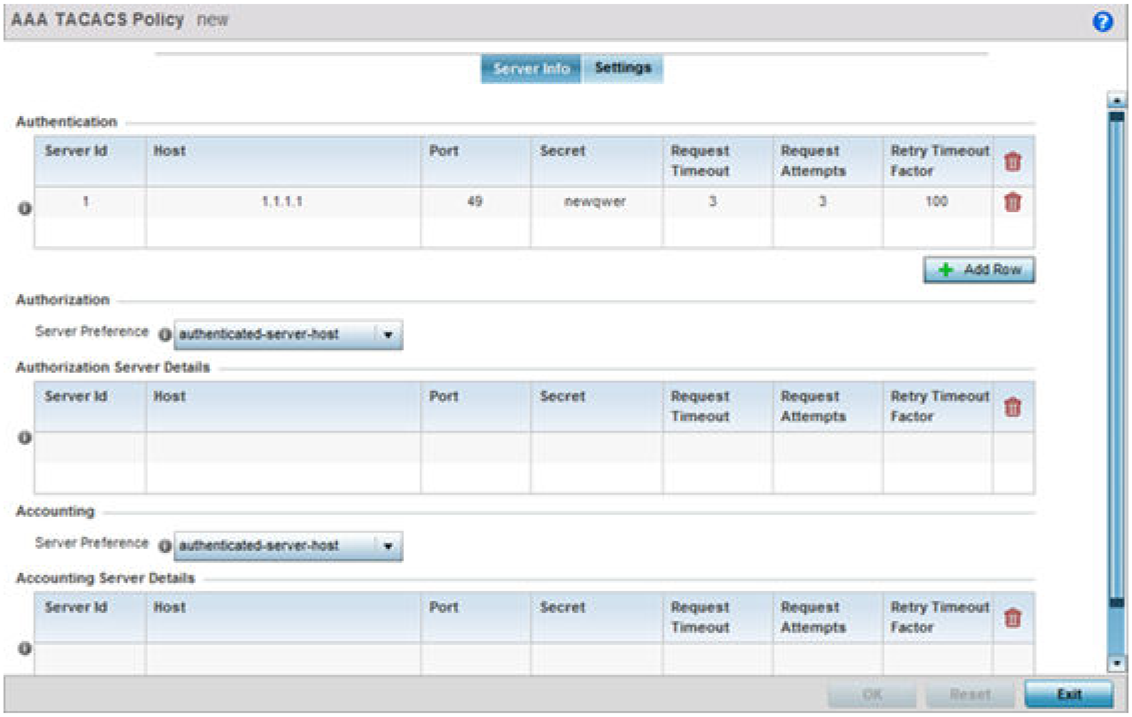
2 Refer to the following information for each existing AAA TACACS policy:

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.



AAA TACACS Policy new

Authentication

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor
1	1.1.1.1	49	newqwer	3	3	100

Authorization

Server Preference: authenticated-server-host

Authorization Server Details

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor

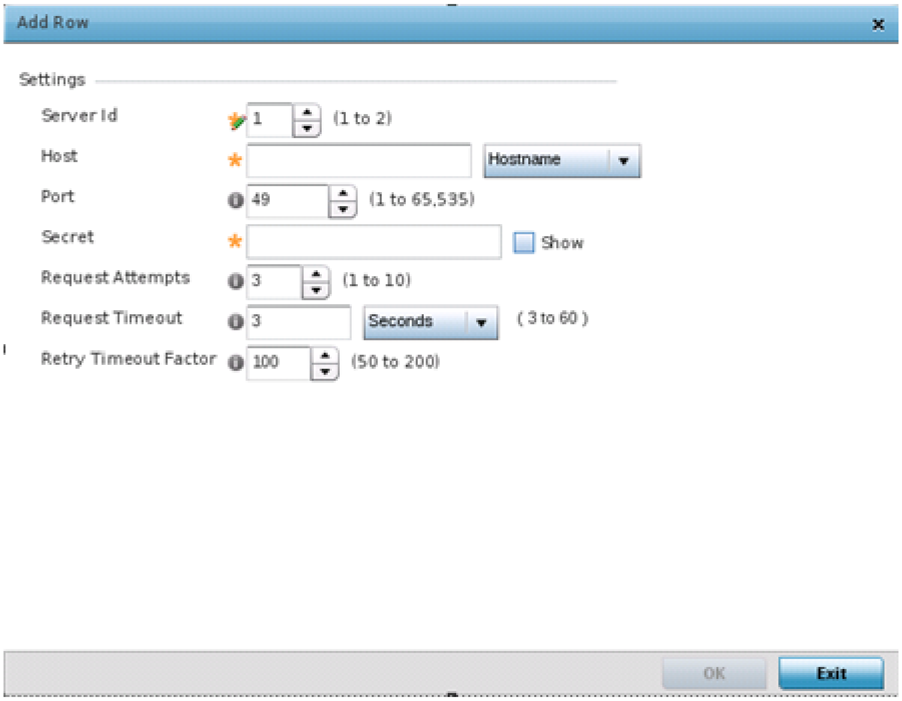
Accounting

Server Preference: authenticated-server-host

Accounting Server Details

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor

5 Under the **Authentication** table, select **+ Add Row**.



Add Row

Settings

Server Id: 1 (1 to 2)
Host: Hostname
Port: 49 (1 to 65,535)
Secret: ☐ Show
Request Attempts: 3 (1 to 10)
Request Timeout: 3 Seconds (3 to 60)
Retry Timeout Factor: 100 (50 to 200)

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.

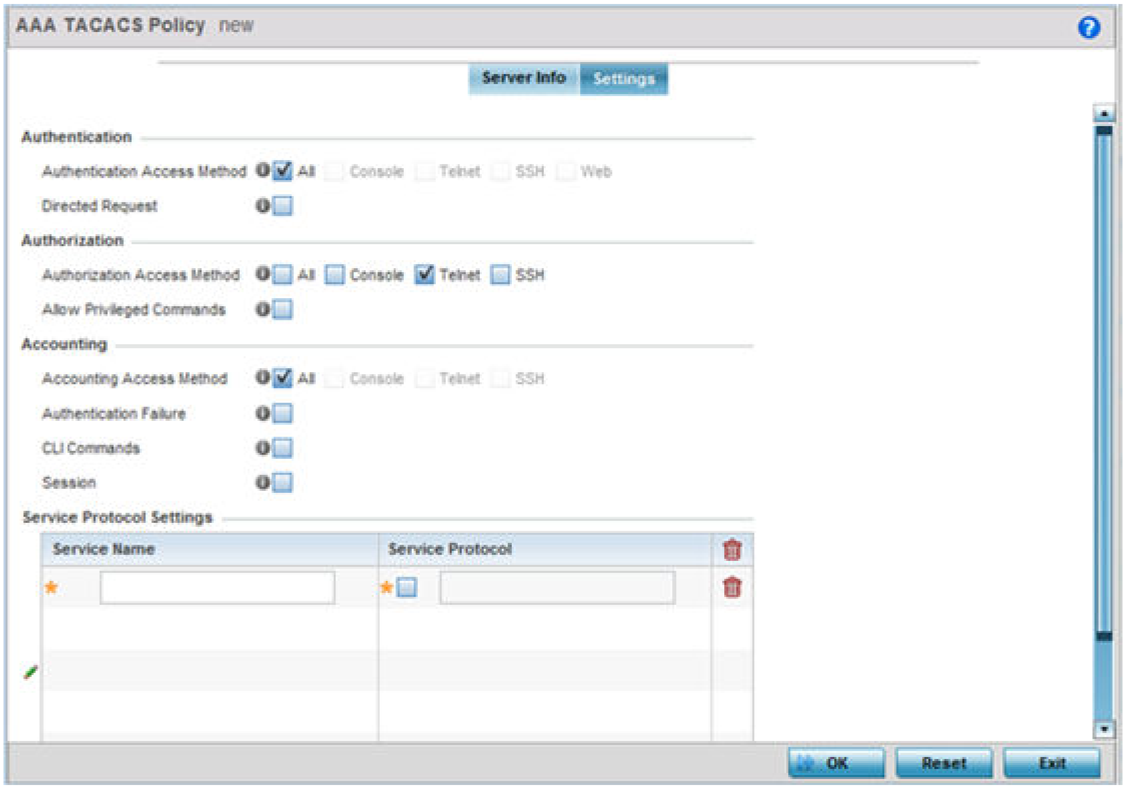
11 Set the **Server Preference**, within the Accounting field, to select the accounting server, from the pool of servers, to receive accounting requests. Options inlcude None, authenticated-server-host, authenticated-server-number, authorized-server-host and authorized-server-number. The default is authenticated-server-host. 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.



Authentication

Authentication Access Method ☑ All ☐ Console ☐ Telnet ☐ SSH ☐ Web

Directed Request ☐

Authorization

Authorization Access Method ☐ All ☐ Console ☑ Telnet ☐ SSH

Allow Privileged Commands ☐

Accounting

Accounting Access Method ☑ All ☐ Console ☐ Telnet ☐ SSH

Authentication Failure ☐

CLI Commands ☐

Session ☐

Service Protocol Settings

15 Set the following AAA TACACS **Authentication** server configuration parameters:

Authentication Access Method	Specify the connection method(s) for authentication requests. • All – Authentication is performed for all types of access without prioritization. • Console – Authentication is performed only for console access. • Telnet – Authentication is performed only for access through Telnet. • SSH – Authentication is performed only for access through SSH. • 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. • All – Authorization is performed for all types of access without prioritization. • Console – Authorization is performed only for console access. • Telnet – Authorization is performed only for access through Telnet. • 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. • All – Accounting is performed for all types of access without prioritization. • Console – Accounting is performed only for console access. • Telnet – Accounting is performed only for access through Telnet. • 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.

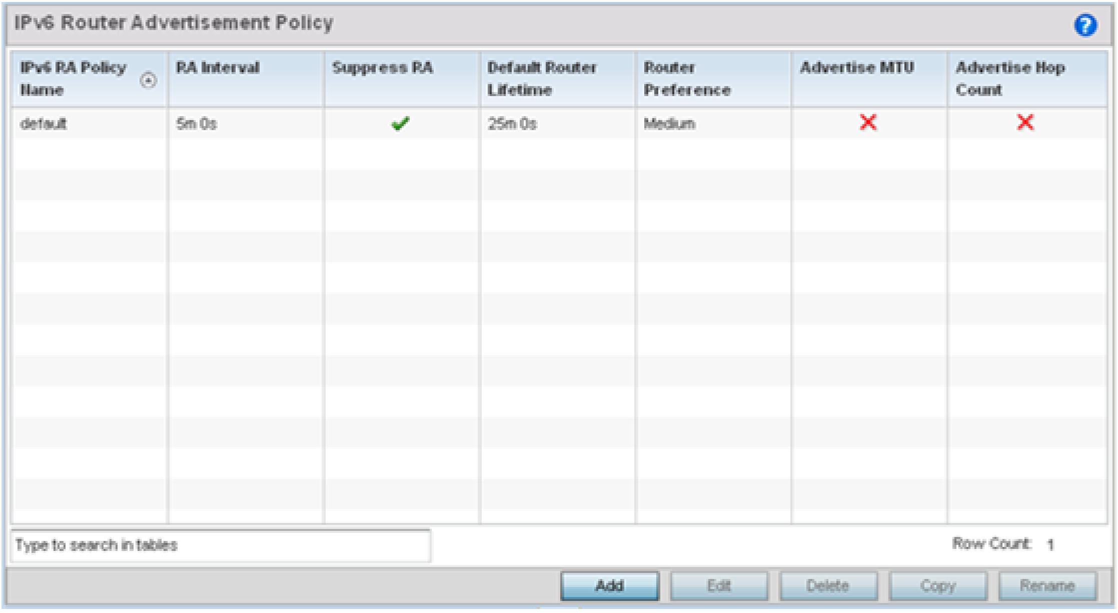
IPv6 Router Advertisment Policy

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**.



IPv6 Router Advertisement Policy

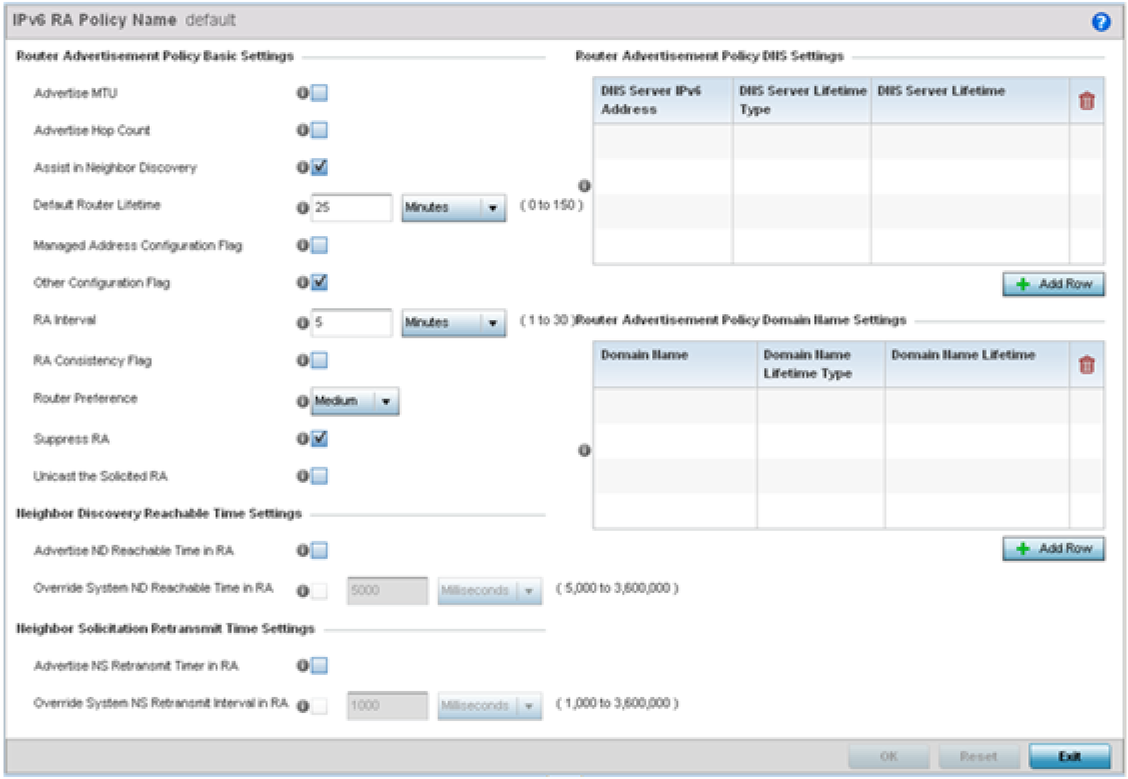
IPv6 RA Policy Name	RA Interval	Suppress RA	Default Router Lifetime	Router Preference	Advertise MTU	Advertise Hop Count
default	5m 0s	✓	25m 0s	Medium	✗	✗

Type to search in tables

Row Count: 1

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.



IPv6 RA Policy Name default

Router Advertisement Policy Basic Settings

Advertise MTU ☐
Advertise Hop Count ☐
Assist in Neighbor Discovery ☑
Default Router Lifetime 25 Minutes (0 to 150)
Managed Address Configuration Flag ☐
Other Configuration Flag ☑
RA Interval 5 Minutes (1 to 30)
RA Consistency Flag ☐
Router Preference Medium
Suppress RA ☑
Unicast the Solicited RA ☐

Neighbor Discovery Reachable Time Settings

Advertise ND Reachable Time in RA ☐
Override System ND Reachable Time in RA ☐ 5000 Milliseconds (5,000 to 3,600,000)

Neighbor Solicitation Retransmit Time Settings

Advertise NS Retransmit Timer in RA ☐
Override System NS Retransmit Interval in RA ☐ 1000 Milliseconds (1,000 to 3,600,000)

Router Advertisement Policy DNS Settings

DNS Server IPv6 Address	DNS Server Lifetime Type	DNS Server Lifetime

Router Advertisement Policy Domain Name Settings

Domain Name	Domain Name Lifetime Type	Domain Name Lifetime

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.

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is an inter-ISP routing protocol for establishing routes 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 set by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This includes AS information the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions are created and rules enforced.

An Autonomous System (AS) is a set of routers under the same administration using Interior Gateway Protocol (IGP) and common metrics to define how to route packets. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears as a single coherent interior routing plan and presents a consistent picture of reachable destinations.

Routing information exchanged through BGP supports only destination based forwarding (it assumes that a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes TCP supports a graceful close (all outstanding data is delivered before the connection is closed).

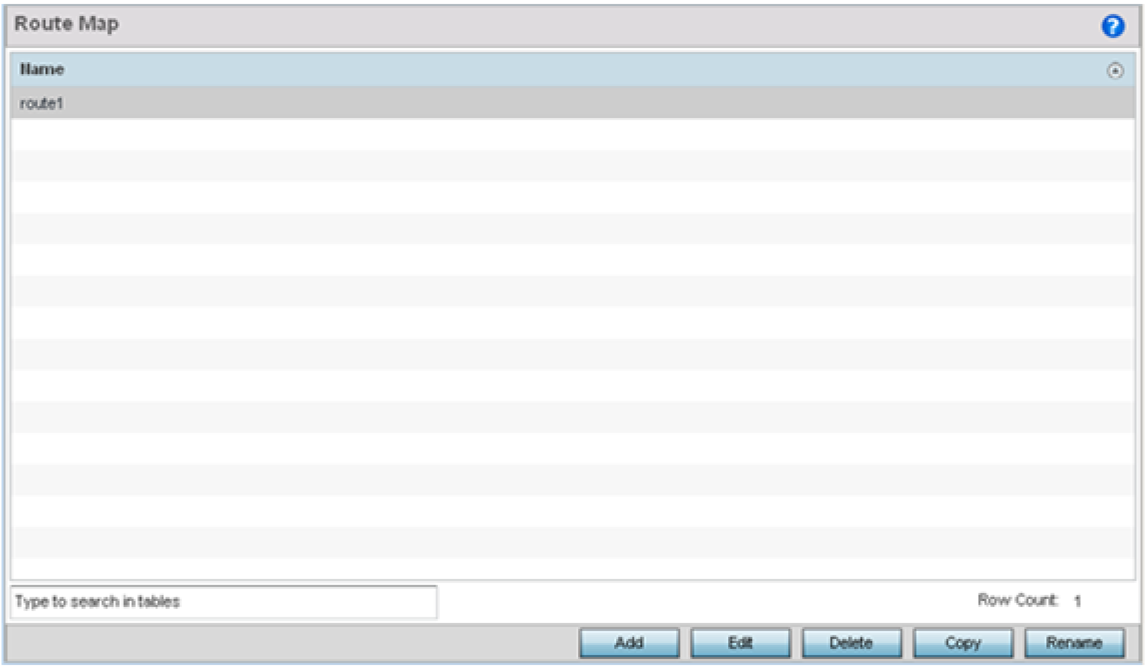
Refer to the following to configure access lists, path lists, IP prefix lists, community lists and external community lists for BGP:

- IP Access List on page 491
- AS Path List on page 492
- IP Prefix List on page 494
- Community List on page 495
- External Community List on page 497

To review existing BGP configurations or potentially create new ones:

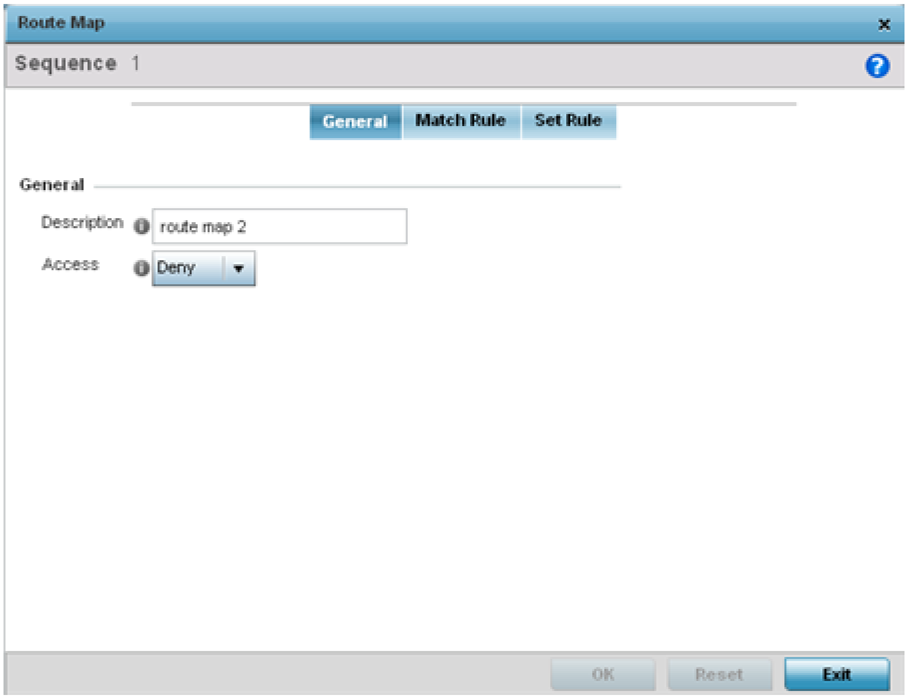
1 Select the **Configuration** > **Network** > **BGP** > **Route Map**.

In a BGP implementation, a route map is a method to control and modify routing information. The control and modification of routing information occurs using route redistribution rules.



2 Select **Add** to create a new route map, **Edit** to modify the attributes of a selected route. Existing route map configurations can be copied or renamed as needed.

The Route Map Rule screen lists existing rules and their access permissions.The Generaltab is displayed by default when adding or editing route maps.



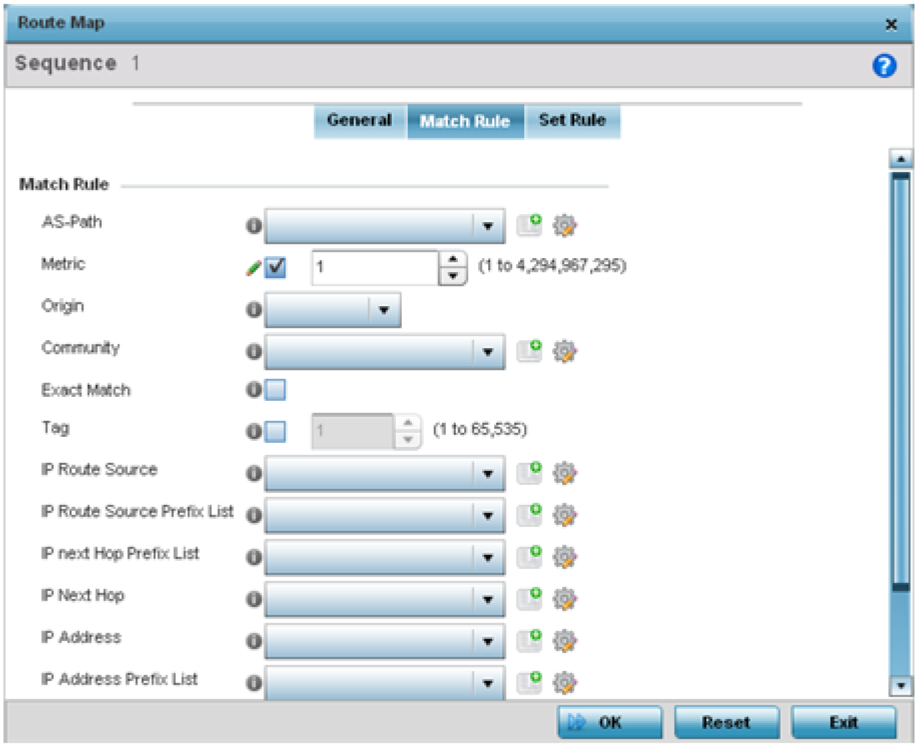
Description: route map 2

Access: Deny

3 Set the following General settings:

Description	Provide a 64 character maximum description to help distinguish this route map from others with similar access permissions.
Access	Set the permit or deny access designation for the route map. The default setting is deny.

4 Select the **Match Rule** tab.



Sequence 1

Match Rule

AS-Path
Metric ☑ 1 (1 to 4,294,967,295)
Origin
Community
Exact Match ☐
Tag ☐ 1 (1 to 65,535)
IP Route Source
IP Route Source Prefix List
IP next Hop Prefix List
IP Next Hop
IP Address
IP Address Prefix List

5 Set the following **Match Rule** settings:

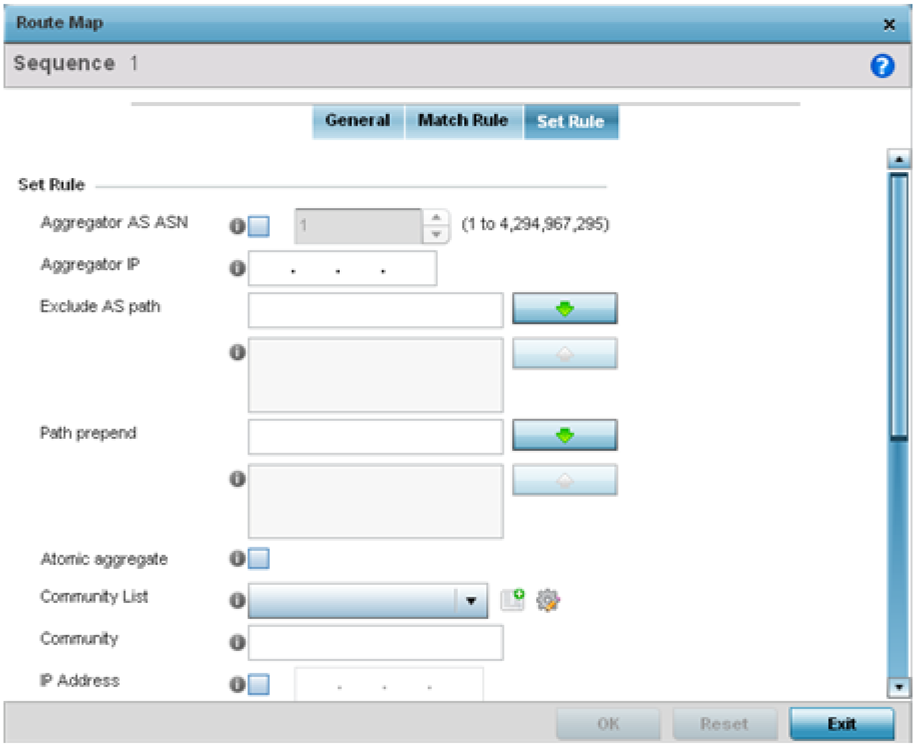
AS-Path	An AS path is a list of Autonomous Systems (AS) a packet traverses to reach its destination. From the drop-down menu, select a pre-configured AS-Path list. Use the Create icon to create an AS-Path list or select an existing one and use the Edit icon.
Metric	Select this option to define the exterior metric (1 - 4,294,967,295) used for route map distribution. BGP uses a route table managed by the external defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.

Origin	Use the drop-down menu to set the source of the BGP route. Options include: • egp - Matches if the origin of the route is from the exterior gateway protocol (eBGP). eBGP exchanges routing table information between hosts outside an autonomous system. • igp - Matches if the origin of the route is from the interior gateway protocol (iBGP). iBGP exchanges routing table information between routers within an autonomous system. • incomplete - Matches if the origin of the route is not identifiable.
Community	Use the drop-down menu to set the autonomous system community. A new community can be defined by selecting the Create icon, or an existing autonomous system community can be modified by selecting the Edit icon. Options include: • internet - Advertises this route to the Internet. This is a global community. • local-AS - Prevents the transmit of packets outside the local AS. • no-advertise - Do not advertise this route to any peer, either internal or external. • no-export - Do not advertise to BGP peers, keeping this route within an AS. • aa:nn - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.
Exact Match	When matching the Community, use exact matching. The default setting is disabled.
Tag	The Tag is a way to preserve a route's AS path information for routers in iBGP. The default setting is disabled.
IP Route Source	The IP Route Source is a list of IP addresses used to filter routes based on the advertised IP address of the source. Use the drop-down menu to set the IP route source. A new route source can be defined by selecting the Create icon, or an existing one can be modified by selecting the Edit icon.
IP Route Source Prefix List	The IP Route Source Prefix List is a list of prefixes used to filter routes based on the prefix list used for the source. Use the drop-down menu to set the IP route source prefix list. A new list can be defined by selecting the Create icon, or an existing AS-Path can be modified by selecting the Edit icon.
IP Next Hop Prefix List	The IP Next Hop Prefix List is a list of prefixes for the route's next hop determining how the route is filtered. Use the drop-down menu to set the IP next hop prefix list. A new list can be defined by selecting the Create icon, or an existing IP next hop prefix list can be modified by selecting the Edit icon.

IP Next Hop	The IP Next Hop is a list of IP addresses used to filter routes based on the IP address of the next hop in the route. Use the drop-down menu to set an IP next hop. A new next hop can be defined by selecting the Create icon, or an existing IP next hop can be modified by selecting the Edit icon.
IP Address	The IP Address parameter is a list of IP addresses in the route used to filter the route. Use the drop-down menu to set the IP address. A new address can be defined by selecting the Create icon, or an existing IP address can be modified by selecting the Edit icon.
IP Address Prefix List	The IP Address Prefix List is a list of prefixes in the route used to filter the route. Use the drop-down menu to set the IP address prefix list. A new community can be defined by selecting the Create icon, or an existing IP address prefix list can be modified by selecting the Edit icon.

6 Use the drop-down menu to set the **Math Rule Experimental Feature** External Community setting. A new External Community setting can be defined by selecting the **Create** icon, or an existing External Community setting can be modified by selecting the **Edit** icon.

7 Select the Set Rule tab.



8 Define the following Set Rule parameters:

Aggregator AS ASN	Select the Autonomous System Number (ASN) for the BGP aggregator. Aggregates minimize the size of routing tables. Aggregation combines the characteristics of multiple routes and advertises them as a single route. Select the ASN for this aggregator. Set a value from 1 - 4,294,967,295. This setting is disabled by default.
Aggregator IP	Provide the IP address of the route aggregator. BGP allows the aggregation of specific routes into one route using an aggregate IP address.
Exclude AS Path	Enter an AS, or a list of ASs, excluded from the AS path.
Path Prepend	Enter an AS, or a list of ASs, prepended to the AS path.
Atomic Aggregate	When a BGP enabled wireless controller or service platforms receives a set of overlapping routes from a peer, or if the set of routes selects a less specific route, then the local device must set this value when propagating the route to its neighbors. This setting is disabled by default.
Community List	The Community List is a list of communities added to the route. A BGP community is a group of routes sharing a common attribute.
Community	The Community is the community attribute set to this route.
IP Address	Set the IP address for this route.
Enable (Next Hop Peer)	Select this option to enable the identification of the next hop address for peer devices. This setting is disabled by default.
Local Preference	Select this option to enable the communication of preferred routes out of the AS between peers. This setting is disabled by default.
Metric	BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost. Set a metric value for this route from 1 - 4,294,967,295.
Origin	Select the origin code for this BGP route. • egp - Sets the origin of the route to eBGP. • igp - Sets the origin of the route to iBGP. • incomplete - Sets the origin of the route as not identifiable. Set this if the route is from a source other than eBGP or iBGP.
Originator ID	Set the IP address of the originator of this route map.
Source ID	Set the IP address of the source of this route map.

Tag	The Tag is a way to preserve a route's AS path information for routers in iBGP. Set a tag value from 1 - 65535.
Weight	Select this option to enable the assignment of a weighted priority to the aggregate route. The range is 1 - 4,294,967,295.

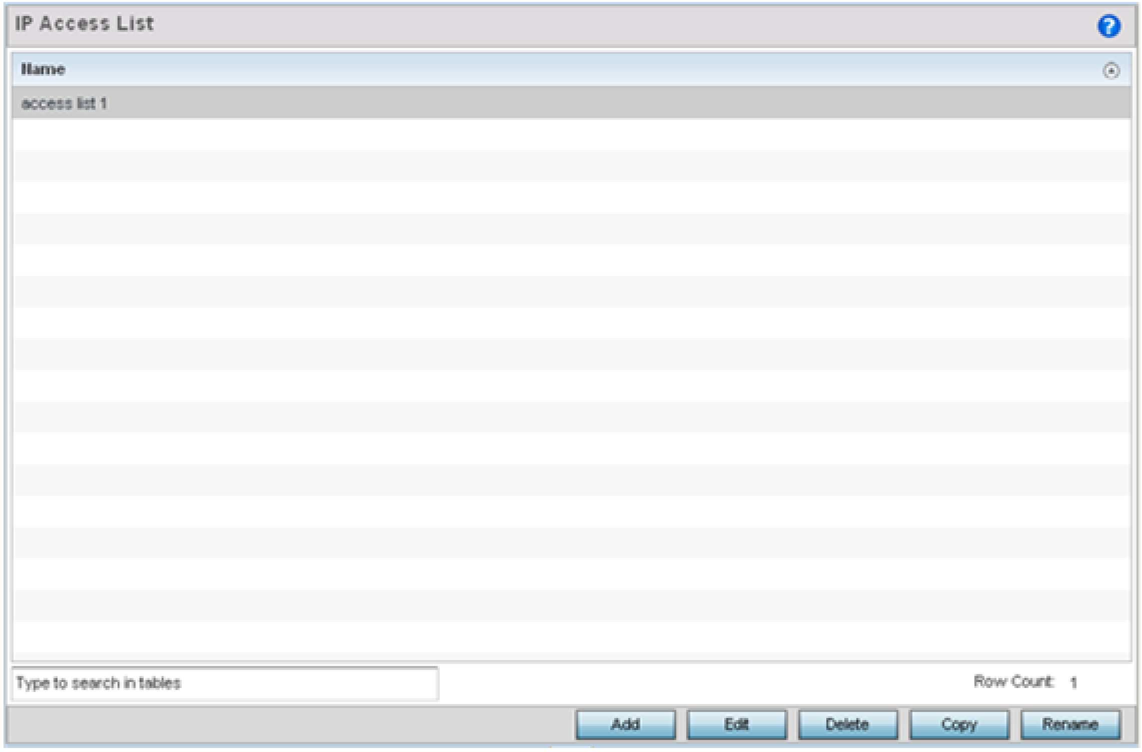
9 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

IP Access List

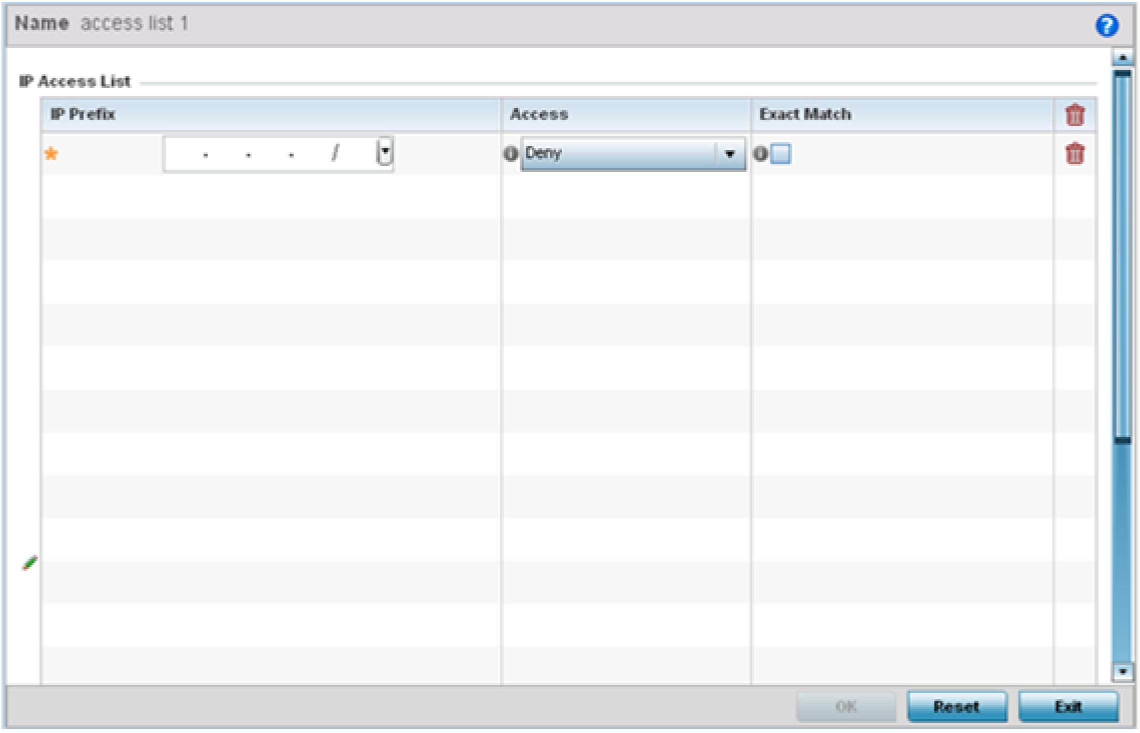
BGP peers and route maps can reference a single IP based access list. Apply IP access lists to both inbound and outbound route updates. Every route update is passed through the access list. BGP applies each rule in the access list in the order it appears in the list. When a route matches a rule, the decision to permit or deny the route is applied. No additional rules are processed.

To define a IP access list:

1 Select the **Configuration** > **Network** > **BGP** > **IP Access List**.



2 Select **Add** to create a new IP access list, **Edit** to modify the attributes of a selected list or **Delete** to remove an obsolete list. Existing policies can be copied or renamed as needed.



3 Set the following IP Access List settings:

IP Prefix	Provide the IP address used to define the prefix list rule.
Access	Use the drop-down menu to Permit or Deny requests for network access originating from IP addresses with the IP prefix. The default setting is deny.
Exact Match	Check to require an exact match for the IP prefix before access is granted. Permit and deny apply only when there is an exact match between the regular expression and the autonomous system path.This setting is disabled by default.

4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

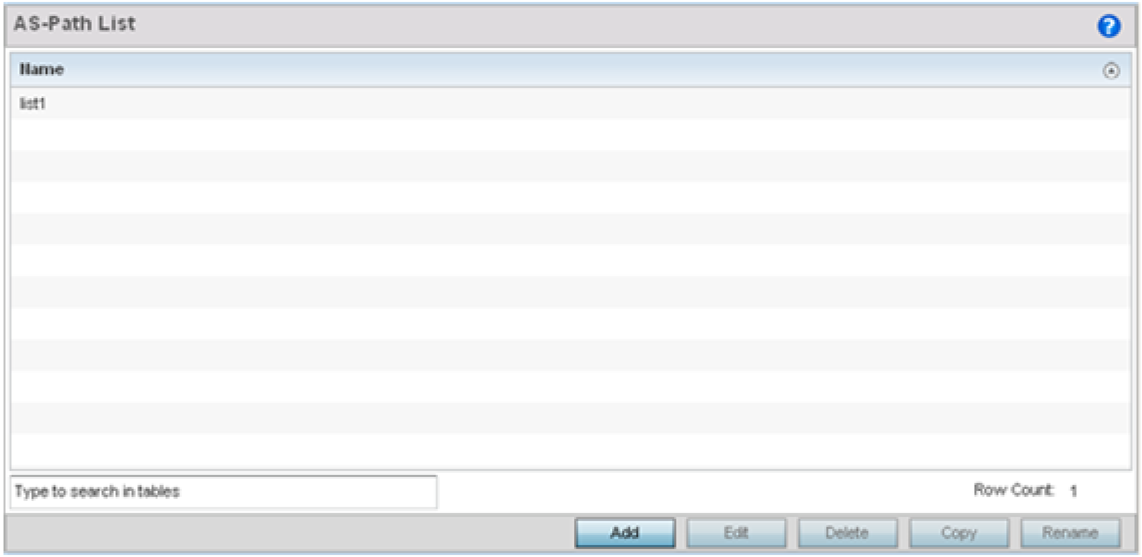
AS Path List

BGP uses a routing algorithm to exchange network reachability information with other BGP supported devices. Network availability ad reachability information is exchanged between BGP peers in routing updates. This information contains a network number, path specific attributes and the list of autonomous system numbers a route transits to reach a destination. This list is contained in the AS path. BGP prevents routing loops by rejecting any routing update that contains a local autonomous system number, as this indicates the route has already traveled through that autonomous system and a loop would be created. BGP's routing algorithm is a combination of a distance vector routing algorithm and AS path loop detection.

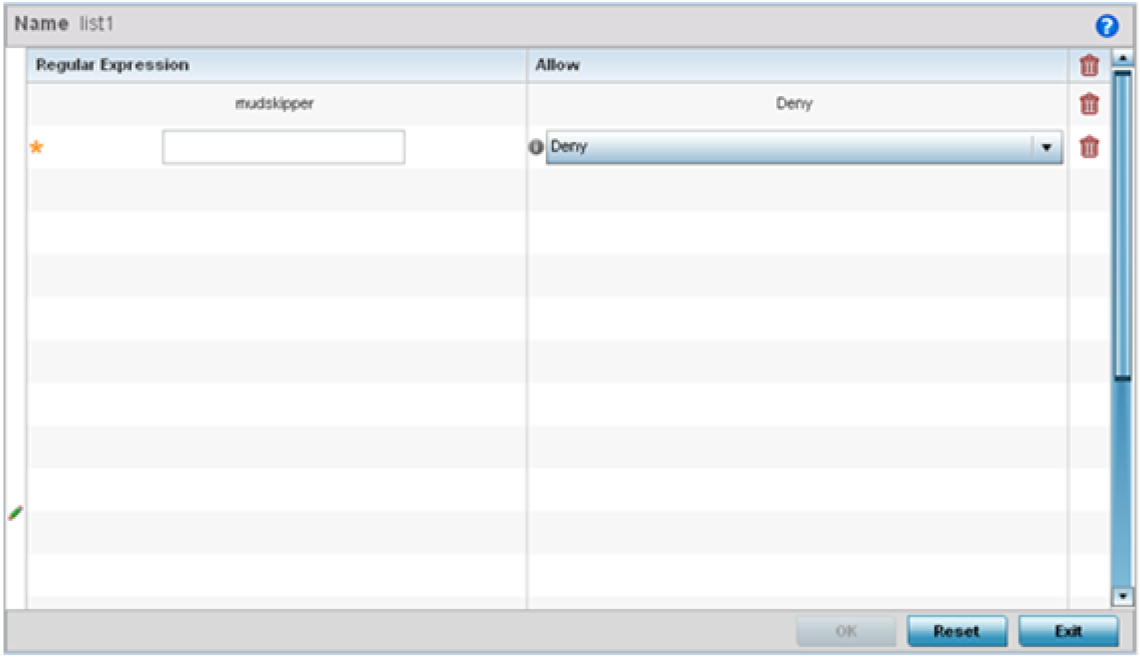
The AS path contains a set of numbers for passing routing information. A BGP supported device adds its own autonomous system number to the list when it forwards an update message to external peers.

To define an AS path list:

1 Select the **Configuration** > **Network** > **BGP** > **AS Path List**.



2 Select **Add** to create a new AS path list or **Edit** to modify the attributes of a selected path list. Existing policies can be copied or renamed as needed.



3 Set the following AS Path List settings:

Regular Expression	Provide a 64 character maximum regular expression unique to the AS path list rule. Regular expressions are used to specify patterns to match community attributes.
Allow	Use the drop-down menu to Permit or Deny requests for network access using the defined AS path list. The default setting is deny.

4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

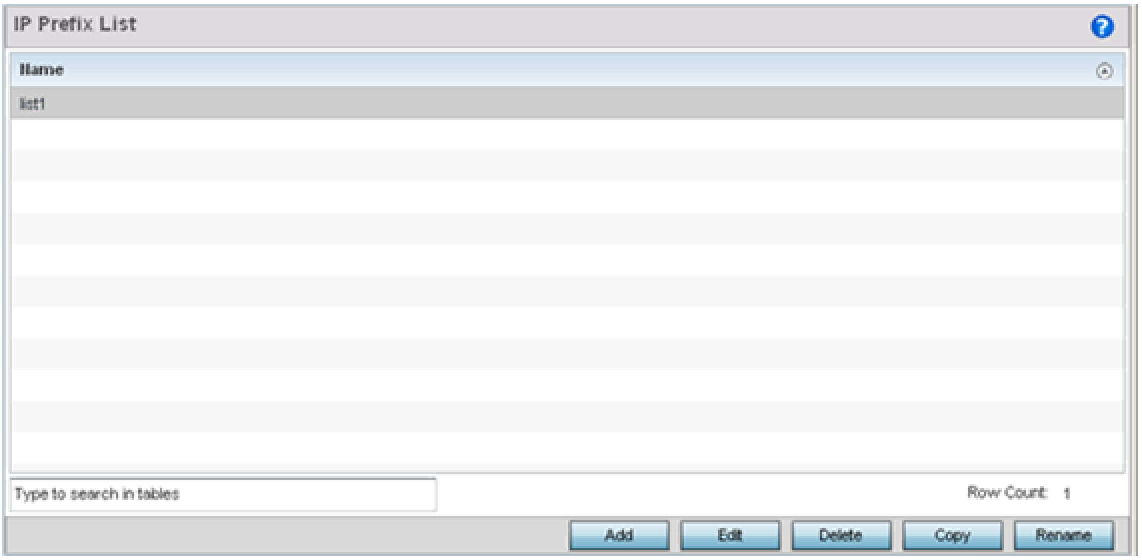
IP Prefix List

IP prefix lists are a convenient way to filter networks in BGP supported networks. IP prefix lists work similarly to access lists. A prefix list contains ordered entries processed sequentially. Like access lists, the evaluation of a prefix against a prefix list ends as soon as a match is found.

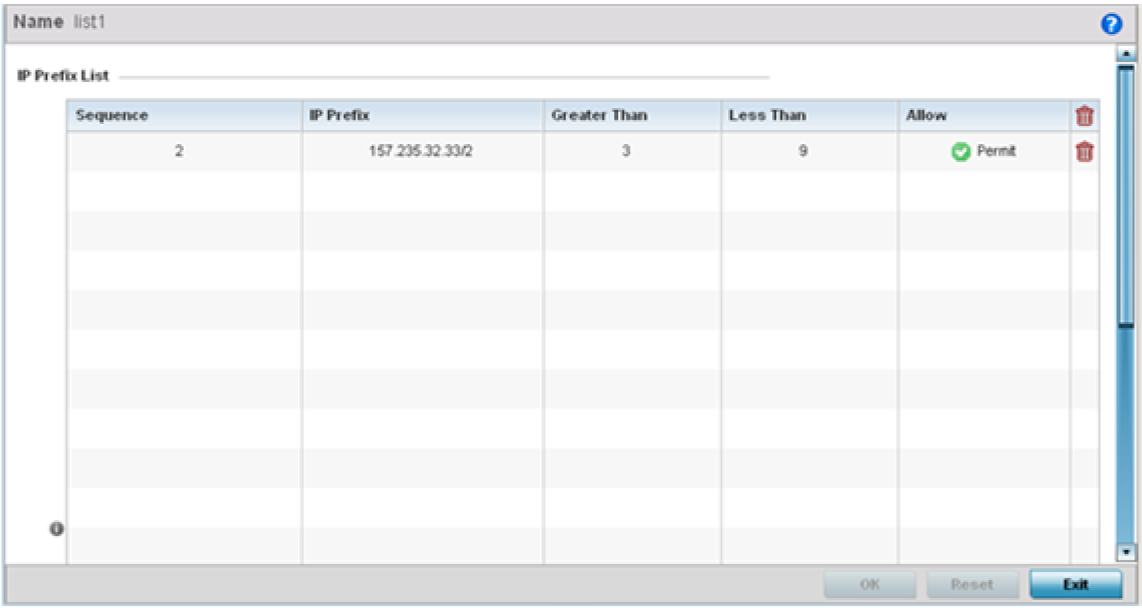
To restrict the routing information advertised, use filters consisting of an IP prefix list applied to updates both to and from neighbors.

To define an IP prefix list:

1 Select **Configuration** > **Network** > **BGP** > **IP Prefix List**.



2 Select **Add** to create a new IP prefix list or **Edit** to modify the attributes of a selected list. Existing policies can be copied or renamed as needed.



Name list1

IP Prefix List

Sequence	IP Prefix	Greater Than	Less Than	Allow
2	157.235.32.33/2	3	9	✓ Permit

3 Define the following **IP Prefix List** settings:

Sequence	Supply a sequence number to determine the prefix utilization order for existing lists.
IP Prefix	Set the IP prefix used as an prefix list rule.
Greater Than	Specify a greater than or equal to value for an IP prefix range.
Less Than	Specify a less than or equal to value for an IP prefix range.
Allow	Use the drop-down menu to set a Permit or Deny designation to the rule configuration.

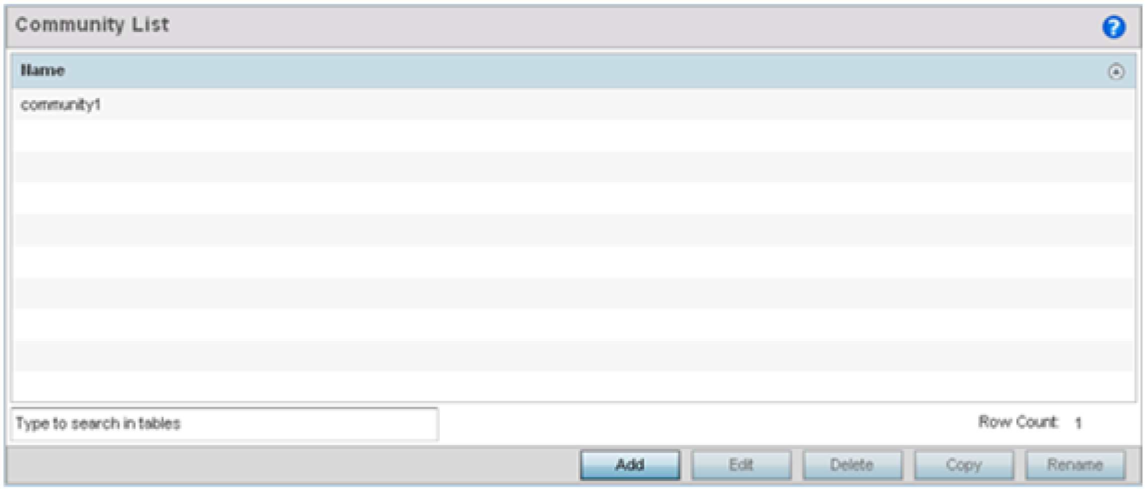
4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

Community List

A BGP community is a group of routes sharing a common attribute. The BGP list enables an administrator to assign names to community lists and increase the number of community lists configurable. A community list can be configured with regular expressions and numbered community lists. All the rules in numbered communities apply to named community lists, except there is no limitation in the number of community attributes configurable for a named community list.

To define a BGP community list:

1 Select **Configuration** > **Network** > **BGP** > **Community List**.

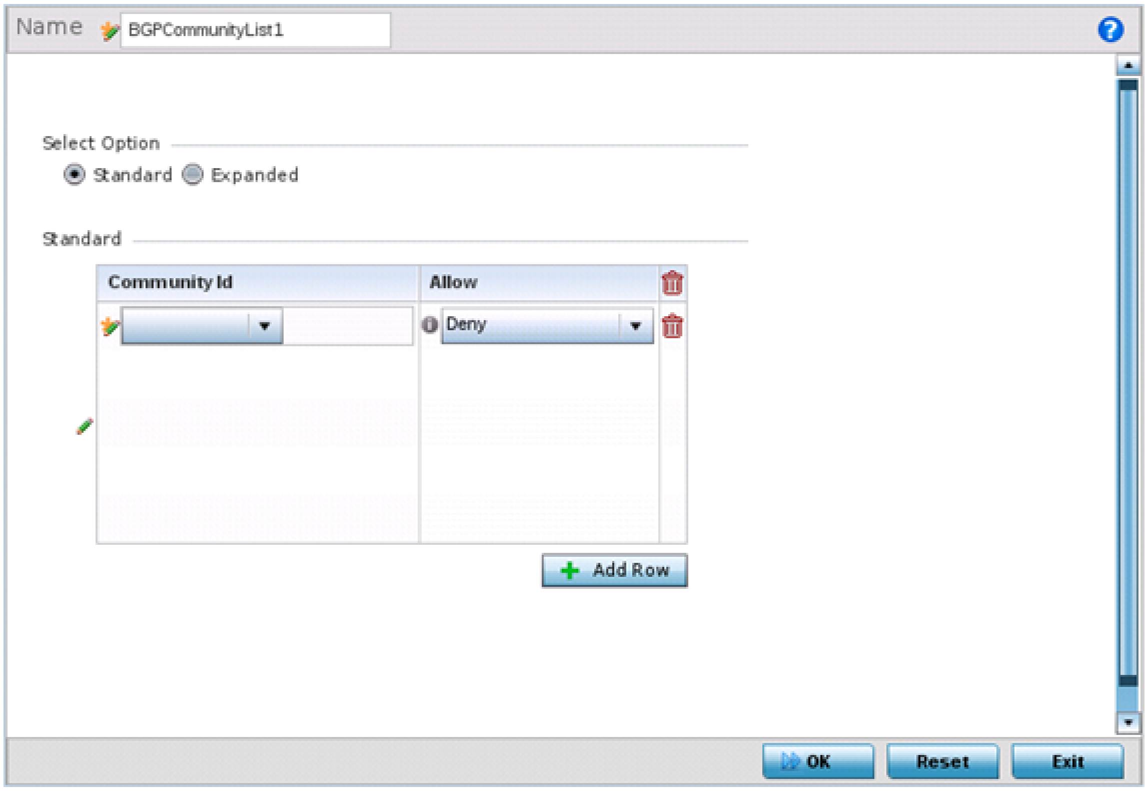


Name
community1

Type to search in tables

Row Count: 1

2 Select **Add** to create a new community list or **Edit** to modify the attributes of a selected list. Existing lists can be copied or renamed as needed.



Name: BGPCommunityList1

Select Option

● Standard ○ Expanded

Standard

Community Id	Allow
	Deny

3 Define whether the list is **Standard** or **Expanded**.

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

4 Set the following **Community List** settings:

Community Id	Provide a community ID unique to this particular rule. The following are available: • internet - Advertises this route to the Internet. This is a global community. • local-AS - Prevents the transmit of packets outside the local AS. • no-advertise - Do not advertise this route to any peer, either internal or external. • no-export - Do not advertise to BGP peers (keeping) this route within an AS. • aa:nn - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.
Allow	Use the drop-down menu to Permit or Deny requests for the community ID. The default setting is deny.

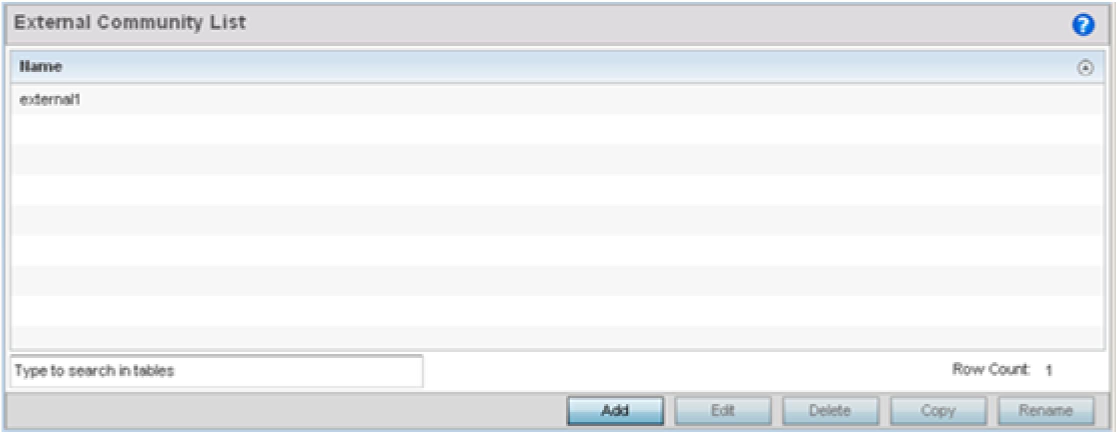
5 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

External Community List

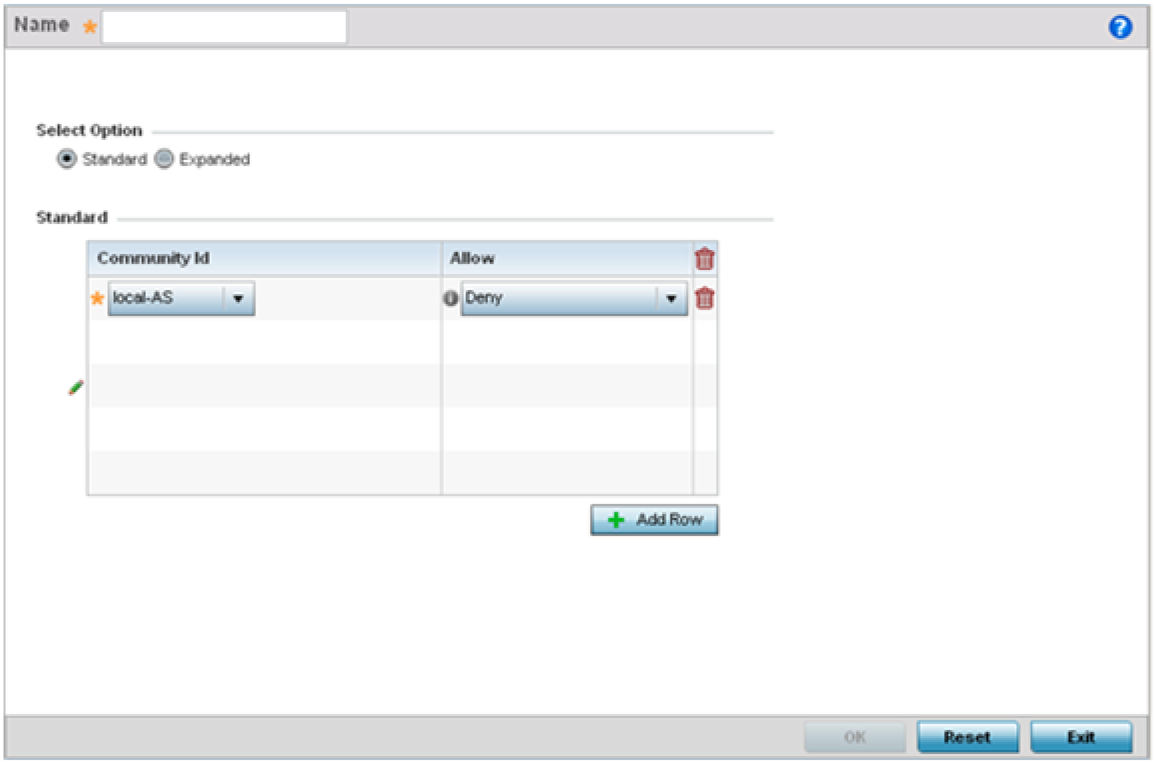
A BGP external community is a group of routes sharing a common attribute, regardless of their network or physical boundary. By using a BGP community attribute, routing policies can implement inbound or outbound route filters based on a community tag, rather than a long list of individual permit or deny rules. A BGP community list is used to create groups of communities to use in a match clause of a route map. An external community list can be used to control which routes are accepted, preferred, distributed, or advertised.

To define a BGP external community list:

1 Select **Configuration** > **Network** > **BGP** > **External Community List**



2 Select **Add** to create a new community list or **Edit** to modify the attributes of a selected list. Existing lists can be copied or renamed as needed.



3 Define whether the list is **Standard** or **Expanded**.

Standard community lists specify known communities and community numbers. Expanded community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

4 Set the following based on the Standard or Extended option selected:

Community Id	If selecting Standard, enter a numeric community ID unique to this particular rule. If selecting Extended, enter a regular expression unique to this particular rule.
Allow	Use the drop-down menu to Permit or Deny requests for the external community ID. The default setting is deny.

5 Click **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 499
- Network Group Alias Configuration on page 502
- Network Group Alias Configuration on page 502

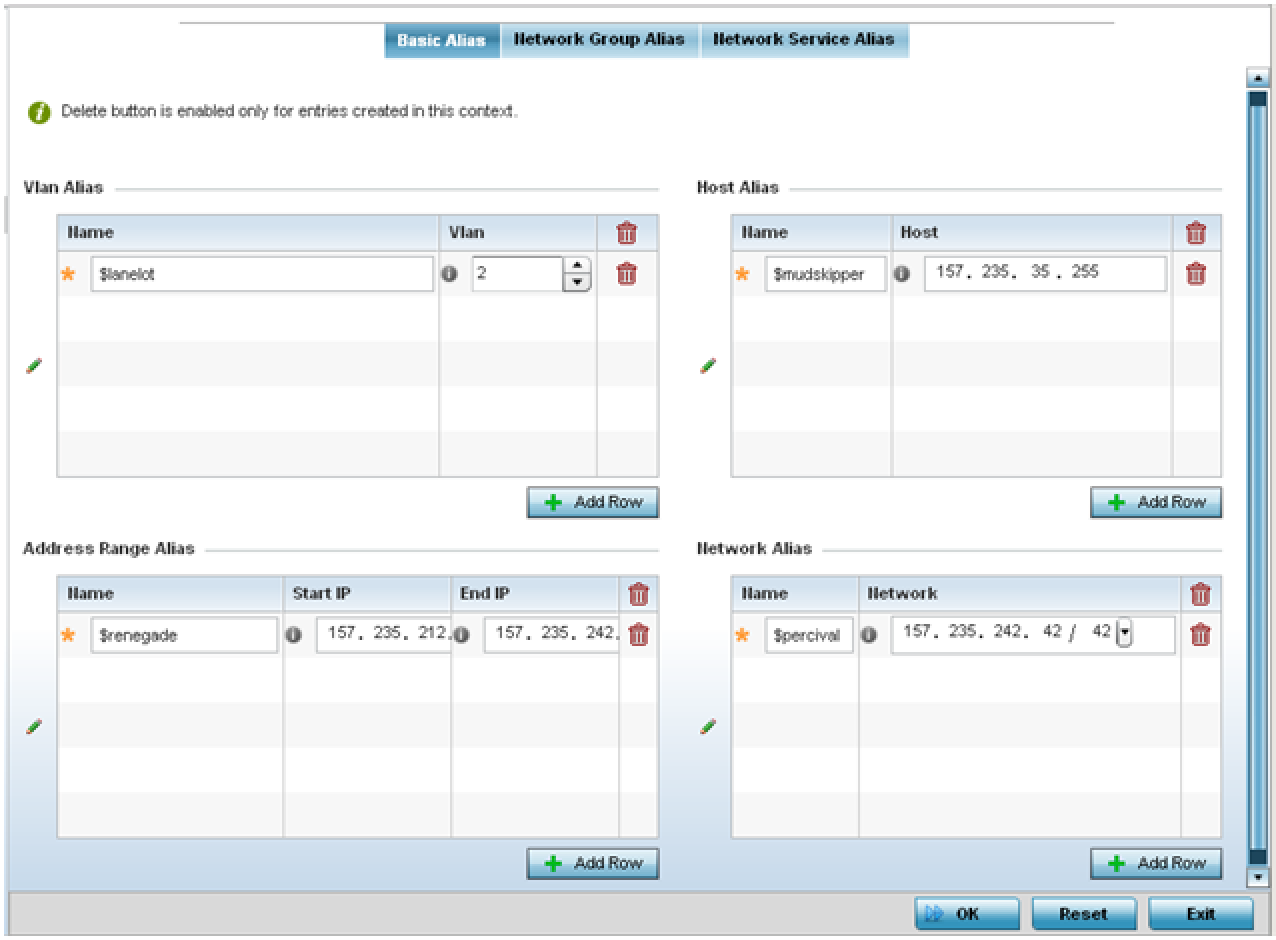
Network Basic Alias Configuration

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.



Delete button is enabled only for entries created in this context.

Vlan Alias

Name	Vlan
$lanelot	2

Host Alias

Name	Host
$mudskipper	157 . 235 . 35 . 255

Address Range Alias

Name	Start IP	End IP
$renegade	157 . 235 . 212.	157 . 235 . 242.

Network Alias

Name	Network
$percival	157 . 235 . 242 . 42 / 42

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.

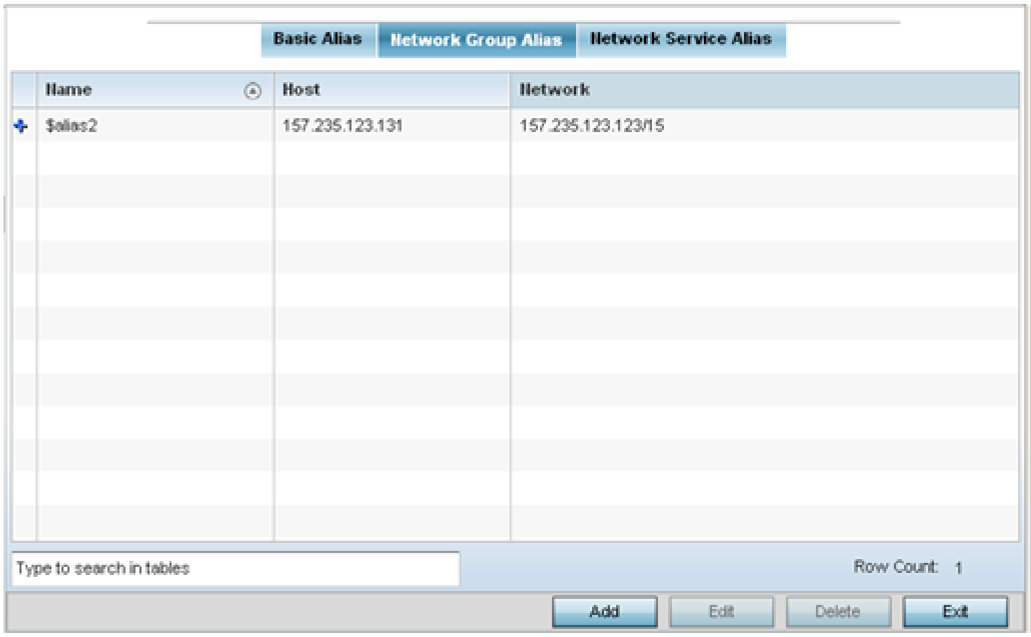
Network Group Alias Configuration

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.



Name	Host	Network
$alias2	157.235.123.131	157.235.123.123/15

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.

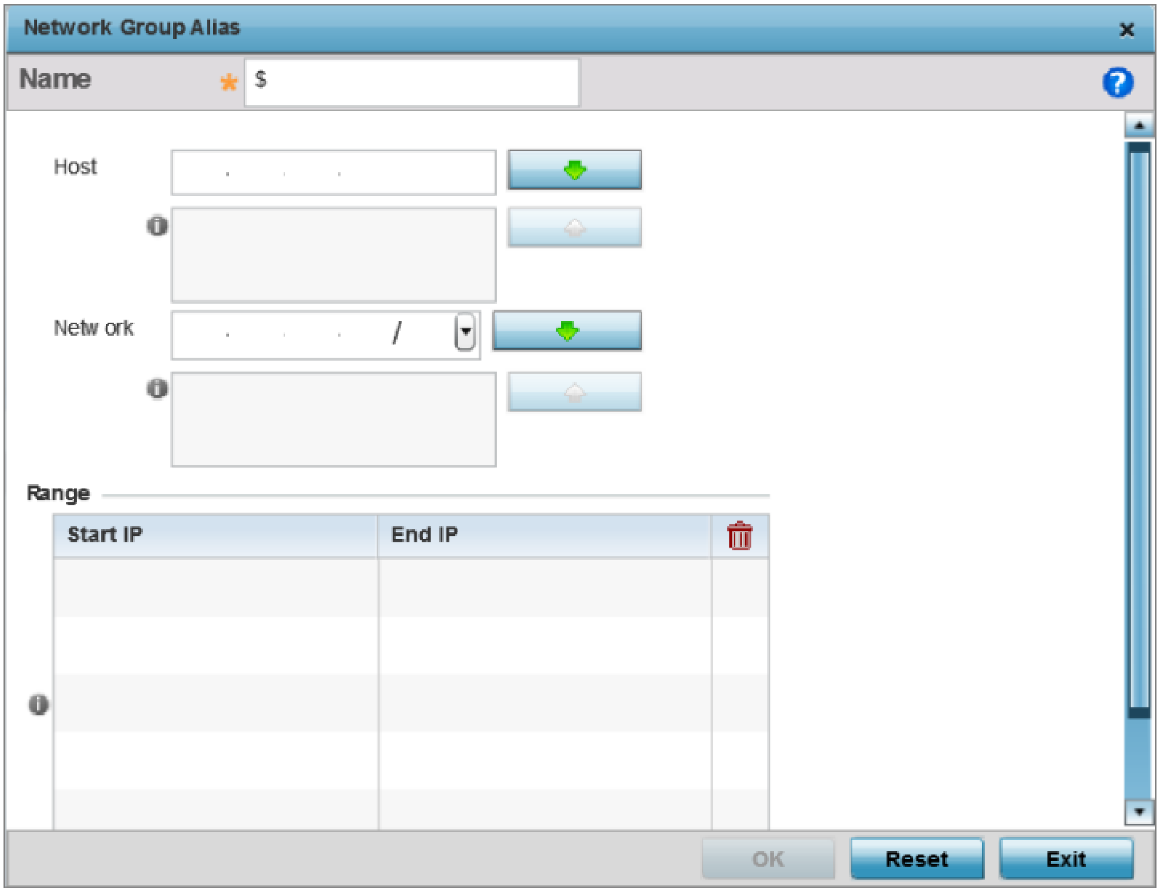


Figure 233: Network Group Alias - Add/Edit Screen

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.

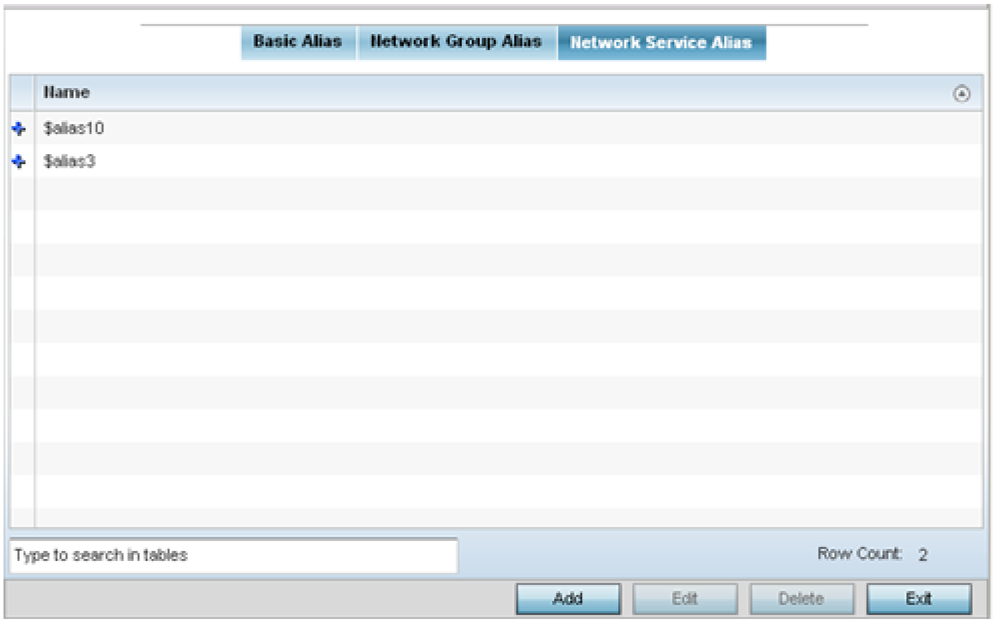
Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

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.

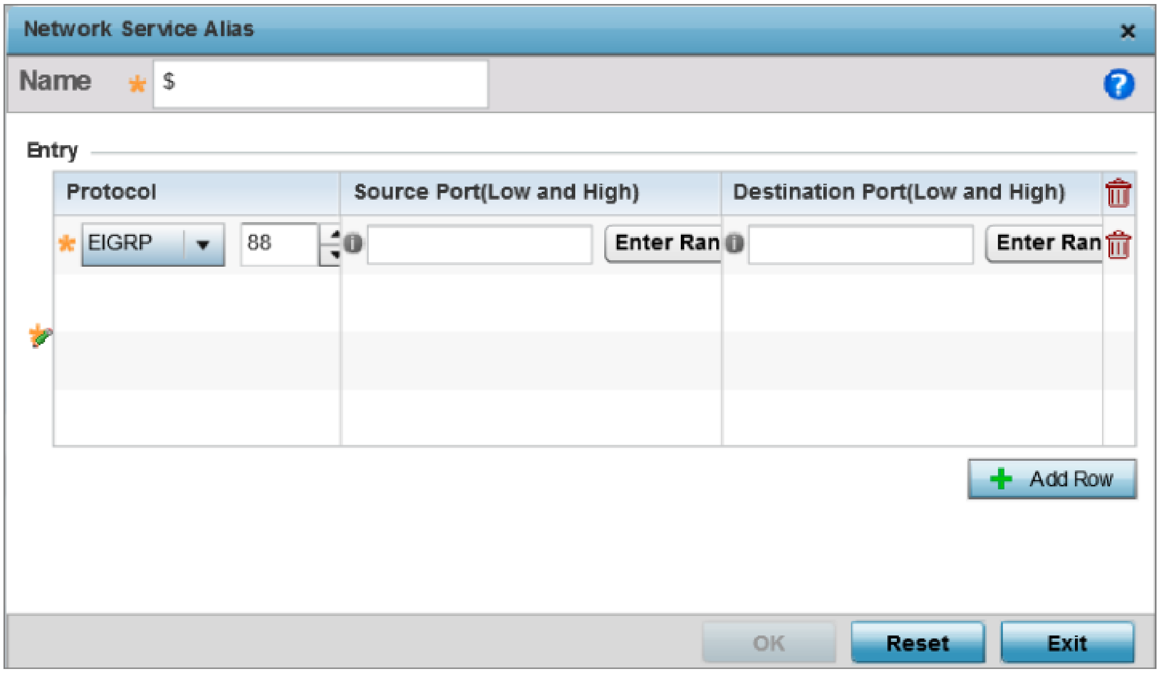


Figure 234: Network Alias - Network Service Alias Add screen

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*. 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*. 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 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

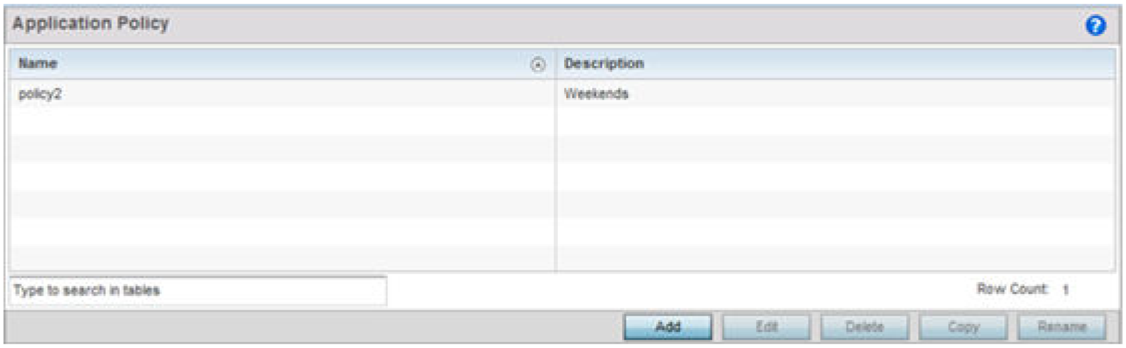
For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A deny rule is exclusive, as no other action can be combined with a deny. An allow rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting 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.

To define an application policy configuration:

1 Select **Configuration** → **Network** → **Application Policy**.

The screen lists the application policy configurations defined thus far.



Application Policy

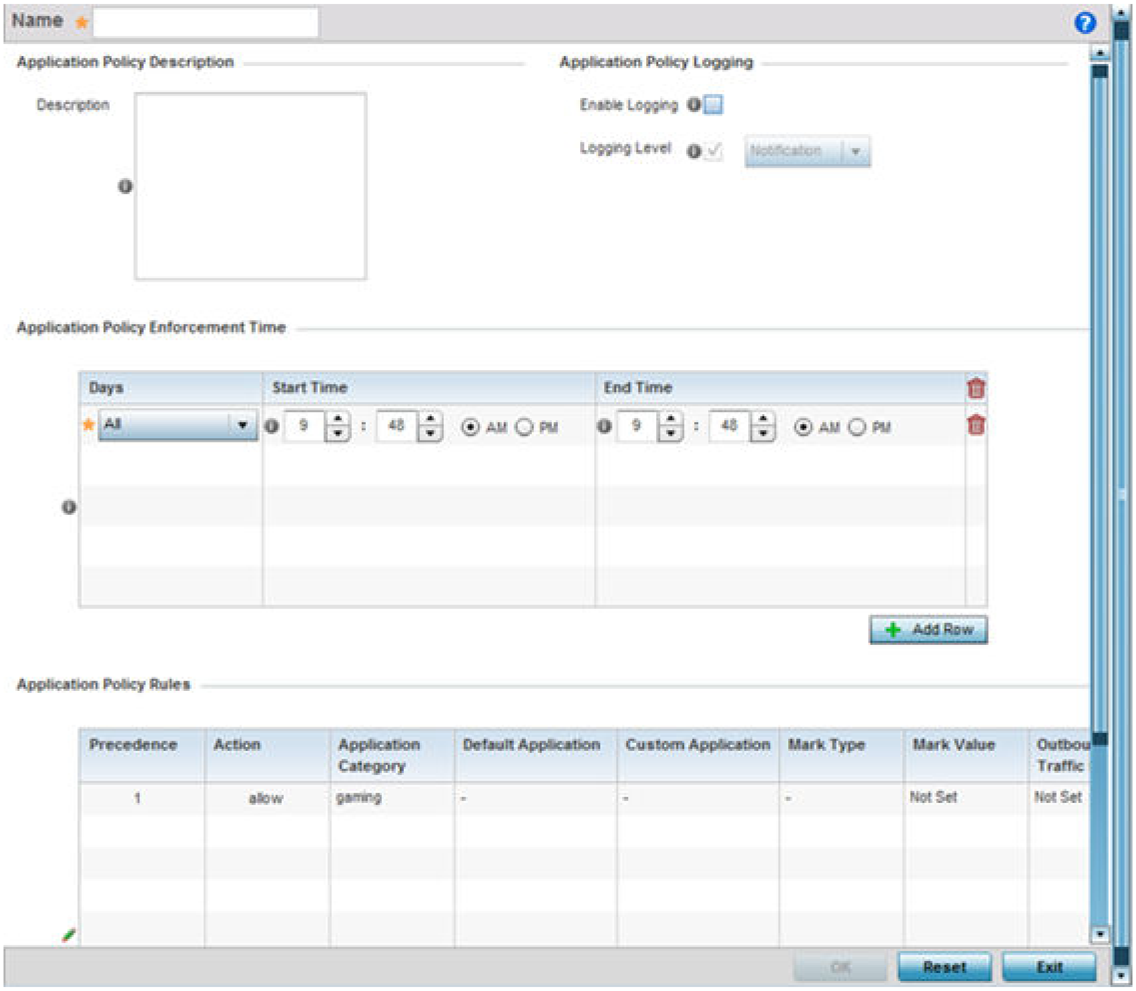
Name	Description
policy2	Weekends

Row Count: 1

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.



Days	Start Time	End Time
All	9 : 48 ● AM ○ PM	9 : 48 ● AM ○ PM

Precedence	Action	Application Category	Default Application	Custom Application	Mark Type	Mark Value	Outbou Traffic
1	allow	gaming	-	-	-	Not Set	Not Set

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:

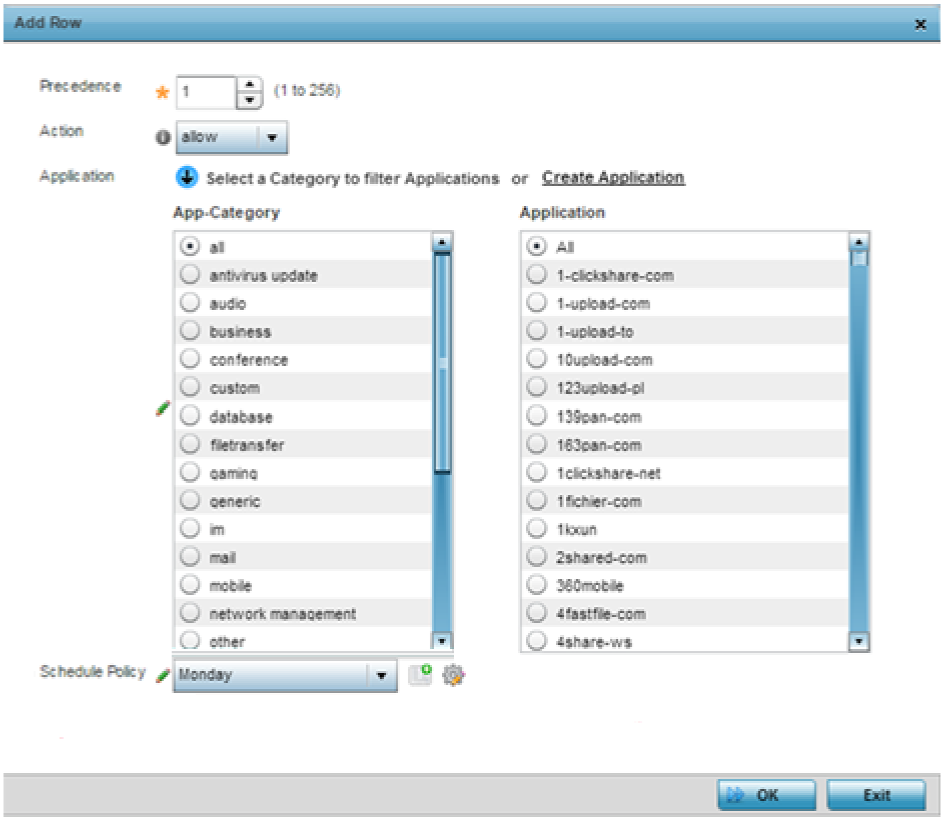
Enable Logging	Enables the log functionality, where each new flow is shown with the corresponding matched application, the action taken and the policy name. When enabled, logging just shows what applications are getting recognized.
Logging Level	Select this option to log application events by severity. 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.



Add Row

Precedence: 1 (1 to 256)

Action: allow

Application: Select a Category to filter Applications or Create Application

App-Category: ● all

Application: ● All

Schedule Policy: Monday

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 513

12 Select **OK** to save the updates to the application policy. Select **Reset** to revert to the last saved configuration.

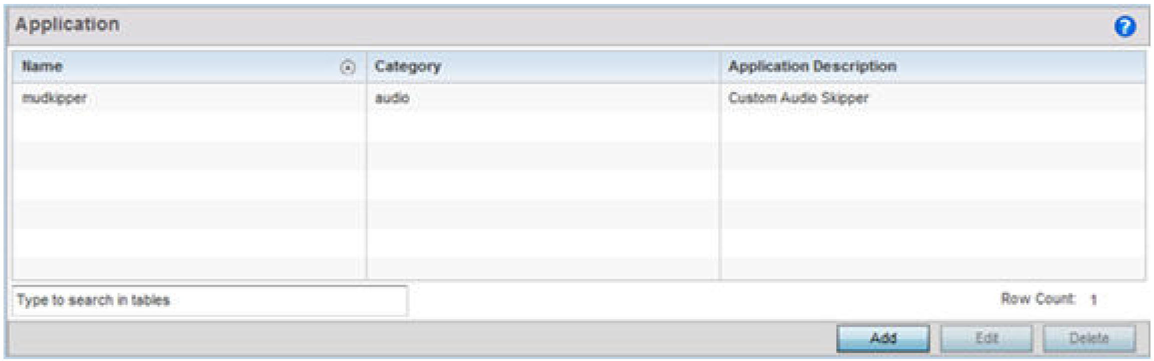
Application

Use the Application screen to create custom application configurations.

To create a user-defined application:

1 Select **Configuration** → **Network** → **Application**.

The Application screen displays. This screen lists the application configurations defined thus far.



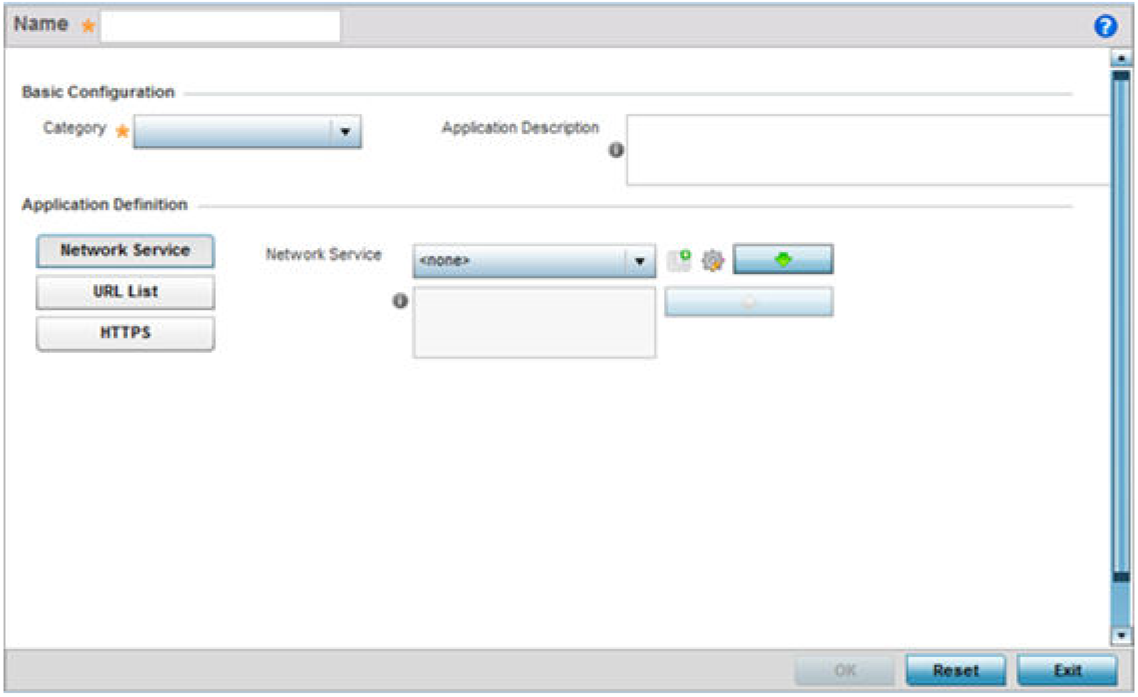
Application

Name	Category	Application Description
mudkipper	audio	Custom Audio Skipper

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 userdefined 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.

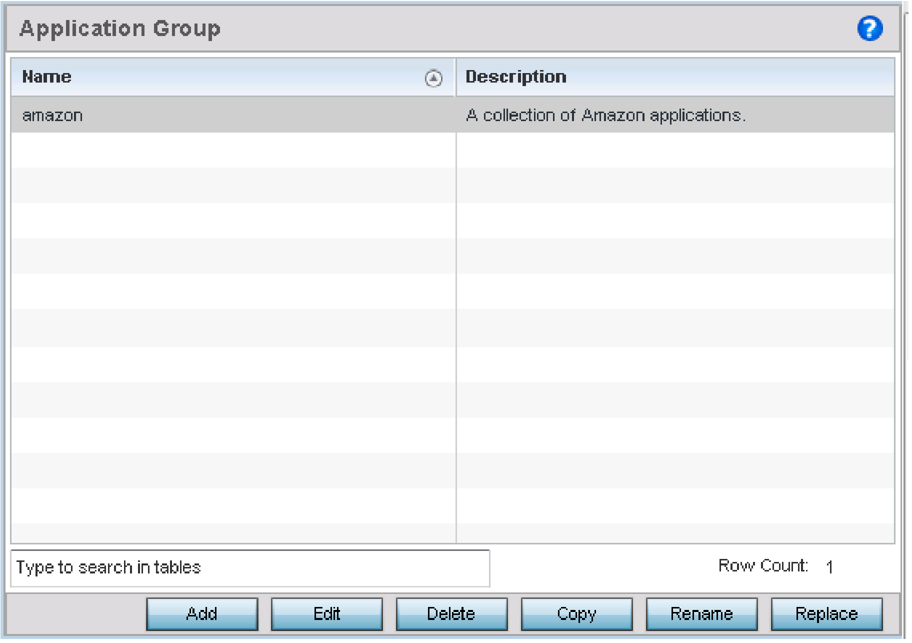
Application Group

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.

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.

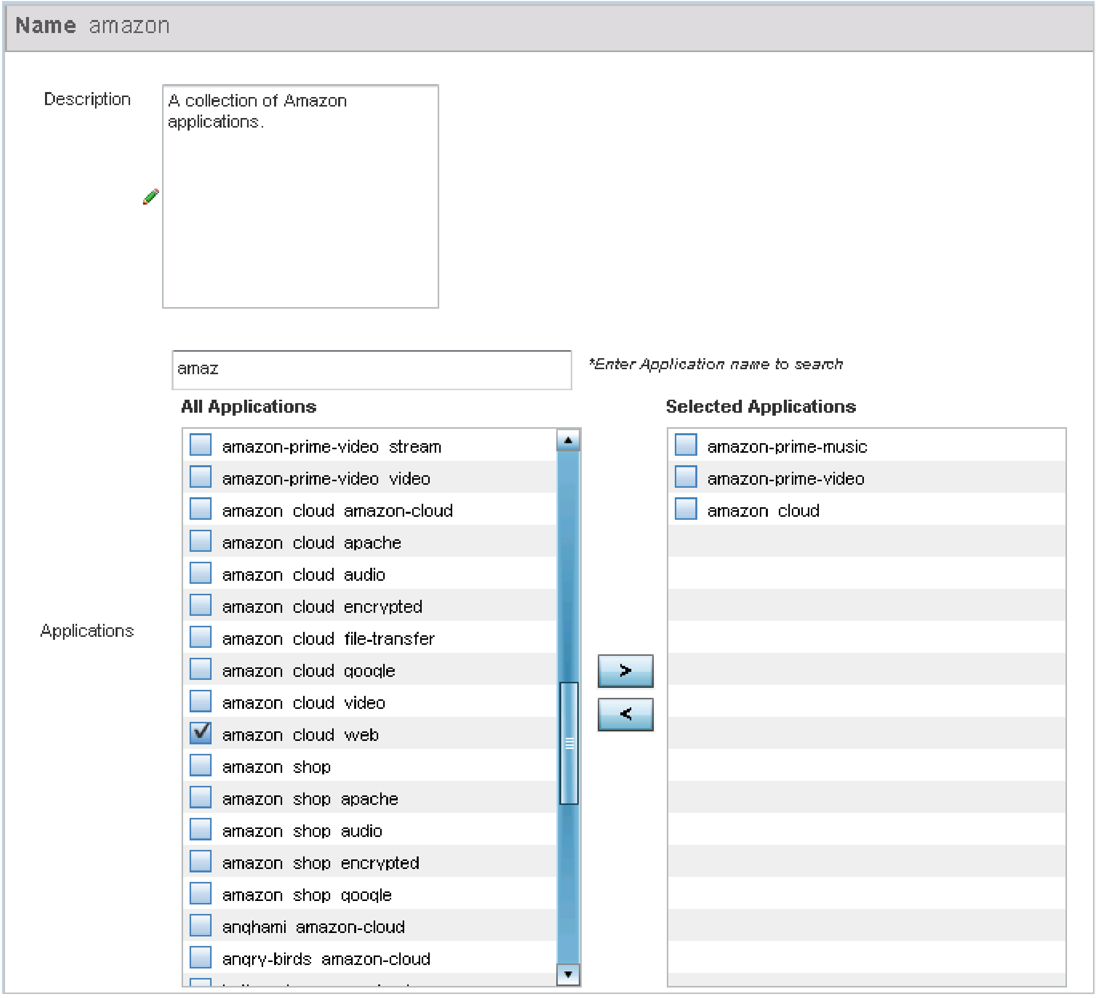


Name	Description
amazon	A collection of Amazon applications.

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.



Name amazon

Description: A collection of Amazon applications.

amaz

*Enter Application name to search

Applications

All Applications

- ☐ amazon-prime-video stream
- ☐ amazon-prime-video video
- ☐ amazon cloud amazon-cloud
- ☐ amazon cloud apache
- ☐ amazon cloud audio
- ☐ amazon cloud encrypted
- ☐ amazon cloud file-transfer
- ☐ amazon cloud google
- ☐ amazon cloud video
- ☑ amazon cloud web
- ☐ amazon shop
- ☐ amazon shop apache
- ☐ amazon shop audio
- ☐ amazon shop encrypted
- ☐ amazon shop google
- ☐ anghami amazon-cloud
- ☐ angry-birds amazon-cloud

Selected Applications

- ☐ amazon-prime-music
- ☐ amazon-prime-video
- ☐ amazon cloud

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.

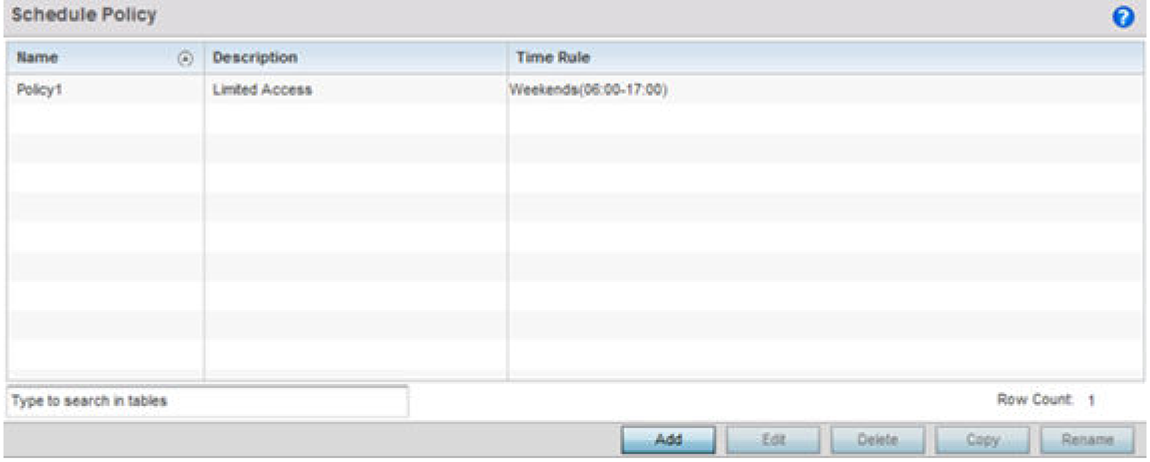
7 Select the applications to be included in the application group and move to the **Selected Applications** list.

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**.



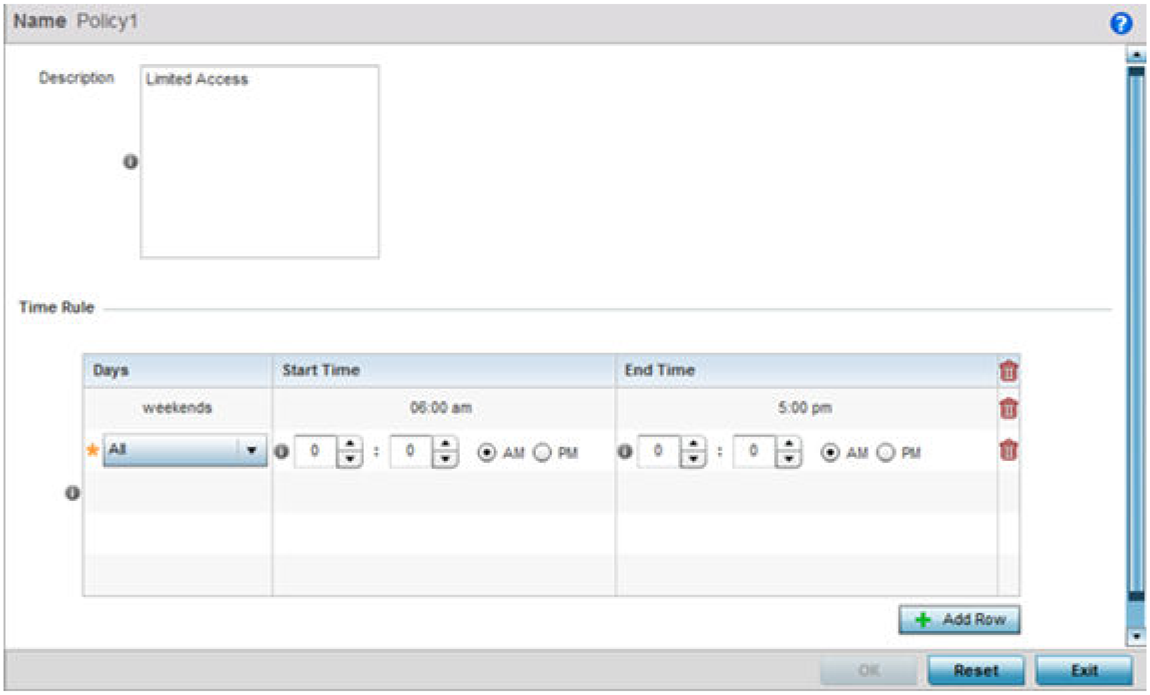
Schedule Policy

Name	Description	Time Rule
Policy1	Limited Access	Weekends(06:00-17:00)

Type to search in tables

Row Count: 1

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.



Name Policy1

Description: Limited Access

Time Rule

Days	Start Time	End Time
weekends	06:00 am	5:00 pm
All	0 : 0 ● AM ○ PM	0 : 0 ● AM ○ PM

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.

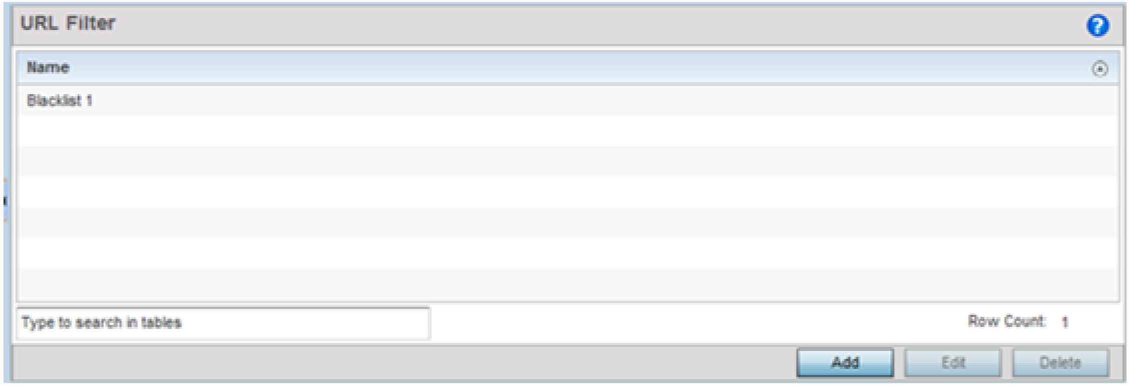
6 Select **OK** to save the updates to the schedule policy time rule configuration. Select **Reset** to revert to the last saved configuration.

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:

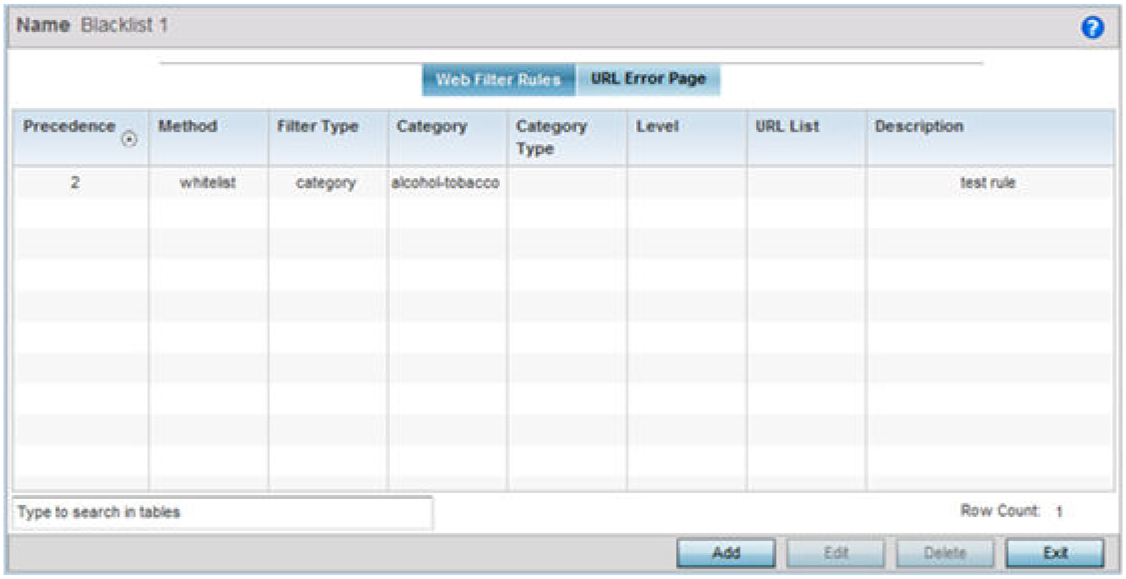
1 Select **Configuration** → **Network** → **URL Filter**.



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.



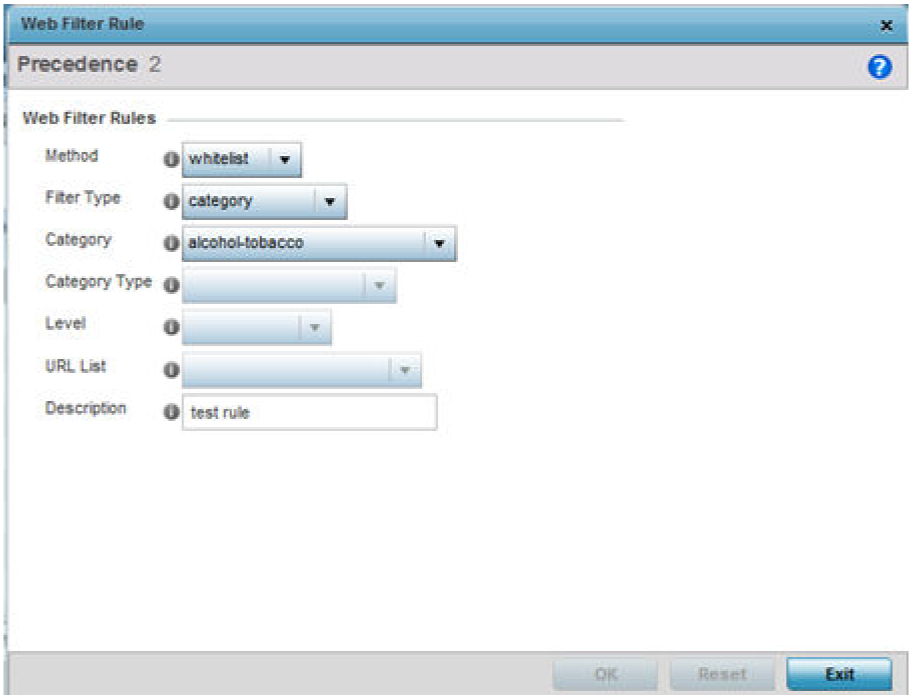
Name Blacklist 1

Precedence	Method	Filter Type	Category	Category Type	Level	URL List	Description
2	whitelist	category	alcohol-tobacco				test rule

Type to search in tables

Row Count: 1

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.



Precedence 2

Web Filter Rules

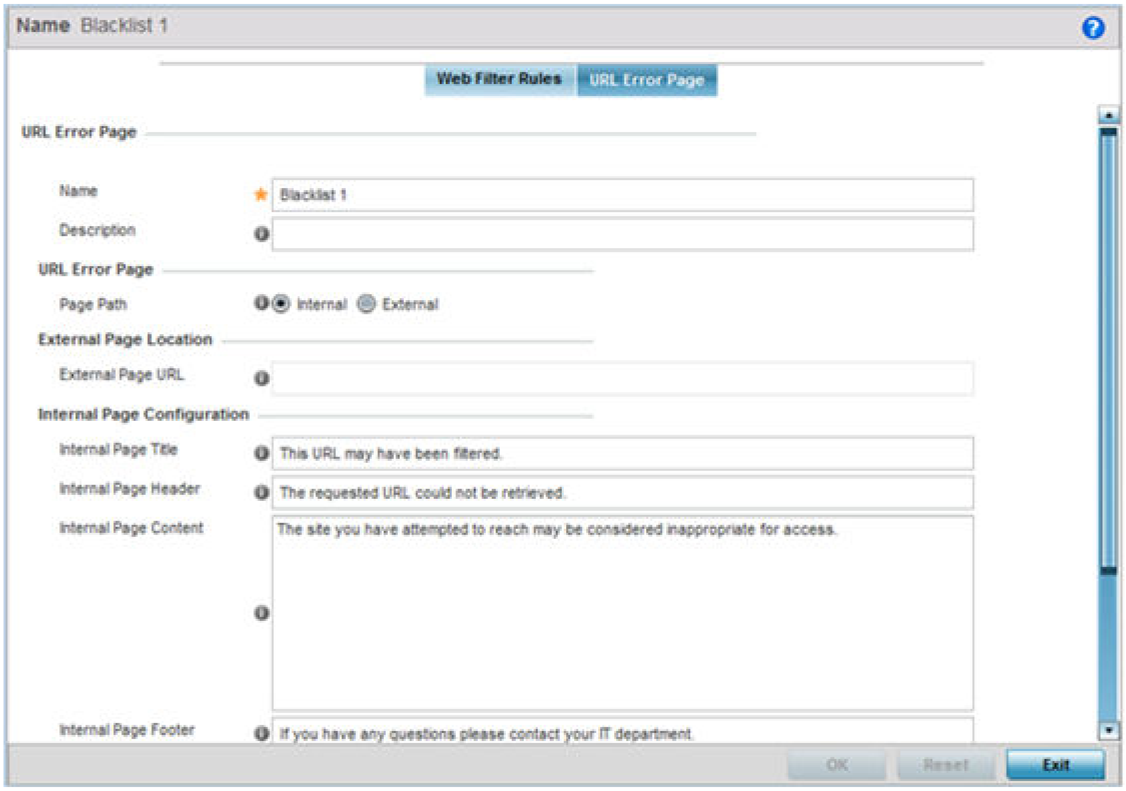
Method	whitelist
Filter Type	category
Category	alcohol-tobacco
Category Type	
Level	
URL List	
Description	test rule

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.



Name Blacklist 1

Name * Blacklist 1

Description

Page Path ● Internal ○ External

External Page URL

Internal Page Title: This URL may have been filtered.

Internal Page Header: The requested URL could not be retrieved.

Internal Page Content: The site you have attempted to reach may be considered inappropriate for access.

Internal Page Footer: If you have any questions please contact your IT department.

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).

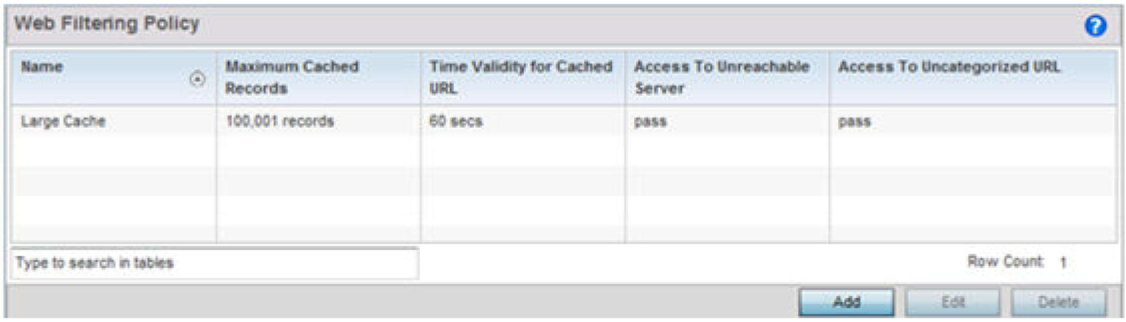
Internal Page Footer	Either enter a 255 character maximum footer for the bottom of the URL blocking page or use the existing default text (If you have any questions contact your IT department).
Internal Page Org Name	Enter a 255 character maximum organizational name responsible for the URL blocking page. 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**.

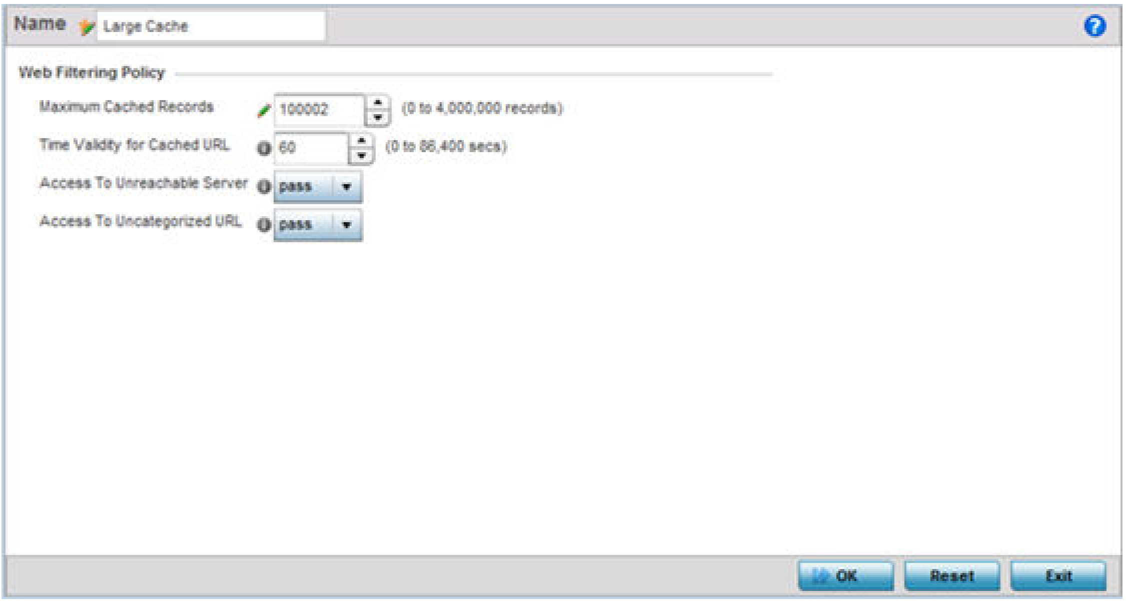


Web Filtering Policy

Name	Maximum Cached Records	Time Validity for Cached URL	Access To Unreachable Server	Access To Uncategorized URL
Large Cache	100,001 records	60 secs	pass	pass

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.



Name Large Cache

Web Filtering Policy

Maximum Cached Records 100002 (0 to 4,000,000 records)

Time Validity for Cached URL 60 (0 to 86,400 secs)

Access To Unreachable Server pass

Access To Uncategorized URL pass

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.

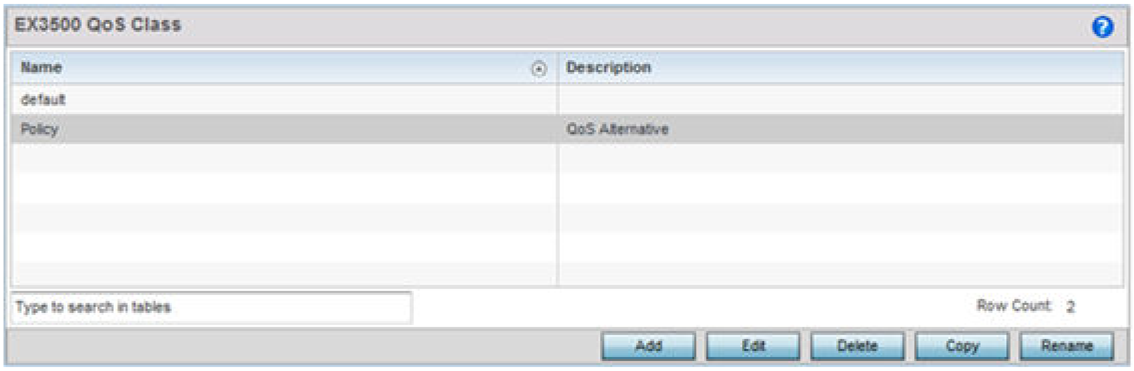
5 Select **OK** to save the changes to the Web filter policy. Select **Exit** to close the screen without saving the updates.

Configuring EX3500 QoS Class

An EX3500 switch can have its own QoS class policy applied as specific interoperability requirements dictate between an EX3500 switch and its connected devices. The QoS class configuration specifies permitted and excluded MAC and IP addresses and the precedence upon which filter rules are applied to EX3500 switch traffic.

To review existing EX3500 QoS policies and assess whether new ones require creation, modification or deletion:

1 Select **Configuration** → **Network** → **EX3500 QoS Class**.

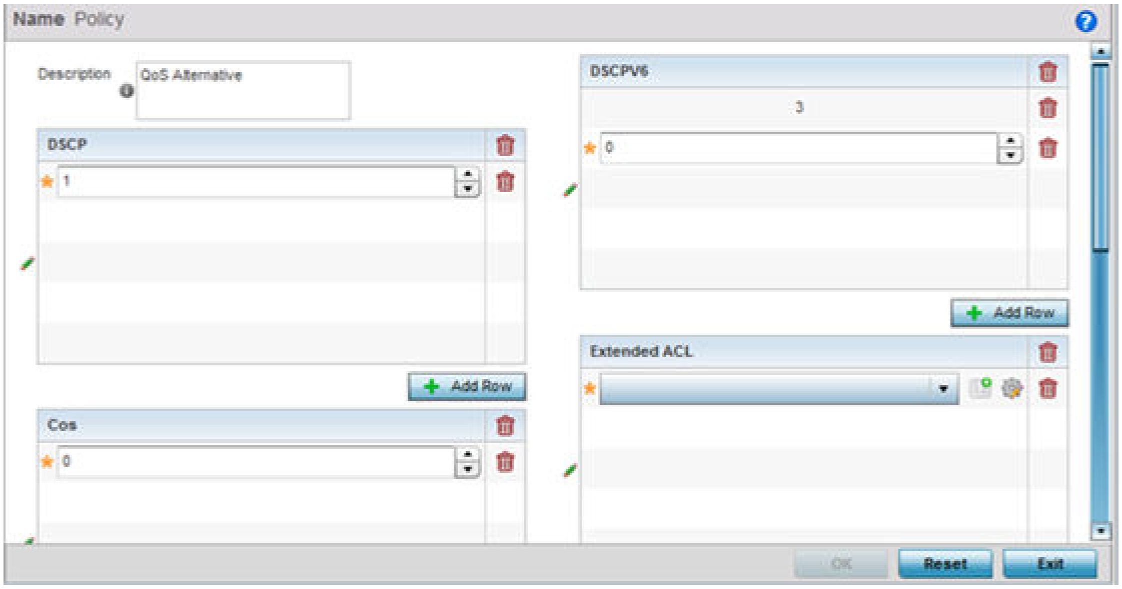


Name	Description
default	
Policy	QoS Alternative

Type to search in tables

Row Count: 2

2 Select **Add** to create a new EX3500 QoS policy, or select an existing policy and **Edit** to modify its attributes. Obsolete policies can be selected and **Deleted** as needed. **Copy** a policy to duplicate an existing QoS policy or **Rename** them as needed.



Name Policy

Description: QoS Alternative

DSCP: 1

Cos: 0

DSCPV6: 3, 0

Extended ACL

3 If creating a EX3500 QoS policy, enter a 64 character maximum Description to help differentiate this policy's EX3500 traffic prioritization scheme.

4 Refer to the **DSCP** field to set the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The range is 0 to 63 like DSCPv6.

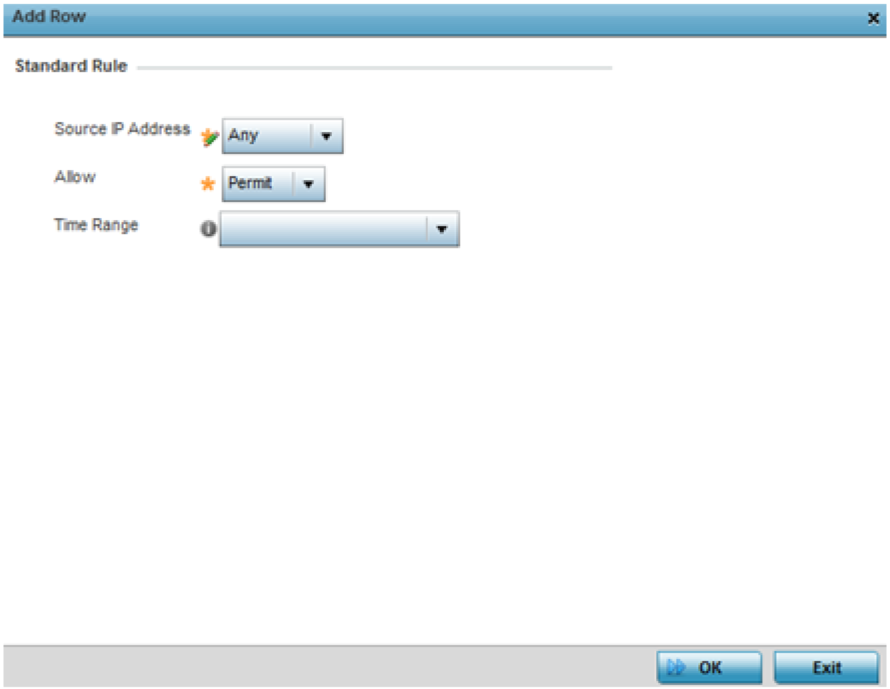
The screen maps the 6-bit Differentiated Service Code Point (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies 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 device models.

5 Use the **Cos** field to Assign a 802.1p priority (0 - 7) as a 3-bit IP precedence value of the IP header used to set the user priority. The valid values for this field are 0 – Best Effort, 1 – Background, 2 – Spare, 3 – Excellent Effort, 4 – Controlled Load, 5 – Video, 6 – Voice, 7 – Network Control.

6 Optionally apply **MAC ACL** rules to EX3500 packet traffic. Use the drop-down menu to select an existing MAC ACL, select the **Create** icon to add a new MAC ACL rule, or select an existing MAC ACL and the **Edit** icon to modify its configuration. For information on creating MAC ACLs, refer to Configuring MAC Firewall Rules on page 10-15.

Administrators can filter Layer 2 EX3500 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.

7 Optionally apply IP based **Standard ACL** rules to EX3500 packet traffic. A standard ACL for an EX3500 is a policy-based ACL that either prevents or allows specific clients from using the device. Select the **Create** icon to add a new ACL rule, or select an existing ACL and the **Edit** icon to modify its configuration. If creating a new standard ACL, provide a name up to 32 characters to help differentiate this rule from others with similar configurations. Select **+ Add Row**. For more information on creating a standard ACL, see EX3500 ACL Standard on page 799.



Source IP Address: Any
Allow: Permit
Time Range:

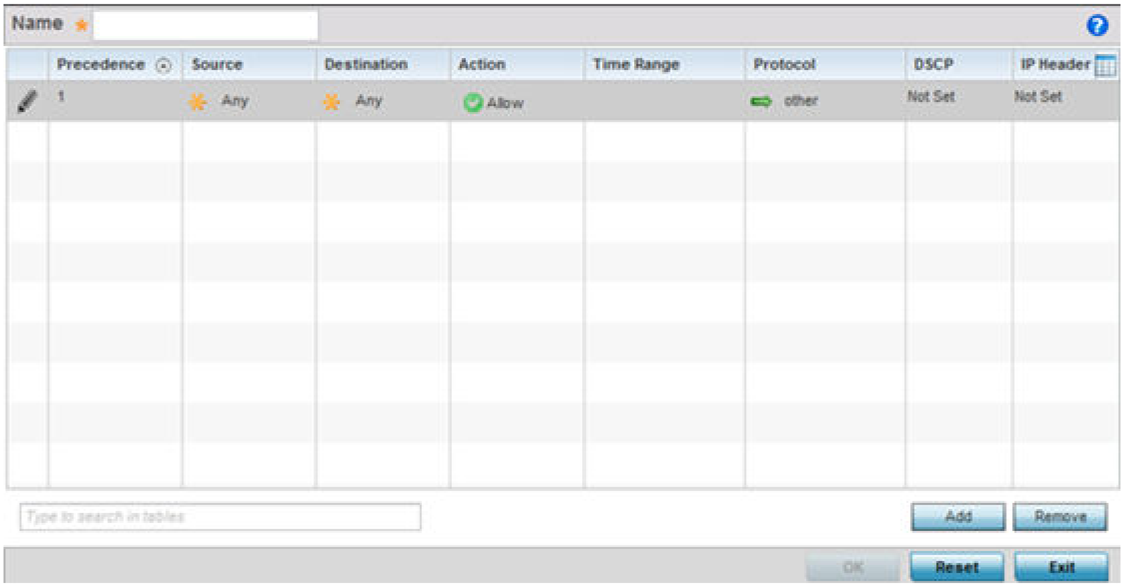
8 Set the following standard ACL attributes:

Source IP Address	Set whether the permit or deny rules assigned to this ACL are applied to a Host IP address, Network IP address and mask or Any address.
Allow	Set the Permit or Deny action on IP packet traffic with the EX3500 switch. The default is Permit.
Time Range	Defines the period when the permit or deny are applied to EX3500 IP traffic.

9 Refer to the **DSCPV6** field and select **+ Add Row** to specify a DSCPV6 value from 0 - 63. DSCPv6 specifies the Differentiated Services Code Point version 6 of a classifier assigned to an interface. Use DSCPv6 for IPv6 multicast traffic support.

10 Refer to the **Extended ACL** field and either select an existing extended IP ACL from the drop-down menu, add a new extended IP ACL by selecting the **Create** icon, or modify an existing one by

selecting the **Edit** icon. For more information on extended IP ACLs, refer to EX3500 ACL Extended on page 10-31.



An extended ACL is comprised of ACEs *(access control entries)*. Each ACE specifies a source and destination for matching and filtering traffic to the EX3500 switch.

Name	If creating a new extended ACL, provide a 32 character maximum name to this extended ACL to differentiate its EX3500 traffic filtering configuration.
Precedence	Specify or modify a precedence for this IP policy between 1-128. 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.
Source	Determine whether filtered packet source for this IP firewall rule do not require any classification (any), are set as a numeric IP address (host) or apply to any.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (any), are set as a numeric IP address (host) or apply to any.
Action	Every 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: • Deny - Instructs the ACL to restrict a packet from proceeding to its destination when filter conditions are matched. • Allow - Instructs the ACL to allow a packet to proceed to its destination when filter conditions are matched.
Time Range	Lists time range when each listed ACL is enabled. An EX3500 Time Range is a set of configurations consisting of periodic and absolute time ranges. Periodic ranges can be configured to reoccur based on periodicity such as daily, weekly, weekends, weekdays and on specific week day such as Sunday. Absolute time ranges can be configured to a range of days during a particular period. Absolute time ranges do not reoccur. For more information, see EX3500 Time Range on page 830.

Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp, udp or other. Select other if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port	Specify a source port for the TCP or UDP protocols. The source specifies the IP address or FQDN from which the packet is sent.The source port is not displayed by default and must be selected from the upper-right hand side of the screen.
Destination Port	Specify a destination port for the TCP or UDP protocols. The destination specifies the IP address or FQDN to which the packet is being sent. The destination port is not displayed by default and must be selected from the upper-right hand side of the screen.
DSCP	Select this option to specify a DSCP value from 0 - 63. DSCP specifies the Differentiated Services Code Point version 6 of a classifier assigned to an interface.
IP Header	Sets the IP precedence level from 0-7.

11 Refer to the **Precedence** field and select **+ Add Row** to assign a precedence (priority) to this EX3500 QoS policy. Rules are applied in order from 0 - 7.

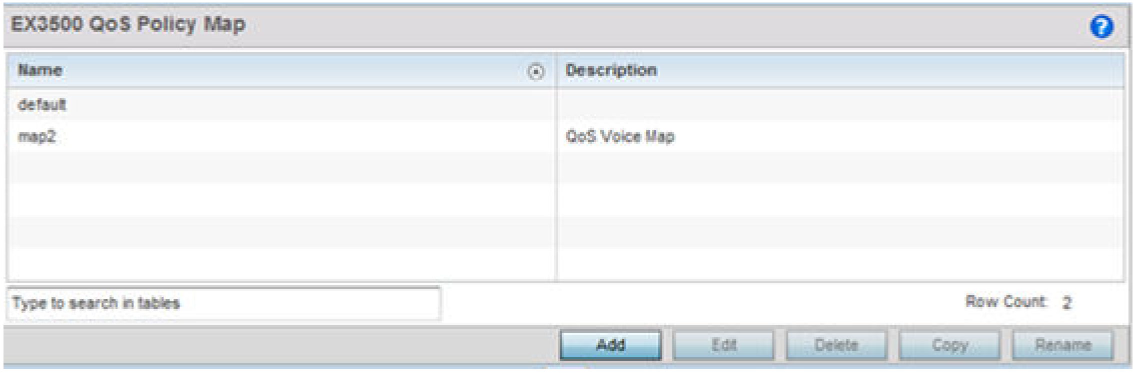
12 Optionally refine the virtual interface (**VLAN**) to which the EX3500 QoS policy is applied by selecting a VLAN from 1 - 4094.

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

Configuring EX3500 QoS Policy Map

An EX3500 switch can have its own WiNG defined policy map that can be attached to an interface to specify a QoS service policy. Use a QoS policy map to assign priority to mission critical EX3500 switch data traffic, prevent EX3500 switch bandwidth congestion and prevent packet drops. To review existing EX3500 QoS policy map configurations and assess whether new ones require creation, modification or deletion:

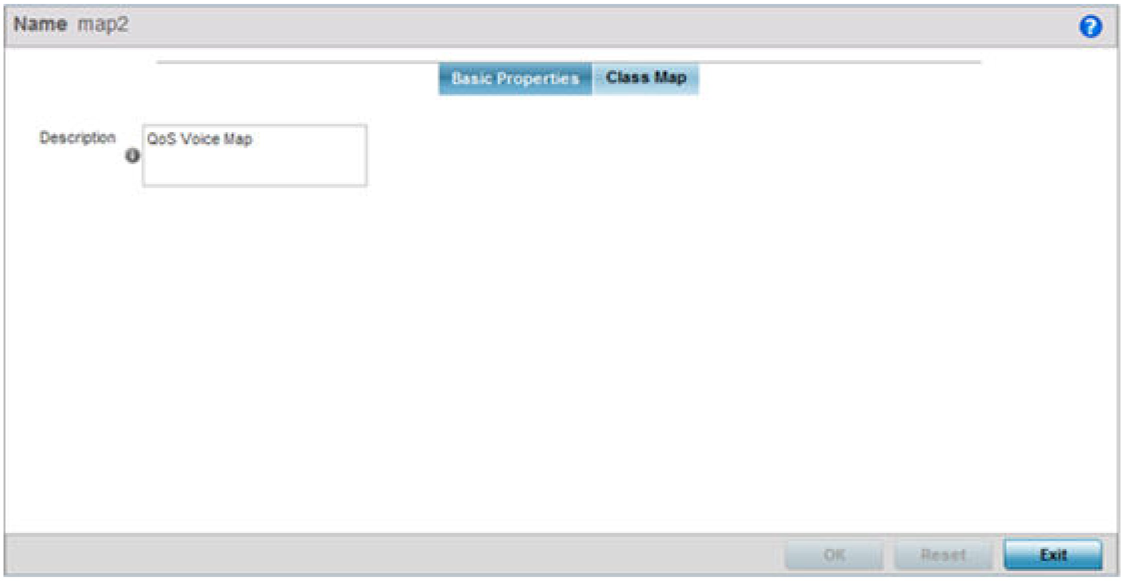
1 Select **Configuration** → **Network** → **EX3500 QoS Policy Map**.



EX3500 QoS Policy Map

Name	Description
default	
map2	QoS Voice Map

2 Select **Add** to create a new EX3500 QoS policy map, or select an existing policy and **Edit** to modify its attributes. Obsolete policy maps can be selected and **Deleted** as needed. **Copy** to duplicate an existing policy map or **Rename** them as needed.



Description: QoS Voice Map

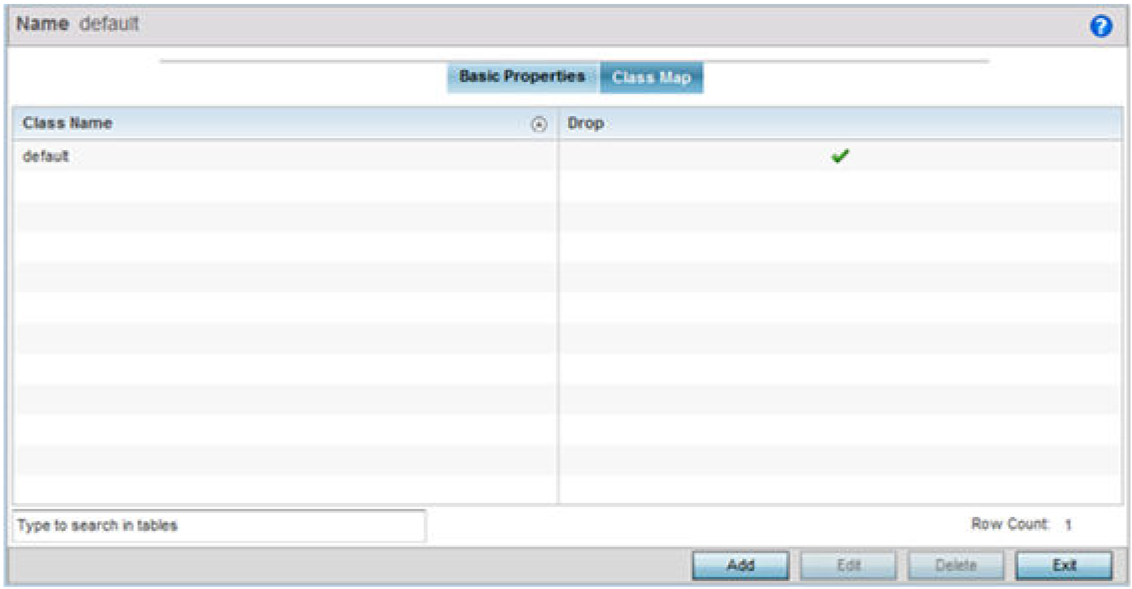
3 If adding a new EX3500 QoS policy map, enter a 32 character maximum **Name** to help differentiate this policy from others with similar attributes.

4 Enter a 64 character maximum **Description** to help differentiate this policy's EX3500 traffic prioritization scheme.

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

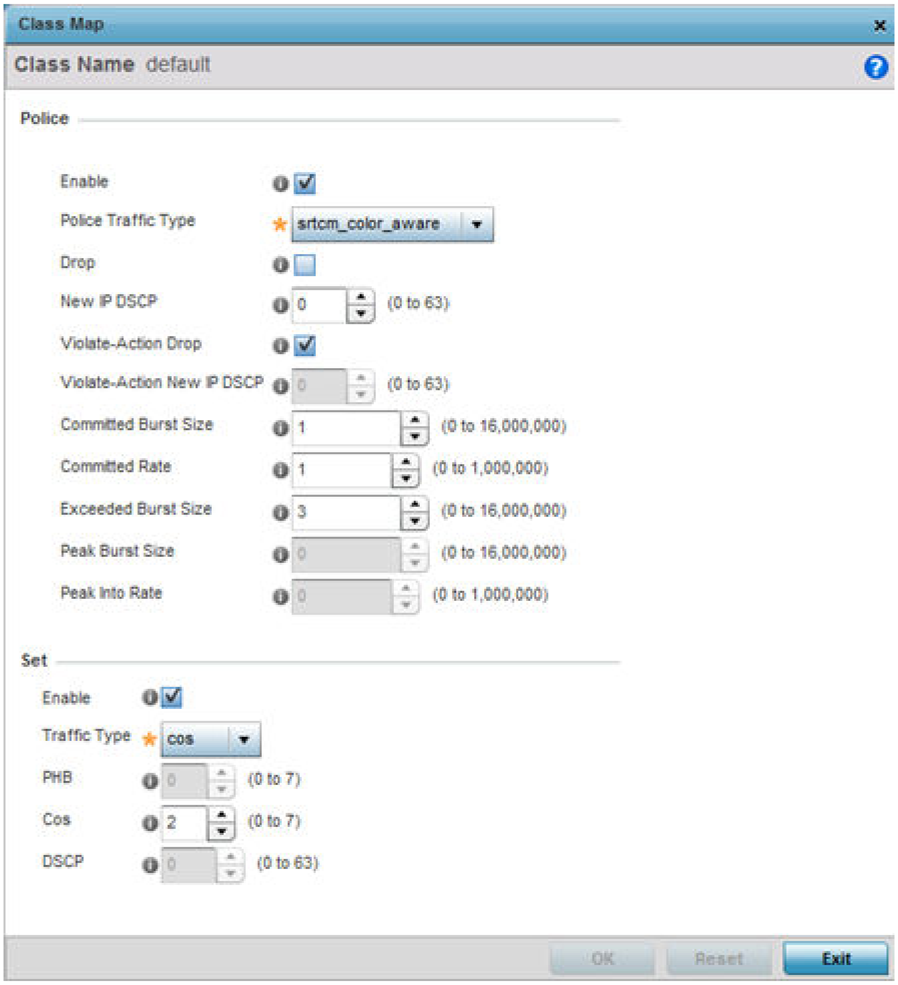
6 Select the **Class Map** tab.

Existing class map configurations display along with their drop designations defining whether packets will be dropped if exceeding the actions set for this class map configuration.



Class Name	Drop
default	✓

7 Select **Add** to create a new EX3500 QoS class map, or select an existing class name and **Edit** to modify its attributes. Obsolete class maps can be selected and **Deleted** as needed.



Class Map

Class Name default

Police

Enable ☑

Police Traffic Type srtcm_color_aware

Drop ☐

New IP DSCP 0 (0 to 63)

Violate-Action Drop ☑

Violate-Action New IP DSCP 0 (0 to 63)

Committed Burst Size 1 (0 to 16,000,000)

Committed Rate 1 (0 to 1,000,000)

Exceeded Burst Size 3 (0 to 16,000,000)

Peak Burst Size 0 (0 to 16,000,000)

Peak Info Rate 0 (0 to 1,000,000)

Set

Enable ☑

Traffic Type cos

PHB 0 (0 to 7)

Cos 2 (0 to 7)

DSCP 0 (0 to 63)

8 Set the following class map **Police** actions to apply traffic restrictions and packet drop criteria to EX3500 switch data traffic:

Enable	Enable this option to apply traffic type classification restrictions and packet drop criteria to EX3500 switch data traffic. This option is dialed by default.
Police Traffic Type	Use the drop-down menu to specify the EX3500 switch traffic type to drop when the specified violation criteria is exceeded. A policing scheme can be applied before writing packets to the TX port by dropping or changing the color (green, yellow or red) of the packet in a static manner, depending on both the input and output colors of the packets. Options include flow, srtcm_color_aware, srtcm_color_blind, trtcm_color_aware and trtcm_color_blind.
Drop	Select this option to drop EX3500 switch packets when the violation action criteria has been exceeded. This option is not available when flow is selected as Police Action Type.
New IP DSCP	Use the spinner control to set a DSCP value (from 0 - 63) as required by an exceeded action criteria. DSCP is the Differentiated Services Code Point field in an IP header for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. This option is not available when flow is selected as the Police Action Type or when Drop is enabled.

Violate-Action Drop	Select this option to drop packets when the specified traffic type classification restrictions and packet drop criteria are exceeded. When enabled (default setting), the Violate Action New IP DSCP setting is disabled.
Violate-Action New IP DSCP	If the Violate-Action Drop option is disabled, set a DSCP value (from 0 - 63) as required by an exceeded action criteria.
Committed Burst Size	Set a committed (maximum) burst size between 0 - 16,000,000. The smaller the burst, the less likely received EX3500 switch packets result in data traffic congestion.
Committed Rate	Set the CIR *(committed information rate)* from 0 - 1,000,000 for EX3500 switch data traffic. The CIR is a bandwidth (expressed in bits per second) allocated to the connection with the EX3500 switch. This form of rate limiting reduces the maximum rate sent or received, and prevents any single EX3500 switch from overwhelming the WiNG managed network.
Exceeded Burst Size	When srtcm_color_aware or srtcm_color_blind are selected as the Police Traffic Type, set an excess burst size (from 0 - 16,000,000 bytes). The excess busrt size allows for periods of bursting traffic exceeding both the CIR and committed burst size.
Peak Burst Size	When trtcm_color_aware or trtcm_color_blind are selected as the Police Traffic Type, set a Peak Burst Size (from 0 - 16,000,000 bytes). The Peak Burst Size defines the maximum number of bytes of unused peak bandwidth capacity that can be accumulated. The accumulated bandwidth allows for periods of bursting traffic exceeding the Peak Info Rate and Committed Burst Size.
Peak Info Rate	When trtcm_color_aware or trtcm_color_blind are selected as the Police Traffic Type, set a Peak Info Rate (from 0 - 1,000,000 kilobytes per second). The Peak Info Rate is the maximum rate for traffic arriving or departing the interface under peak conditions. Traffic exceeding the committed information rate (CIR) and the committed burst size is metered to the Peak Info Rate.

9 Refer to the **Set** field to define the EX3500’s traffic type and set its behavior.

Enable	Select enable to refine the EX3500’s traffic type to either PHB, COS or DSCP.
Traffice Type	Use the drop-down menu to specify the EX3500 switch traffic type. Options include phb, cos and DSCP. Once an option is selected, refine that traffic type’s behavior.
PHB	When PHB is selected as the Traffic Type, set the per-hop behavior value (from 1 - 7) applied to matching packets. The PHB defines the policy and priority applied to a packet when traversing a hop. PHBs are created (one for each combination of the top 3 bits) as bbb000 to match precedence behaviors and leaves other DSCP values open, where each b may take the value zero or 1.
Cos	When Cos is selected as the Traffic Type, assign a 802.1p priority (0 - 7) as a 3-bit IP precedence value of the IP header used to set the EX3500 switch user priority. The valid values for this field are 0 – Best Effort, 1 – Background, 2 – Spare, 3 – Excellent Effort, 4 – Controlled Load, 5 – Video, 6 – Voice, 7 – Network Control.
DSCP	When DSCP is selected as the Traffic Type, set a DSCP value (from 0 - 63). DSCP is the Differentiated Services Code Point field in an IP header for EX3500 switch packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field.

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

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.

8 Manage Profiles

General Profile Configuration
Profile Cluster Configuration (Controllers Only)
Profile Adoption Configuration (Access Points Only)
Profile Adoption Configuration (Controllers Only)
Access Point Radio Power Overrides (AP7161 Only)
Profile 802.1x Configuration
Profile Interface Configuration
Profile Network Configuration
Profile Security Configuration
VRRP Configuration
Critical Resources Configuration
Profile Services Configuration
Profile Management Configuration
Profile Mesh Point Configuration
Environmental Sensor Configuration (AP8132 Only)
Advanced Profile Configuration

Profiles enable administrators to assign a common set of configuration parameters and policies to RFS controllers, NX series service platforms and access points. Profiles can be used to assign common or *unique* network, wireless and security parameters to controllers, service platforms and 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. Controllers, service platforms and access points support both default and user defined profiles implementing new features or updating existing parameters. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Profiles assign configuration parameters, applicable policies and WLANs to one or more controllers and access points, thus allowing smart administration across large wireless network segments. However, individual devices can still be assigned unique configuration parameters that follow the flat configuration model supported in previous software releases. As individual device updates are made, these device no longer share the profile based configuration they originally supported. Changes made to a profile are automatically inherited by all assigned devices, but not those devices who have had their configuration customized. These devices require careful administration, as they no longer can be tracked and as profile members. Their customized configurations overwrite their profile configurations until the profile can be re-applied to the device.

Each device is automatically assigned a default profile unless an AP Auto-Provisioning policy is defined that specifically assigns an access point to a user defined profile. A default profile for each supported model is automatically added to a device's configuration file when the device is provisioned. Default profiles can also be manually added prior to discovery when needed. Default profiles are ideal for single site deployments where controllers, service platforms and access points share a common configuration.

User defined profiles are manually created for each supported device model. User defined profiles can be manually assigned or automatically assigned to access points using an AP Auto-Provisioning policy. AP Adoption policies provide the means to easily assign profiles to access points based on model, serial number, VLAN ID, DHCP option, IP address (subnet) and MAC address.

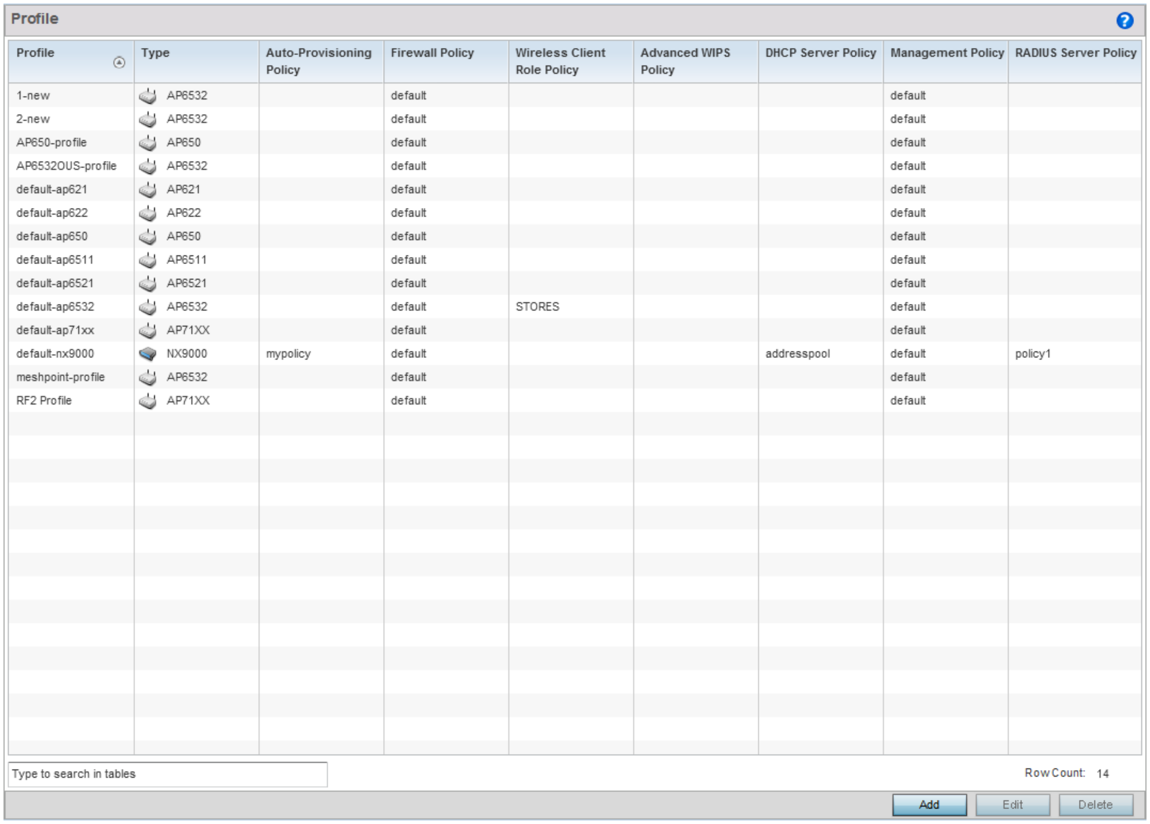
User defined profiles should be utilized in larger deployments when groups of devices (on different floors, buildings or sites) share a common configuration.

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

Review existing profiles to determine whether a new profile requires creation, or an existing profile requires edit or deletion.

To review the existing profiles:

1 Go to **Configuration** → **Profiles** → **Manage Profiles**. A list of default and user-created profiles is displayed.



Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	Advanced WIPS Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
1-new	AP6532		default				default	
2-new	AP6532		default				default	
AP650-profile	AP650		default				default	
AP6532OUS-profile	AP6532		default				default	
default-ap621	AP621		default				default	
default-ap622	AP622		default				default	
default-ap650	AP650		default				default	
default-ap6511	AP6511		default				default	
default-ap6521	AP6521		default				default	
default-ap6532	AP6532		default	STORES			default	
default-ap71xx	AP71XX		default				default	
default-nx9000	NX9000	mypolicy	default			addresspool	default	policy1
meshpoint-profile	AP6532		default				default	
RF2 Profile	AP71XX		default				default	

2 Review the following information on existing profiles:

Profile	Lists the user-assigned name defined for each profile when created. Profile names cannot be edited with a profiles configuration.
Type	Displays the device type (and subsequent device specific configuration) supported by each listed profile.

Auto-Provisioning Policy	Displays the Auto-Provisioning policy applied to this profile. At adoption, an AP solicits and receives multiple adoption responses. These adoption responses contain preference and loading policy information the AP uses to select the optimum controller or access point for adoption. By default, an Auto-Provisioning policy generally distributes AP adoption evenly amongst available adopters. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of this particular profile.
Firewall Policy	Displays an existing firewall policy, if any, assigned to each listed profile. Firewall policies can be assigned when creating or editing a profile.
Wireless Client Role Policy	Lists the name of the wireless client role policy currently applied to the listed device. The wireless client role policy contains the matching rules and IP and MAC Inbound and Outbound policies used to filter traffic to and from clients. This policy can be applied to controllers, service platforms or access points.
Advanced WIPS Policy	Lists the name of the Advanced WIPS Policy used with each listed profile to (among other things) block up to 100 client MAC address from connectivity.
DHCP Server Policy	Lists the name of the DHCP Server Policy used with each listed profile. An internal DHCP server groups wireless clients based on defined user-class option values. 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.
Management Policy	Lists the name of Management policies applied to each listed profile. A management policy is a mechanism to allow/deny management access for separate interfaces and protocols (*HTTP*, *HTTPS*, *Telnet*, *SSH* or *SNMP*). Management access can be enabled/disabled as required for each policy.
RADIUS Server Policy	Displays the name of the RADIUS Server policy applied to each listed profile. A RADIUS Server policy provides customized, profile specific, management of authentication data (usernames and passwords).

3 Select the **Add** button to create a new profile, **Edit** to revise a selected profile configuration or **Delete** to permanently remove a selected profile.

The following tasks comprise required profile configuration activities:

- General Profile Configuration on page 531
- Profile Cluster Configuration (Controllers Only) on page 533
- Profile Adoption Configuration (Access Points Only) on page 535
- Profile Adoption Configuration (Controllers Only) on page 537
- Access Point Radio Power Overrides (AP7161 Only) on page 539
- Profile 802.1x Configuration on page 540
- Profile Interface Configuration on page 541
- Profile Network Configuration on page 607
- Profile Security Configuration on page 676
- VRRP Configuration on page 712
- Critical Resources Configuration on page 716
- Profile Services Configuration on page 719
- Profile Management Configuration on page 723
- Profile Mesh Point Configuration on page 729
- Environmental Sensor Configuration (AP8132 Only) on page 736
- Advanced Profile Configuration on page 737

General Profile Configuration

Each profile requires a provisioning policy and clock synchronization settings as part of its general configuration. Each profile can have a unique provisioning policy and system time.

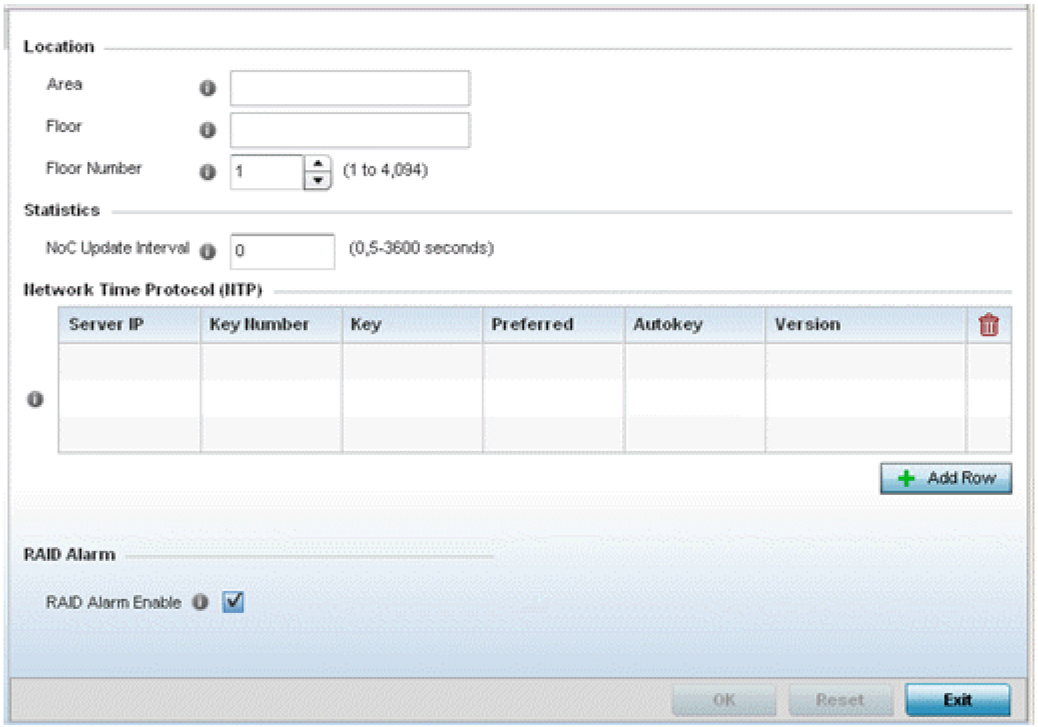
Controllers, service platforms and access points are automatically assigned a default profile unless an AP provisioning policy has been defined that specifically assigns access points to a user defined profile. During the general configuration process, a provisioning policy can be assigned to a specific profile or a new provisioning policy can be created and applied to the profile. Adoption is the process an AP uses to discover potential adopters (Controller APs of the same model, service platforms or controllers) in the network, pick the most desirable one, establish an association and obtain its configuration.

Network Time Protocol (NTP) manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms and access points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a RFS 4000 resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Additionally, if the profile is supporting an access point, the profile’s general configuration provides an option to disable the device’s LEDs.

To define a profile’s general configuration:

1. Select the **Configuration** → **Profiles** tab from the Web UI.
2. Select **Manage Profiles**. A list of device profiles displays in the left-hand UI. This list includes both default and user-defined profiles.
3. Select **Add** to create a new profile. To modify, delete, copy, rename an existing profile, select the profile from the list and click **Edit**, **Delete**, **Copy**, or **Rename** respectively. To replace an existing profile with another profile, select the profile and click **Replace**.
4. Select a device profile from the list. The selected profile's configuration menu is displayed, with the General option selected by default.



5 If creating a new profile, provide a `profile name` (up to 32 characters) within the **Profile** parameter field.

6 Use the **Type** drop-down menu to specify the device model for which the profile applies. Controllers, service platforms and access points can only utilize profile resources with other device's of the same model type.

7 Refer to the Location field to define the device's deployment details.

Area	Enter a 64 character maximum description for the selected device's physical deployment area. This area can be further refined by floor and floor number descriptions.
Floor	Enter a 32 character maximum description for the selected device's building floor placement. This area can be further refined by floor and floor number descriptions.
Floor Number	Use the spinner control to assign a numeric deployment floor number (from 1 - 4094) for this device. The default floor is 1.

8 Within the Statistics field, use the **NoC Update Interval** to set the statistics update interval (from 0, 5 - 3600 seconds) from the RF Domain manager to its adopting controller.

A value of 0 is allowable for an auto mode where the update interval is auto adjusted by the controller based on load information.

9 In the Network Time Protocol (NTP) table, select **+ Add Row** to define NTP server resource configurations. The NTP server is used to obtain system time. Set the following parameters:

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.

10 Refer to the RAID Alarm field to either enable or disable the chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring).

RAID controller drive arrays are available within NX 95XX and NX 96XX series service platforms only. However, they can be administrated on behalf of a NX 95XX and NX 96XX profile by a different model service platform or controller.

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

General Profile Configuration and Deployment Considerations

Before defining a general profile configuration for a RFS controller, NX series service platfrom or access point, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A default profile is applied automatically, and default AP profiles are applied to access points discovered and provisioned by controllers and service platfroms.
- Each user administrator configured profile requires a unique name.
- User defined profiles can be automatically assigned to access points using AP adoption policies.
- Controllers, service platforms and access points are automatically assigned a default profile based on the hardware type selected when the profile is initially created.

Profile Cluster Configuration (Controllers Only)

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed nodes (controllers, service platforms, wireless devices etc.). Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. A RFS controller or NX service platform not only provides a centralized management solution, it provides a centralized management profile that can be shared by any single controller or service platform cluster member. This eliminates dedicating a management entity to manage all cluster members and eliminates a single point of failure.

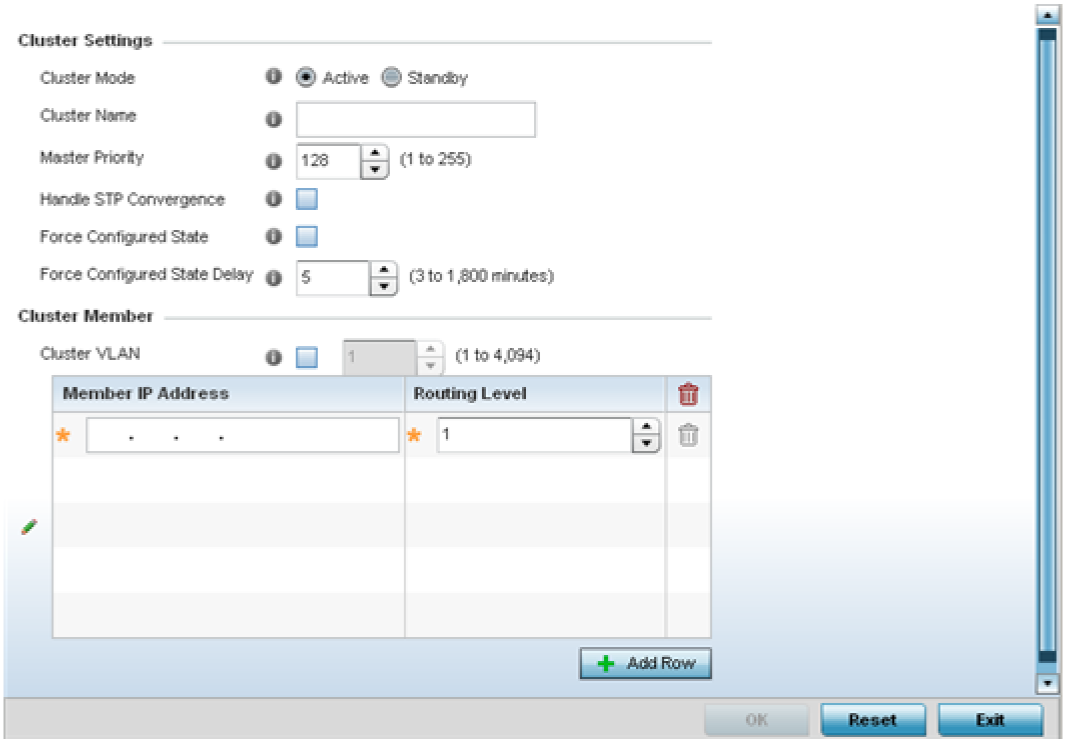
A cluster (or redundancy group) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the cluster, members discover and establish connections to other members and provide wireless network self-healing support in the event of member's failure.

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members join and exit the cluster.

To define a cluster configuration for use with a profile:

1. Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.
2. Select **Cluster.**

   A screen displays where the profile's cluster and AP load balancing configuration can bet set.



3. Define the following **Cluster Settings** parameters to set this profile's cluster mode and deployment settings:

Cluster Mode	A member can be in either an **`Active`** or **`Standby`** mode. All active member can adopt access points. Standby members only adopt access points when an active member has failed or sees an access point not adopted by a controller or service platform. The default cluster mode is *Active* and enabled for use with the profile.
Cluster Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
Master Priority	Set a priority value from 1 - 255, with the higher value given higher priority. This configuration is the device's priority to become the cluster master. In a cluster environment, one device from the cluster is elected as the cluster master. The master priority setting is the device's priority to become cluster master. The active primary controller has the higher master priority. The default value is 128.

Handle STP Convergence	Select the check box to enable *Spanning Tree Protocol* (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 cluster members. The spanning tree protocol disables redundant connections and uses the least costly path to maintain a connection between any two controllers or service platforms in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup. The default setting is disabled.
Force Configured State	Select the check box to enable this cluster member to take over for an active member if it were to fail. A standby controller or service platform takes over APs adopted by the failed member. If the failed cluster member were to come available again, the active member starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby member releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active member goes down and comes up during the Auto Revert Delay interval. The default value is disabled.
Force Configured State Delay	Specify a delay interval in either **`Seconds`** (1 - 1,800) or **`Minutes`** (1 - 30). This is the interval a standby cluster member waits before releasing adopted APs and goes back to a monitoring mode when a controller becomes active again after a failure. The default interval is 5 seconds.

4 Within the Cluster Member field, select the **Cluster VLAN** checkbox to enable a spinner control to designate the VLAN where cluster members are reachable. Specify a VLAN in the range of 1 - 4094.

Specify the IP Addresses of the VLAN's cluster members using the IP Address table.

5 Select **OK** to save the changes made to the profile's cluster configuration. Select Reset to revert to the last saved configuration.

Controller Cluster Profile Configuration and Deployment Considerations

Before defining a profile cluster configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A cluster member cannot adopt more APs than its hardware capacity and license provisions allow. This is important when the number of pooled AP and AAP licenses exceeds the aggregated AP and AAP capacity available after a cluster member has failed. A cluster supported profile should be designed to ensure adequate AP and AAP capacity exists to address failure scenarios involving both APs and AAPs.
- When clustering is enabled for a profile and a failure occurs amongst one of the cluster members, AP and AAP licenses are persistent in the cluster even during reboots or power outages. If a cluster member failure were to occur, clustering should remain enabled on all remaining cluster members or the pooled member licenses will be deprecated.

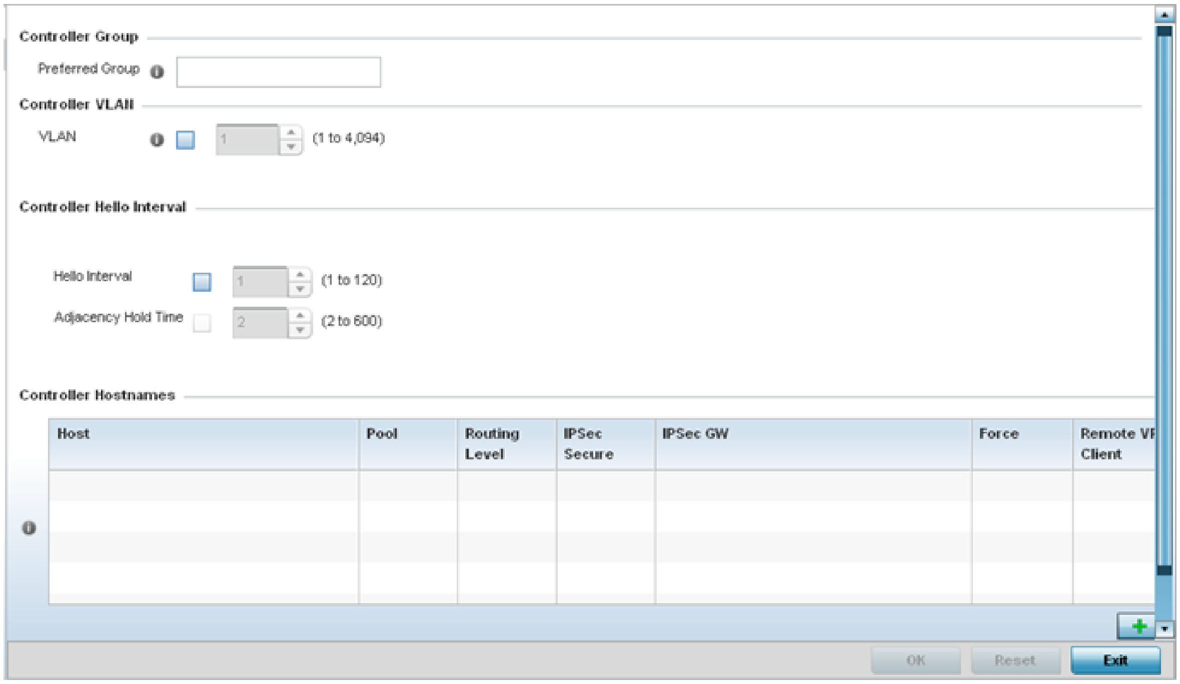
Profile Adoption Configuration (Access Points Only)

Adoption is the process an access point uses to discover available controllers, pick the most desirable controller, establish a controller association and optionally obtain an image upgrade and configuration. Adoption is 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 the adoption requirements of a device and their assigned profile.

To define an access point's adoption configuration:

1 Select the **Configuration** tab from the Web UI.
2 Select **Profiles** from the Configuration tab.
3 Select **Manage Profiles** from the **Configuration** → **Profiles** menu.
4 Select **Adoption**.



5 Within the Controller Group field, use the **Preferred Group** item to set an optimal group for the access point's adoption. The name of the preferred group cannot exceed 64 characters.
6 Select the check box to define a **VLAN** the access point's associating controller or service platform is reachable on.

VLANs 0 and 4,094 are reserved and cannot be used by a controller or service platform VLAN.

7 Set the following **Controller Hello Interval** parameters:

Hello Interval	Define an interval (from 1 - 120 seconds) between hello keep alive messages exchanged with the adopting device. These messages serve as a connection validation mechanism to ensure the availability of the adopting resource.
Adjacency Hold Time	Set the time (from 2 - 600 seconds) after the last hello packet after which the connection between the controller and access point is defined as lost and their connection is re-established.

8 Enter **Controller Hostnames** as needed to define resources for access point adoption.

9 Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as access point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) IP Address or a Hostname. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
Force	Enable this setting to create a forced link between an access point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

10 Click **OK** to save the changes to the access point profile adoption configuration. Select **Reset** to revert to the last saved configuration.

Profile Adoption Configuration (Controllers Only)

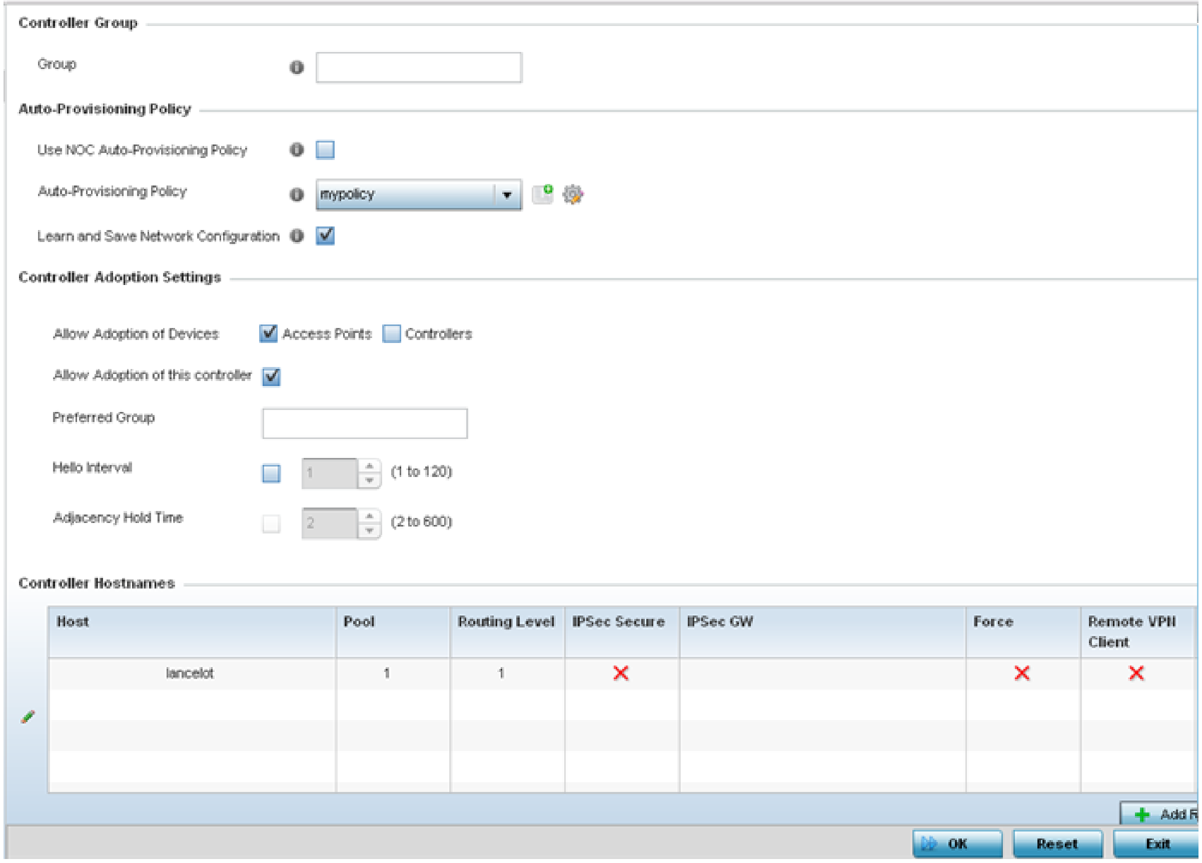
Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the requesting device. Adoption settings are configurable and supported within a profile and applied to other access points 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 the adoption requirements of a device and their assigned profile.

To define a controller or service platform's adoption configuration:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Select **Adoption**.



Controller Group

Group:

Auto-Provisioning Policy

Use NOC Auto-Provisioning Policy ☐

Auto-Provisioning Policy: mypolicy

Learn and Save Network Configuration ☑

Controller Adoption Settings

Allow Adoption of Devices ☑ Access Points ☐ Controllers

Allow Adoption of this controller ☑

Preferred Group:

Hello Interval ☐ 1 (1 to 120)

Adjacency Hold Time ☐ 2 (2 to 600)

Controller Hostnames

Host	Pool	Routing Level	IPSec Secure	IPSec GW	Force	Remote VPN Client
lancelot	1	1	✗		✗	✗

3 Within the Controller Group field, use the **Group** item to set provide the controller group this controller or service platform belongs to. A preferred group can also be selected for the adoption of this controller or service platform. The name of the preferred group cannot exceed 64 characters.

4 Set the following **Auto Provision Policy** parameters:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC's auto provisioning policy instead of the policy local to the controller or service platform. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default.
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.

5 Set the following **Controller Adoption Settings** settings:

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.

6 Enter **Controller Hostnames** as needed to define resources for access point adoption.

7 Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as access point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) IP Address or a Hostname. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
Force	Enable this setting to create a forced link between an access point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

8 Refer to the AP300 Adoption settings:

Adopt List	Select this option to enable the controller or service platform adoption of an AP300 before it has been provisioned with its configuration. This setting is enabled by default.
Adopted List	If the Adopt List setting is disabled, add AP300 MAC addresses that the controller or service platform will optimally adopt.
Deny List	If the Adopt List setting is enabled, add AP300 MAC addresses that the controller or service platform will deny from adoption and configuration provisioning.

9 Click **OK** to save the changes to the controller or service platform profile adoption configuration. Click **Reset** to revert to the last saved configuration.

Access Point Radio Power Overrides (AP7161 Only)

This option is only available for AP 7161 access points.

Use the Power screen to set or override one of two power modes (3af or Auto) for a managed Access Point. 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 radio model and power configuration.

An Access Point uses a *complex programmable logic device* (CPLD). 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 Access Point's 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 hardware SKU and the number of radios.

If the Access Point's POE resource cannot provide sufficient power (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 the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.
2 Select Power.
3 Use the Power Mode drop-down menu to set or override the Power Mode Configuration on this AP.

Note
Single radio model Access Point's always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models.

When an Access Point is powered on for the first time, the system determines the power budget available to the Access Point. 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.

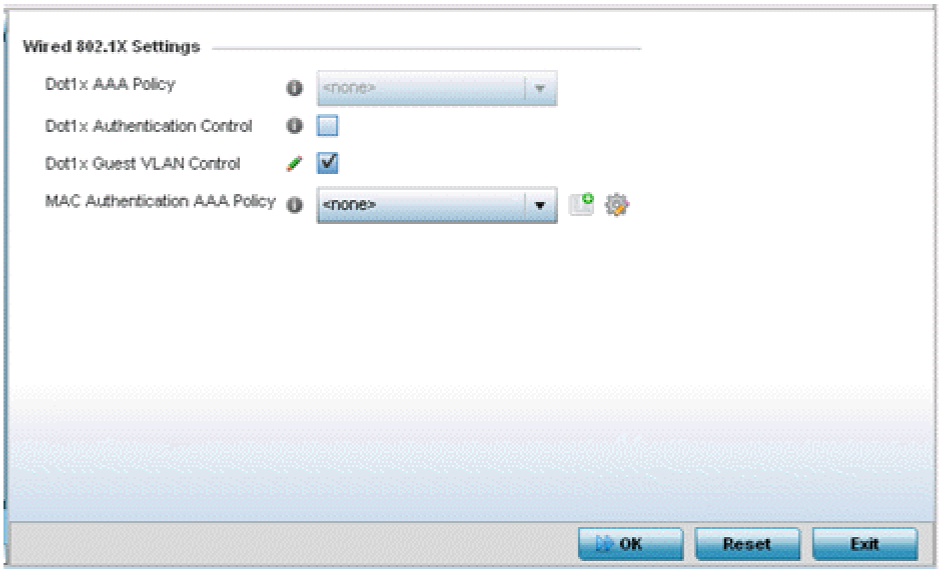
4 Set or override the Access Point radio's 802.3af Power Mode and the radio's 802.3at Power Mode.
5 Use the drop-down menu to define a mode of either *Range* or *Throughput*.
6 Select **Throughput** to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance.
7 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.
8 Click **OK** to save the changes and overrides made to the Access Point power configuration. Click **Reset** to revert to the last saved configuration.

Profile 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.

1 Select the **Configuration** tab from the Web UI.
2 Select **Profiles** from the Configuration tab.
3 Select **Manage Profiles** from the **Configuration>Profiles** menu.
4 Select **Wired 802.1x**.



Wired 802.1X Settings

Dot1x AAA Policy: <none>
Dot1x Authentication Control: ☐
Dot1x Guest VLAN Control: ☑
MAC Authentication AAA Policy: <none>

5 Set the following **Wired 802.1x Settings**:

Dot1x Authentication Control	Select this option to globally enable 802.1x authentication for the selected device. 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.
MAC Authentication Control	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.

6 Click **OK** to save the changes to the 802.1x configuration. Click **Reset** to revert to the last saved configuration.

Profile Interface Configuration

A profile's device interface configuration can be refined to support separate physical Ethernet configurations both unique and specific to RFS 4000, RFS 6000, RFS 7000 model controllers and NX 4500, NX 4524, NX 6500,NX 6524 and NX 9000 series service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces

Controllers, service platforms and access points require their 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 VLAN ID the device is connected to.

If the profile is configured to support an access point radio, additional options are available unique to the radio's capabilities.

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

- Ethernet Port Configuration on page 542
- Virtual Interface Configuration on page 553
- Port Channel Configuration on page 569
- VM Interface Configuration on page 575
- Access Point Radio Configuration on page 580
- WAN Backhaul Configuration on page 599
- PPPoE Configuration on page 601
- Overriding Bluetooth Configuration on page 163

For interface deployment considerations, see Profile Interface Deployment Considerations.

Ethernet Port Configuration

Port placement and quantity varies depending on controller, service platform or access point model.

The following ports are available on RFS controllers:

- *RFS 4000*- ge1, ge2, ge3, ge4, ge5, up1

The following ports are available on NX series service platforms:

- NX 9000 series - ge1, ge2 (10GigE ports (xge1-xge4) are available on NX9610 models)

UP ports are available on RFS 4000 wireless controllers. A UP port connects the to the backbone network. A UP port supports either RJ-45 or fiber. A UP port is the preferred means to connect to the backbone, as it has a non-blocking 1gbps connection unlike GE ports.

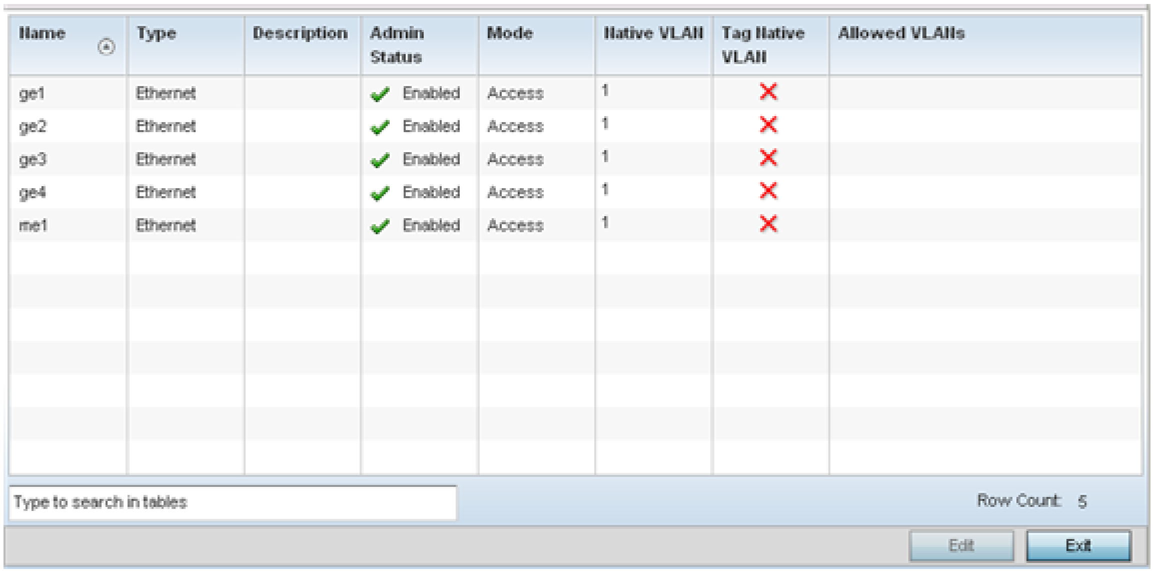
The following ports are available on access points:

- AP 6511 - fe1, fe2, fe3, fe4, up1
- AP 6521 - GE1/POE (LAN)
- AP 6522 - GE1/POE (LAN)
- AP 6532- GE1/POE
- AP 6562 - GE1/POE
- AP7131 - GE1/POE (LAN), GE2 (WAN)
- AP 7131N - GE1/POE (LAN), GE2 (WAN)
- AP 7161 - GE1/POE (LAN), GE2 (WAN)
- AP 7181 - GE1/POE (LAN), GE2 (WAN)
- AP 8132 - GE1/POE (LAN), GE2 (WAN)

To define a profile's Ethernet port configuration:

1. Select **Configuration** > **Profiles** > **Interface**.
2. Expand the Interface menu to display its submenu options.
3. Select **Ethernet Ports**.

   The Ethernet Ports screen displays configuration, runtime status and statistics regarding the physical ports on the controller.



Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
ge1	Ethernet		✓ Enabled	Access	1	✗	
ge2	Ethernet		✓ Enabled	Access	1	✗	
ge3	Ethernet		✓ Enabled	Access	1	✗	
ge4	Ethernet		✓ Enabled	Access	1	✗	
me1	Ethernet		✓ Enabled	Access	1	✗	

Row Count: 5

4. Refer to the following to assess port status and performance:

Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on controller, service platform or access point model.
Type	Displays the physical port type. Cooper is used on RJ45 Ethernet ports and Optical materials are used on fiber optic gigabit Ethernet ports.
Description	Displays an administrator defined description for each listed device port.
Admin Status	A green checkmark defines the port as active and currently enabled with the profile. A red "X" defines the port as currently disabled and not available for use. The interface status can be modified with the port configuration as needed.
Mode	Displays the profile's switching mode as currently either *Access* or *Trunk* (as defined within the Ethernet Port Basic Configuration screen). If Access is selected, the listed port accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set 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	A green checkmark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. 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	Displays those VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to Trunk.

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

Editing Ethernet Port Configurations

Port placement and quantity varies depending on controller, service platform or access point model.

The following ports are available on RFS controllers:

- *RFS 4000*- ge1, ge2, ge3, ge4, ge5, up1

The following ports are available on NX series service platforms:

- NX 9000 series - ge1, ge2 (10GigE ports (xge1-xge4) are available on NX9610 models)

UP ports are available on RFS 4000 model wireless controller. A UP port connects the to the backbone network. A UP port supports either RJ-45 or fiber. A UP port is the preferred means to connect to the backbone, as it has a non-blocking 1gbps connection unlike GE ports.

The following ports are available on access points:

- AP 6522 - GE1/POE (LAN)
- AP 6562 - GE1/POE
- AP 7161 - GE1/POE (LAN), GE2 (WAN)

For more information, see:

- Basic Ethernet Port Configuration
- Ethernet Port Security
- Ethernet Port Spanning Tree

Basic Ethernet Port Configuration

To define a profile's Ethernet port basic configuration:

1 Select **Configuration → Profiles**.

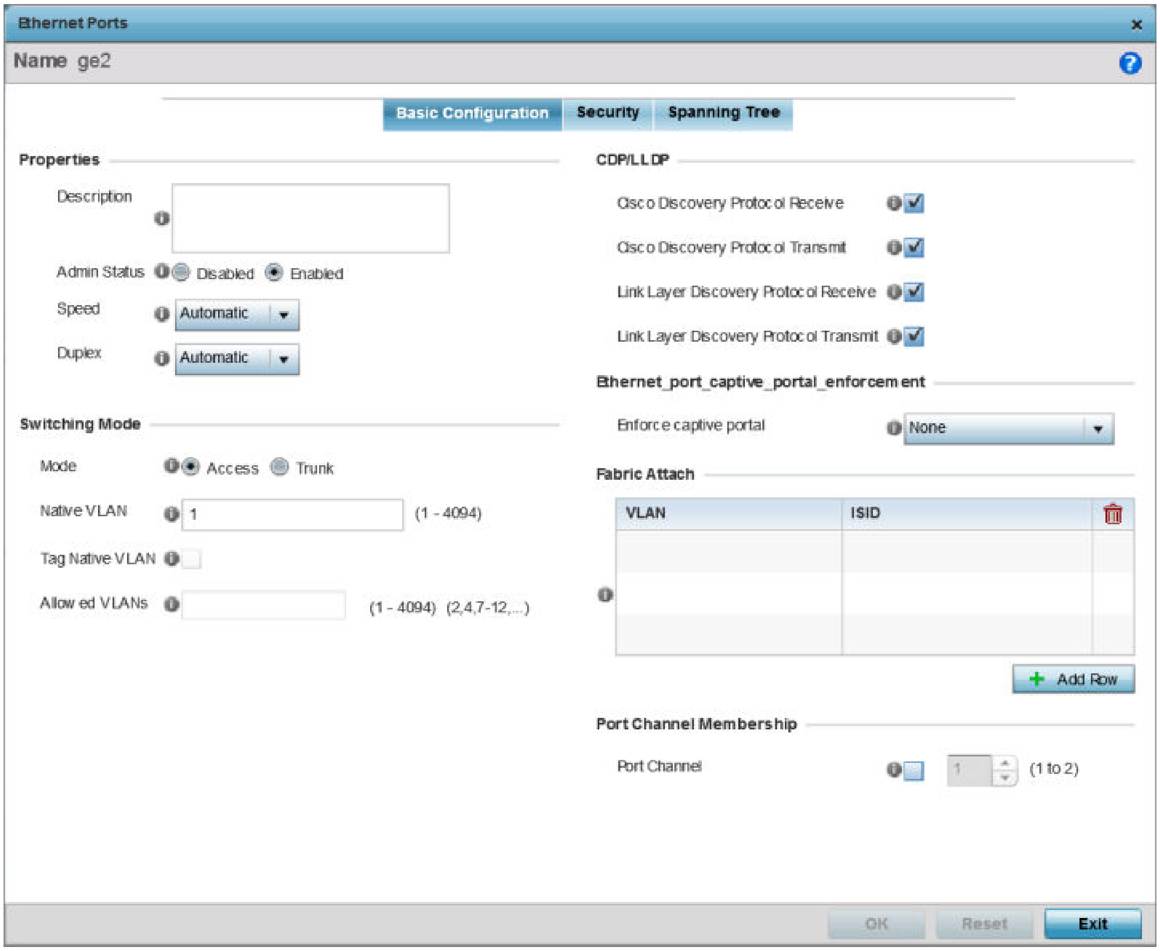
The Profile screen, listing device profiles is displayed.

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. The Ethernet port **Basic Configuration** screen displays by default.



Name ge2

Description
Admin Status ○ Disabled ● Enabled
Speed Automatic
Duplex Automatic

Mode ● Access ○ Trunk
Native VLAN 1 (1 - 4094)
Tag Native VLAN ☐
Allowed VLANs (1 - 4094) (2,4,7-12,...)

Cisco Discovery Protocol Receive ☑
Cisco Discovery Protocol Transmit ☑
Link Layer Discovery Protocol Receive ☑
Link Layer Discovery Protocol Transmit ☑

Enforce captive portal None

Port Channel ☐ 1 (1 to 2)

5 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.

6 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.

7 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, uncheck 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.

8 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.

9 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: AP 7562, AP 7602, AP-7612, AP-8432, AP-8533, NX 5500, NX 75XX, NX 95XX, NX 9600, and VX. 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. 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. 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. The passive port only responds to LACPDU received from its corresponding active port. 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. 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.

10 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.

11 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. Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port. 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. 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.

12 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.

13 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.

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 771.

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. 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 **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. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

6 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.

7 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** → **Profiles**.

The Profile screen, listing device profiles is displayed.

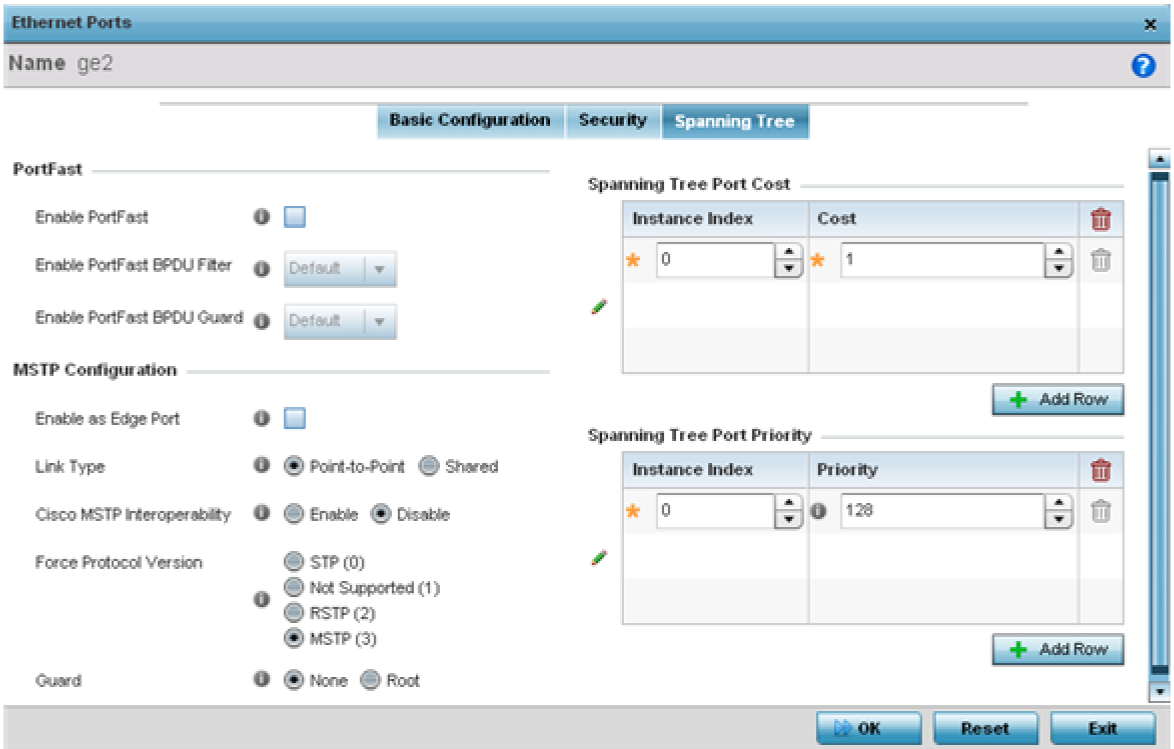
2 Select a device profile from those listed on the screen.

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.



Name ge2

Enable PortFast ☐

Enable PortFast BPDU Filter: Default

Enable PortFast BPDU Guard: Default

Enable as Edge Port ☐

Link Type: ● Point-to-Point ○ Shared

Cisco MSTP Interoperability: ○ Enable ● Disable

Force Protocol Version: ○ STP (0) ○ Not Supported (1) ○ RSTP (2) ● MSTP (3)

Guard: ● None ○ Root

Instance Index	Cost
0	1

Instance Index	Priority
0	128

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.

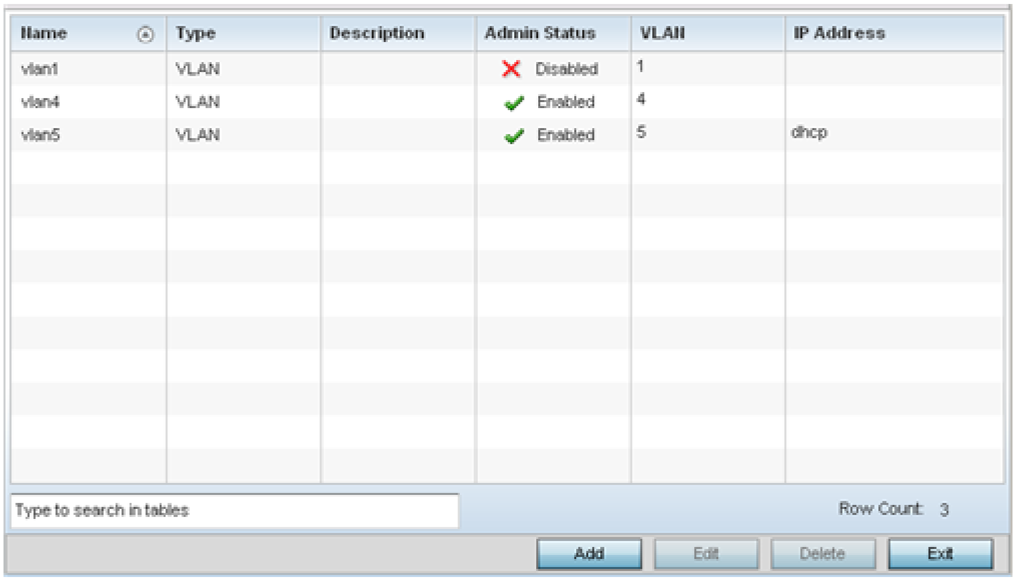
    Define an **Instance Index** using the spinner control and assign a **Priority** value. The lower the priority, a greater likelihood of the port becoming a designated port. Thus applying an higher value impacts the port's likelihood of becoming a designated port.
12. Select **+ Add Row** needed to include 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 or to provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each connected VLAN ID. 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 networks for routing.

To review, create, modify or delete a Virtual Interface configuration:

1 Select **Configuration** → **Profiles** → **Interface**.
2 Expand the Interface menu to display its submenu options.
3 Select **Virtual Interfaces**.



Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		✗ Disabled	1	
vlan4	VLAN		✓ Enabled	4	
vlan5	VLAN		✓ Enabled	5	dhcp

Row Count: 3

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

Name	Displays 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	Displays the type of Virtual Interface for each listed interface.
Description	Displays the description defined for the Virtual Interface when it was either initially created or edited.
Admin Status	A green checkmark defines the listed Virtual Interface configuration as active and enabled with its supported profile. A red "X" defines the Virtual Interface as currently disabled. The interface status can be modified when a new Virtual Interface is created or an existing one modified.
VLAN	Displays the numerical VLAN ID associated with each listed interface.
IP Address	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.

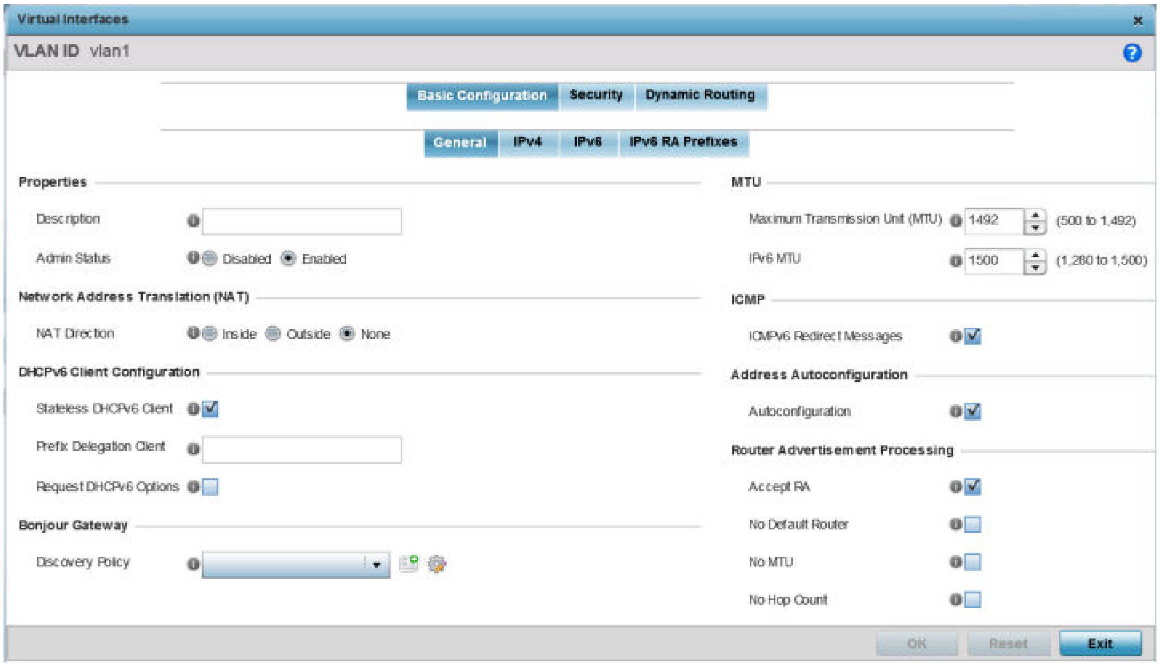
5 Select **Add** to define a new Virtual Interface configuration, **Edit** to modify the configuration of an existing Virtual Interface or **Delete** to permanently remove a selected Virtual Interface.

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.



VLAN ID vlan1

Properties
Description
Admin Status ○ Disabled ● Enabled

Network Address Translation (NAT)
NAT Direction ○ Inside ○ Outside ● None

DHCPv6 Client Configuration
Stateless DHCPv6 Client ☑
Prefix Delegation Client
Request DHCPv6 Options ☐

Bonjour Gateway
Discovery Policy

MTU
Maximum Transmission Unit (MTU) 1492 (500 to 1,492)
IPv6 MTU 1500 (1,280 to 1,500)

ICMP
ICMPv6 Redirect Messages ☑

Address Autoconfiguration
Autoconfiguration ☑

Router Advertisement Processing
Accept RA ☑
No Default Router ☐
No MTU ☐
No Hop Count ☐

Figure 235: 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.

Note

Refer to Setting the Profile's NAT Configuration on page 698 for instructions on creating a profile’s NAT configuration.

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.

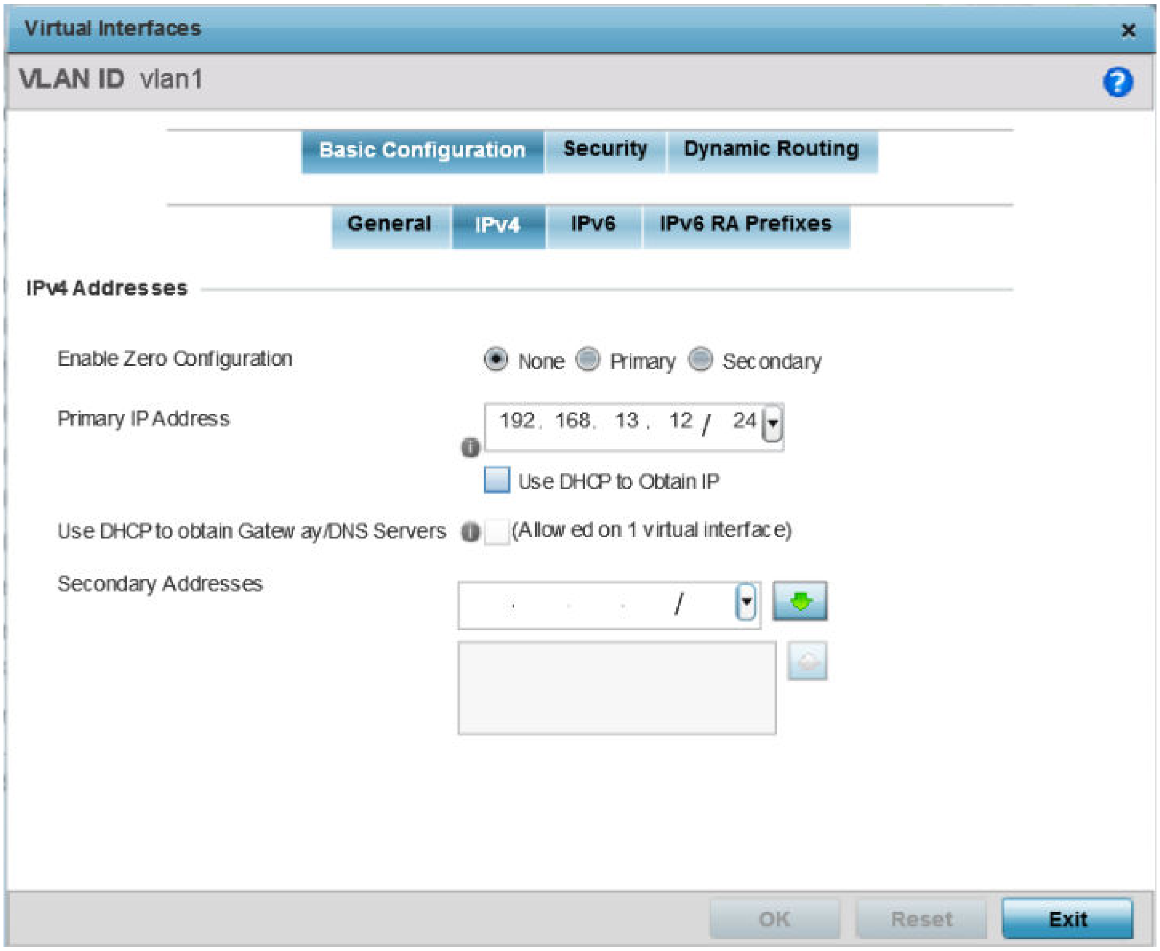
Click **Reset** to revert to the last saved configuration.

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.



Enable Zero Configuration ● None ○ Primary ○ Secondary

Primary IP Address 192 . 168 . 13 . 12 / 24

☐ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ☐ (Allowed on 1 virtual interface)

Secondary Addresses

Figure 236: 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 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the virtual interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
DHCP Relay	Provide IP addresses for DHCP server relay resources. 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.

4 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.

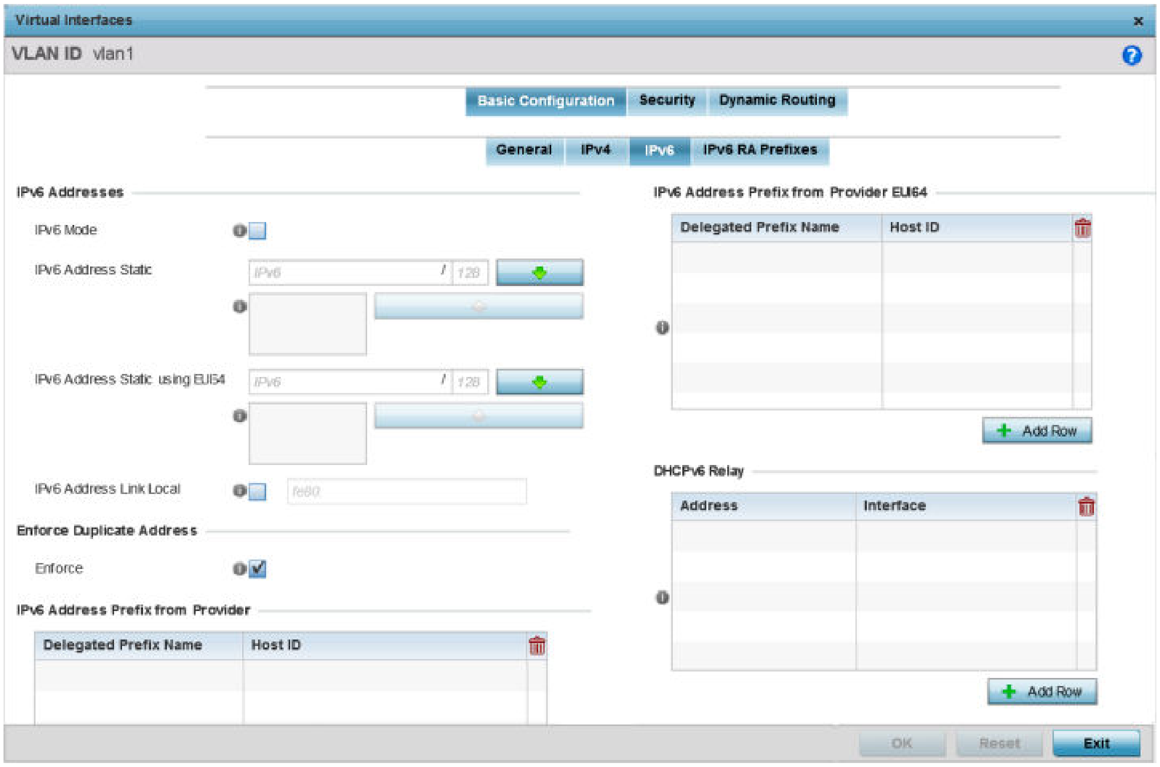


Figure 237: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab

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.

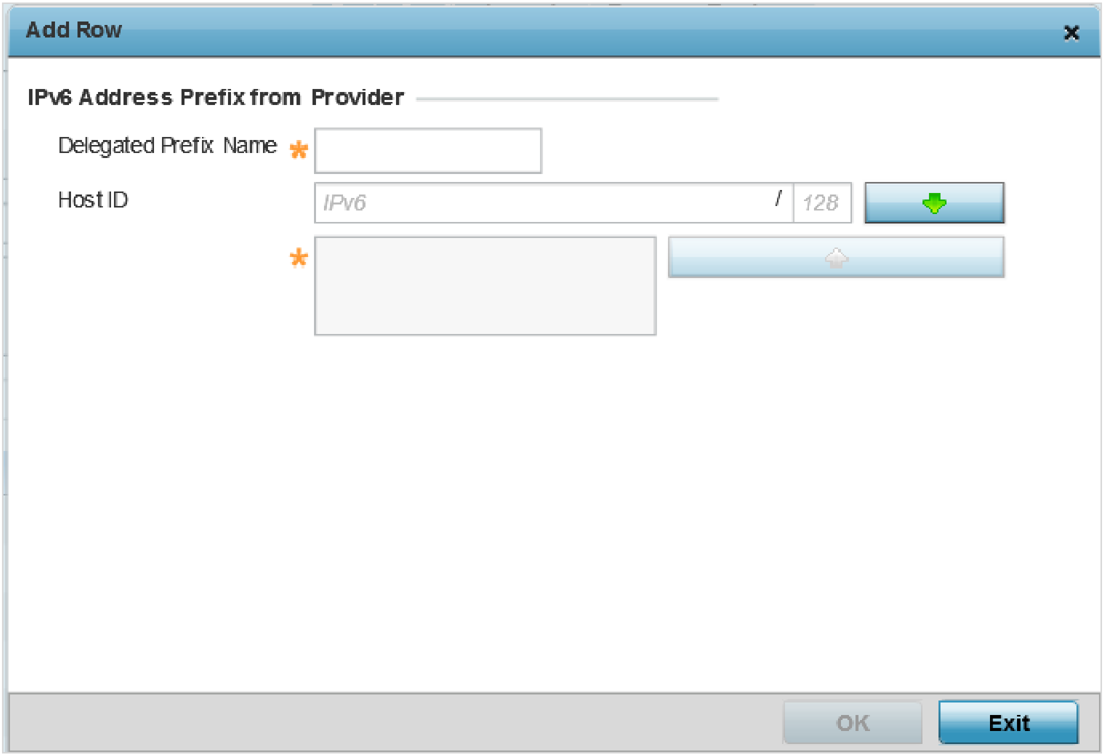


Figure 238: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider

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.

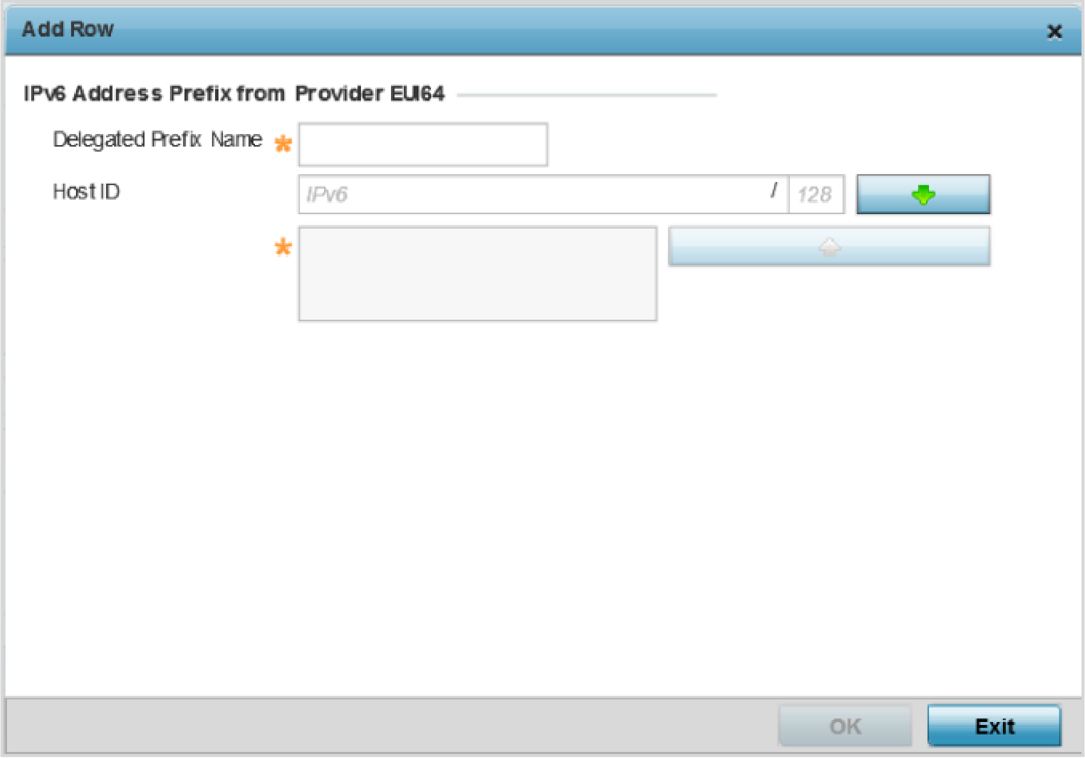


Figure 239: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64

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.

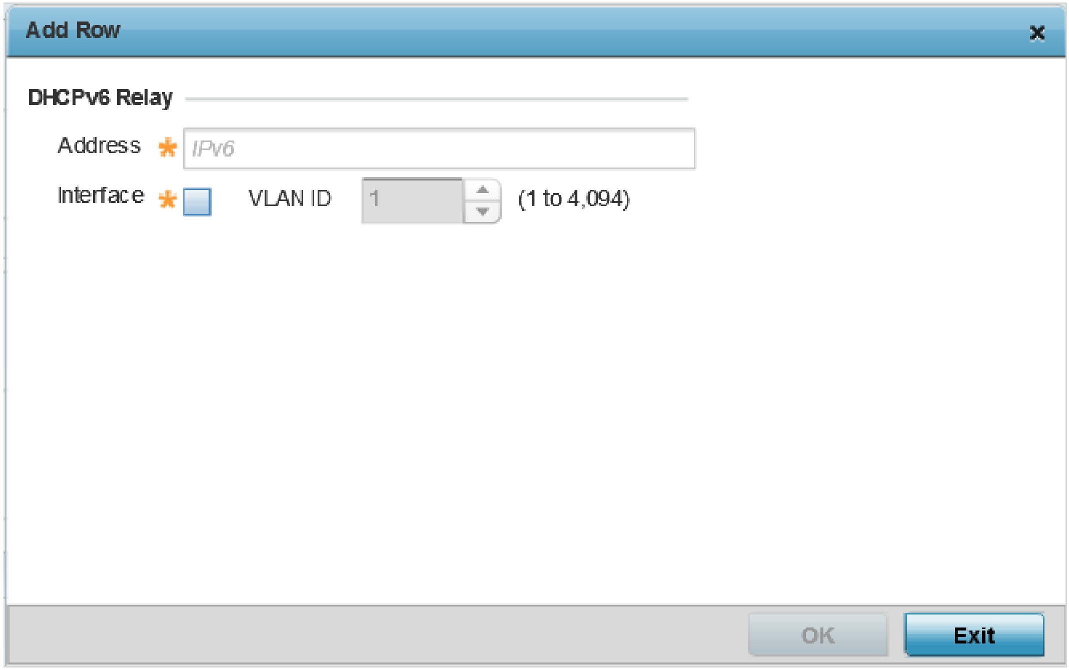


Figure 240: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add DHCPv6 Relay

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.

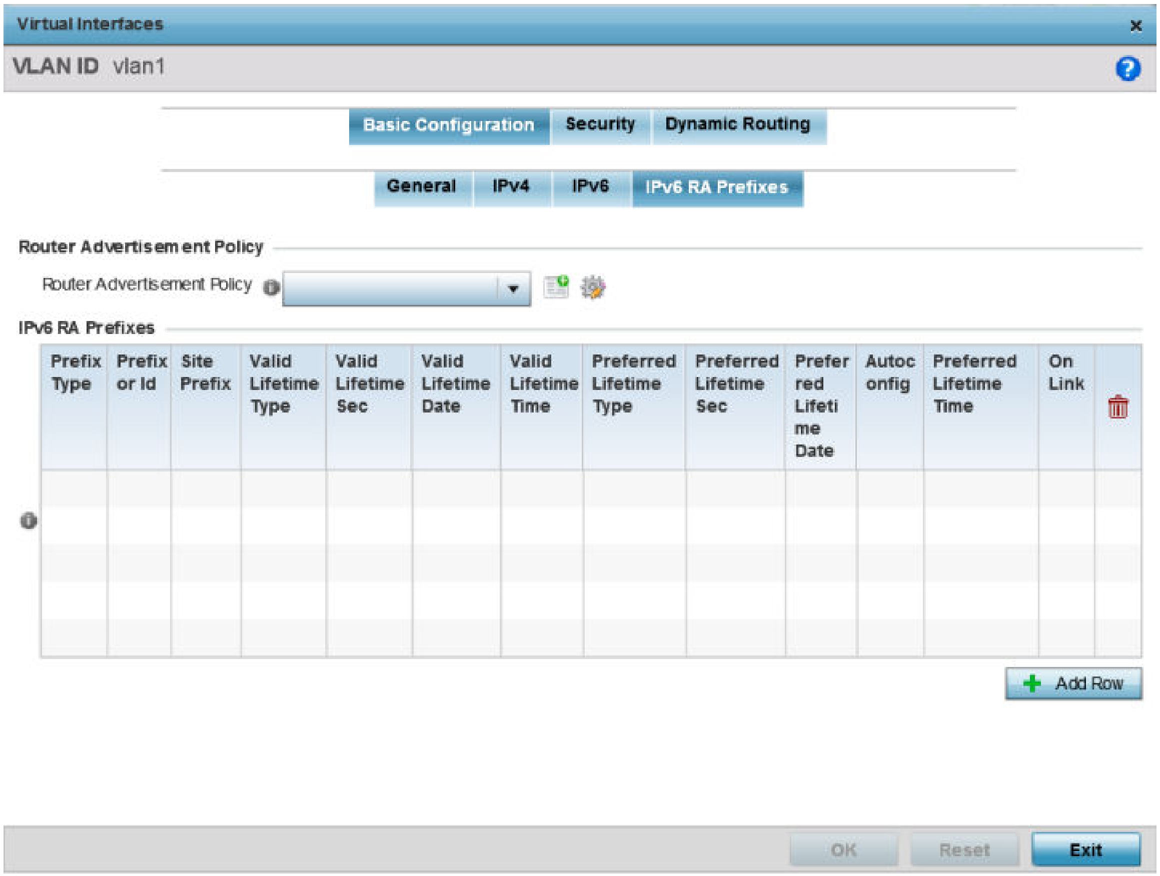


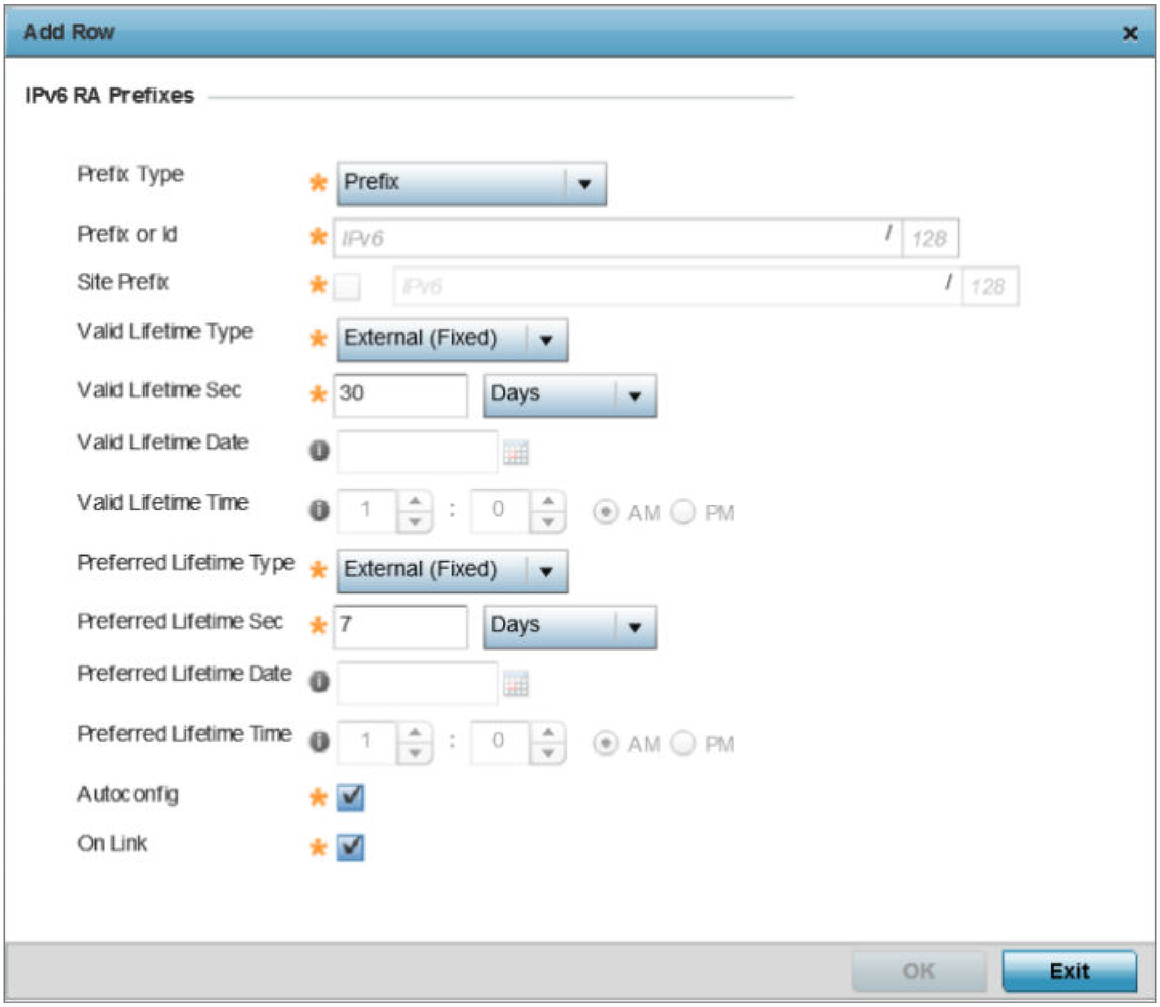
Figure 241: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab

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.



Add Row

IPv6 RA Prefixes

Prefix Type: Prefix
Prefix or Id: IPv6 / 128
Site Prefix: ☐ IPv6 / 128
Valid Lifetime Type: External (Fixed)
Valid Lifetime Sec: 30 Days
Valid Lifetime Date:
Valid Lifetime Time: 1 : 0 ● AM ○ PM
Preferred Lifetime Type: External (Fixed)
Preferred Lifetime Sec: 7 Days
Preferred Lifetime Date:
Preferred Lifetime Time: 1 : 0 ● AM ○ PM
Autoconfig: ☑
On Link: ☑

Figure 242: 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.
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.
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 771.

To set the VLAN security configuration:

1 Select the **Security** tab.

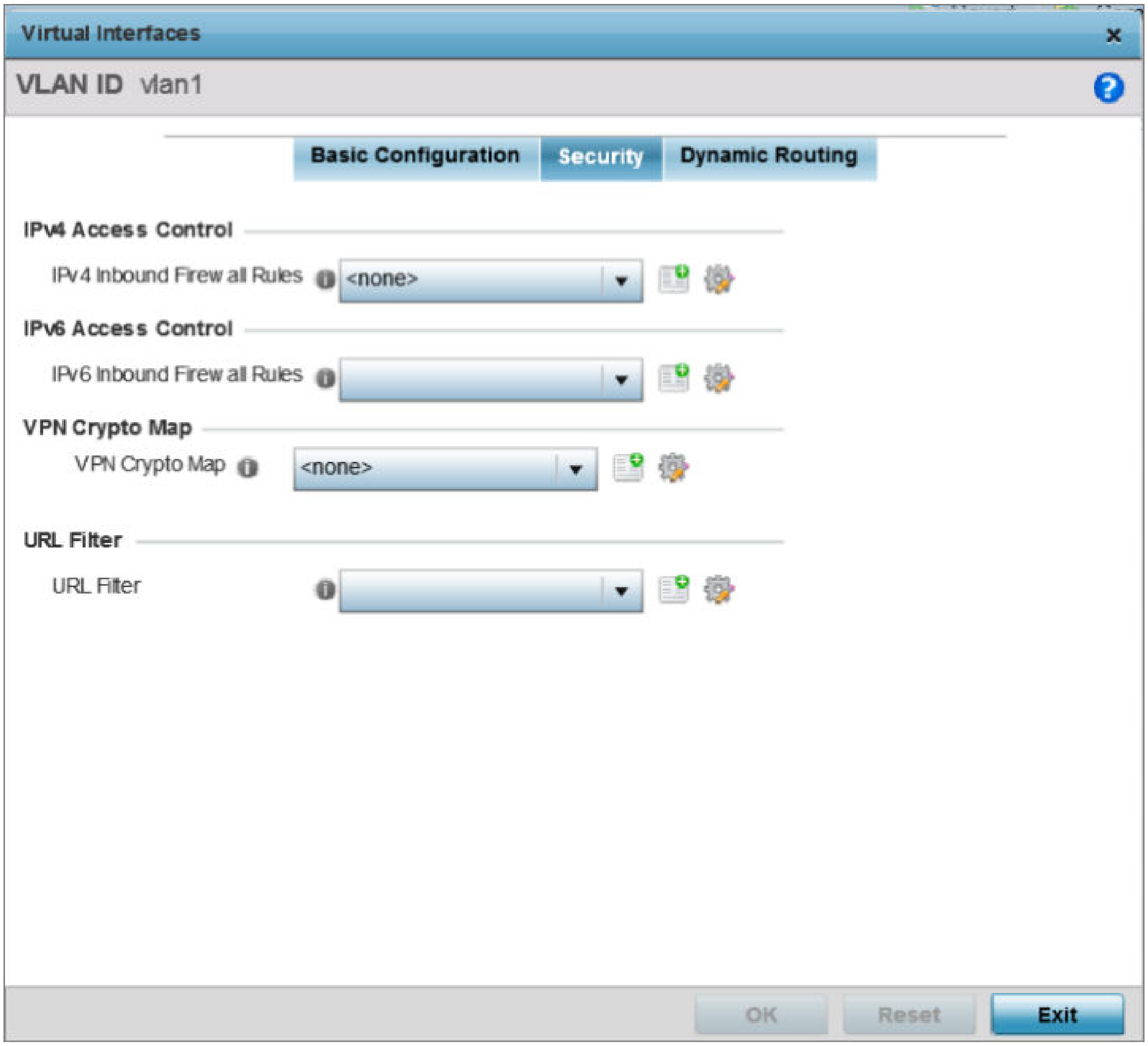


Figure 243: Profile Overrides - Virtual Interfaces Security Screen

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).

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 789.
4. Use the **VPN Crypto Map** drop-down menu to select or override the Crypto Map configuration applied to this virtual interface.

   Crypto Map entries are sets of configuration parameters for encrypting packets that pass through the VPN Tunnel. If there is no Crypto Map configuration that meets the needs of this virtual interface, click the **Create** icon to define a new Crypto Map configuration or click the **Edit** icon to modify an existing configuration. For more information, see Overriding VPN Configuration on page 257.
5. 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.
6. 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.

Note

The Dynamic Routing tab is not available for controllers or service platforms.

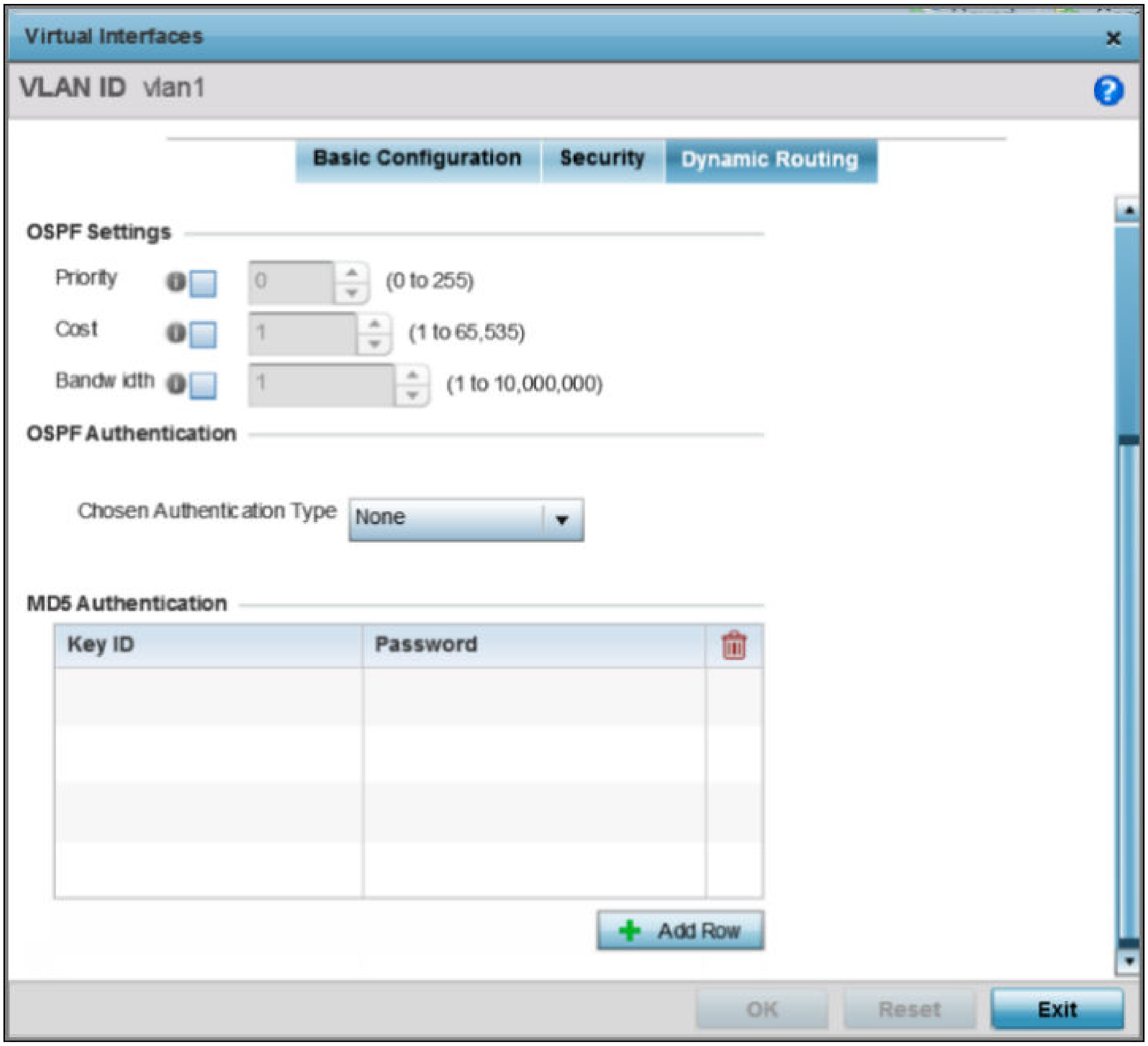


Figure 244: Profile Overrides - Virtual Interfaces Dynamic Routing Screen

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

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 bandwidth from 1 - 10,000,000 KBps.

3 From the **Chosen Authentication Type** drop-down list, select the authentication type used to validate credentials within the OSPF dynamic route.

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

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.

To define a port channel configuration for a device profile:

1 Select **Configuration** → **Profiles**.

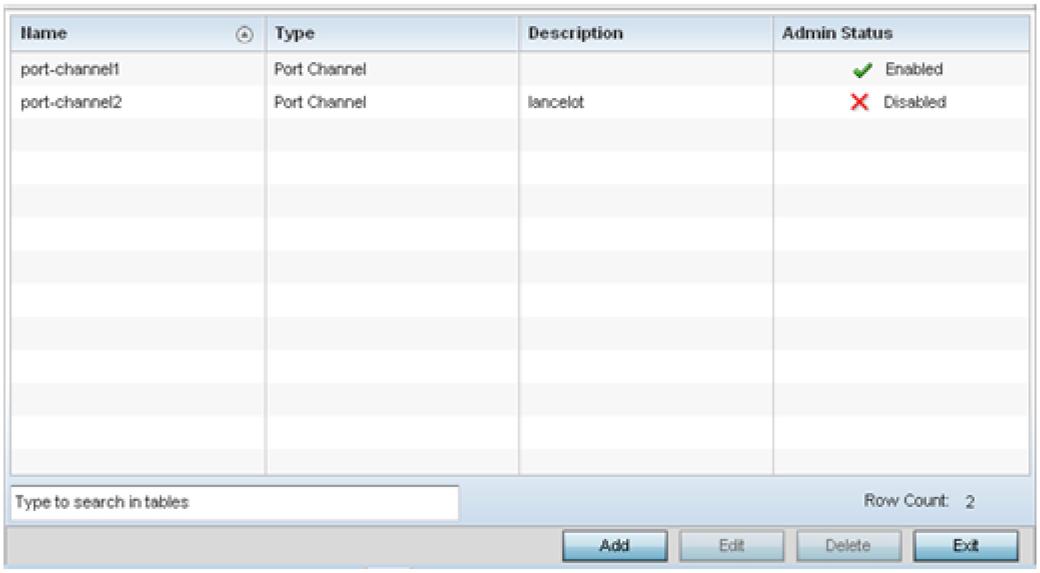
The Profile screen, listing device profiles, is displayed.

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.



Name	Type	Description	Admin Status
port-channel1	Port Channel		✓ Enabled
port-channel2	Port Channel	lancelot	✗ Disabled

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.

Adding and Editing a Port Channel Configuration

Profiles can be applied customized port channel configurations as part of their Interface configuration.

For more information, refer to the following:

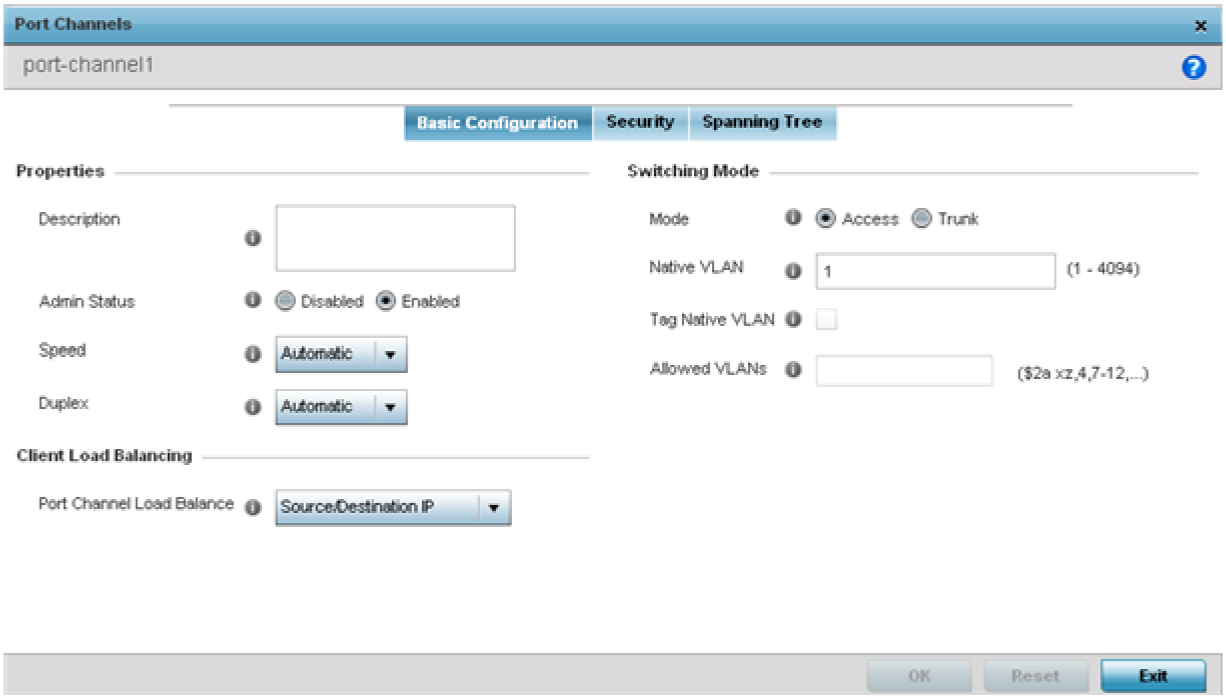
- Port Channel Basic Configuration on page 570
- Port Channel Security on page 572
- Port Channel Spanning Tree on page 573

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.



Description
Admin Status ○ Disabled ● Enabled
Speed Automatic
Duplex Automatic
Port Channel Load Balance Source/Destination IP
Mode ● Access ○ Trunk
Native VLAN 1 (1 - 4094)
Tag Native VLAN ☐
Allowed VLANs ($2a xz,4,7-12,...)

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.

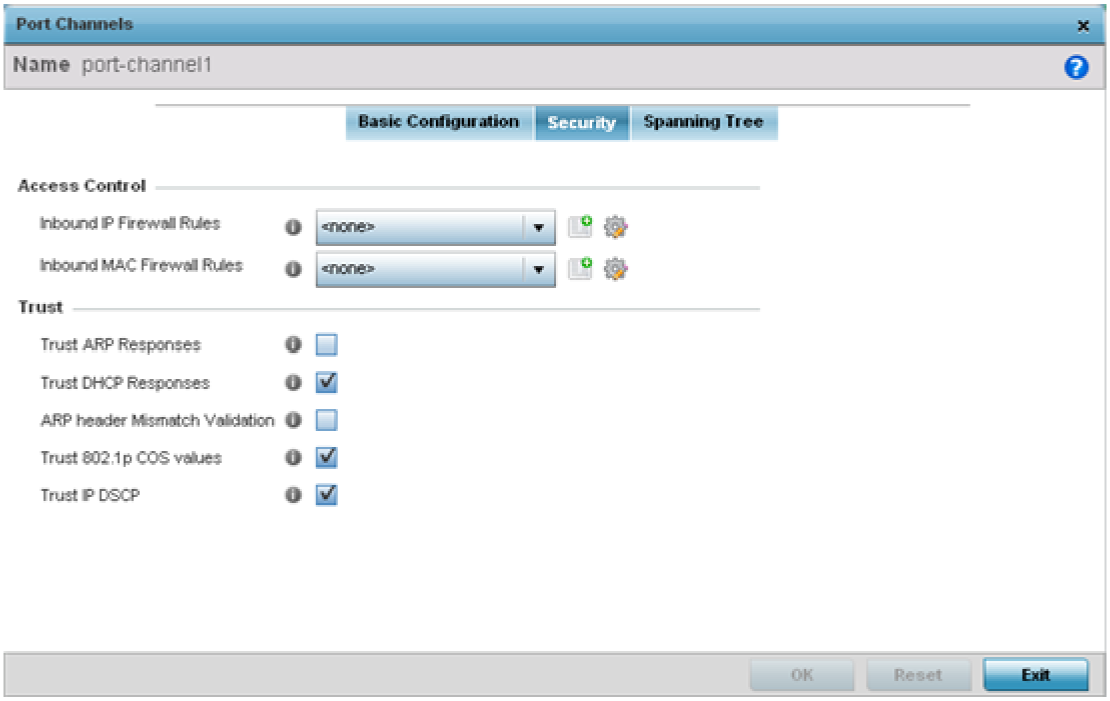
Tag the Native VLAN	Select the checkbox to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream 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.



Port Channels

Name port-channel1

Access Control

Inbound IP Firewall Rules <none>

Inbound MAC Firewall Rules <none>

Trust

Trust ARP Responses ☐

Trust DHCP Responses ☑

ARP header Mismatch Validation ☐

Trust 802.1p COS values ☑

Trust IP DSCP ☑

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 771.

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:

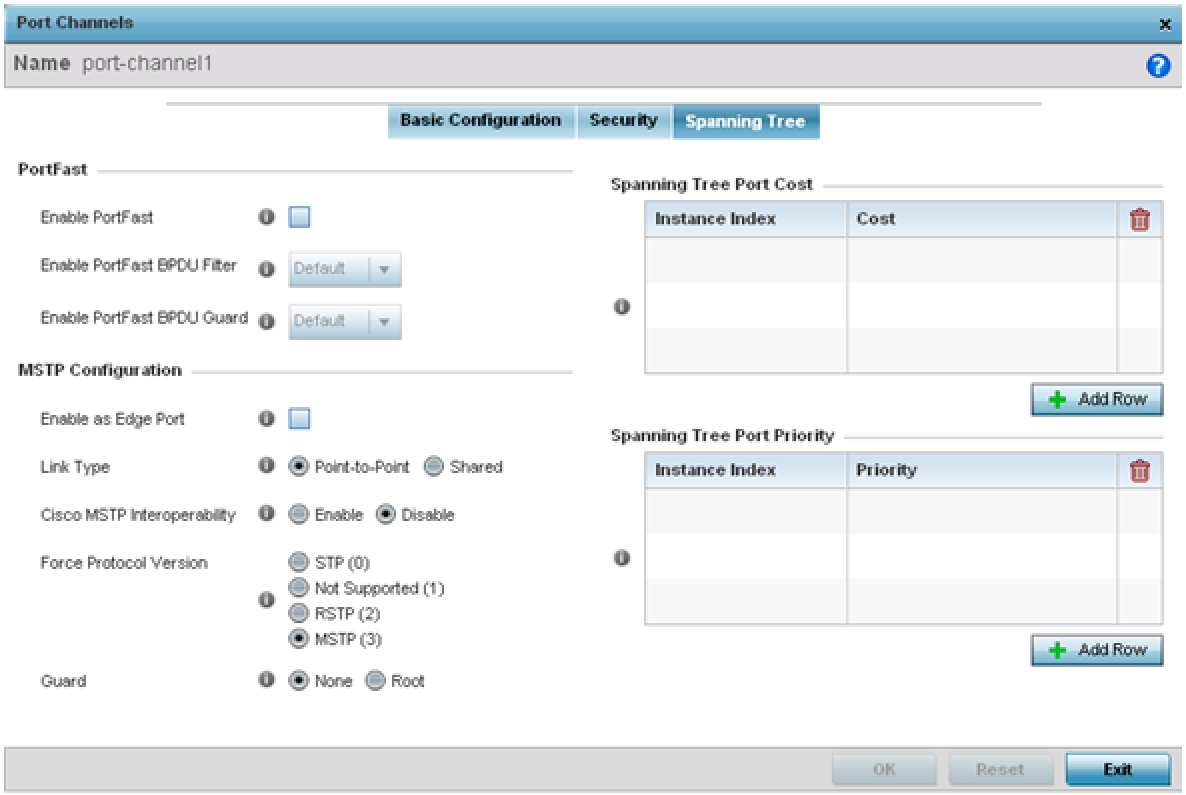
Trust ND Requests	Select to enable the trust of neighbor discovery requests required on an IPv6 network. This setting is disabled by default.
Trust DHCPv6 Responses	Select to enable the trust all DHCPv6 responses. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes, 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.



Name port-channel1

Enable PortFast ☐

Enable PortFast BPDU Filter: Default

Enable PortFast BPDU Guard: Default

Enable as Edge Port ☐

Link Type ● Point-to-Point ○ Shared

Cisco MSTP Interoperability ○ Enable ● Disable

Force Protocol Version ○ STP (0) ○ Not Supported (1) ○ RSTP (2) ● MSTP (3)

Guard ● None ○ Root

Instance Index	Cost

Instance Index	Priority

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
<=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.

VM Interface Configuration

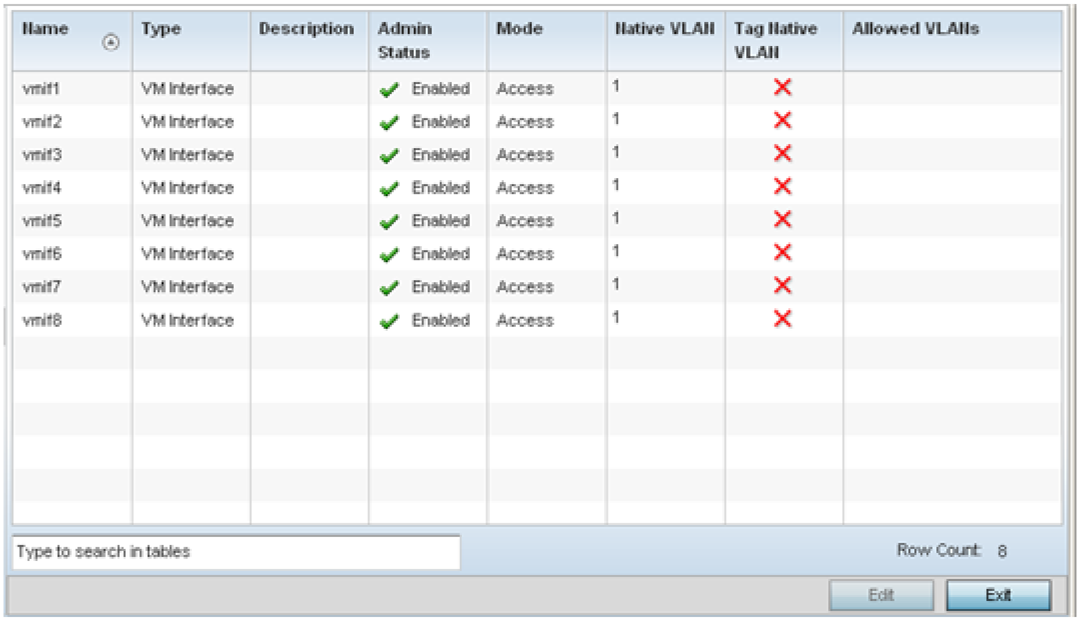
WiNG provides a dataplane bridge for external network connectivity for Virtual Machines (VMs). VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of sixteen VMIF ports on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1 is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.

Note
VM interfaces are only supported for NX9000 series service platforms.

To define a VM interface profile configuration:

1 Select **Configuration** > **Profiles** > **Interface**.
2 Expand the **Interface** menu to display its submenu options.
3 Select **VM**.



Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
vmif1	VM Interface		✓ Enabled	Access	1	✗	
vmif2	VM Interface		✓ Enabled	Access	1	✗	
vmif3	VM Interface		✓ Enabled	Access	1	✗	
vmif4	VM Interface		✓ Enabled	Access	1	✗	
vmif5	VM Interface		✓ Enabled	Access	1	✗	
vmif6	VM Interface		✓ Enabled	Access	1	✗	
vmif7	VM Interface		✓ Enabled	Access	1	✗	
vmif8	VM Interface		✓ Enabled	Access	1	✗	

4 Refer to the following to review VM interface configurations and status:

Name	Displays the VM interface numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
Type	Displays whether the type is VM interface.
Description	Lists a short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed VM interface as active and currently enabled with the profile. A red “X” defines the VM interface as currently disabled and not available for use. The interface status can be modified with the VM interface Basic Configuration screen as required.
Mode	Displays the layer 3 mode of the VM interface as either Access or Trunk (as defined within the VM Interfaces Basic Configuration screen). If Access is selected, the listed VM interface 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. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A VM interface configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.

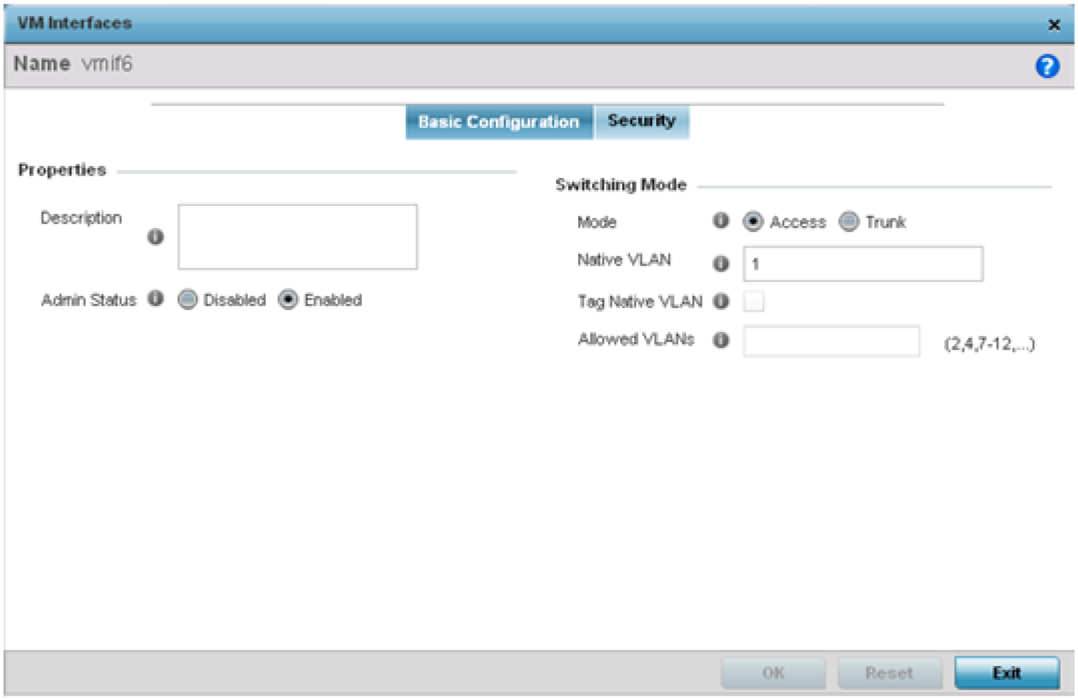
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a VM interface in trunk mode.
Tag Native VLAN	A green check mark defines the native VLAN as tagged. A red “X” defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream VM interface ports 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 VM interface classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays those VLANs allowed to send packets over the listed VM interface. Allowed VLANs are only listed when the mode has been set to Trunk.

5. To edit the configuration of an existing VM interface, select it from amongst those displayed and select the **Edit** button.

VM Basic Configuration

To set a VM interface basic configuration for a profile:

1. Select **Configuration** > **Profiles** > **Interface**.
2. Expand the **Interface** menu to display its submenu options.
3. Select **VM**.
4. Select an existing VM interface configuration and select the **Edit** button. The **Basic Configuration** tab displays by default.



Name vmif6

Description

Admin Status ○ Disabled ● Enabled

Mode ● Access ○ Trunk

Native VLAN 1

Tag Native VLAN ☐

Allowed VLANs (2,4,7-12,...)

5. Set the following VM interface **Properties**:

Description	Enter a brief description for the controller or service platform VM interface (64 characters maximum).
Admin Status	Select the *Enabled* radio button to define this VM interface as active to the profile it supports. Select the *Disabled* radio button to disable this VM interface configuration in the profile. It can be activated at any future time when needed. The default setting is disabled.

6 Define the following **Switching Mode** parameters to apply to the VM Interface configuration:

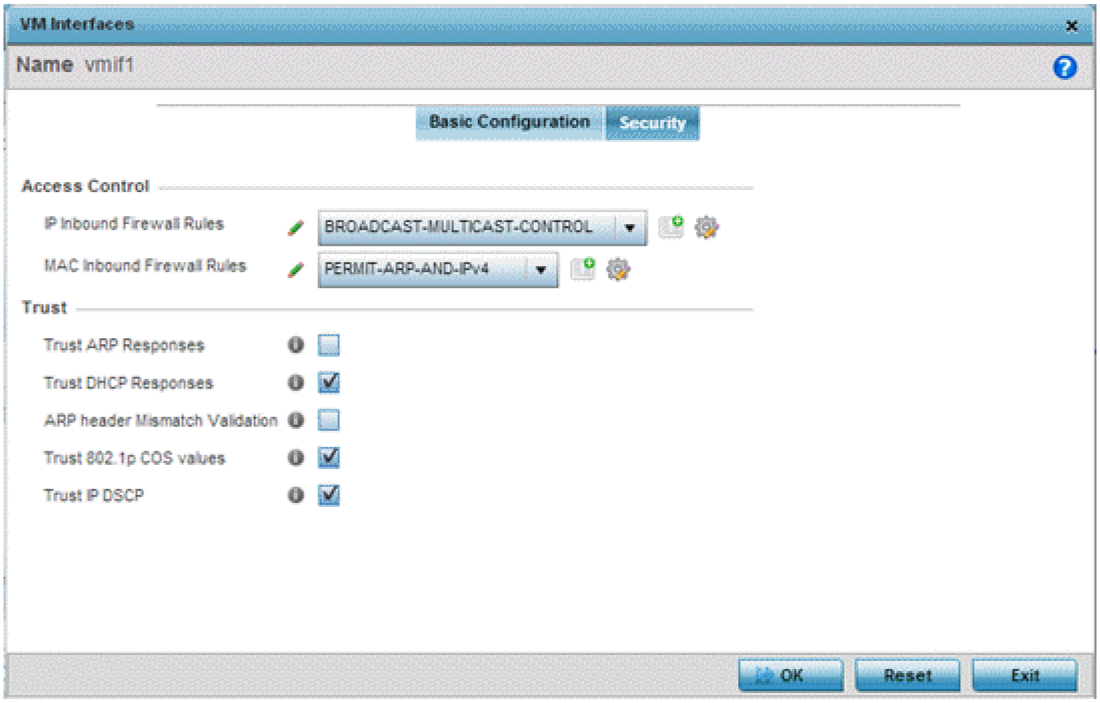
Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the VM interface. If Access is selected, the VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VM port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the VM interface allows packets from a list of VLANs you add to the trunk. A VM interface 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 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 the Native VLAN	Select this option to tag the native VLAN. 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 VMIF that the frame belongs. If the upstream VMIF does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between VM interface ports, both VM interfaces 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 VM interfaces know which VLAN ID the frame belongs to. The 12 bit VLAN ID is read and the frame is forwarded to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VMIF classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows a VM interface 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 VM interface. The available range is from 1 - 4094. The maximum number of entries is 256.

7 Select **OK** to save the changes to the VM interface basic configuration. Select **Reset** to revert to the last saved configuration.

VM Security Settings

To set VM interface security settings for a NX service platform profile:

1 Select the **Security** tab.



Name vmif1

Access Control

IP Inbound Firewall Rules: BROADCAST-MULTICAST-CONTROL

MAC Inbound Firewall Rules: PERMIT-ARP-AND-IPv4

Trust

Trust ARP Responses ☐

Trust DHCP Responses ☑

ARP header Mismatch Validation ☐

Trust 802.1p COS values ☑

Trust IP DSCP ☑

2 Refer to the Access Control field. IP Inbound and MAC Inbound address firewall rules are required.

Use the IP Inbound Firewall Rules and MAC Inbound Firewall Rules drop-down menus to select the firewall rules to apply to this profile's VM interface 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 VM interface configuration, select the Create icon to define a new rule configuration, or the Edit icon to modify an existing firewall rule configuration.

3 Refer to the Trust field to define the following:

Trust ARP Responses	Select this option to enable ARP trust on this VM interface. ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. The default value is disabled.
Trust DHCP Responses	Select this option to enable DHCP trust on this VM interface. If enabled, only DHCP responses are trusted and forwarded on this VM interface, 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 source MAC mismatch check in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this VM interface. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this VM interface. The default value is enabled.

4 Select OK to save the changes to the VM interface security 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 model Controller AP, controller or NX service platform:

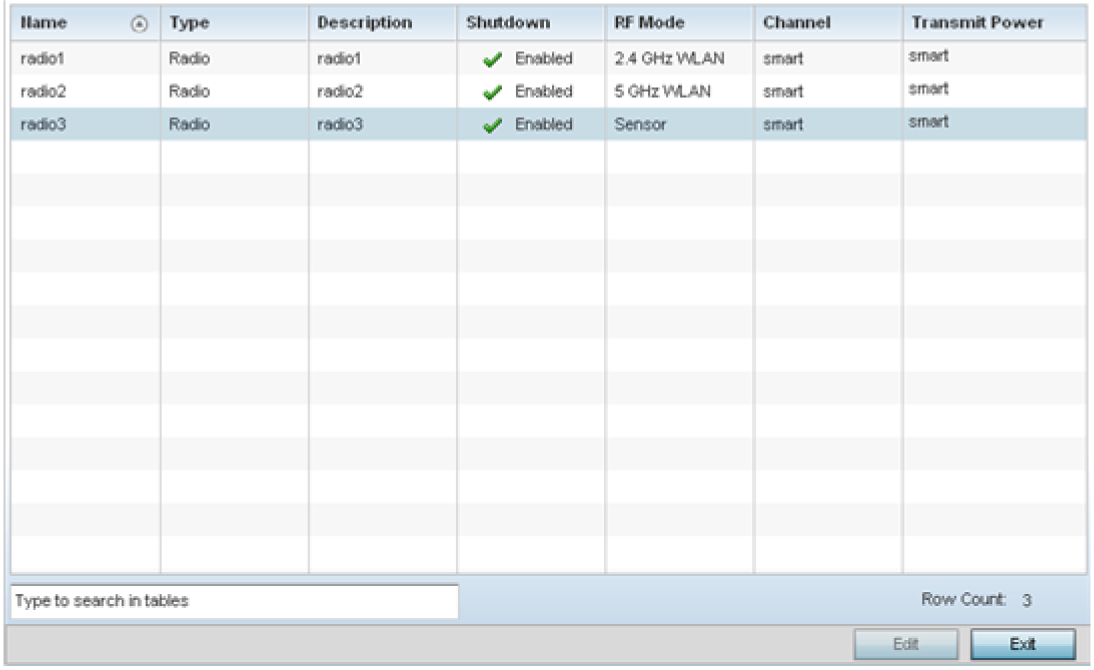
1 Select **Configuration → Profiles**.

The Profile screen, listing device profiles, is displayed.

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**.



Name	Type	Description	Shutdown	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart

Row Count: 3

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. AP 6511and AP 6521 models have one radio. AP 6522, AP 6532, AP 6562, AP 7161 and AP 8132 models have two radios. Certain AP 7131N model SKUs have three radios.
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.

Editing Radio Configurations

The configuration screen supporting an access point's radio configuration is partitioned into 4 tabs, each supporting a unique configuration attribute of the radio.

For more information, see:

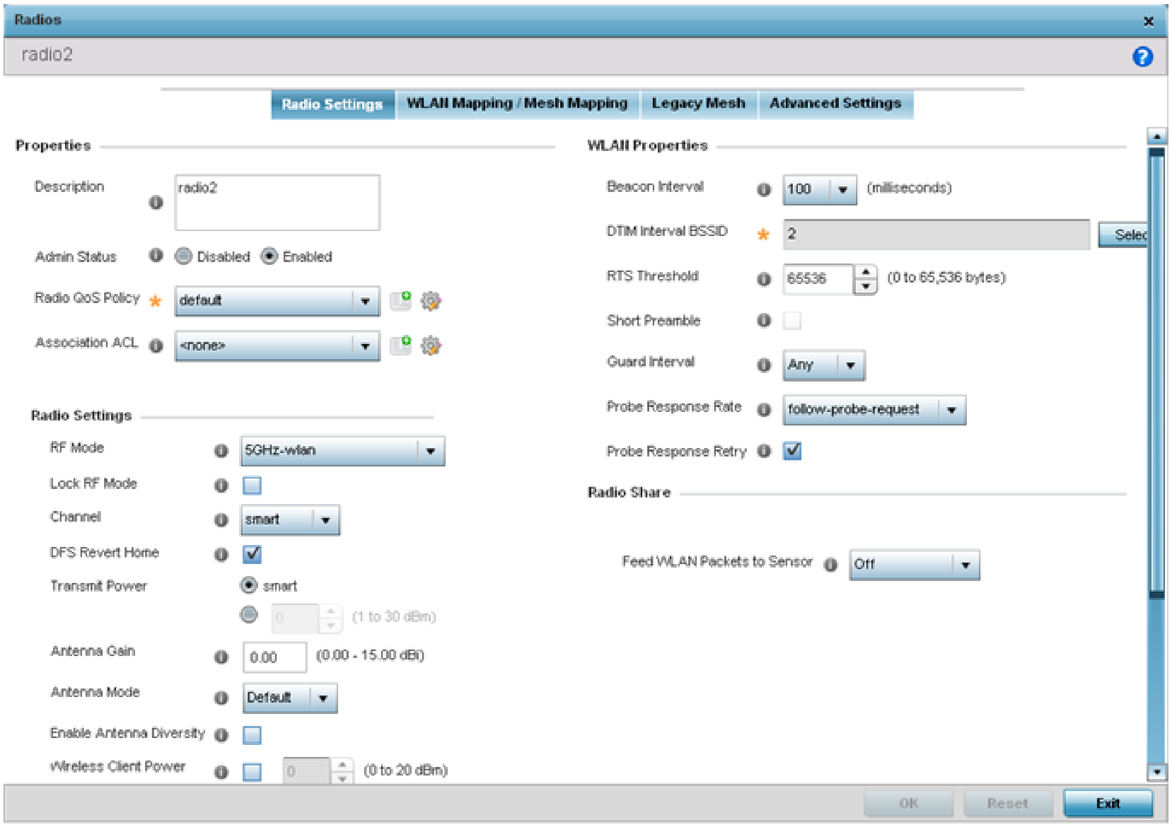
- Radio Settings on page 581
- WLAN Mapping / Mesh Mapping on page 587
- Mesh Legacy on page 588
- Client Bridge Settings on page 590
- Advanced Settings on page 594

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**.



Properties

Description: radio2
Admin Status: ○ Disabled ● Enabled
Radio QoS Policy: default
Association ACL: <none>

Radio Settings

RF Mode: 5GHz-wlan
Lock RF Mode: ☐
Channel: smart
DFS Revert Home: ☑
Transmit Power: ● smart ○ 0 (1 to 30 dBm)
Antenna Gain: 0.00 (0.00 - 15.00 dBi)
Antenna Mode: Default
Enable Antenna Diversity: ☐
Wireless Client Power: ☐ 0 (0 to 20 dBm)

WLAN Properties

Beacon Interval: 100 (milliseconds)
DTIM Interval BSSID: 2
RTS Threshold: 65536 (0 to 65,536 bytes)
Short Preamble: ☐
Guard Interval: Any
Probe Response Rate: follow-probe-request
Probe Response Retry: ☑

Radio Share

Feed WLAN Packets to Sensor: Off

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	Set the mode to either *2.4 GHz WLAN* or *5 GHz WLAN* depending on the radio's intended client support requirement. Set the mode to *Sensor* if using the radio for rogue device detection. To a radio as a detector, disable Sensor support on the other access point radio. 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.
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). 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. 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).
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. AP 6511 and AP 6521 model access points can only support 128 clients.
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. 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. 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. 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 *short guard intervals* (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 *short guard intervals* (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

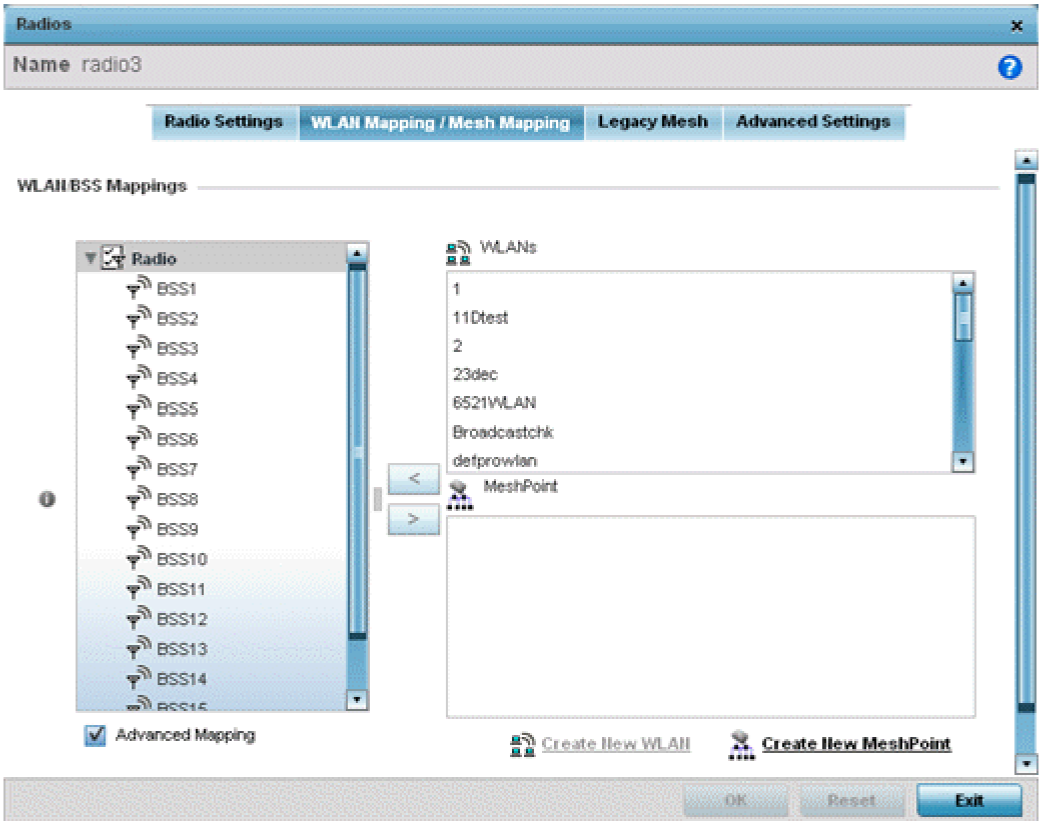
6. Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

WLAN Mapping / Mesh Mapping

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.

To set a radio's WLAN mapping configuration:

1 Select the **WLAN Mapping** tab.



Name radio3

☑ Advanced Mapping

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.

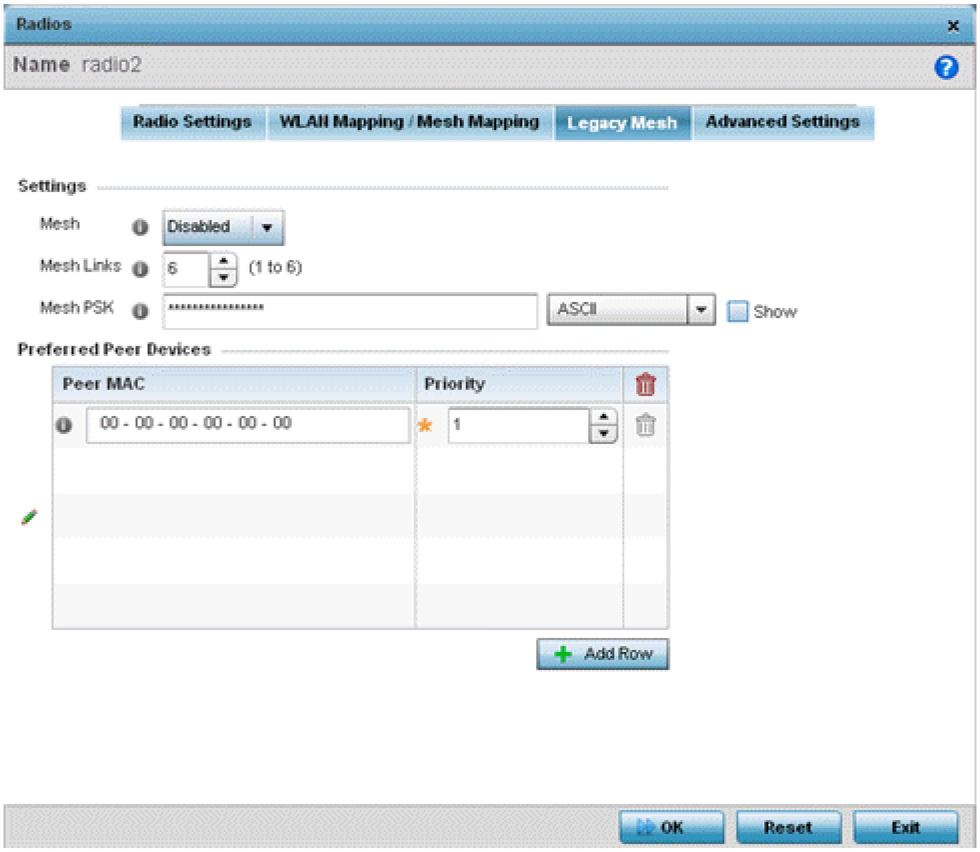
4 Select **OK** to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

Mesh Legacy

Each radio 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.

To set a radio's legacy mesh configuration:

1 Select the **Legacy Mesh** tab.



Name radio2

Mesh: Disabled

Mesh Links: 6 (1 to 6)

Mesh PSK: **************** ASCII ☐ Show

Peer MAC	Priority
00 - 00 - 00 - 00 - 00 - 00	1

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. **Note:** Only single hop mesh links are supported at this time. **Note:** The mesh encryption key is configurable from the CLI *(Command Line Interface)* 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.

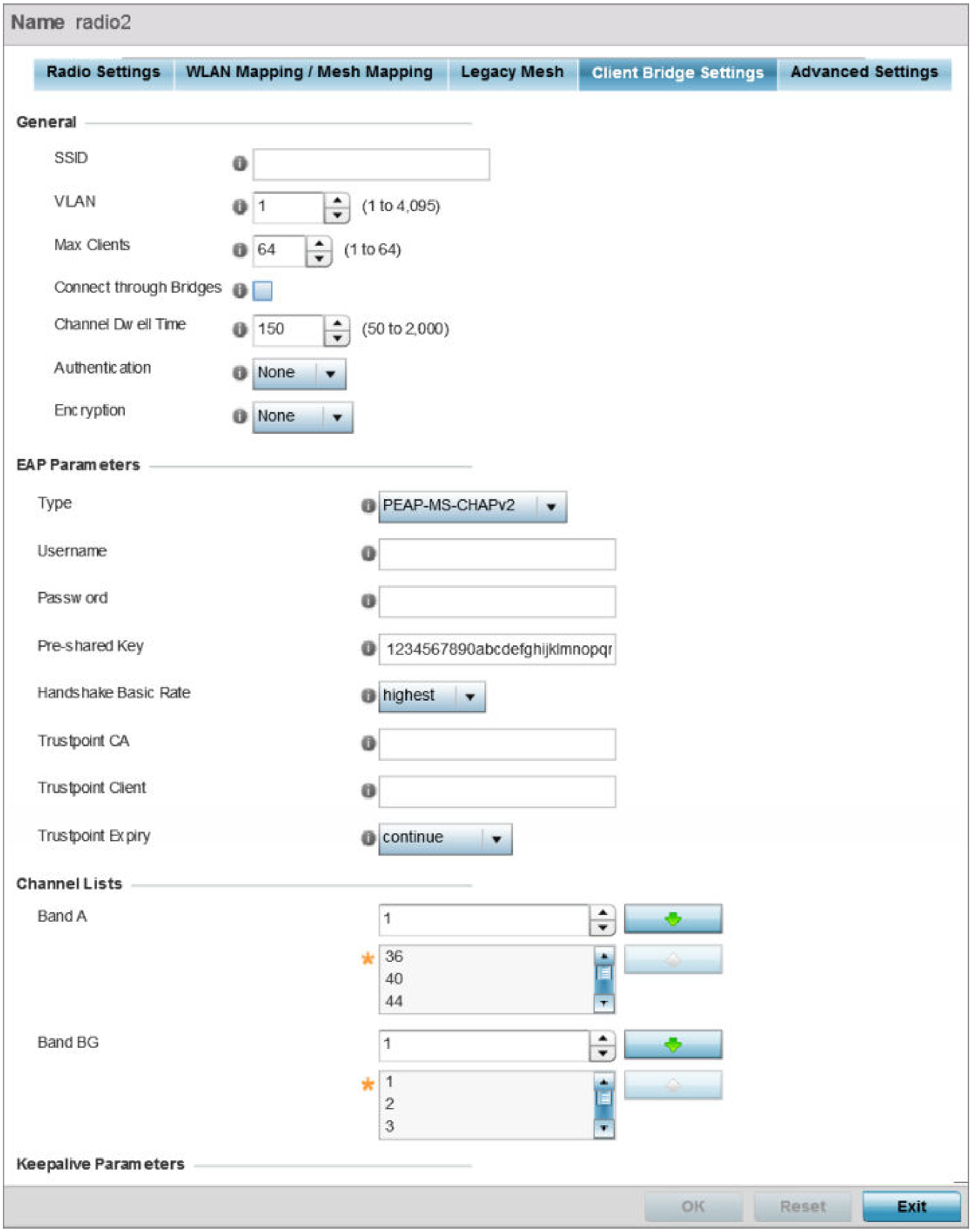
Client Bridge Settings

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. This feature is supported only on the AP7522, AP7532, AP7562, AP7602, AP7622.

To configure a radio's client bridge settings:

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

   The selected radio's client bridge configuration screen displays.



Name radio2

General

SSID

VLAN 1 (1 to 4,095)

Max Clients 64 (1 to 64)

Connect through Bridges ☐

Channel Dwell Time 150 (50 to 2,000)

Authentication None

Encryption None

EAP Parameters

Type PEAP-MS-CHAPv2

Username

Password

Pre-shared Key 1234567890abcdefghijklmnopqr

Handshake Basic Rate highest

Trustpoint CA

Trustpoint Client

Trustpoint Expiry continue

Channel Lists

Band A 1

* 36 40 44

Band BG 1

* 1 2 3

Keepalive Parameters

Figure 245: 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*. For information on WLAN authentication, see Configuring WLAN Security on page 334.
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*. For information on WLAN encryption, see Configuring WLAN Security on page 334.

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. 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. 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. **`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. **`discontinue`** – Terminates the CB once the certificate (CA/client) has expired. Note: 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 462.

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. 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.

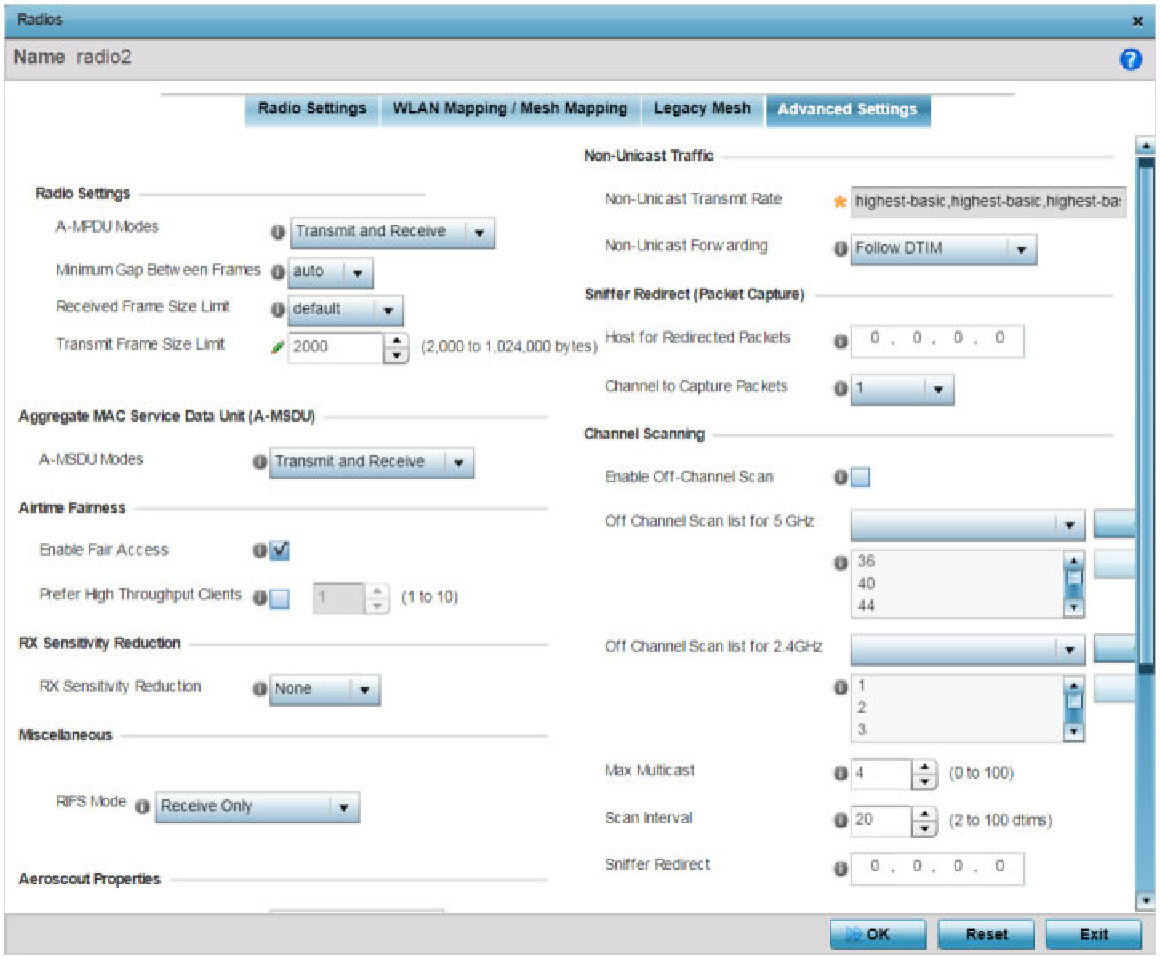
Advanced Settings

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.



Name radio2

Radio Settings

A-MPDU Modes: Transmit and Receive
Minimum Gap Between Frames: auto
Received Frame Size Limit: default
Transmit Frame Size Limit: 2000 (2,000 to 1,024,000 bytes)

Aggregate MAC Service Data Unit (A-MSDU)

A-MSDU Modes: Transmit and Receive

Airtime Fairness

Enable Fair Access ☑
Prefer High Throughput Clients ☐ 1 (1 to 10)

RX Sensitivity Reduction

RX Sensitivity Reduction: None

Miscellaneous

RIFS Mode: Receive Only

Aeroscout Properties

Non-Unicast Traffic

Non-Unicast Transmit Rate: highest-basic,highest-basic,highest-ba
Non-Unicast Forwarding: Follow DTIM

Sniffer Redirect (Packet Capture)

Host for Redirected Packets: 0 . 0 . 0 . 0
Channel to Capture Packets: 1

Channel Scanning

Enable Off-Channel Scan ☐
Off Channel Scan list for 5 GHz: 36, 40, 44
Off Channel Scan list for 2.4GHz: 1, 2, 3
Max Multicast: 4 (0 to 100)
Scan Interval: 20 (2 to 100 dtims)
Sniffer Redirect: 0 . 0 . 0 . 0

Figure 246: 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: • **`0`** – Configures the minimum gap as 0 microseconds • **`1`** – Configures the minimum gap as 1 microseconds • **`2`** – Configures the minimum gap as 2 microseconds • **`4`** – Configures the minimum gap as 4 microseconds • **`8`** – Configures the minimum gap as 8 microseconds • **`16`** – Configures the minimum gap as 16 microseconds • **`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: • **`8191`** - Advertises the maximum received frame size limit as 8191 bytes. • **`16383`** - Advertises the maximum received frame size limit as 16383 bytes. • **`32767`** - Advertises the maximum received frame size limit as 32767 bytes. • **`65535`** - Advertises the maximum received frame size limit as 65535 bytes. • **`128000`** - Advertises the maximum received frame size limit as 128000 bytes. • **`256000`** - Advertises the maximum received frame size limit as 256000 bytes. • **`512000`** - Advertises the maximum received frame size limit as 512000 bytes. • **`1024000`** - Advertises the maximum received frame size limit as 1024000 bytes. • **`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. For 802.11ac capable APs, the range is as follows: • **`2000 - 65,535 bytes`** - For radio 1, the range is 2000 - 65,535 bytes. The default value is 65,535 bytes. Note: 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. • **`2000 - 1,024,000 bytes`** - For radio 2, the range is 2000 - 1,024,000 bytes. The default value is 1,024,000 bytes. Note: The WiNG 802.11ac capable APs are: AP7522, AP7532, AP7562, AP7602, AP7612, AP7632, AP7662, AP8432, and AP8533. For non 802.11ac capable APs the range is as follows: • **`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.

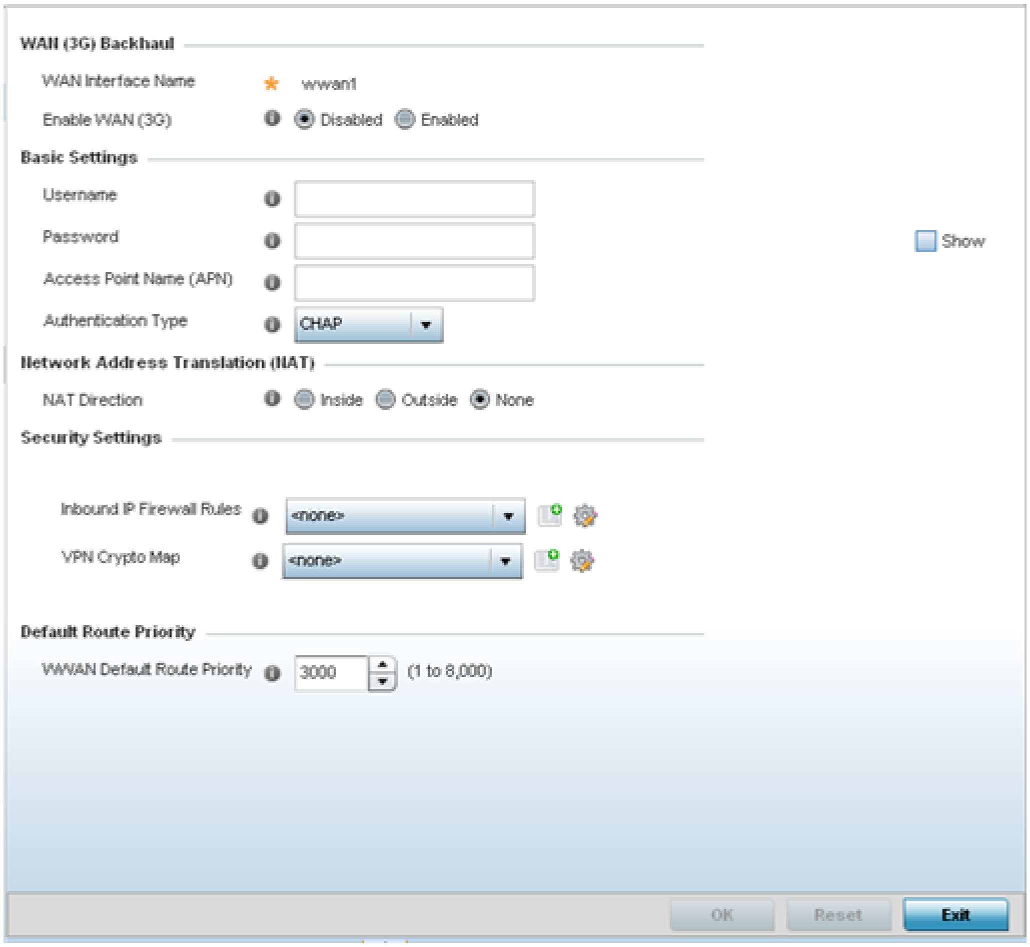
11 Select **OK** to save the changes to the advanced settings screen. Select **Reset** to revert to the last saved configuration.

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 AP7131N model access points and RFS4000 controllers utilize a PCI Express card slot that supports 3G WWAN cards. 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 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.

To define a WAN Backhaul configuration:

1 Select **Configuration** → **Profiles** → **Interface**.
2 Expand the **Interface** menu to display its submenu options.
3 Select **WAN Backhaul**.



WAN (3G) Backhaul
WAN Interface Name: wwan1
Enable WAN (3G): ● Disabled ○ Enabled
Basic Settings
Username:
Password:
Access Point Name (APN):
Authentication Type: CHAP
☐ Show
Network Address Translation (NAT)
NAT Direction: ○ Inside ○ Outside ● None
Security Settings
Inbound IP Firewall Rules: <none>
VPN Crypto Map: <none>
Default Route Priority
WWAN Default Route Priority: 3000 (1 to 8,000)

4 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	Displays the WAN Interface name for the WAN 3G Backhaul card.
Enable WAN (3G)	Check this box to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work.

5 Set the following authentication parameters from within the **Basic Settings** field:

Username	Provide a username for authentication support by the cellular data carrier.
Password	Provide a 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 pull-down menu to specify authentication type used by your cellular data provider. Supported authentication types are *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.

6 Define the following NAT parameters from within the **Network Address Translation (NAT)** field:

NAT Direction	Define the Network Address Translation (NAT) direction. Options include: **`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 controller or service platform 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 network. **`None`** - No NAT activity takes place. This is the default setting.

7 Set the following security parameters from within the **Security Settings** field:

IP Inbound Firewall Rules	Use the drop-down menu to select an inbound IP ACL to associate with traffic on the WAN backhaul. If an appropriate IP ACL does not exist, select the Add button to create a new one.
VPN Crypto Map	If necessary, specify a crypto map for the wireless WAN. A crypto map can be up to 256 characters long. If a suitable crypto map is not available, click the Create button to configure a new one.

8 Define the following route parameters from within the **Default Route Priority** field:

WWAN Default Route Priority	Use the spinner control to define a priority from 1 - 8,000 for the default route learned by the wireless WAN. The default value is 3000.

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

PPPoE Configuration

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows an access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) 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 a point-to-point connection, each PPPoE session determines 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 Wired WAN were to fail.

Note

Devices with PPPoE enabled continue to support VPN, NAT, PBR and 3G failover over the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

Note

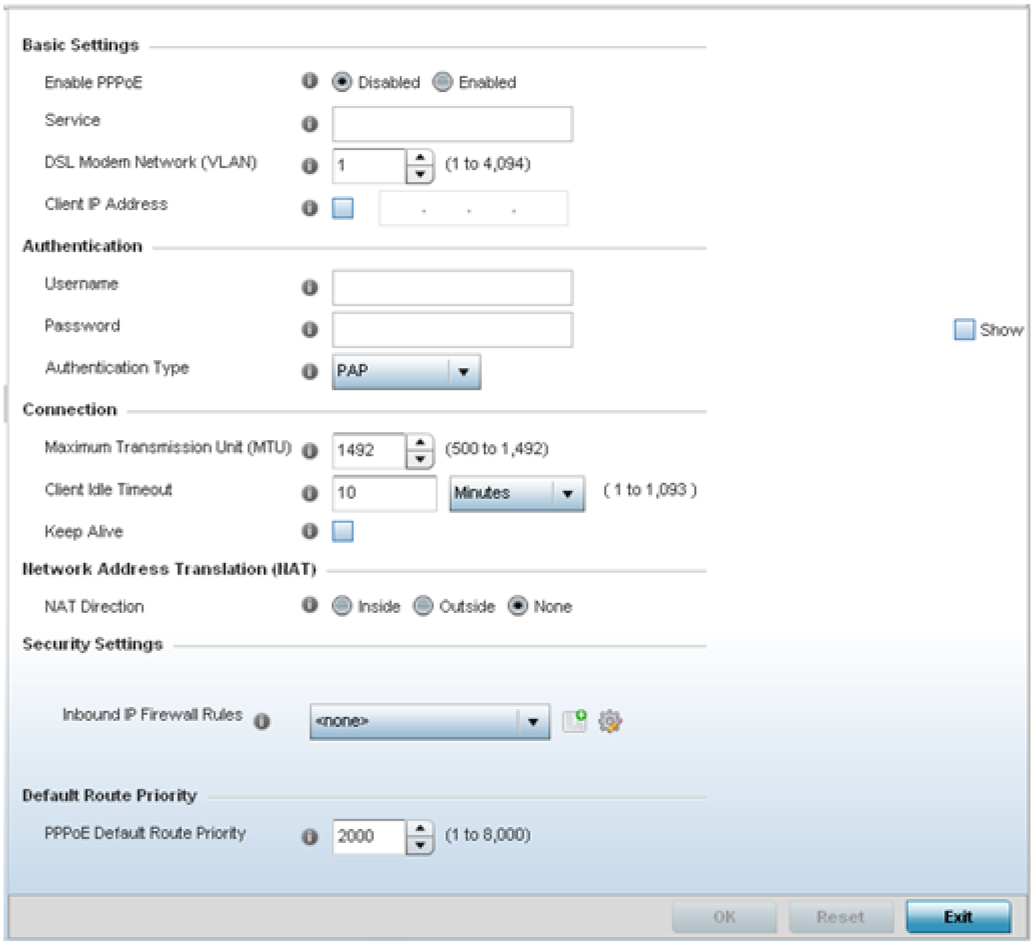
PPPoE is supported on AP 6522, AP 6532, AP 6562, and AP 8132 models, and is not available on AP 6521 and AP 6511 model access points.

When PPPoE client operation is enabled, a requesting client discovers an available server and establishes a PPPoE link for its traffic flow. 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, client 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.

To create a PPPoE point-to-point configuration

1. Select **Configuration** → **Profiles** → **Interface**.
2. Expand the **Interface** menu to display its submenu options.
3. Select **PPPoE**.



Basic Settings

Enable PPPoE ● Disabled ○ Enabled

Service

DSL Modem Network (VLAN) 1 (1 to 4,094)

Client IP Address ☐

Authentication

Username

Password ☐ Show

Authentication Type PAP

Connection

Maximum Transmission Unit (MTU) 1492 (500 to 1,492)

Client Idle Timeout 10 Minutes (1 to 1,093)

Keep Alive ☐

Network Address Translation (NAT)

NAT Direction ○ Inside ○ Outside ● None

Security Settings

Inbound IP Firewall Rules <none>

Default Route Priority

PPPoE Default Route Priority 2000 (1 to 8,000)

4 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client

Enable PPPoE	Select *Enable* 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)	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 - 4,094. The default VLAN is VLAN1
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.
Authentication Type	Use the drop-down menu to specify 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 *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.` 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 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 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 or outside).

8 Define the following **Security Settings** for the PPPoE configuration:

Inbound IP 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.
VPN Crypto Map	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

9 Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE.

Select a priority from 1 - 8,000. The default setting is 2,000.

10 Select **OK** to save the changes to the PPPoE screen. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

Overriding Bluetooth Configuration

AP-8432 and AP-8533 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.

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 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.

To define a Bluetooth radio interface configuration:

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

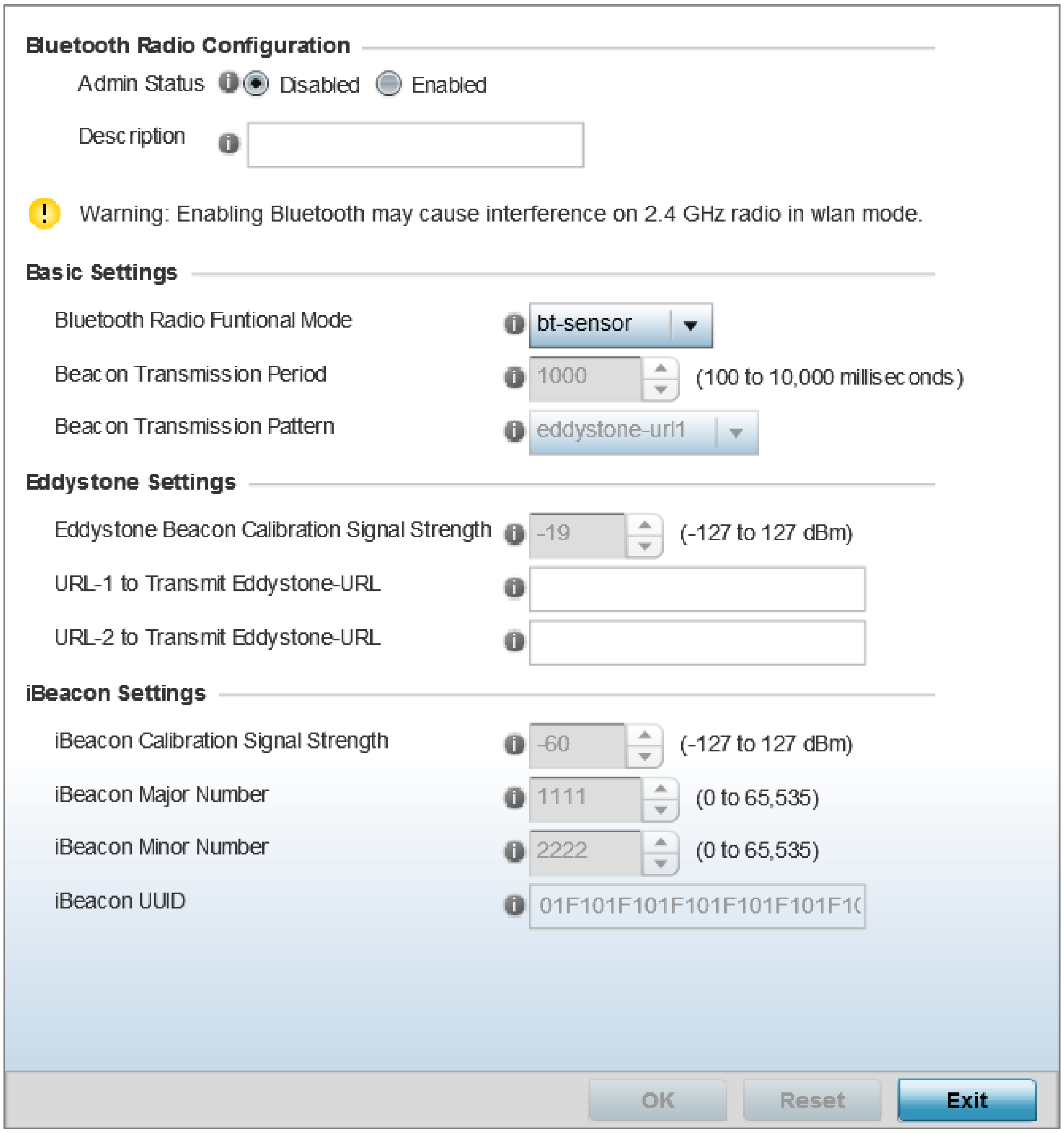
The Device Configuration screen displays in the right-hand UI. This screen lists managed devices or peer controllers, service platforms, or access points.

2 Select a target access point in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the Device Configuration screen.

3 Select **Profile Overrides** → **Interface**.

4 Select **Bluetooth**.



Bluetooth Radio Configuration

Admin Status ● Disabled ○ Enabled

Description

Warning: Enabling Bluetooth may cause interference on 2.4 GHz radio in wlan mode.

Basic Settings

Bluetooth Radio Funtional Mode: bt-sensor

Beacon Transmission Period: 1000 (100 to 10,000 milliseconds)

Beacon Transmission Pattern: eddystone-url1

Eddystone Settings

Eddystone Beacon Calibration Signal Strength: -19 (-127 to 127 dBm)

URL-1 to Transmit Eddystone-URL

URL-2 to Transmit Eddystone-URL

iBeacon Settings

iBeacon Calibration Signal Strength: -60 (-127 to 127 dBm)

iBeacon Major Number: 1111 (0 to 65,535)

iBeacon Minor Number: 2222 (0 to 65,535)

iBeacon UUID: 01F101F101F101F101F101F1(

Figure 247: Profile Overrides - Bluetooth Screen

5 Set the following Bluetooth Radio Configuration parameters:

Admin Status	**`Enable`** or **`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.

6 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`**. Use **`bt-sensor`** mode for ADSP Bluetooth classic sensing. Use **`le-beacon`** mode to have the access point transmit both ibeacon and Eddystone-URL low energy beacons. The *bt-sensor* option is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. 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`**. 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. 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.

7 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. The encoding process is for getting the URL to fit within the beacon's payload.
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. The encoding process is for getting the URL to fit within the beacon's payload.

8 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 UUID. The UUID classification contains 32 hexadecimal digits The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

9 Click **OK** to save the changes made to the Bluetooth configuration.

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

Profile Interface Deployment Considerations

Before defining a profile's interface configuration (supporting Ethernet port, Virtual Interface, port channel and access point radio configurations) refer to the following deployment guidelines to ensure these configuration are optimally effective:

- Power over Ethernet is supported on RFS 4000 and RFS 6000 model controllers and NX 4524and NX 6524 model service platforms only. When enabled, the 802.3af PoE is supported on each ge ports.
- When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when a controller or service platform is accessed from a subnet not directly connected and the default route was set from DHCP.
- Take care not to modify an access point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a controller or service platform profile, or risk the access point having a configuration independent from the profile until the profile can be uploaded to the access point once again.

Profile Network Configuration

Setting a profile's network configuration is a large task comprised of numerous administration activities.

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

- Setting a Profile's DNS Configuration on page 608
- ARP Configuration on page 609
- L2TPV3 Configuration on page 610
- GRE Tunnel Configuration on page 619
- IGMP Snooping on page 621
- MLD Snooping Configuration on page 623
- QoS Traffic Shaping Basic Configuration on page 625
- IPv4 Routing Configuration on page 630
- OSPF on page 634
- Forwarding Database on page 654
- Bridge VLAN Configuration on page 655
- Cisco Discovery Protocol Configuration on page 663
- Link Layer Discovery Protocol Configuration on page 664
- Miscellaneous Network Configuration on page 665

- Alias Configuration on page 666
- IPv6 Neighbor Configuration on page 675

Before beginning any of the profile network configuration activities described in the sections above, review the configuration and deployment considerations available in Profile Network Configuration and Deployment Considerations.

Setting a Profile's DNS Configuration

Domain Naming System (DNS) 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.

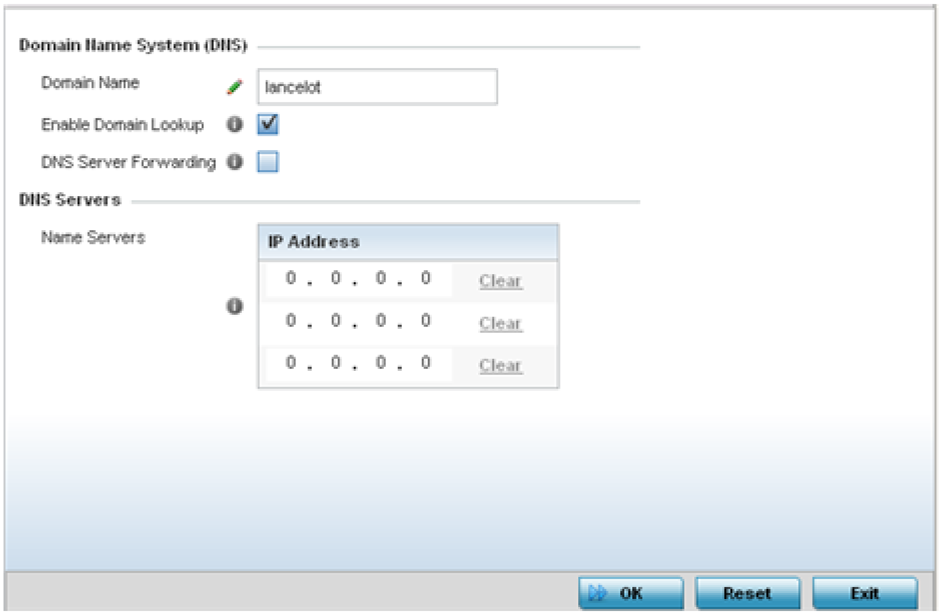
As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (for example, *www.domainname.com*).

To define the DNS configuration:

1 Select **Configuration** → **Profiles** → **Network**.

2 Expand the **Network** menu to display its submenu options.

3 Select **DNS**.



Domain Name System (DNS)

Domain Name: lancelot

Enable Domain Lookup ☑

DNS Server Forwarding ☐

DNS Servers

Name Servers

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

4 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.

5 Set the following DNS Servers configuration data:

Name Servers	Provide a list of up to three DNS servers to forward DNS queries if local DNS resources are unavailable. The DNS name servers are used to resolve IP addresses. Use the *Clear* link (next to each DNS server) to clear the DNS name server's IP address from the list.

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

ARP Configuration

Address Resolution Protocol (ARP) 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.

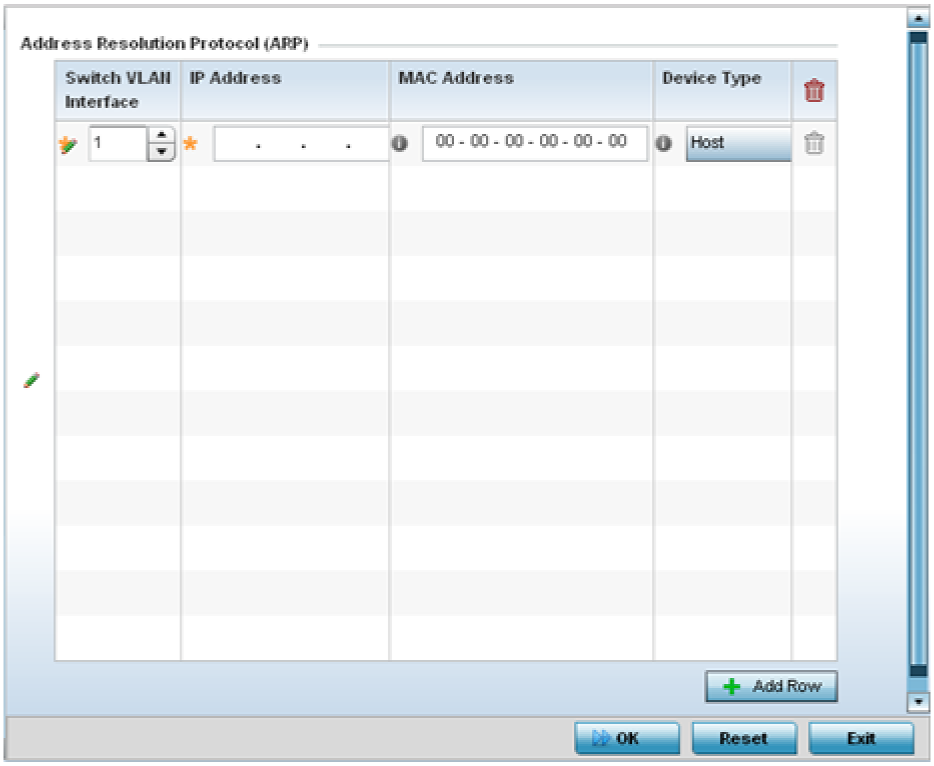
When an incoming packet destined for a host arrives, ARP is used to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to its destination. If 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 Select **Configuration** → **Profiles** → **Network**.

2 Expand the **Network** menu and select **ARP**.

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 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.

5 To add additional ARP settings select **+ Add Row** and enter the configuration information.

6 Select the **OK** button located at the bottom right of the screen to save the changes to the ARP configuration. Select **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.

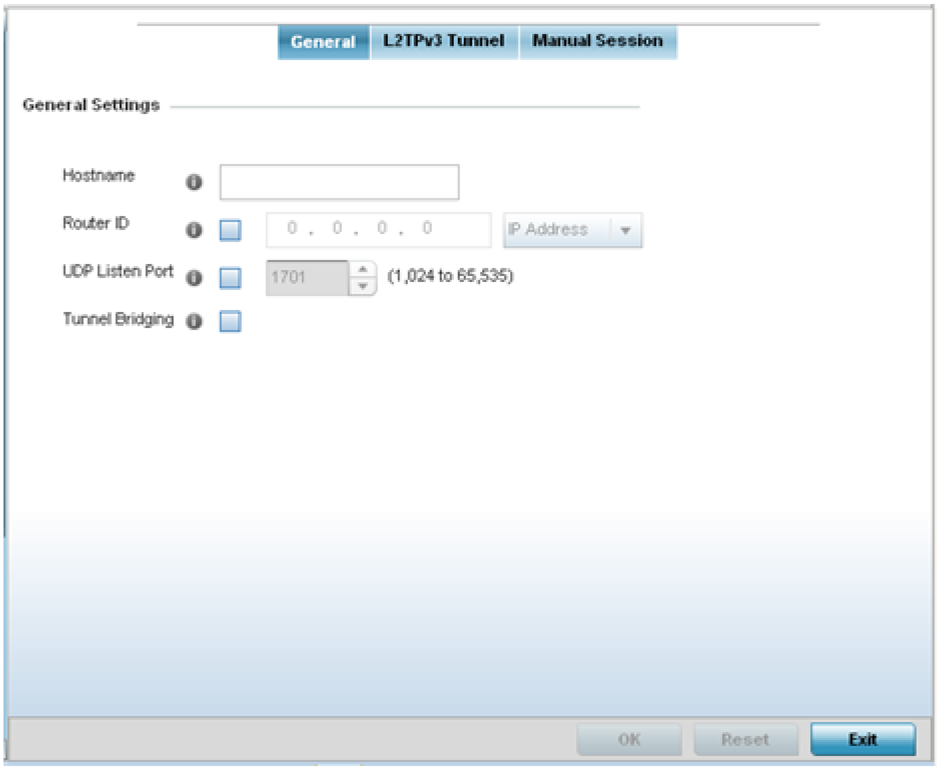
Note
If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

General

To define an L2TPV3 configuration for a profile:

1. Select **Configuration** → **Profiles**.
2. Expand the **Network** menu and select L2TPv3.

   The General tab displays by default.



3 Set the following **General Settings** for a L2TPv3 profile configuration:

Host Name	Define a 64 character maximum host name 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 virtual port used for listening to incoming traffic. Select a port from 1,024 - 65,353.
Device Type	Select this option to *enable* or *disable* bridge packets between two tunnel end points. This setting is disabled by default.

4 In the **Logging Settings** filed, configure the following settings:

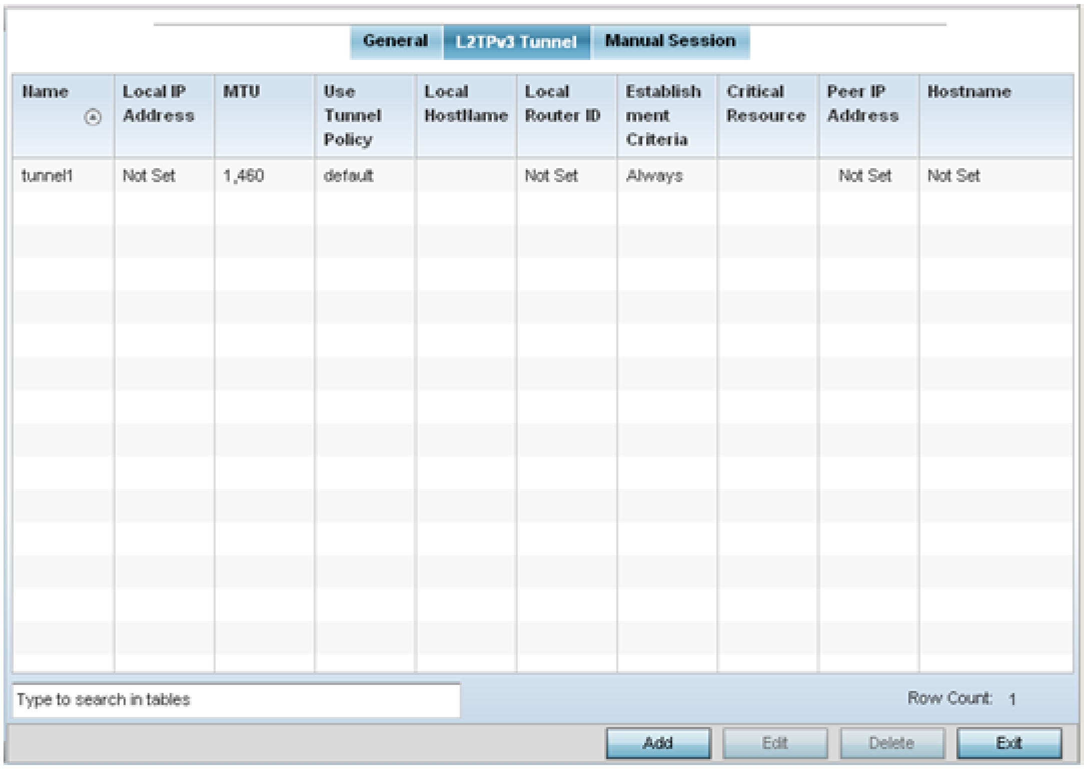
Enable Logging	Select this option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is disabled by default.
IP Address	Optionally use a peer tunnel ID address to capture and log L2TPv3 events.
Hostname	If 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.

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



Name	Local IP Address	MTU	Use Tunnel Policy	Local HostName	Local Router ID	Establishment Criteria	Critical Resource	Peer IP Address	Hostname
tunnel1	Not Set	1,460	default		Not Set	Always		Not Set	Not Set

2 Review the following L2TPv3 tunnel configuration data:

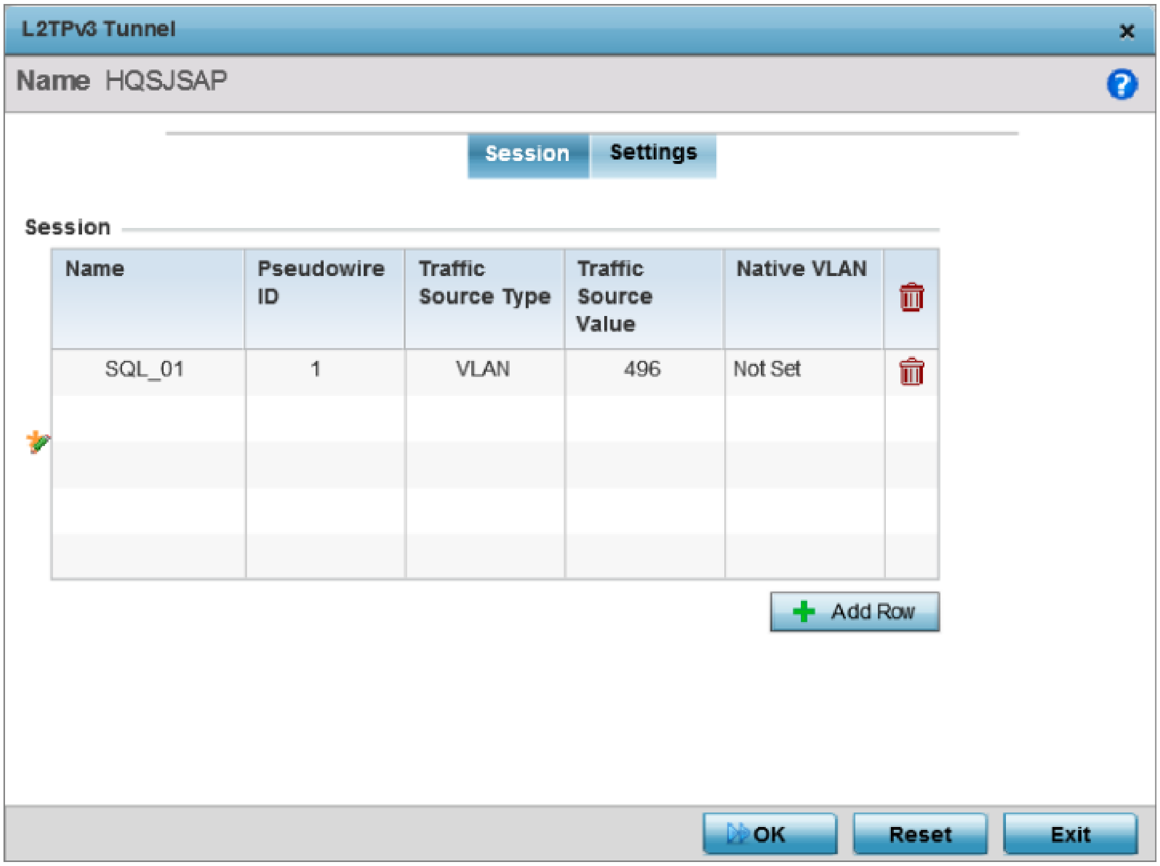
Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation.
Local IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is 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.



Name	Pseudowire ID	Traffic Source Type	Traffic Source Value	Native VLAN
SQL_01	1	VLAN	496	Not Set

Figure 248: 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.

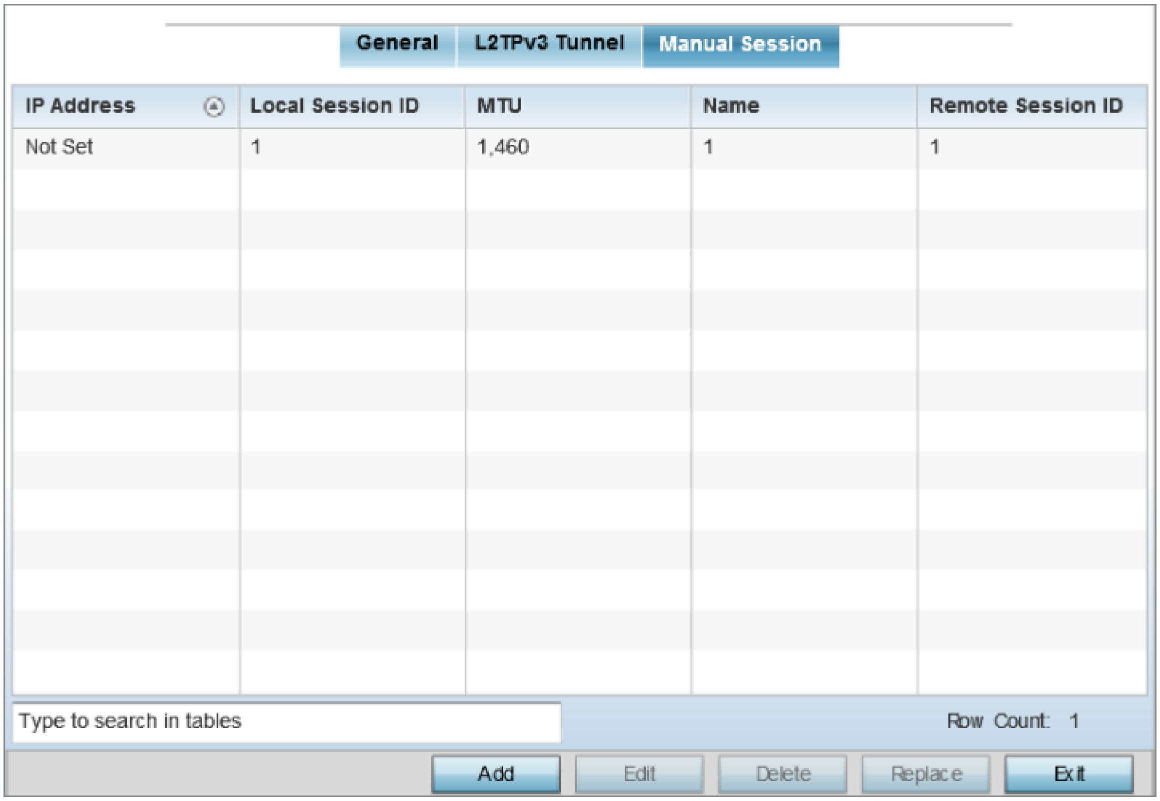
8 Select OK to save the changes within the L2TP Tunnel screen. Select Reset to revert the screen to its last saved configuration.

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.



IP Address	Local Session ID	MTU	Name	Remote Session ID
Not Set	1	1,460	1	1

Figure 249: L2TPv3 Tunnel - Manual Session Configuration Screen

2 Refer to the following manual session configurations to determine whether one should be created or modified:

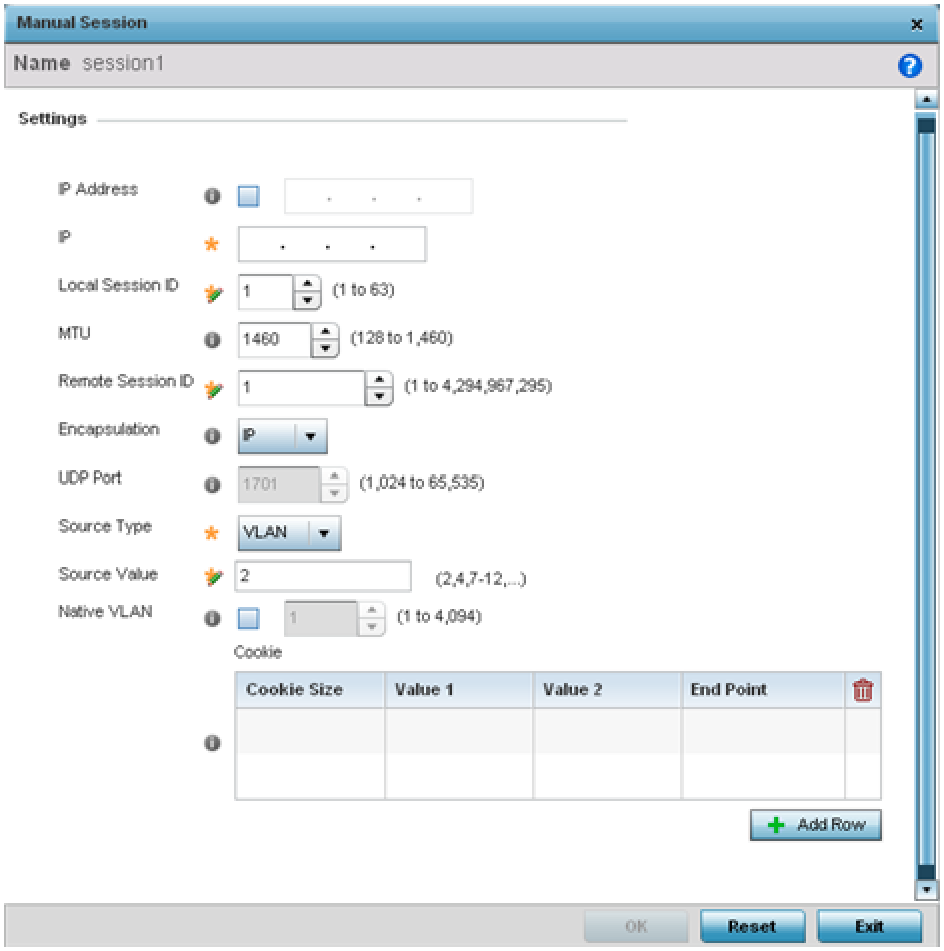
IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable 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.



Name session1

IP Address ☐ . . .

IP . . .

Local Session ID 1 (1 to 63)

MTU 1460 (128 to 1,460)

Remote Session ID 1 (1 to 4,294,967,295)

Encapsulation IP

UDP Port 1701 (1,024 to 65,535)

Source Type VLAN

Source Value 2 (2,4,7-12,...)

Native VLAN ☐ 1 (1 to 4,094)

Cookie

Cookie Size	Value 1	Value 2	End Point

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**.

The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

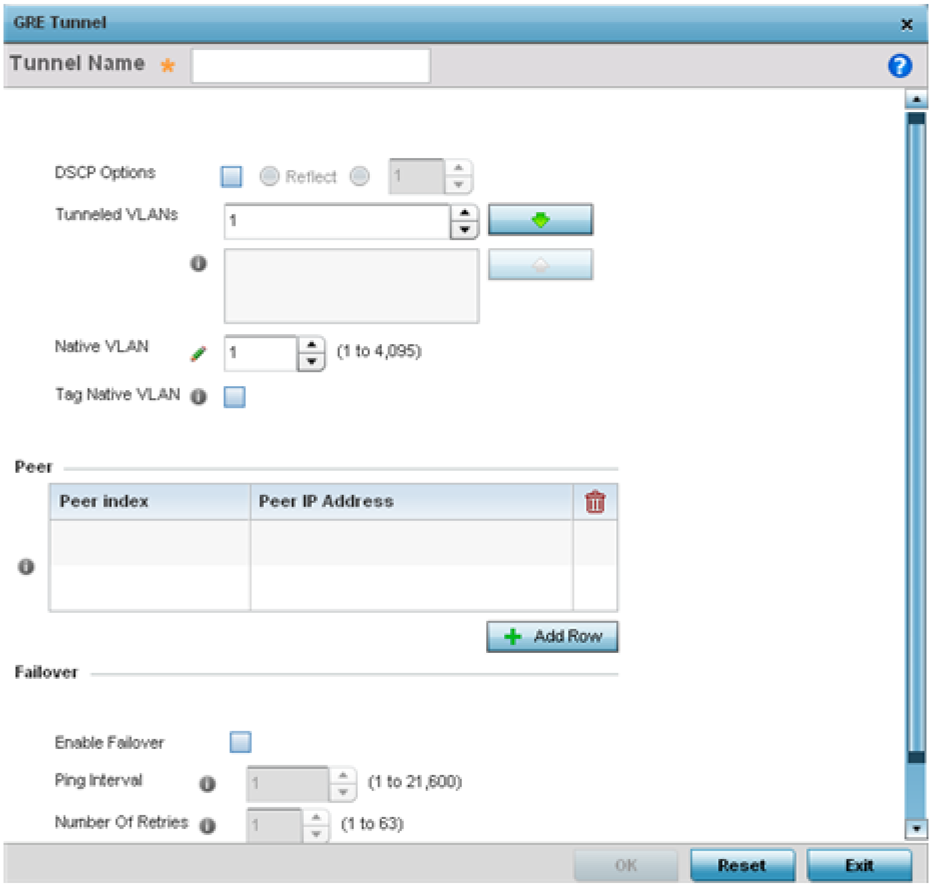
2 Select a device from the list displayed.

The selected device's configuration screen 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.



Tunnel Name *

DSCP Options ☐ ○ Reflect ○ 1

Tunneled VLANs 1

Native VLAN 1 (1 to 4,095)

Tag Native VLAN ☐

Peer index	Peer IP Address

Enable Failover ☐

Ping Interval 1 (1 to 21,600)

Number Of Retries 1 (1 to 63)

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.

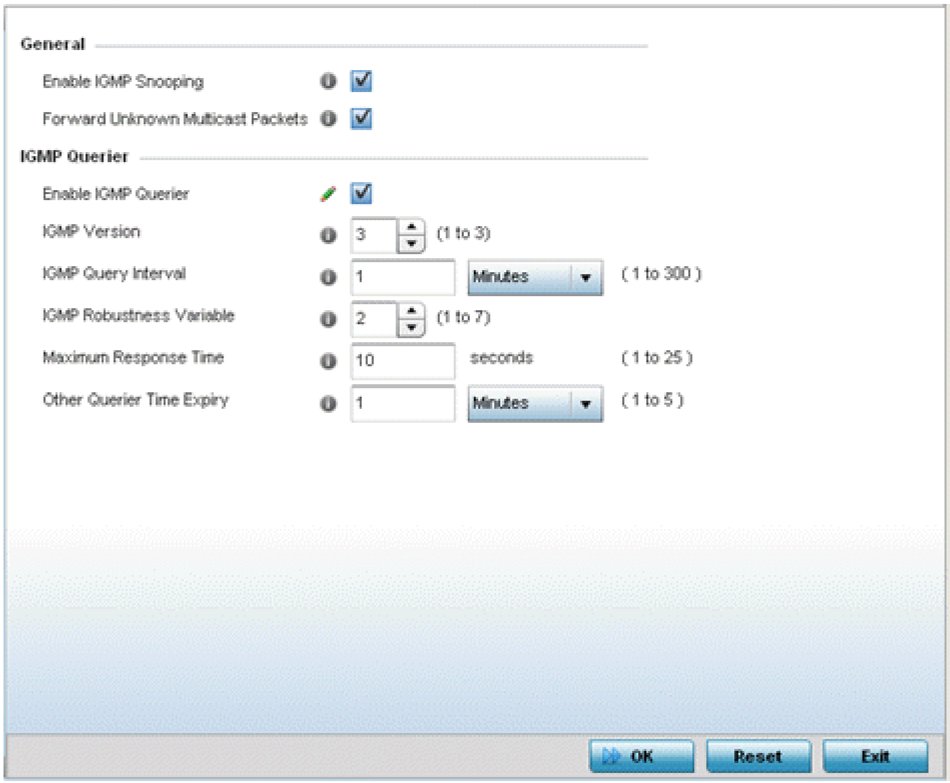
Click **Reset** to revert to the last saved configuration.

IGMP Snooping

The *Internet Group Management Protocol* (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 IGMP settings:

1 Select **Configuration** → **Profiles** → **Network**.
2 Expand the **Network** menu and select **IGMP Snooping**.



General

Enable IGMP Snooping ☑
Forward Unknown Multicast Packets ☑

IGMP Querier

Enable IGMP Querier ☑
IGMP Version 3 (1 to 3)
IGMP Query Interval 1 Minutes (1 to 300)
IGMP Robustness Variable 2 (1 to 7)
Maximum Response Time 10 seconds (1 to 25)
Other Querier Time Expiry 1 Minutes (1 to 5)

3 Set the following **General** IGMP Snooping parameters for the Bridge VLAN configuration:

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..

4 Set the following **IGMP Querier** parameters for the profile's bridge VLAN 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.

5. Select the **OK** button to save the changes to the IGMP Snooping tab. Select **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.

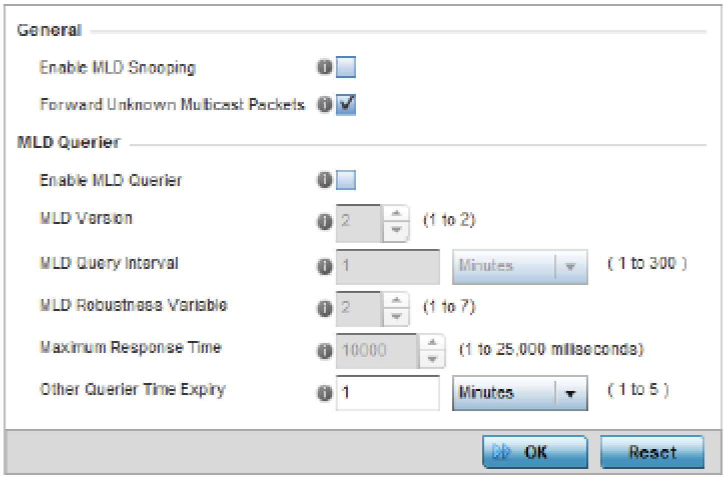
MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or access point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or access point 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** → **Profiles** → **Network**.

   The Device Configuration screen displays. This screen lists wireless controllers, service platforms and access points within the managed network.

2 Expand the **Network** node and select **MLD Snooping**.



General

Enable MLD Snooping ☐

Forward Unknown Multicast Packets ☑

MLD Querier

Enable MLD Querier ☐

MLD Version 2 (1 to 2)

MLD Query Interval 1 Minutes (1 to 300)

MLD Robustness Variable 2 (1 to 7)

Maximum Response Time 10000 (1 to 25,000 milliseconds)

Other Querier Time Expiry 1 Minutes (1 to 5)

Figure 250: Profile - Network MLD Snooping screen

3 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.

4 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.

5 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 QoS *(Quality of Service)* screens to define WLAN and device radio QoS configurations. The QoS configuration 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 priority of service to some packets over others. 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 DSCP *(Differentiated Service Code Point)* 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 applied to a packet.

1 Expand the **Network** node and select **Quality of Service (QoS)**.

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.

The Traffic Shaping screen displays with the Basic Configuration tab selected by default.

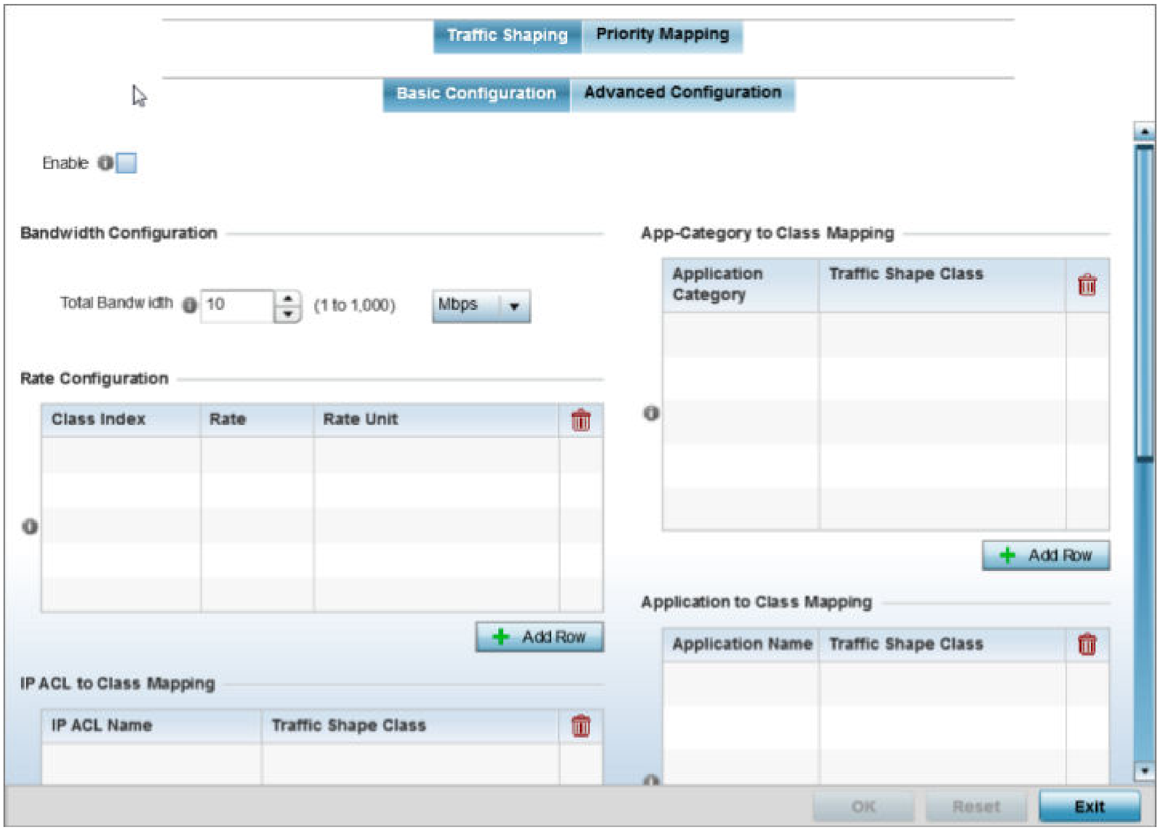


Figure 251: Profile Overrides - Network QoS Traffic Shaping Basic Configuration Screen

2 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

3 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.

4 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.

5 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.

6 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.

7 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 509.

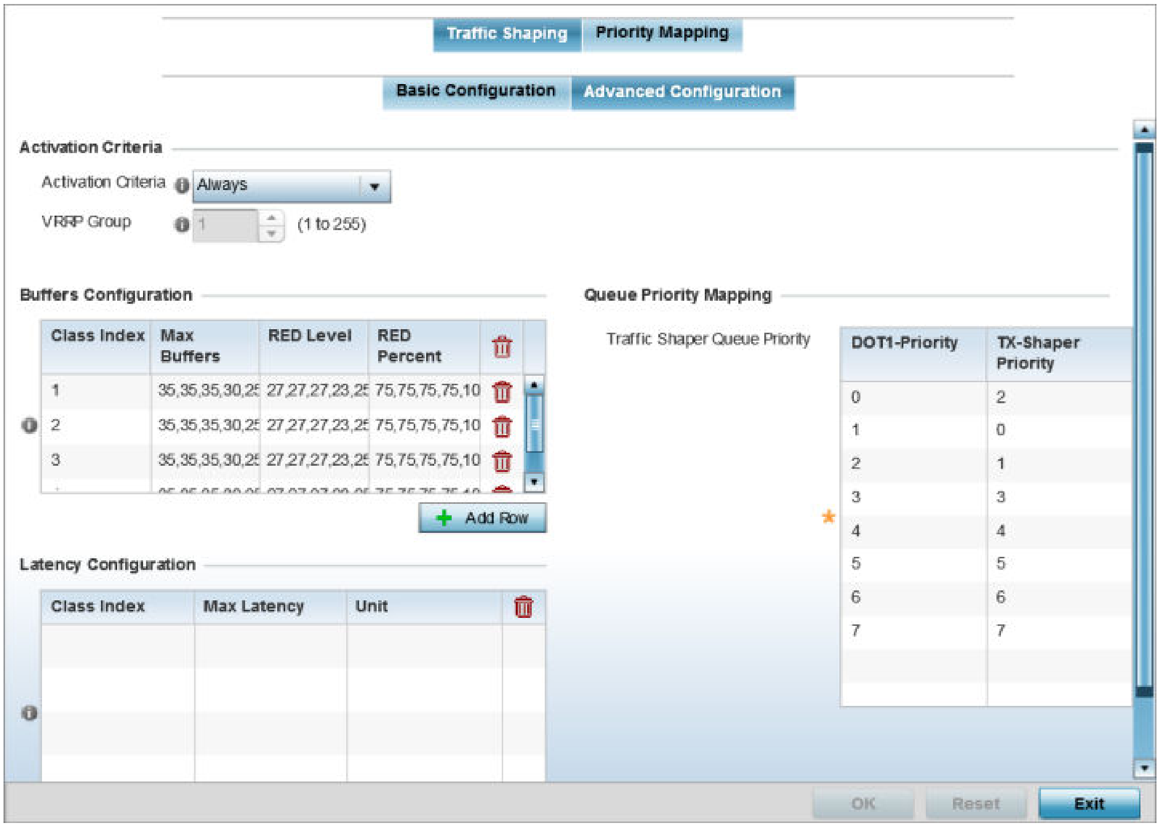
8 Refer to the Application to Class Mapping table and select + Add Row to apply an application to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application and its traffic shaper class. For more information on creating an application, refer to Application on page 509.

9 Select the **OK** button located to save the changes to the traffic shaping basic configuration. 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.



Activation Criteria

Activation Criteria: Always

VRRP Group: 1 (1 to 255)

Buffers Configuration

Class Index	Max Buffers	RED Level	RED Percent
1	35,35,35,30,2	27,27,27,23,2	75,75,75,75,10
2	35,35,35,30,2	27,27,27,23,2	75,75,75,75,10
3	35,35,35,30,2	27,27,27,23,2	75,75,75,75,10

Latency Configuration

Class Index	Max Latency	Unit

Queue Priority Mapping

Traffic Shaper Queue Priority

DOT1-Priority	TX-Shaper Priority
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 252: 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.

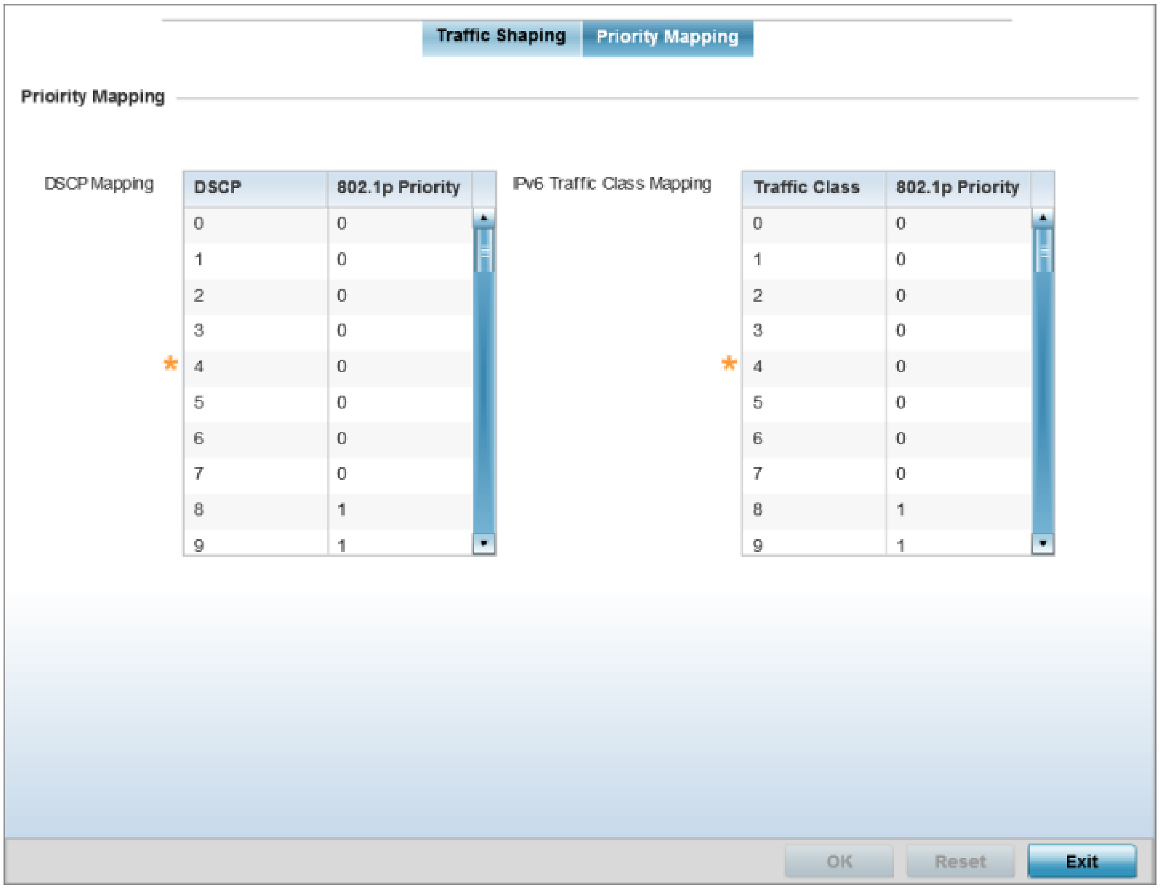
   When a new packet arrives it knows how much time to wait in the queue. If a packet takes longer than the latency value, it is dropped. By default latency is not set, so packets remain in queue for long time.
5. Refer to the **Queue Priority Mapping** table to set the traffic shaper queue priority and 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 Configuration

To configure QoS priority mapping:

1 Select the **Priority Mapping** tab.



DSCP Mapping

DSCP	802.1p Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1

IPv6 Traffic Class Mapping

Traffic Class	802.1p Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1

Figure 253: Network - Quality of Service (QoS) Screen

2 Set the following parameters for 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: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control* Use the spinner controls within the **802.1p Priority** field for each DSCP row to change its priority value.

3 Set or override the following parameters for IPv6 Traffic Class Mapping 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: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control*

4 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 create static routes:

1 Go to **Configuration** → **Profile**.

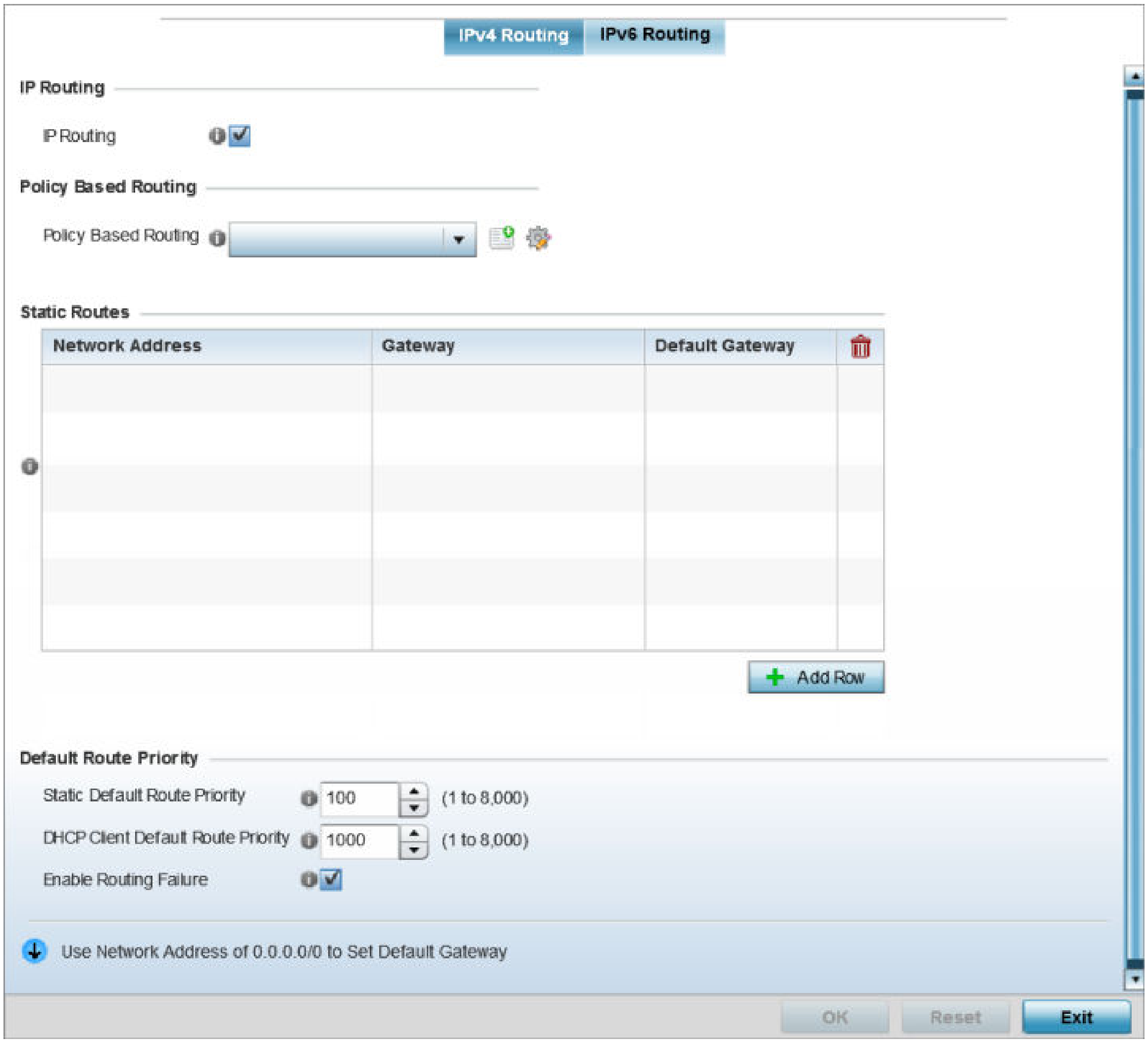
The Profile screen displays. This screen lists profiles of wireless controllers, service platforms and access points within the managed network.

2 Select a profile from the list displayed.

The selected profile's configuration screen displays.

3 Expand the **Network** node and select **Routing**.

The IPv4 Routing tab displays by default.



IP Routing ☑

Policy Based Routing

Static Default Route Priority 100 (1 to 8,000)

DHCP Client Default Route Priority 1000 (1 to 8,000)

Enable Routing Failure ☑

Use Network Address of 0.0.0.0/0 to Set Default Gateway

Figure 254: Network - Routing screen

4 Select **IP Routing** to enable static routes using IPv4 addresses. This option is enabled by default.

5 Select the **Policy Based Routing** policy to apply to this profile. 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 454.

6 Select **Add Row +** as needed to include single rows with in the static IPv4 route table.

7 Add IP addresses and network masks in the **Network Address** column of the Static Routes table.

8 Provide the **Gateway** used to route traffic.

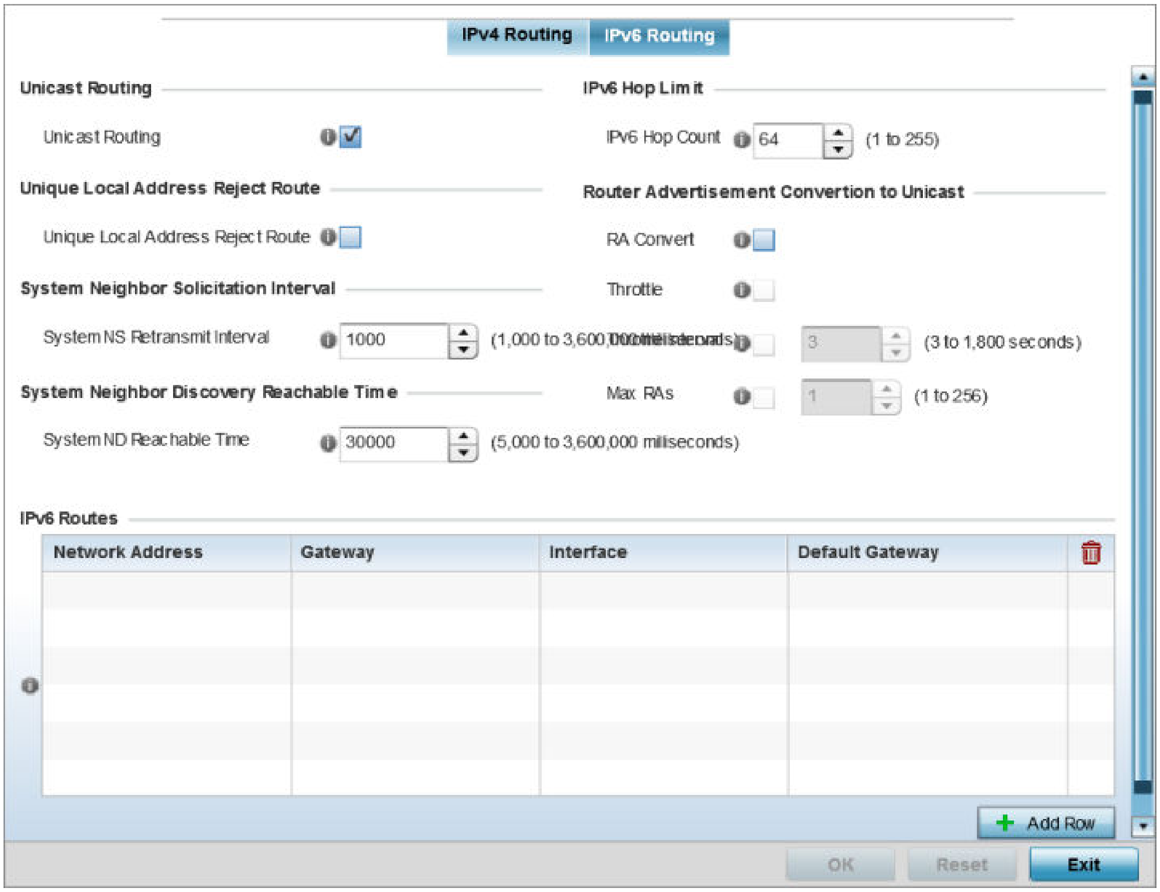
9 Refer to the Default Route Priority field and set the following parameters:

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.

IPv6 Routing Configuration

To configure IPv6 routing settings:

1 Select the **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.



Unicast Routing
Unicast Routing ☑

Unique Local Address Reject Route
Unique Local Address Reject Route ☐

System Neighbor Solicitation Interval
System NS Retransmit Interval 1000 (1,000 to 3,600,000 milliseconds)

System Neighbor Discovery Reachable Time
System ND Reachable Time 30000 (5,000 to 3,600,000 milliseconds)

IPv6 Hop Limit
IPv6 Hop Count 64 (1 to 255)

Router Advertisement Convertion to Unicast
RA Convert ☐
Throttle ☐
☐ 3 (3 to 1,800 seconds)
Max RAs ☐ 1 (1 to 256)

IPv6 Routes

Network Address	Gateway	Interface	Default Gateway

Figure 255: Static Routes Screen - IPv6 Routing Tab

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 *neighbor solicitation* (NS) 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 *neighbor discovery* (ND) 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 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 Select **+ Add Row** as needed within the IPv6 Routes table to add an additional 256 IPv6 route resources.

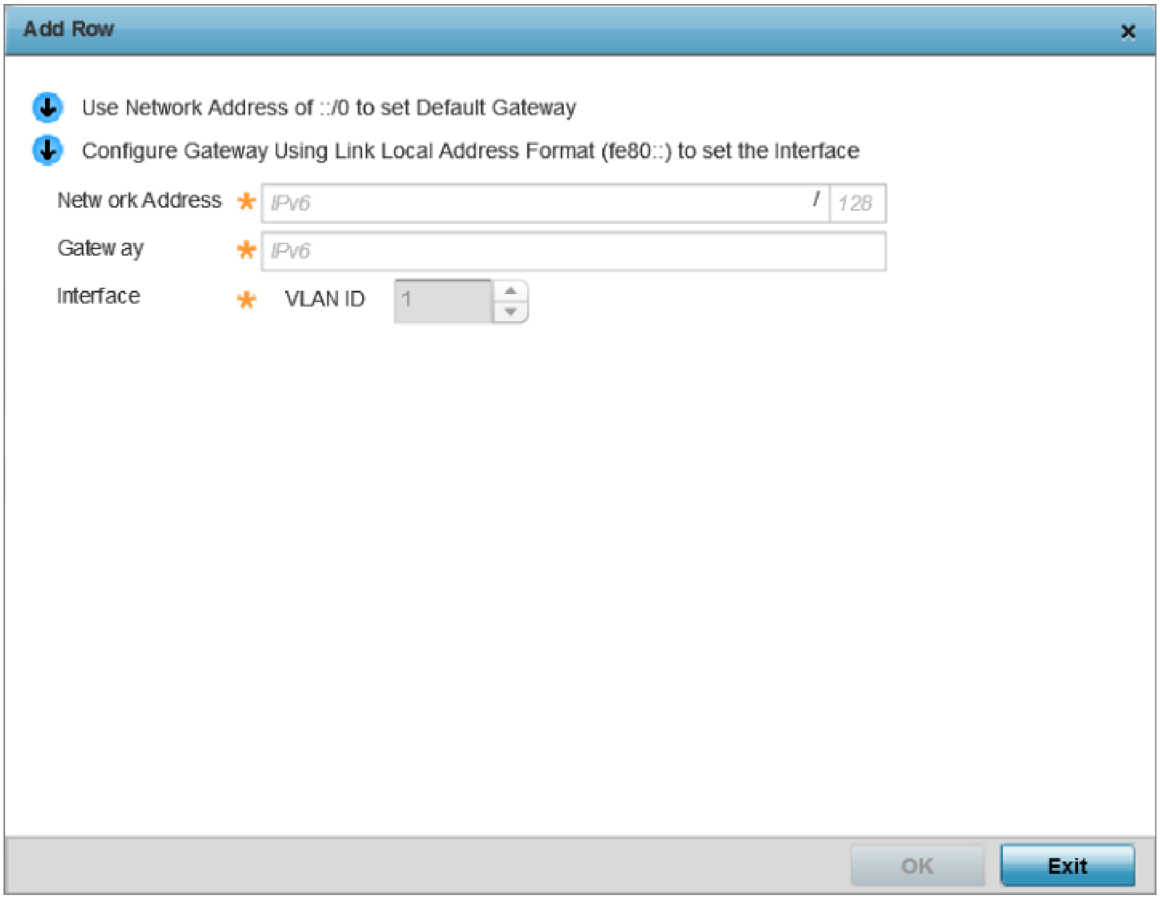

Add Row
Use Network Address of ::/0 to set Default Gateway
Configure Gateway Using Link Local Address Format (fe80::) to set the Interface
Netw ork Address
IPv6
/
128
Gatew ay
IPv6
Interface
VLAN ID
1
OK
Exit

Figure 256: Static Routes screen - Add IPv6 Route

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 the **OK** button located at the bottom right of the screen to save the changes.

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

OSPF

Open Shortest Path First (OSPF) is a link-state *interior gateway protocol* (IGP). 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.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers.

OSPF uses a route table managed by the link *cost* (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability. Setting a cost value provides a dynamic way to load balancing traffic between routes of equal cost.

An OSPF network can be subdivided into routing areas 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 by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can defined as:

stub area - A stub area is an area which does not receive route advertisements external to the *autonomous system* (AS) and routing from within the area is based entirely on a default route.

totally-stub - A totally stubby area does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there's only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.

non-stub - A non-stub area imports autonomous system external routes and send them to other areas. However. it still cannot receive external routes from other areas.

nssa - NSSA is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.

totally nssa - Totally nssa is an NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an autonomous system boundary router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

A router running 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.

OSPF Settings

To define a dynamic routing configuration:

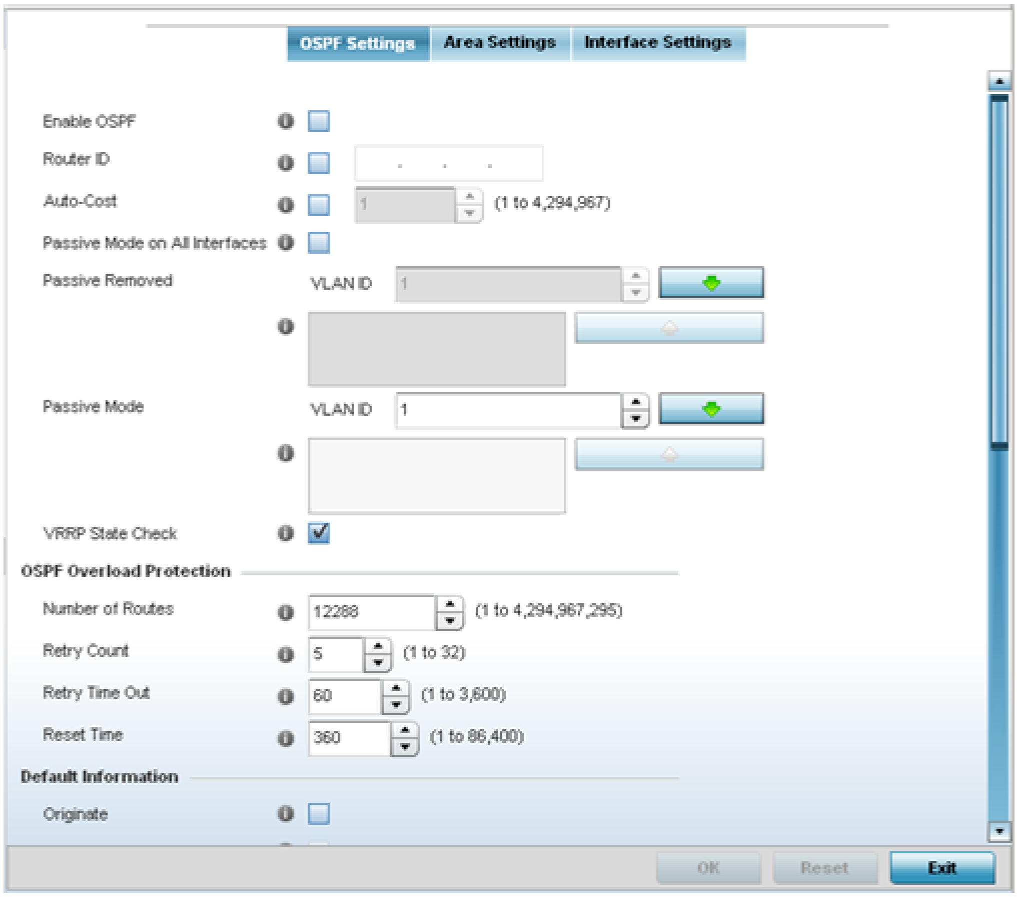
1 Go to **Configuration** → **Profile**.

The Profile screen displays. This screen lists profiles of wireless controllers, service platforms and access points within the managed network.

2 Select a profile from the list displayed.

The selected profile's configuration screen displays.

3 Expand the **Network** menu and select **OSPF.**



Enable OSPF ☐

Router ID ☐ . . .

Auto-Cost ☐ 1 (1 to 4,294,967)

Passive Mode on All Interfaces ☐

Passive Removed VLAN ID 1

Passive Mode VLAN ID 1

VRRP State Check ☑

OSPF Overload Protection

Number of Routes 12288 (1 to 4,294,967,295)

Retry Count 5 (1 to 32)

Retry Time Out 60 (1 to 3,600)

Reset Time 360 (1 to 86,400)

Default Information

Originate ☐

4 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.

5 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.

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 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*.

8 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.

9 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.

10 Set an OSPF Default Route Priority (1 - 8,000) as the priority of the default route defined from OSPF.

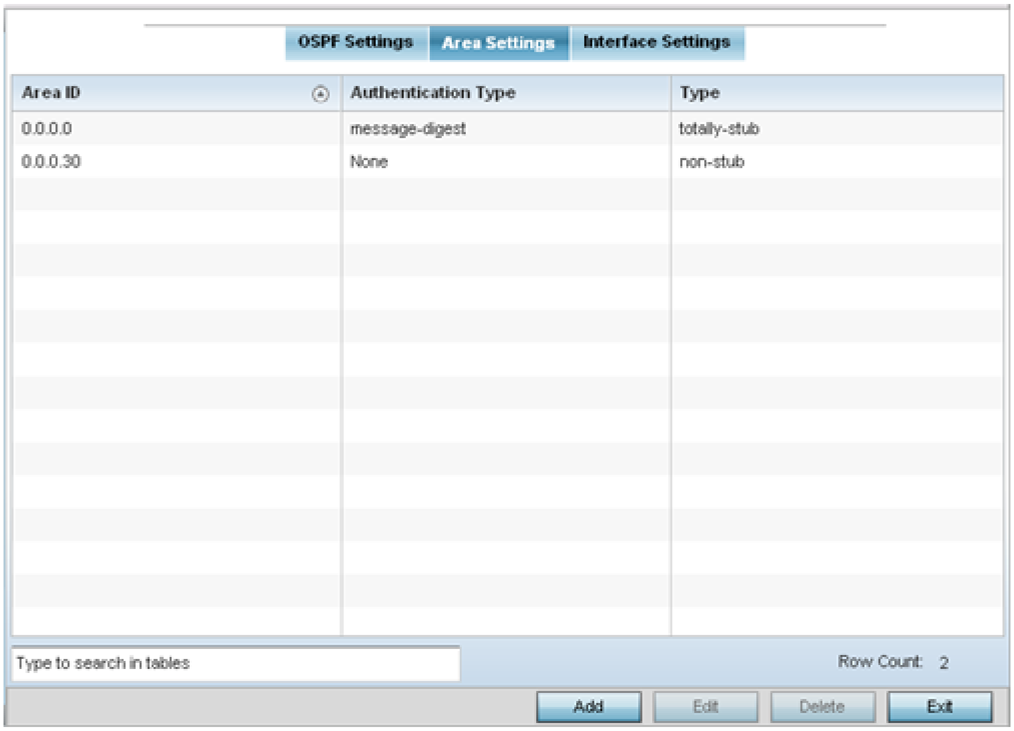
11 Click **OK** to save the changes made within the screen. Click **Reset** to revert to the last saved configuration.

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.



Area ID	Authentication Type	Type
0.0.0.0	message-digest	totally-stub
0.0.0.30	None	non-stub

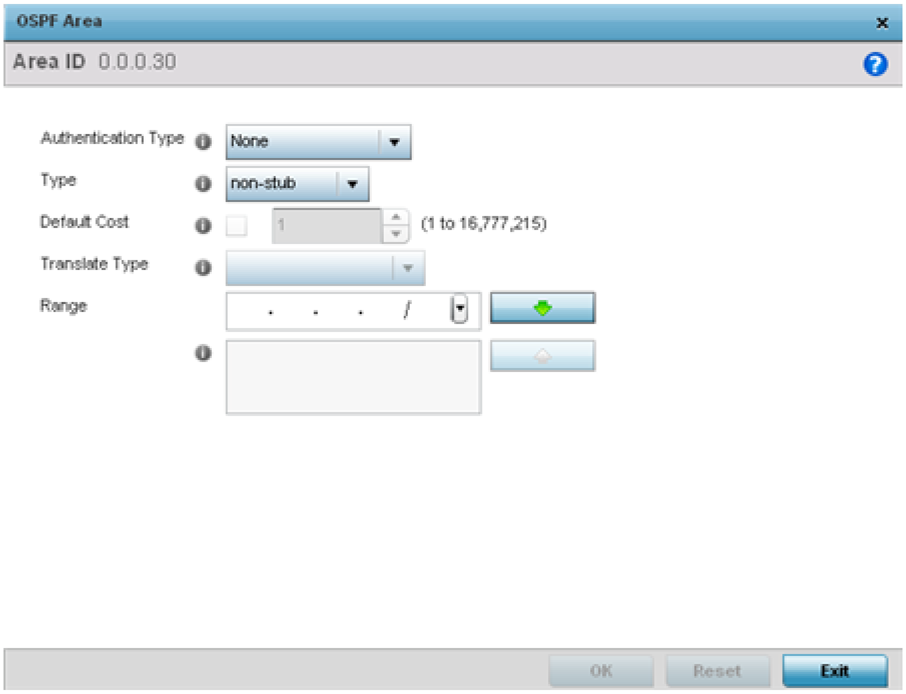
2 Review the following Area Setting configurations to determine if a new configuration needs to be added or existing settings warrants modifications:

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.



OSPF Area

Area ID 0.0.0.30

Authentication Type: None

Type: non-stub

Default Cost: 1 (1 to 16,777,215)

Translate Type

Range

2 Set the following **OSPF Area** configurations:

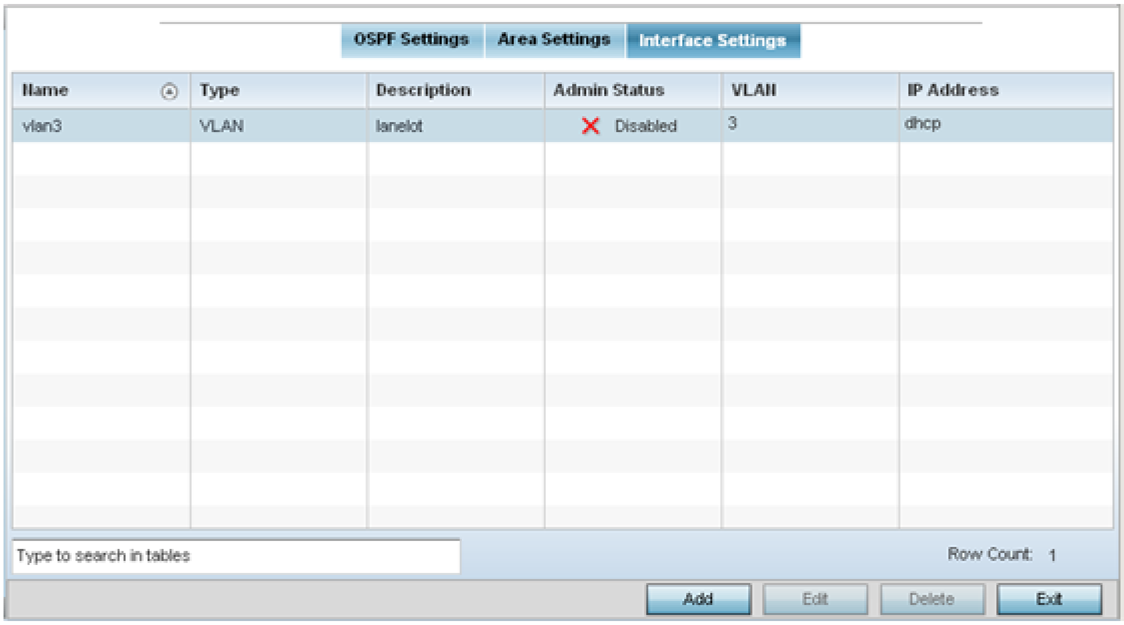
Area ID	If adding a new OSPF Area, use the drop-down menu and specify the Area ID either as an *IP address* or *Integer*.
Authentication Type	Select either *None*, *simple-password* or *message-digest* as the credential validation scheme used with the OSPF dynamic route. The default setting is None (no 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.



Name	Type	Description	Admin Status	VLAN	IP Address
vlan3	VLAN	lanelot	✗ Disabled	3	dhcp

Row Count: 1

2 Review existing Interface Settings using the following:

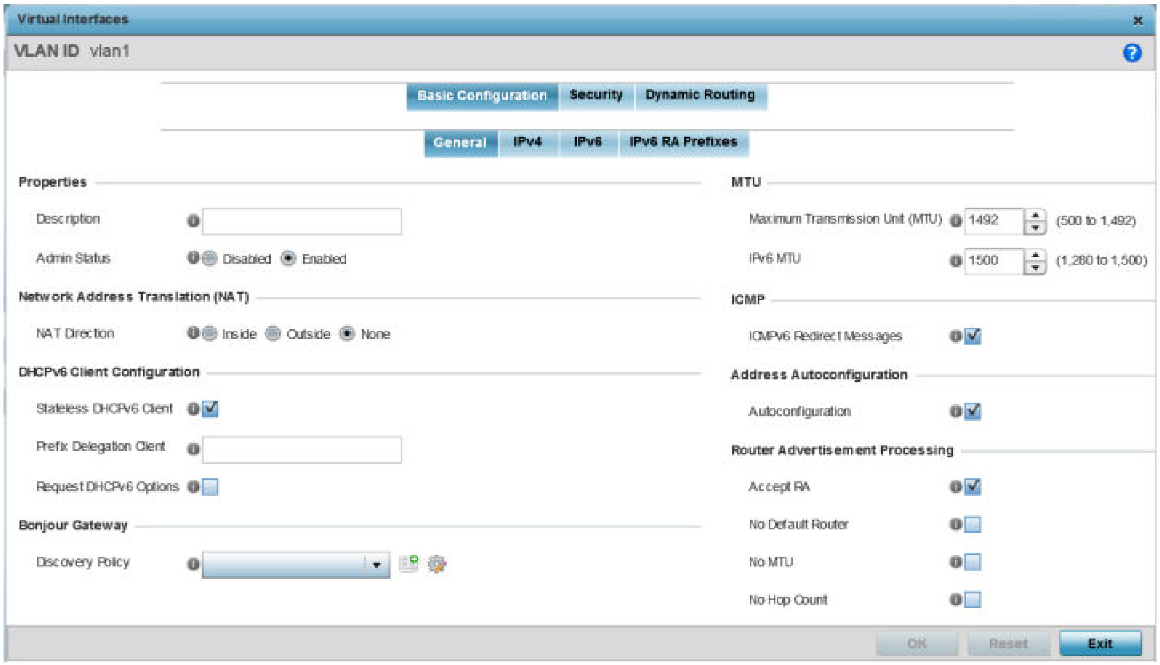
Name	Displays the name defined for the interface configuration.
Type	Displays the type of interface.
Description	Lists each interface's 32 character maximum description.
Admin Status	Displays whether Admin Status privileges have been *enabled* or *disabled* for the OSPF route's virtual interface connection.
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.



VLAN ID vlan1

Properties

Description

Admin Status ○ Disabled ● Enabled

Network Address Translation (NAT)

NAT Direction ○ Inside ○ Outside ● None

DHCPv6 Client Configuration

Stateless DHCPv6 Client ☑

Prefix Delegation Client

Request DHCPv6 Options ☐

Bonjour Gateway

Discovery Policy

MTU

Maximum Transmission Unit (MTU) 1492 (500 to 1,492)

IPv6 MTU 1500 (1,280 to 1,500)

ICMP

ICMPv6 Redirect Messages ☑

Address Autoconfiguration

Autoconfiguration ☑

Router Advertisement Processing

Accept RA ☑

No Default Router ☐

No MTU ☐

No Hop Count ☐

Figure 257: 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.

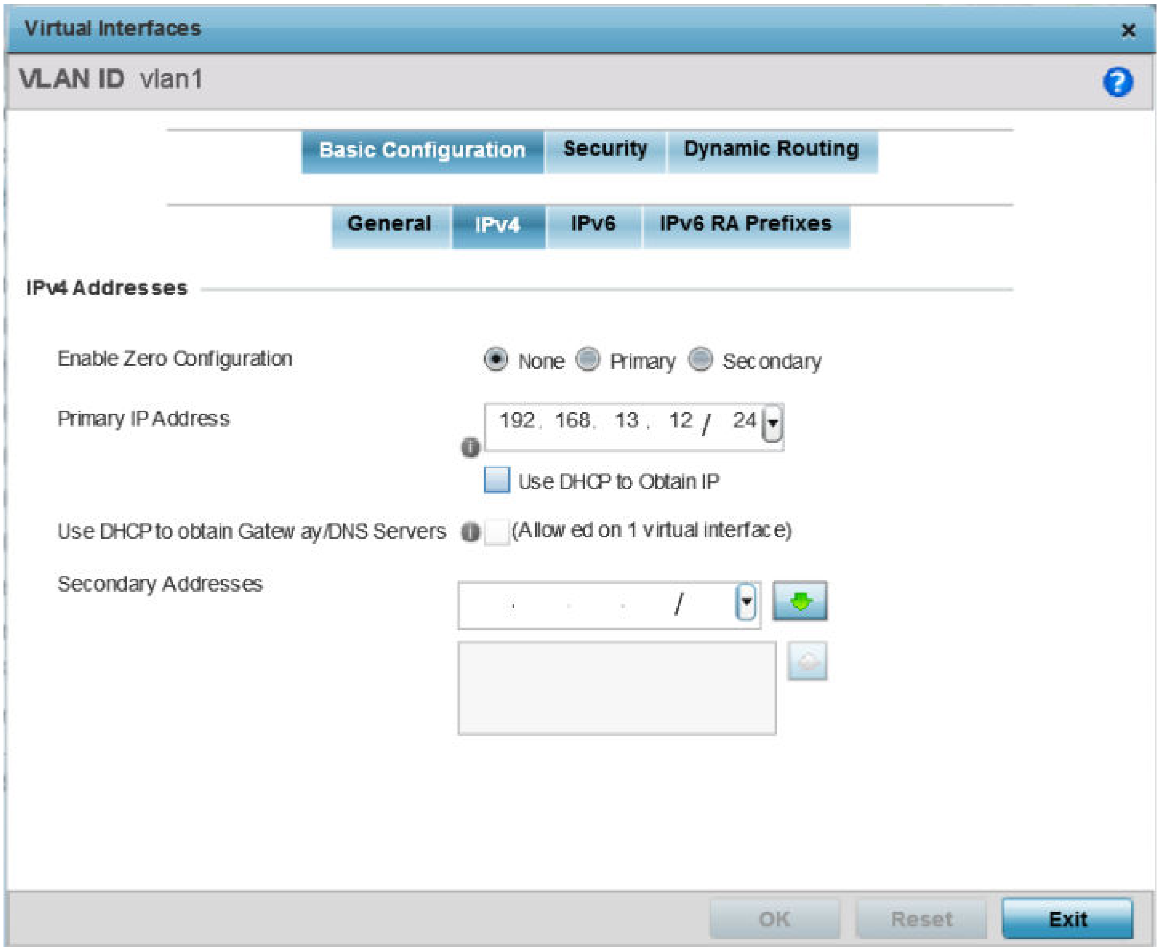
11 Select **OK** to save the changes to the basic configuration. Select **Reset** to revert to the last saved configuration.

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).



Enable Zero Configuration ● None ○ Primary ○ Secondary

Primary IP Address 192 . 168 . 13 . 12 / 24

☐ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ☐ (Allowed on 1 virtual interface)

Figure 258: 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 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the virtual interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
DHCP Relay	Provide IP addresses for DHCP server relay resources. 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.

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

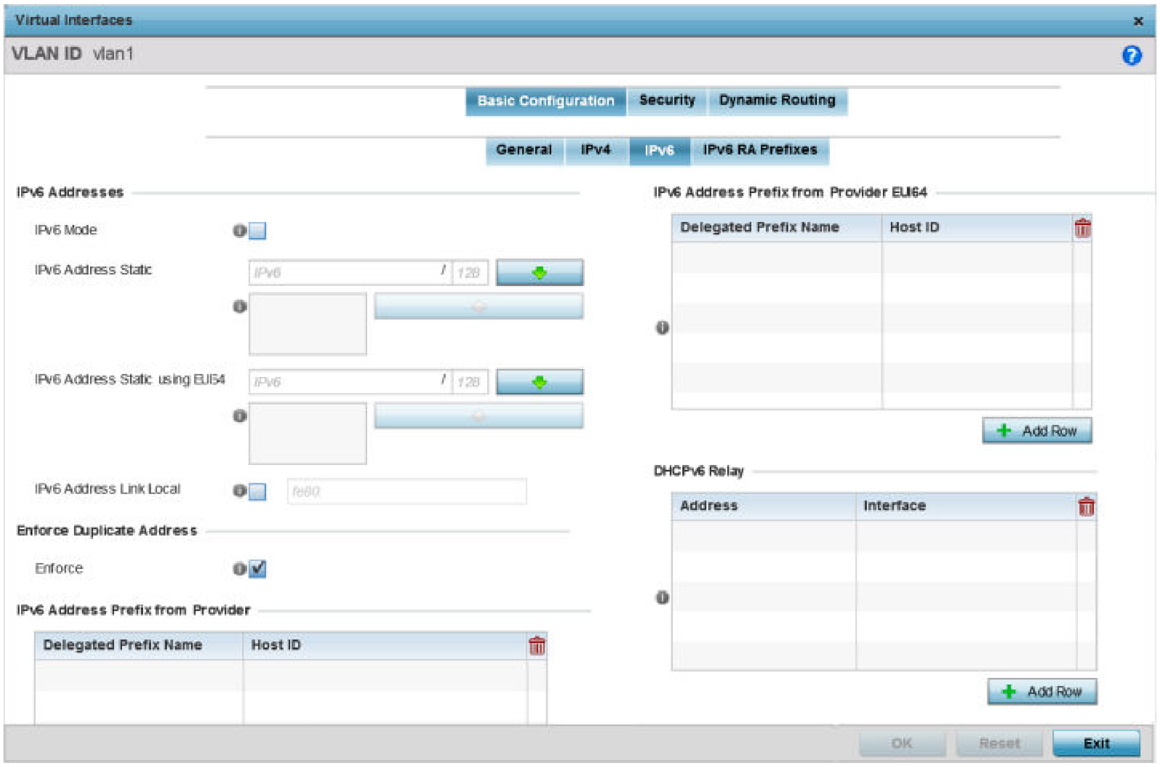
Click **Reset** to revert to the last saved configuration.

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.



IPv6 Mode ☐

Enforce ☑

Figure 259: 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.

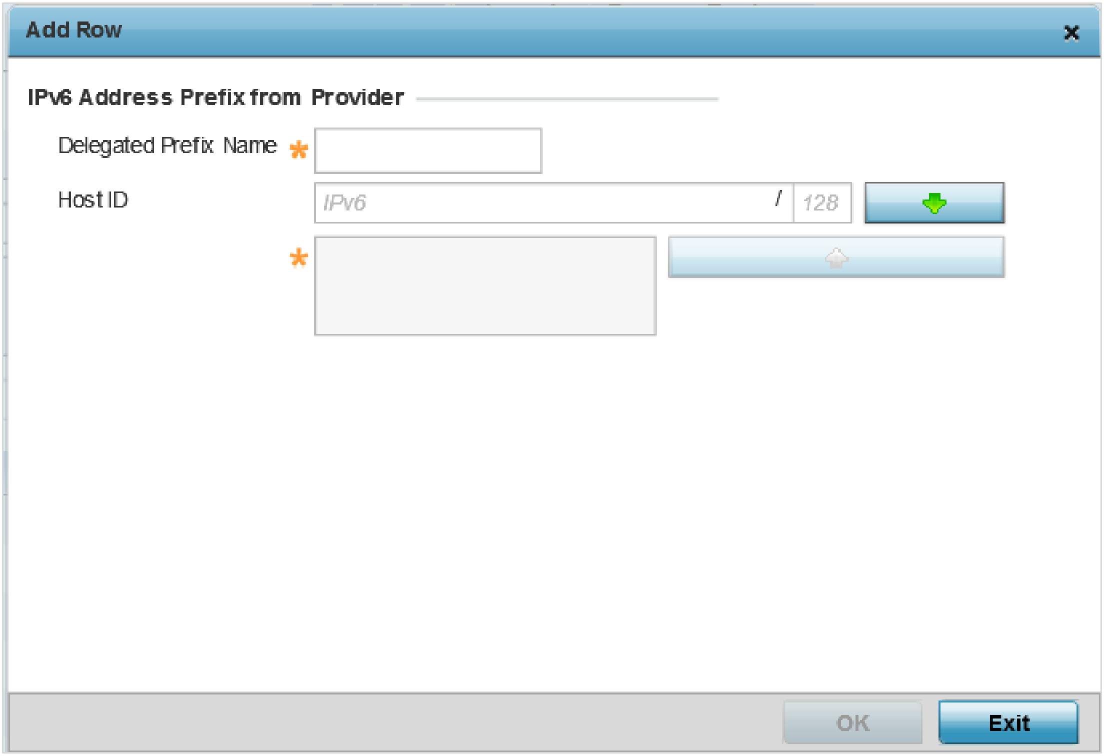


Figure 260: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider

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.

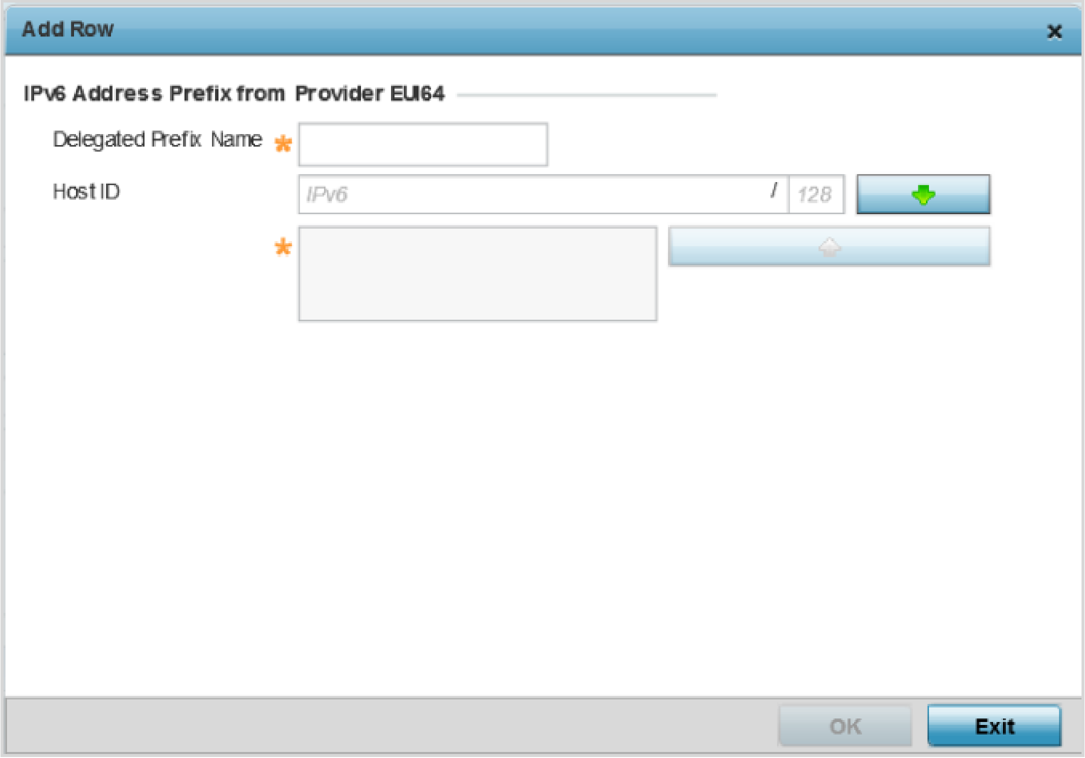


Figure 261: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64

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.

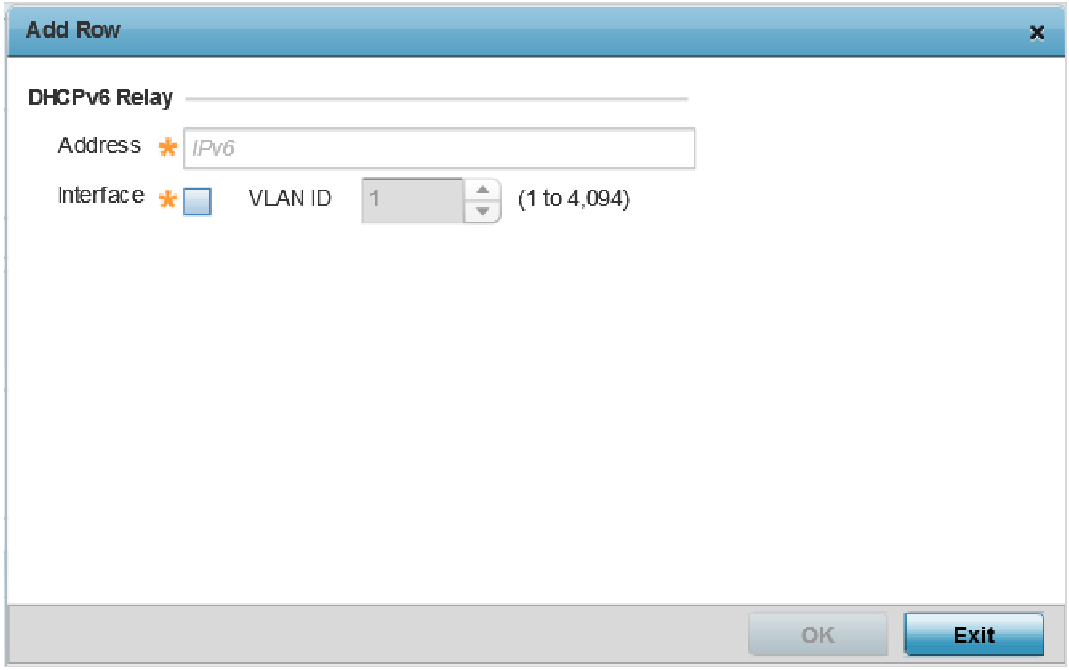


Figure 262: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add DHCPv6 Relay

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.

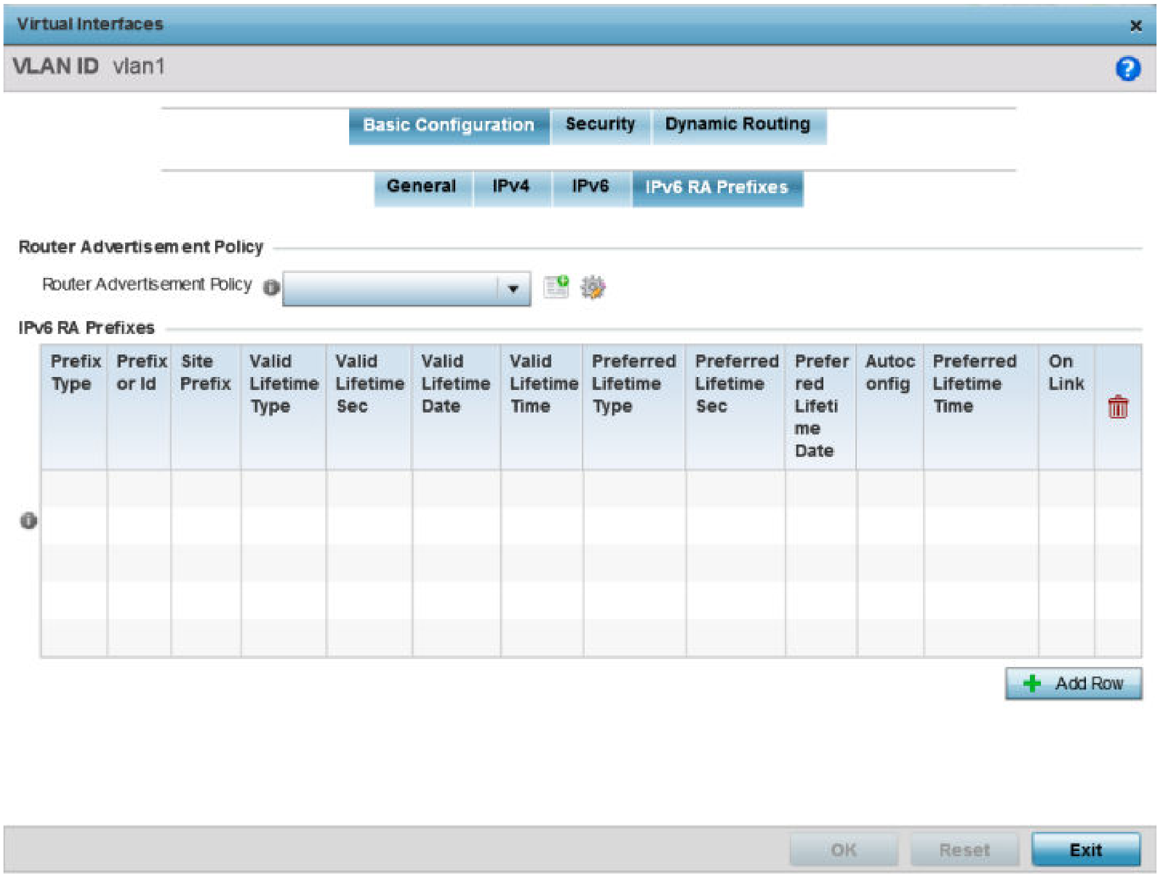


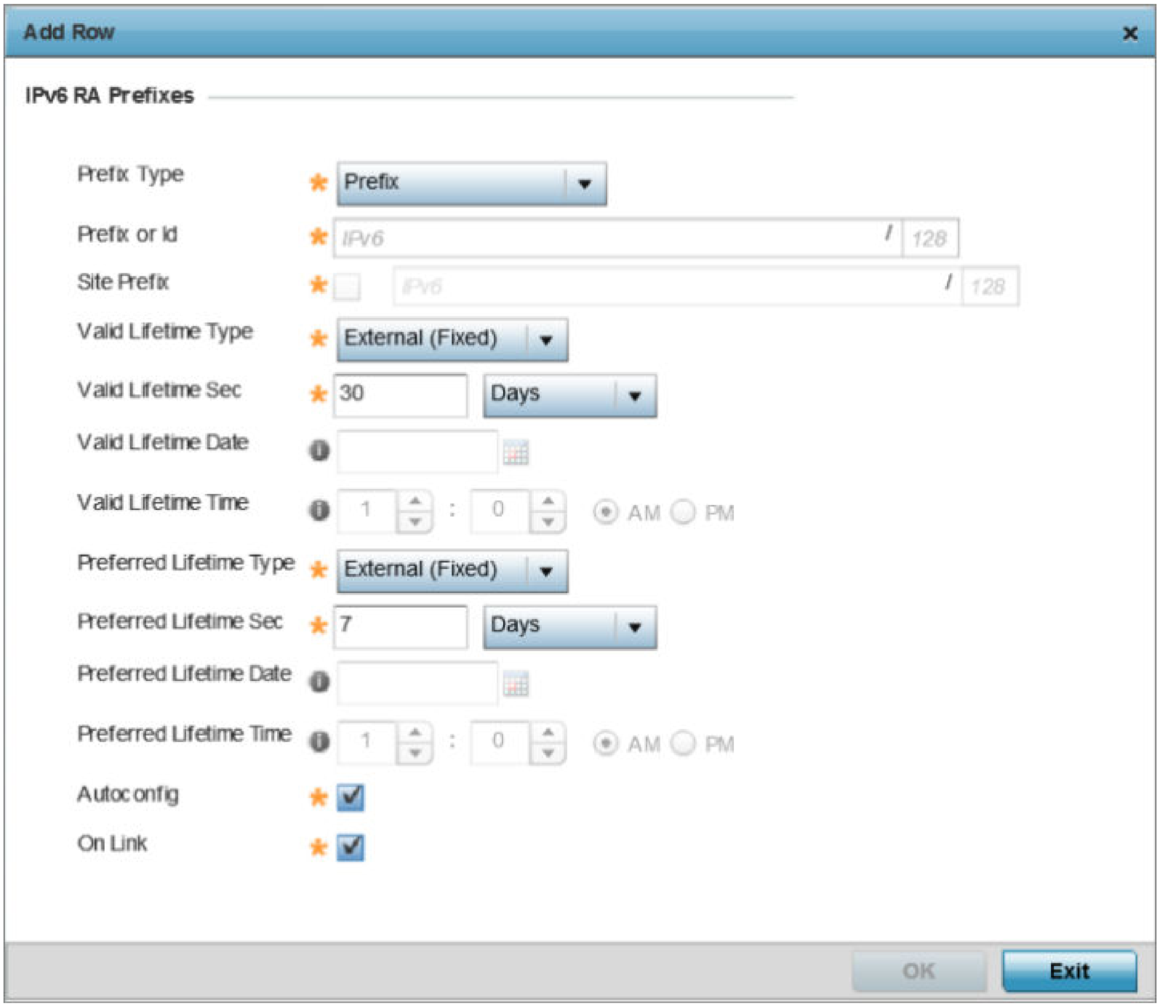
Figure 263: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab

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.



Prefix Type: Prefix
Prefix or Id: IPv6 / 128
Site Prefix: ☐ IPv6 / 128
Valid Lifetime Type: External (Fixed)
Valid Lifetime Sec: 30 Days
Valid Lifetime Date:
Valid Lifetime Time: 1 : 0 ● AM ○ PM
Preferred Lifetime Type: External (Fixed)
Preferred Lifetime Sec: 7 Days
Preferred Lifetime Date:
Preferred Lifetime Time: 1 : 0 ● AM ○ PM
Autoconfig: ☑
On Link: ☑

Figure 264: 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.
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.
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**.

   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.

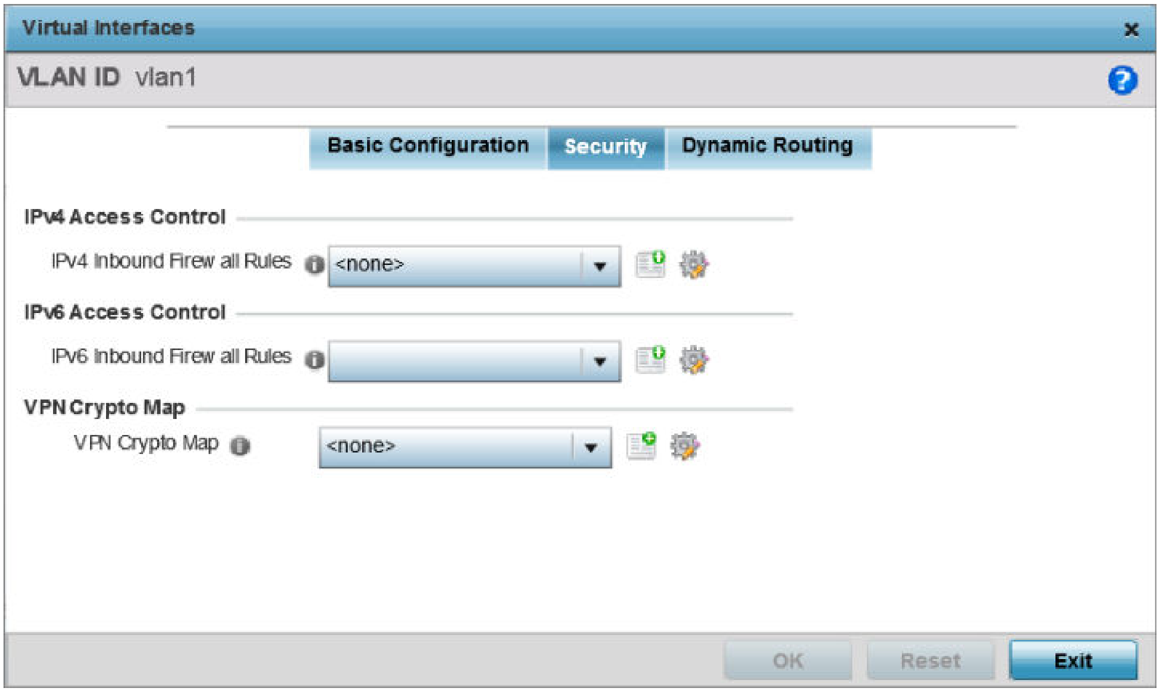


Figure 265: OSPF - VLAN Interface Security Configuration Screen

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 Set the following OSPF Settings:

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 bandwidth from 1 - 10,000,000 KBps.

2 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.

3 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).

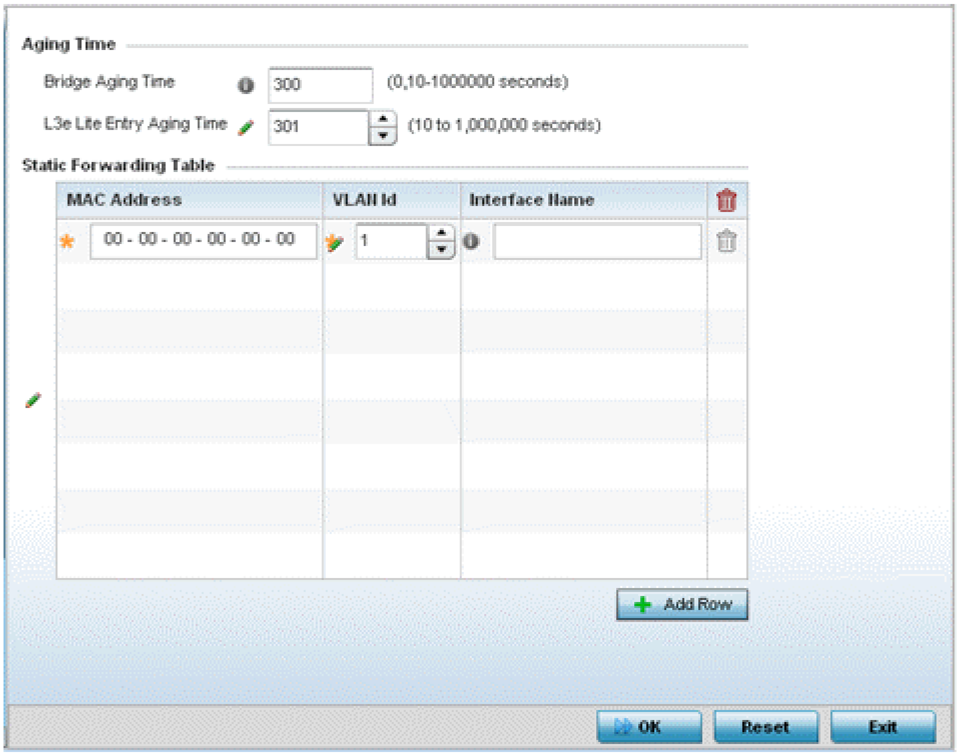
4 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration

Forwarding Database

A *Forwarding Database* is used to forward or filter packets on behalf of a controller, service platform or access point. The packet's destination MAC address is read and the controller, service platform or access point decides to either forward the packet or drop (filter) it. If it is 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 filter or forward the packet.

To define a forwarding database configuration:

1 Select Configuration > Profiles > Network.
2 Expand the Network menu to display its submenu options.
3 Select Forwarding Database.



Aging Time

Bridge Aging Time 300 (0,10-1000000 seconds)

L3e Lite Entry Aging Time 301 (10 to 1,000,000 seconds)

Static Forwarding Table

MAC Address	VLAN Id	Interface Name
00 - 00 - 00 - 00 - 00 - 00	1	

4 Define a **Bridge Aging Time** between 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry remains in the a bridge's forwarding table before being deleted due to inactivity. 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 Define a L3e Lite Entry Aging Time between 10-1,000,000 seconds.

The default setting is 300 seconds.

6 Use the **+Add Row** button to create a new row within the MAC address table.

7 Set a destination **MAC Address** 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).

8 Define the target **VLAN ID** if the destination MAC is on a different network segment.

9 Provide an **Interface Name** used as the target destination interface for the target MAC address.

10 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.

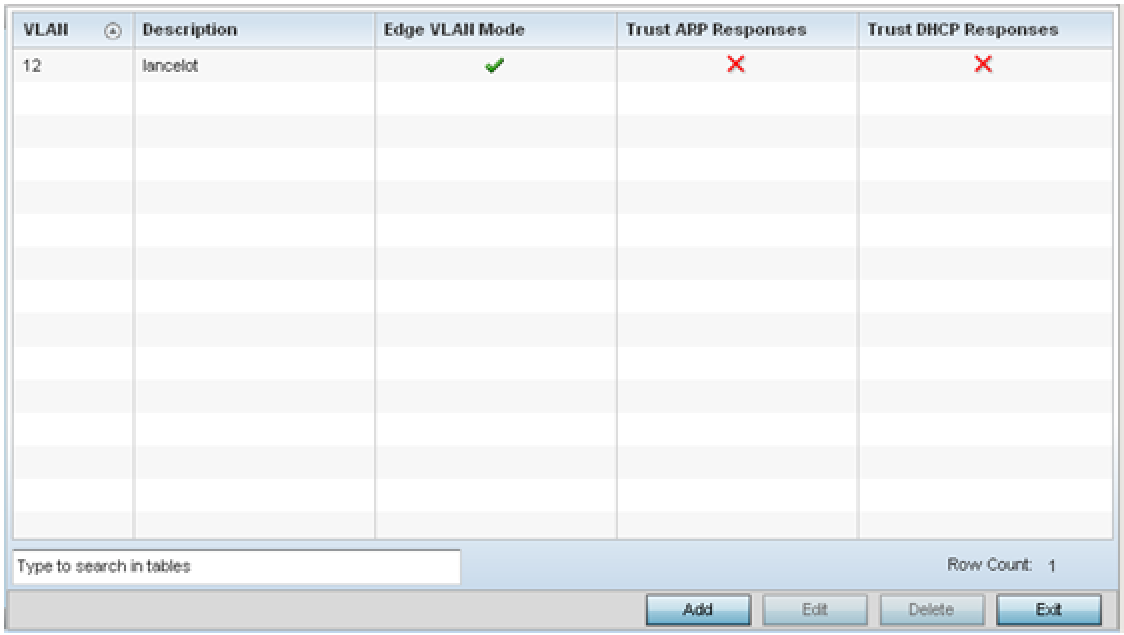
To define a bridge VLAN configuration:

1 Go to **Configuration → Profiles**.

  The Profile screen displays. This screen lists device profiles of wireless controllers, service platforms and access points within the managed network.

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.



VLAN	Description	Edge VLAN Mode	Trust ARP Responses	Trust DHCP Responses
12	lancelot	✓	✗	✗

Row Count: 1

4 Review the following VLAN configuration parameters to determine whether an update is warranted:

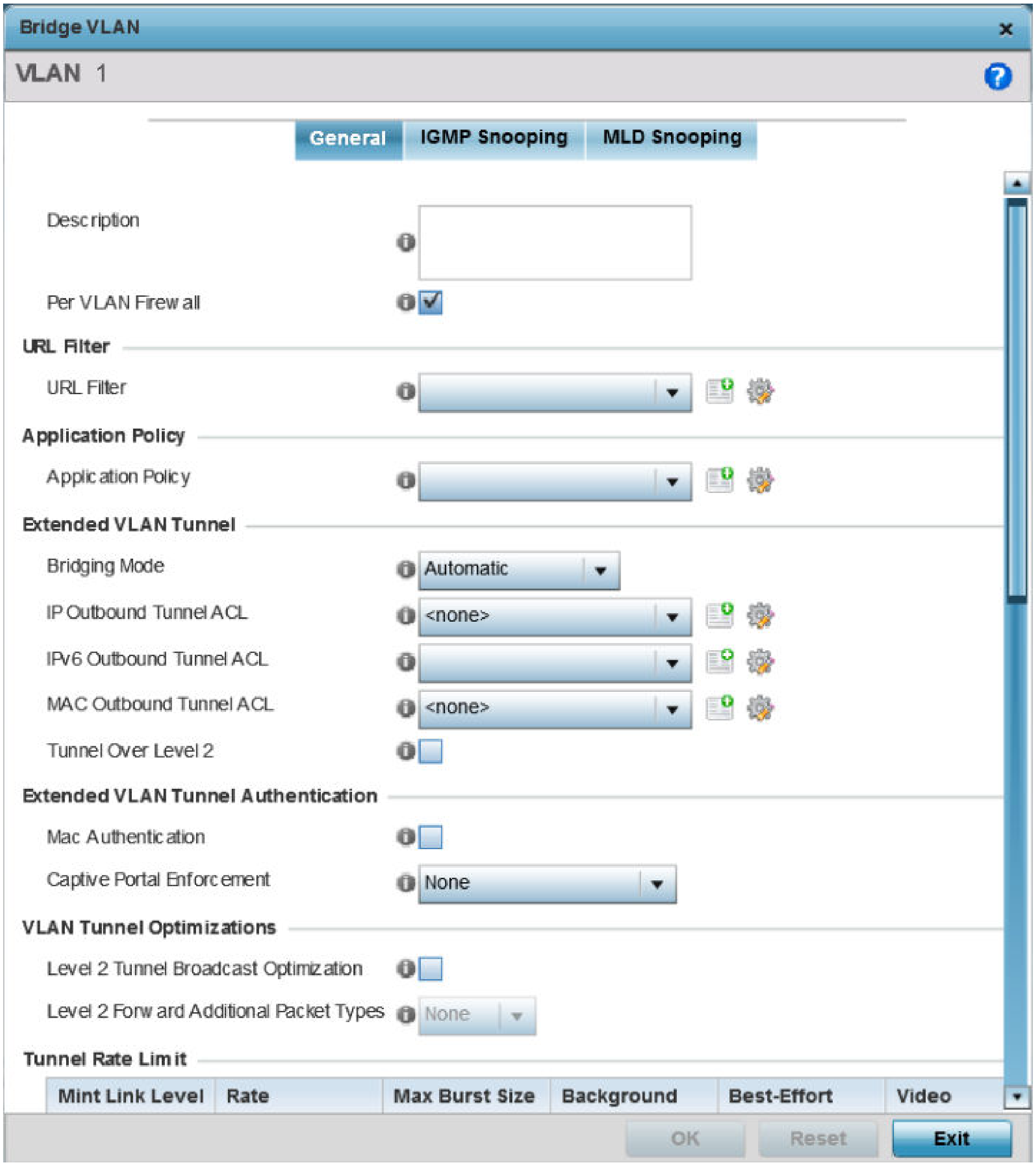
VLAN	Lists the numerical identifier defined for the Bridge VLAN when initially created. The available range is from 1 - 4095. This value cannot be modified during the edit process.
Description	Lists a description of the VLAN assigned when it was created or modified. The description should be unique to 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. *Automatic*: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN. *Local*: Select Local to use local bridging mode for bridging traffic on the VLAN. *Tunnel*: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. *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: **`None`** – No Authentication mode used. This is the default setting. **`Authentication Failure`** – Configures MAC Authentication as the primary and Captive-Portal Authentication as the fall-back authentication mode. **`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.

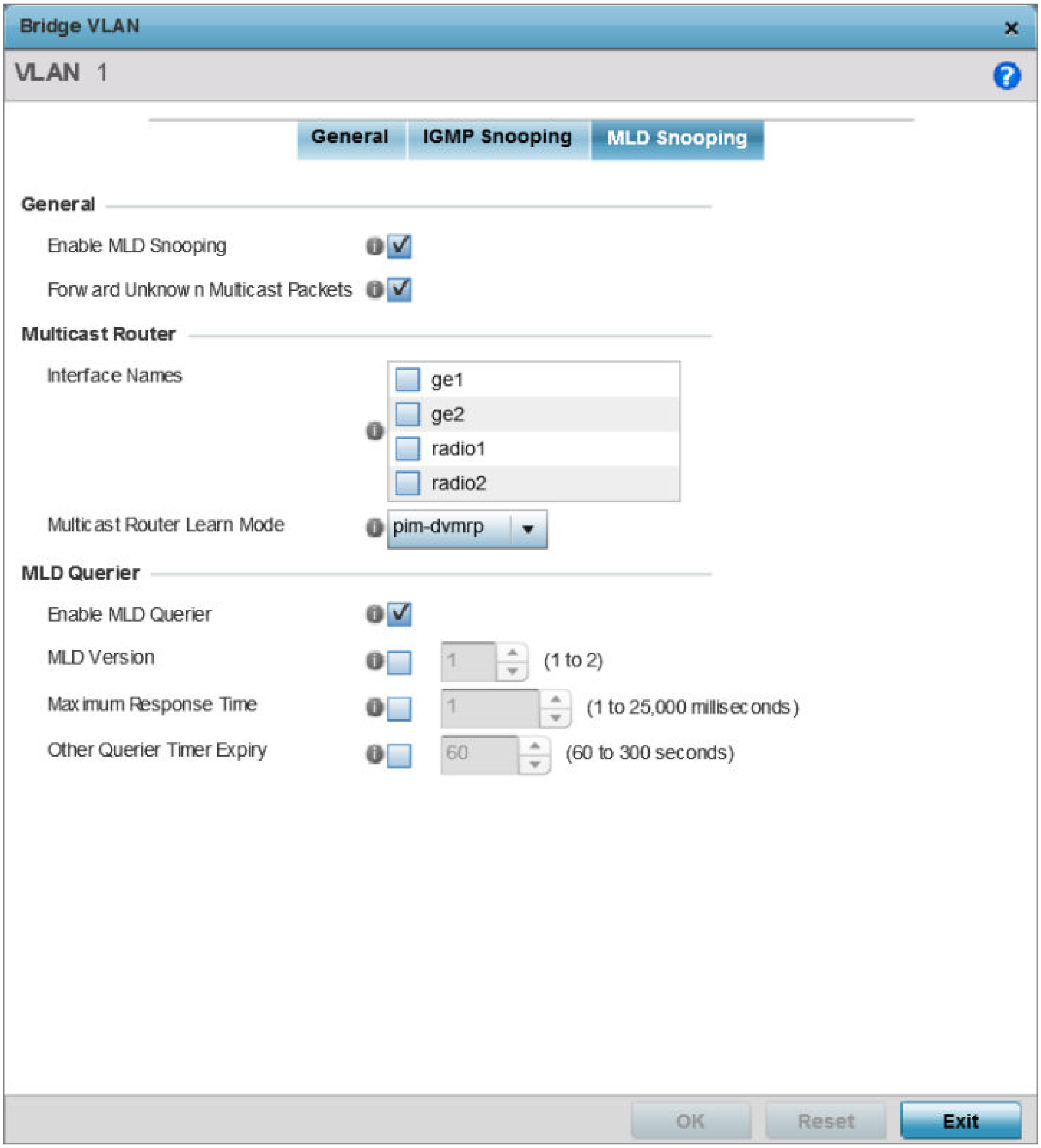
Bridge VLAN MLD Snooping

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.



General

Enable MLD Snooping ☑

Forward Unknown Multicast Packets ☑

Multicast Router

Interface Names
☐ ge1
☐ ge2
☐ radio1
☐ radio2

Multicast Router Learn Mode: pim-dvmrp

MLD Querier

Enable MLD Querier ☑

MLD Version ☐ 1 (1 to 2)

Maximum Response Time ☐ 1 (1 to 25,000 milliseconds)

Other Querier Timer Expiry ☐ 60 (60 to 300 seconds)

Figure 266: 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

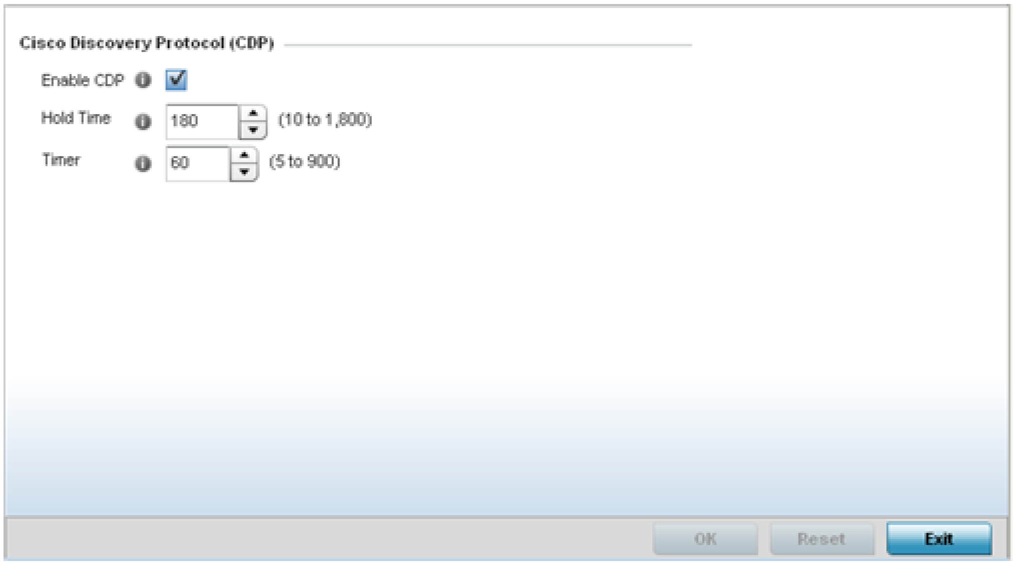
The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share network information amongst different vendor wireless devices.

To set a profile's CDP configuration:

1 Select Configuration > Profiles > Network.

2 Expand the Network menu to display its submenu options.

3 Select Cisco Discovery Protocol.



Cisco Discovery Protocol (CDP)

Enable CDP ☑

Hold Time 180 (10 to 1,800)

Timer 60 (5 to 900)

4 Check the **Enable CDP** box to enable Cisco Discovery Protocol on the device.

5 Refer to the **Hold Time** field and use the spinner control to define a hold time between 10 - 1800 seconds for transmitted CDP Packets. The default value is 180 seconds.

6 Refer to the **Timer** field and use the spinner control to define a interval between 5 - 900 seconds to transmit CDP Packets. The default value is 60 seconds.

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

Link Layer Discovery Protocol Configuration

The *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) 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. Both LLDP snooping and ability to generate and transmit LLDP packets is provided.

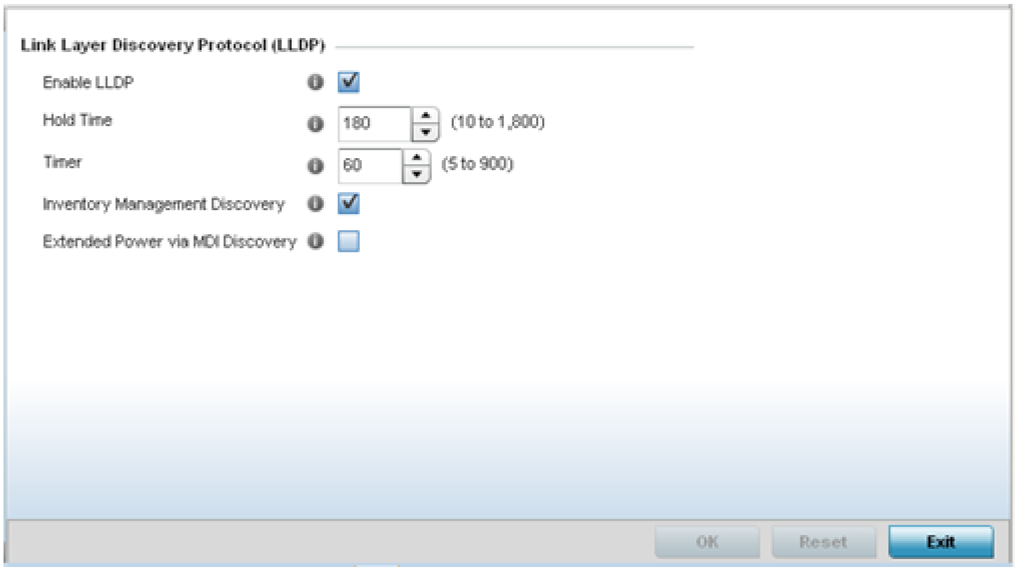
Information obtained via CDP and LLDP snooping is available in the UI. Information obtained using LLDP is provided during the adoption process, so the layer 2 device detected by the access point can be used as a criteria in the provisioning policy.

To set a profile's LLDP configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the **Network** menu to display its submenu options.

3 Select **Link Layer Discovery Protocol**.



Link Layer Discovery Protocol (LLDP)

Enable LLDP ☑

Hold Time 180 (10 to 1,800)

Timer 60 (5 to 900)

Inventory Management Discovery ☑

Extended Power via MDI Discovery ☐

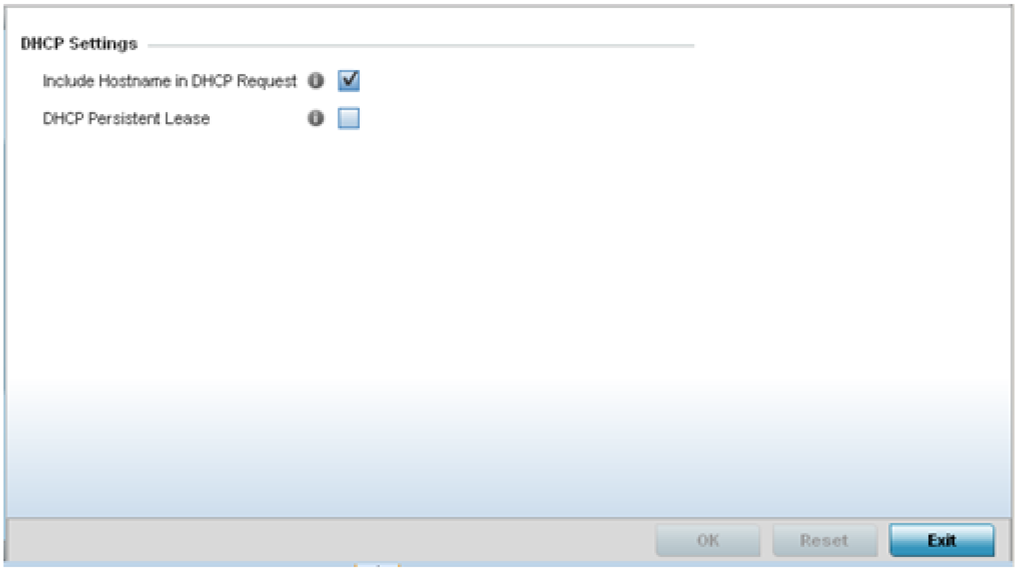
4 Check the **Enable LLDP** box to enable Link Layer Discovery Protocol on the device.
5 Refer to the **Hold Time** field and use the spinner control to define a hold time from 10 - 1800 seconds for transmitted LLDP packets. The default value is 180 seconds.
6 Refer to the **Timer** field and use the spinner control to define the interval between 5 - 900 seconds to transmit LLDP packets. The default value is 60 seconds.
7 Enable **Inventory Management Discovery** to track and identify inventory attributes including manufacturer, model or software version.
8 Enable **Extended Power via MDI Discovery** to provide detailed power information from end points and other connected devices.
9 Select the **OK** button to save the changes. Select **Reset** to revert to the last saved configuration.

Miscellaneous Network Configuration

A profile can be configured to include a hostname within a DHCP lease for a requesting device and its profile. This helps an administrator track a profile's leased DHCP IP addresses by assigned (and recognizable) hostnames for easier administration.

To include a hostnames in DHCP request:

1 Select **Configuration** > **Profiles** > **Network**.
2 Expand the Network menu to display its submenu options
3 Select **Miscellaneous**.



DHCP Settings

Include Hostname in DHCP Request ☑

DHCP Persistent Lease ☐

4 Refer to the **DHCP Settings** field to configure miscellaneous DHCP Settings.

Include Hostname in DHCP Request	Select *Include Hostname in DHCP Request* to include a hostname in a DHCP lease for a requesting device. This feature is disabled by default.
DHCP Persistent Lease	Enables a persistent DHCP lease for a requesting device. A persistent DHCP lease assigns the same IP Address and other network information to the device each time it renews its DHCP lease.

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.

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 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:

- Basic Alias on page 667
- Network Group Alias on page 671
- Network Service Alias on page 673

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:

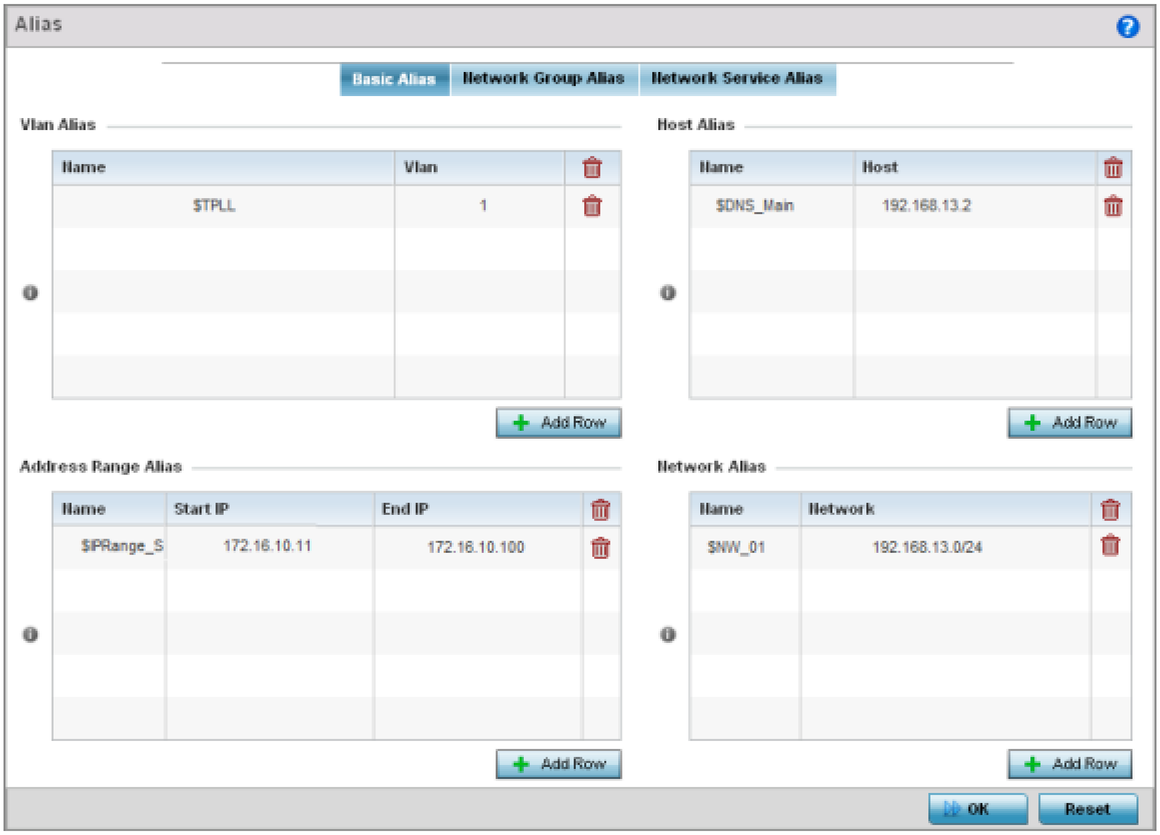
1. Go to **Configuration** → **Profiles**.

   The Profile screen displays. This screen lists device profiles of wireless controllers, service platforms and access points within the managed network.
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.



Vlan Alias

Name	Vlan
$TPLL	1

Host Alias

Name	Host
$DNS_Main	192.168.13.2

Address Range Alias

Name	Start IP	End IP
$IPRange_S	172.16.10.11	172.16.10.100

Network Alias

Name	Network
$NW_01	192.168.13.0/24

Figure 267: 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 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

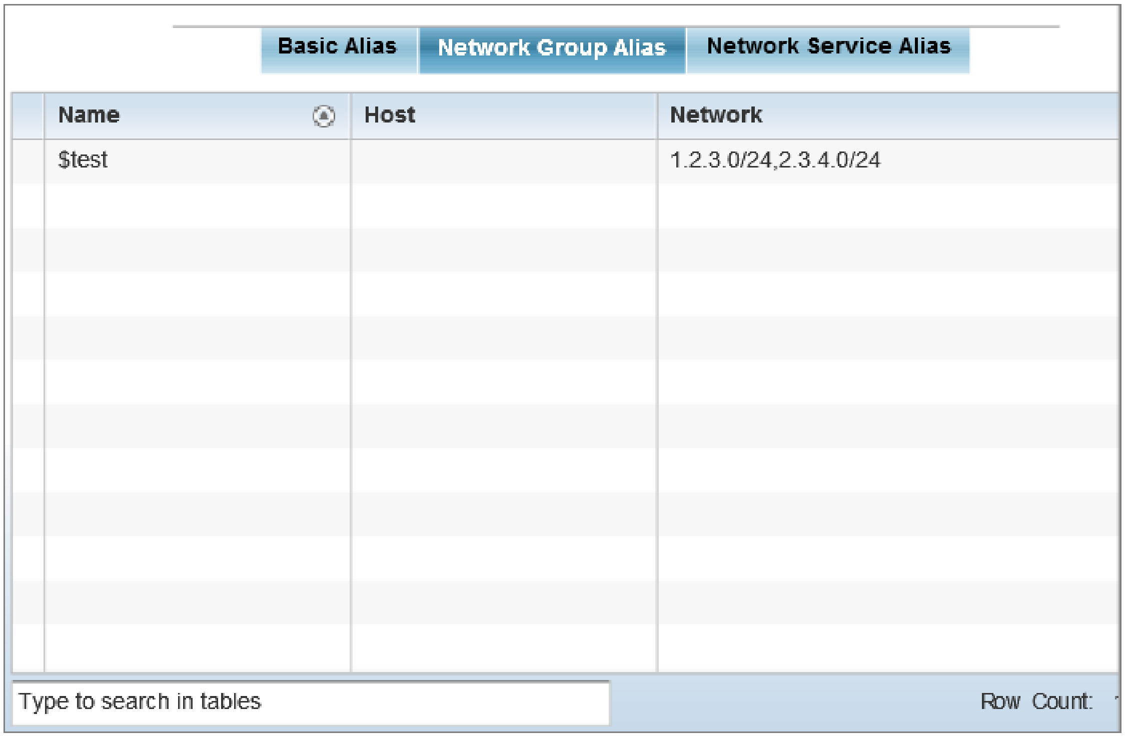
A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address,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

To edit or delete a network alias configuration:

Select the **Network Group Alias** tab.



Name	Host	Network
$test		1.2.3.0/24,2.3.4.0/24

Figure 268: Network Alias - Network Group Alias Screen

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.

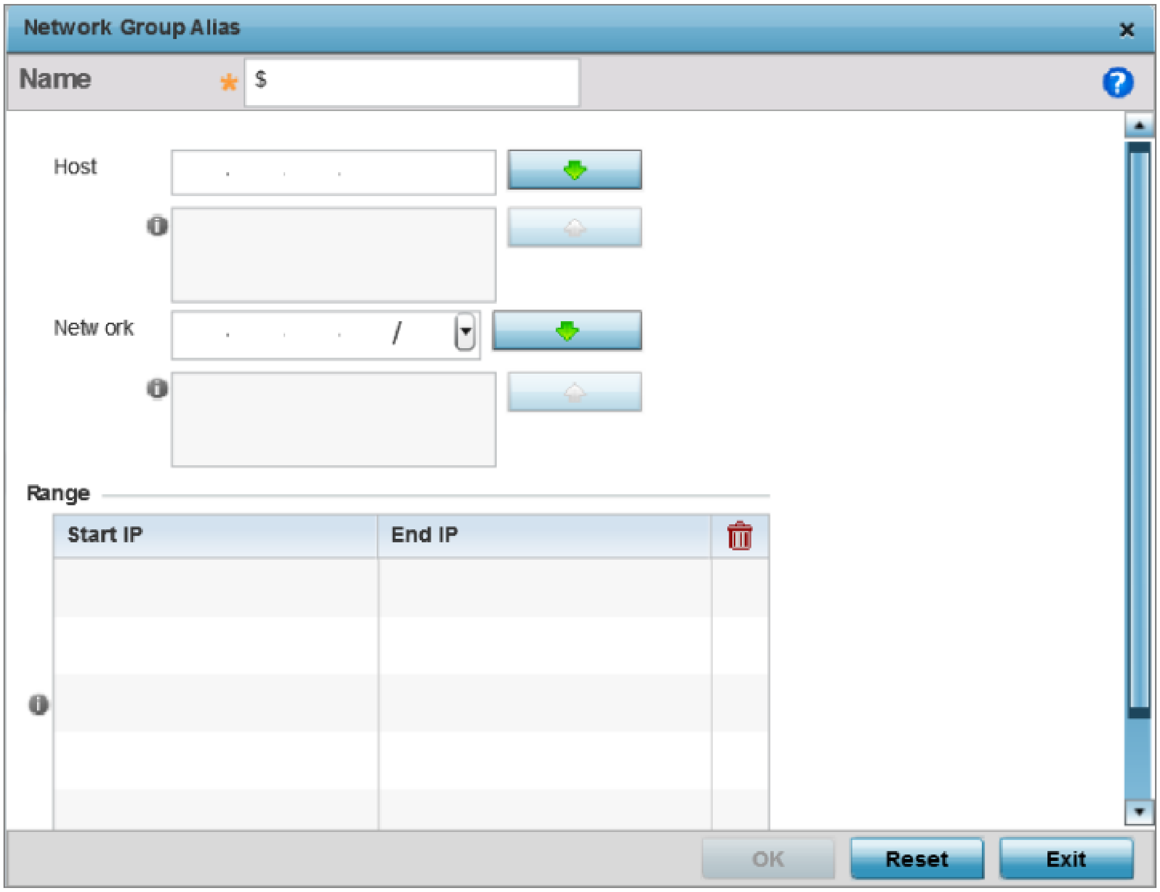


Figure 269: Network Alias - Network Group Alias Add Screen

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.

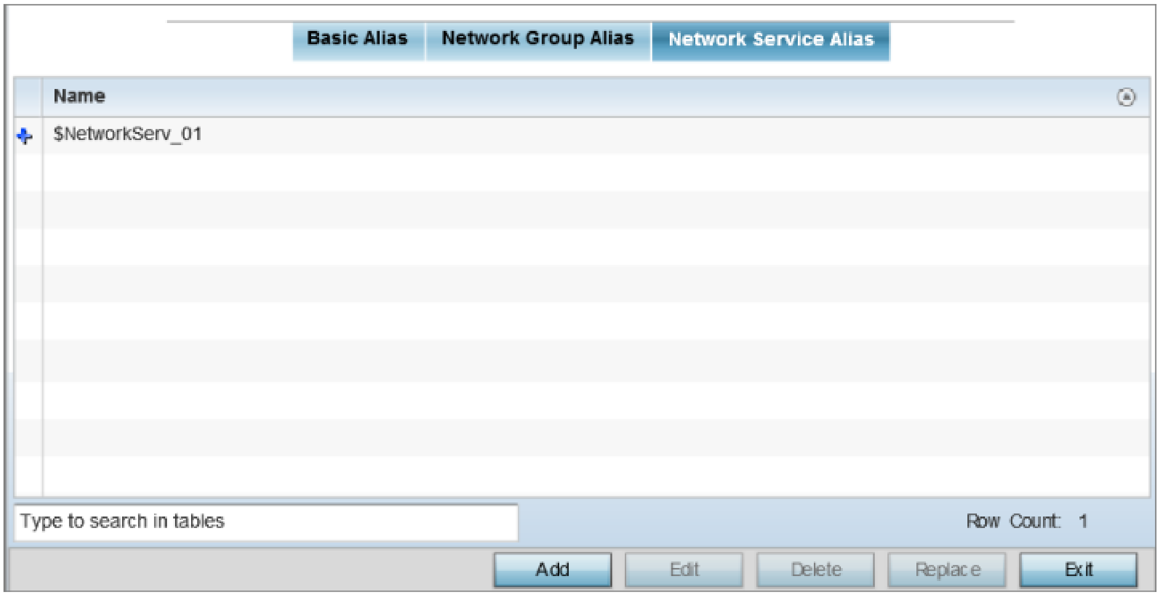


Figure 270: Network Alias - Network Service Alias Screen

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.

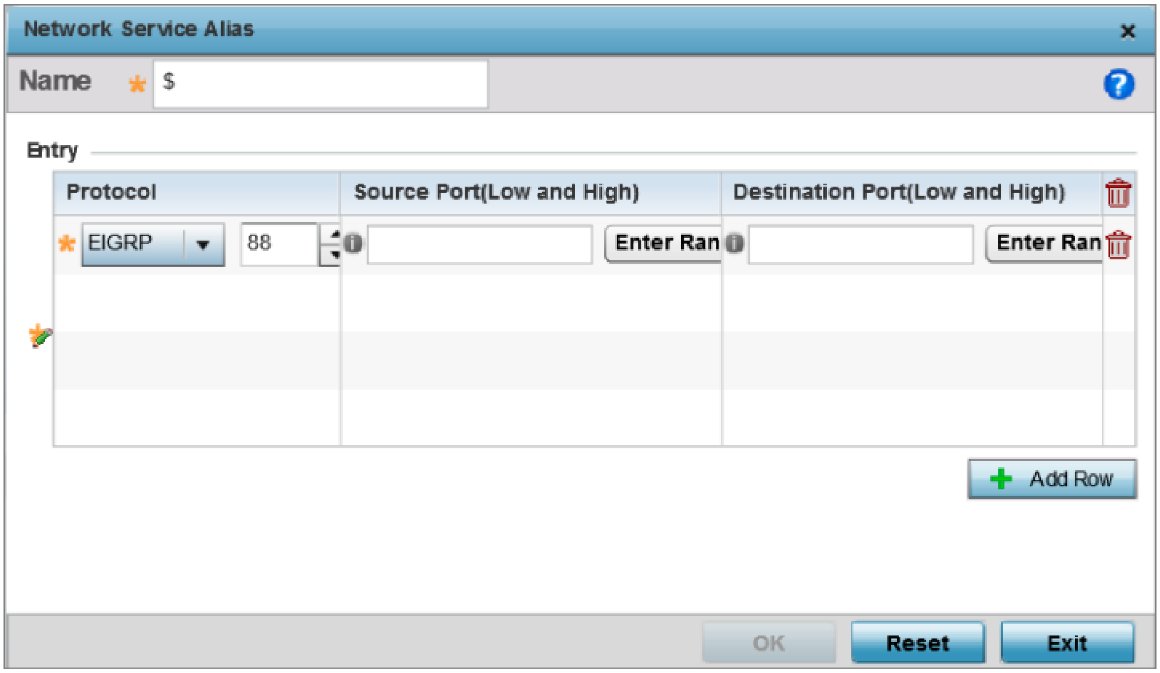


Figure 271: Network Alias - Network Service Alias Add screen

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*. 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*. 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:

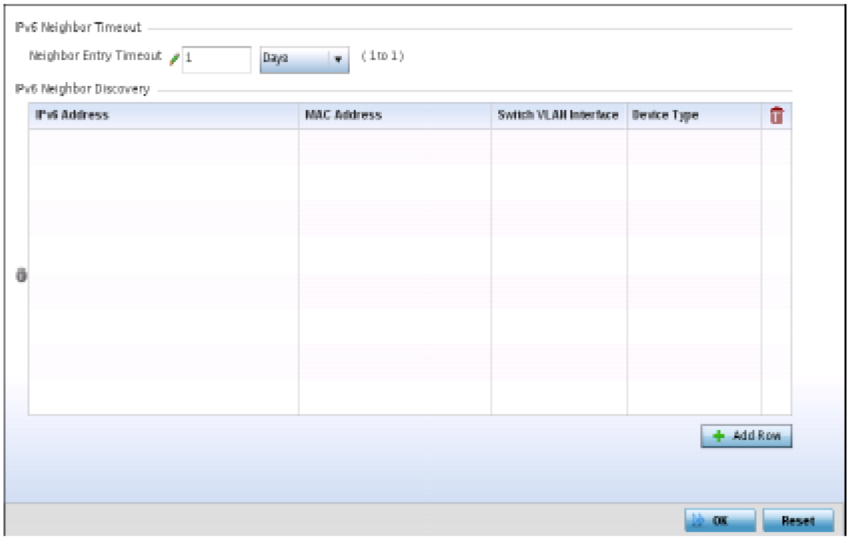
1 Go to **Configuration** → **Profiles**.

The **Profile** screen displays. This screen lists device profiles of wireless controllers, service platforms and access points within the managed network.

2 Select a profile from the list.

The selected profile's configuration menu displays.

3 Expand **Network** menu and select **IPv6 Neighbor**.



IPv6 Neighbor Timeout

Neighbor Entry Timeout 1 Days (1 to 1)

IPv6 Neighbor Discovery

IPv6 Address	MAC Address	Switch VLAN Interface	Device Type

Figure 272: 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 Network Configuration and Deployment Considerations

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 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, an administrator 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 in a network, the more routes need that 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'll need a minimum of 81 routes (9 x 9 = 81).

Profile Security Configuration

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy (controller only) applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can create the required security policy configuration. Once created, separate policies can be applied to the profile to best support the data protection and security requirements of the controller, service platform or access point model supported by the profile.

For more information, refer to the following:

- Defining Security Settings on page 677
- Setting the Certificate Revocation List (CRL) Configuration on page 678
- Setting the Profile's VPN Configuration on page 679
- Auto IPSec Tunnel on page 697
- Setting the Profile's NAT Configuration on page 698
- Setting the Profile's NAT Configuration on page 698
- Bridge NAT Configuration on page 708

Defining Security Settings

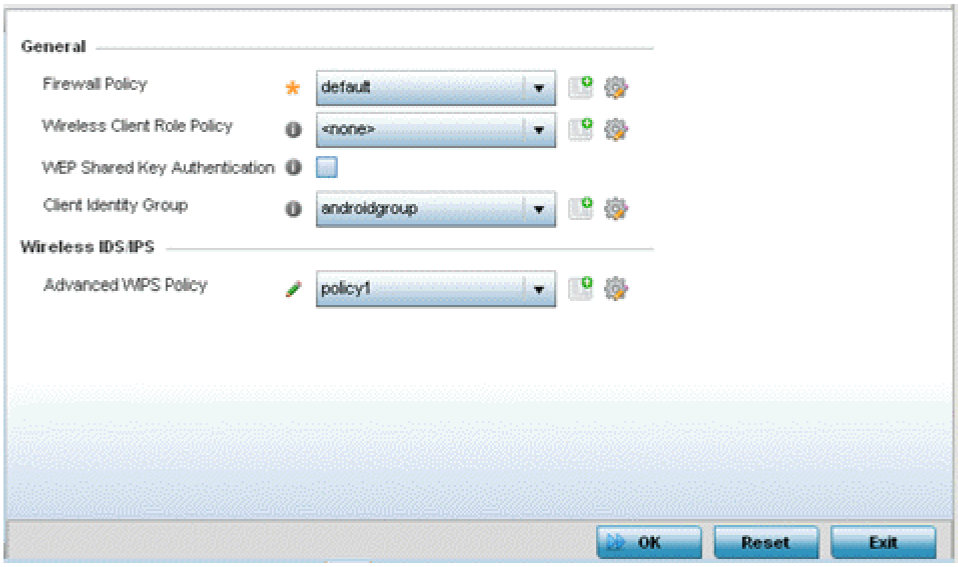
A profile can leverage existing firewall, wireless client role and WIPS policies and apply them to the profile's configuration. This affords each profile a truly unique combination of data protection policies best meeting the data protection requirements of the profile's supported controller, service platform or access point device model and its unique data protection requirements.

To define a profile's security settings:

1 Select the **Configuration** tab from the Web UI.

2 Got to **Profiles** → **Manage Profiles**from the Configuration tab.

3 Select **Security** → **Settings**



General

Firewall Policy: default

Wireless Client Role Policy: <none>

WEP Shared Key Authentication: ☐

Client Identity Group: androidgroup

Wireless IDS/IPS

Advanced WIPS Policy: policy1

4 Refer to the General field to assign or create the following security policy's to the profile:

Firewall Policy	Use the drop-down menu to select an existing Firewall Policy to use as an additional security mechanism with this profile. 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 *denying* 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.
Wireless Client Role Policy	Use the drop-down menu to select a client role policy used to strategically filter client connections based on a pre-defined set of filter rules and connection criteria. If an existing Wireless Client Role policy does not meet your requirements, select the *Create* icon to create a new configuration that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.
WEP Shared Key Authentication	Select this option to require devices to use a WEP key to access the network using this profile. Controllers, service platforms and access points, other proprietary routers, and clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.
Client Identity Group	Client Identity is a set of unique fingerprints used to identify a class of devices. This information is then used to configure the permissions and access rules for the class of devices in the network. Client Identity Group is a collection of client identities that identifies devices and apply specific permissions and restrictions on these devices. From the drop-down select the client identity group to use with this device profile. For more information, see Device Fingerprinting on page 811. Note: An Advanced WIPS Policy is only supported on controllers and service platforms and requires a dedicated WIPS sensor, but does not require a sensor license. Standard WIPS is available on all RF Domain managers and supports on channel, off channel and dedicated sensor scanning modes.

5. Select an **Advanced WIPS Policy** from the drop-down menu. Define an advanced WIPS configuration to optionally remove (terminate) unwanted device connections, and *sanction* (allow) or *unsanaction* (disallow) specific events within the network.

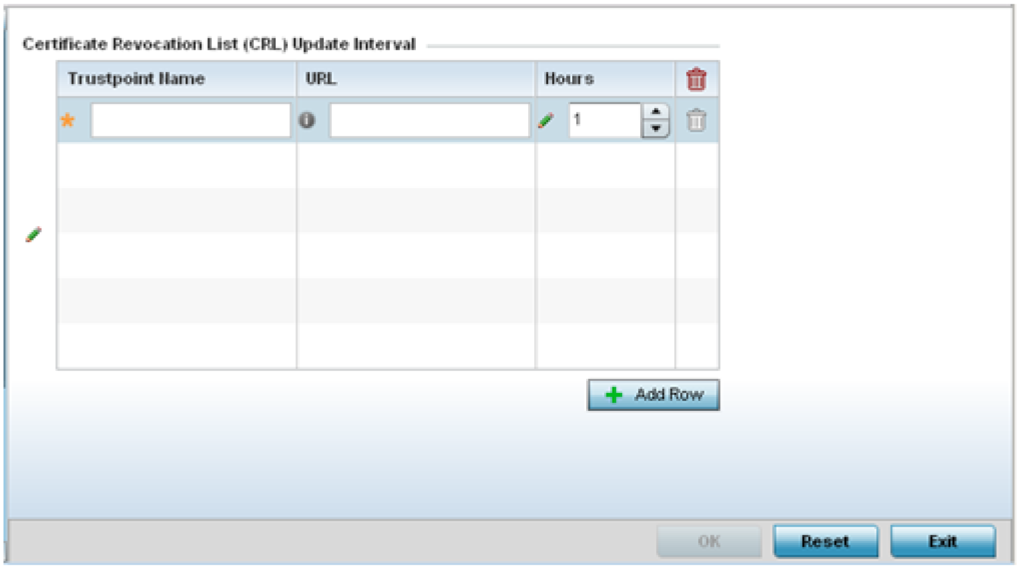
   If an existing Advanced WIPS policy does not meet the profile's data protection requirements, select the **Create** icon to create a new configuration that can be applied to the profile. An existing policy can also be selected and edited as needed using the **Edit** icon.
6. Select **OK** to save the changes made within the Settings screen. Select **Reset** to revert to the last saved configuration.

Setting the Certificate Revocation List (CRL) Configuration

A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the *certificate authority* (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.

To define a CRL configuration that can be applied to a profile:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.
2 Expand Security and select Certificate Revocation.



3 Select the + Add Row button to add a column within the Certificate Revocation List (CRL) Update Interval table to quarantine certificates from use in the network.
4 Additionally, a certificate can be placed on hold for a defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

   a Provide the name of the trustpoint in question within the Trustpoint Name field. The name cannot exceed 32 characters.
   b Enter the resource ensuring the trustpoint's legitimacy within the URL field.
   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.

5 Select OK to save the changes made within the Certificate Revocation screen. Select Reset to revert to the last saved configuration.

Setting the Profile's VPN Configuration

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're 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 SAs *(security associations)* 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*).

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 pre-configuration.

IKE Policy

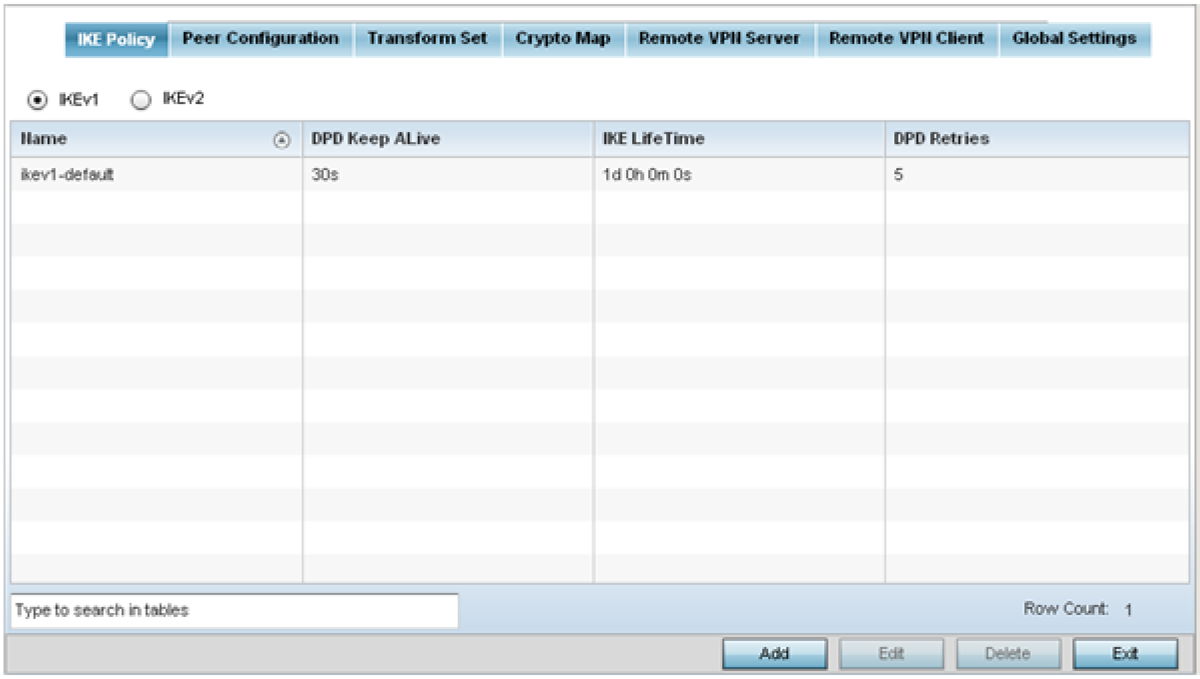
Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

To define a profile's VPN policy settings:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Expand Security and select VPN.

The IKE Policy tab displays by default.



Name	DPD Keep ALive	IKE LifeTime	DPD Retries
ikev1-default	30s	1d 0h 0m 0s	5

3 Select either the IKEv1 or IKEv2 radio button to enforce VPN peer key exchanges 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 IKE Policy screens differ depending on the selected IKEv1 or IKEv2 mode.

4 Refer to the following to determine whether an IKE Policy requires creation, modification or removal:

Name	Displays 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. This screen only appears when IKEv1 is selected.

5 Select Add to define a new IKE Policy configuration, Edit to modify an existing configuration or Delete to remove an existing configuration.

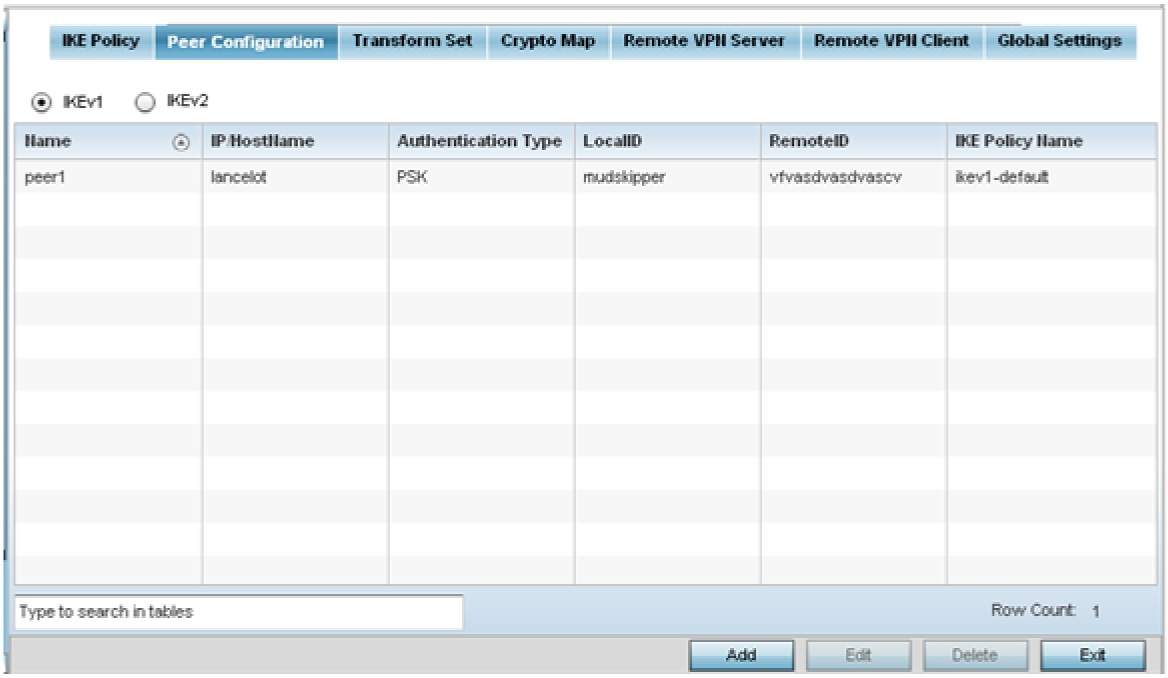
Peer Configuration

To define a profile's VPN peer configuration:

1 Go to **Configuration** → **Profiles** → **Manage Profiles**.

2 Expand Security and select **VPN**.

3 Select the Peer Configuration tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.



● IKEv1 ○ IKEv2

Name	IP/HostName	Authentication Type	LocalID	RemoteID	IKE Policy Name
peer1	lancelot	PSK	mudskipper	vfvasdvasdvascv	ikev1-default

Row Count: 1

4 Select either the IKEv1 or IKEv2 radio button to enforce VPN key exchanges using either *IKEv1* or *IKEv2*.

5 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 upon creation.
IP/Hostname	Displays the IP address (or host address FQDN) of the IPSec VPN peer targeted for secure tunnel connection and data transfer.

Authentication Type	Lists whether the peer configuration has been defined to use *pre-shared key* (PSK) or RSA. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for both signing and encryption. If using IKEv2, this screen displays both *local* and *remote* authentication, as both ends of the VPN connection require authentication.
LocalID	Lists the local identifier used within this peer configuration for an IKE exchange with the target VPN IPSec peer.
RemoteID	Displays the means the target remote peer is to be identified (string, FQDN etc.) within the VPN tunnel.
IKE Policy Name	Lists the IKEv1 or IKE v2 policy used with each listed peer configuration. If a policy requires creation, select the *Create* button.

6 Select 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 be defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected

Adding and Editing a Peer IKE V1 Configuration

To add or edit a profile's VPN peer configuration settings:

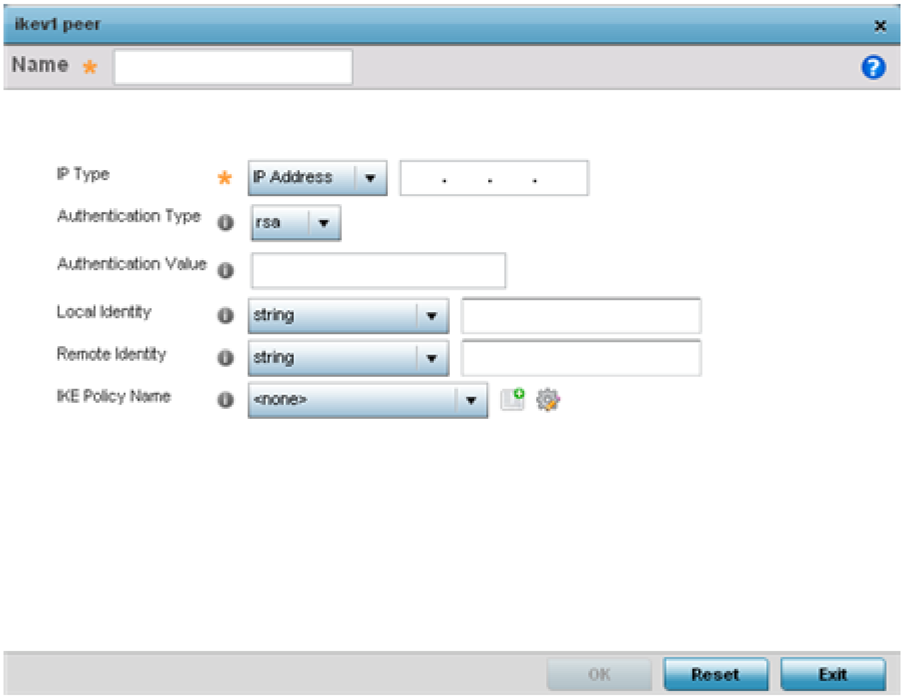
1 Go to **Configuration** → **Profiles** → **Manage Profiles** .

Select a target profile from those displayed on the screen.

2 Expand **Security** and select **VPN**..

3 Select the Peer Configuration tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.

4 Select 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 be defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected.



ikev1 peer

Name *

IP Type * IP Address

Authentication Type rsa

Authentication Value

Local Identity string

Remote Identity string

IKE Policy Name <none>

5 Configure the following parameters:

Name	If 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 FQDN *hostname* of the IPSec VPN peer used in the tunnel setup. If IKEv1 is used, this value is titled *IP Type*, if IKEv2 is used, this parameter is titled *Select IP/Hostname*.
Authentication Type	Select either *pre-shared key* (PSK) or RSA. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing and encryption If using IKEv2, this screen displays both *local* and *remote* authentication options, as both ends of the VPN connection require authentication. RSA is the default value for both local and remote authentication (regardless of IKEv1 or IKEv2).
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* and *string*. 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 a policy requires creation, select the *Create* icon.

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

Adding and Editing a Peer IKE V2 Configuration

To add or edit a profile's VPN peer configuration settings:

1. Select the Configuration tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Select **Manage Profiles** from the Configuration > Profiles menu.
4. Select **Security**.
5. Select **VPN**.
6. Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.
7. Select **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.

Name	If 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 or Select IP/ Hostname	Enter either the *IP address* or FQDN *hostname* of the IPSec VPN peer used in the tunnel setup. If IKEv1 is used, this value is titled *IP Type*, if IKEv2 is used, this parameter is titled *Select IP/Hostname*.

Local Authentication Type	Select either *pre-shared key* (PSK) or RSA. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing and encryption If using IKEv2, this screen displays both *local* and *remote* authentication options, as both ends of the VPN connection require authentication. RSA is the default value for both local and remote authentication (regardless of IKEv1 or IKEv2).
Local 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.
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 a policy requires creation, select the *Create* icon.

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

Adding and Editing an IKE V1 Policy

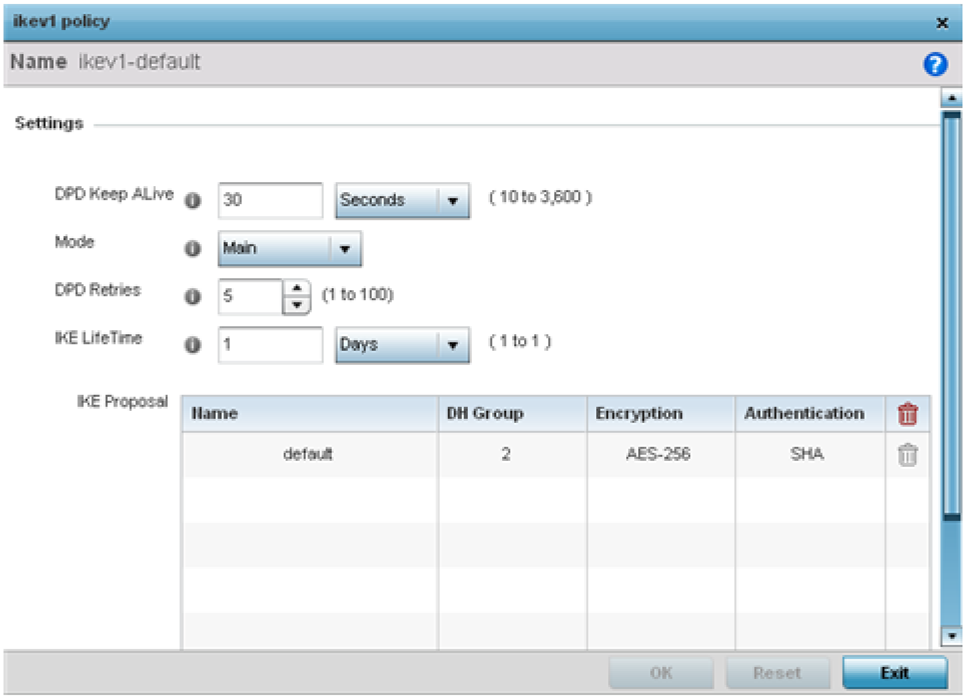
To add or edit profile's VPN settings:

1 Go to **Configuration** → **Profiles** → **Manage Profiles** .

Select a target profile from those displayed on the screen.

2 Expand **Security** and select **VPN**..

3 Select Add to define a new IKe Policy configuration, Edit to modify an existing configuration or Delete to remove an existing configuration.



ikev1 policy

Name ikev1-default

Settings

DPD Keep ALive 30 Seconds (10 to 3,600)

Mode Main

DPD Retries 5 (1 to 100)

IKE LifeTime 1 Days (1 to 1)

IKE Proposal

Name	DH Group	Encryption	Authentication
default	2	AES-256	SHA

4 Set the following 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.
Mode	If using IKEv1, use the pull-down menu to 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 setup the SA, Main requires 6 messages. The default setting is Main.
DPD Retries	Use the spinner control to 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.

5 Select + Add Row 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 *Diffie-Hellman* (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 tunneled peers to securely interoperate. Options include *3DES*, *AES*, *AES-192, 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.

6 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.

Adding and Editing an IKE V2 Policy

To add or edit a profile's VPN settings:

1 Select the Configuration tab from the Web UI.
2 Select Profiles from the Configuration tab.
3 Select Manage Profiles from the Configuration > Profiles menu.
4 Select Security.
5 Select VPN.
6 Select Add to define a new IKe Policy configuration, Edit to modify an existing configuration or Delete to remove an existing configuration.

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.

7 Select **+ Add Row** 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 *Diffie-Hellman* (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 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.

8 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.

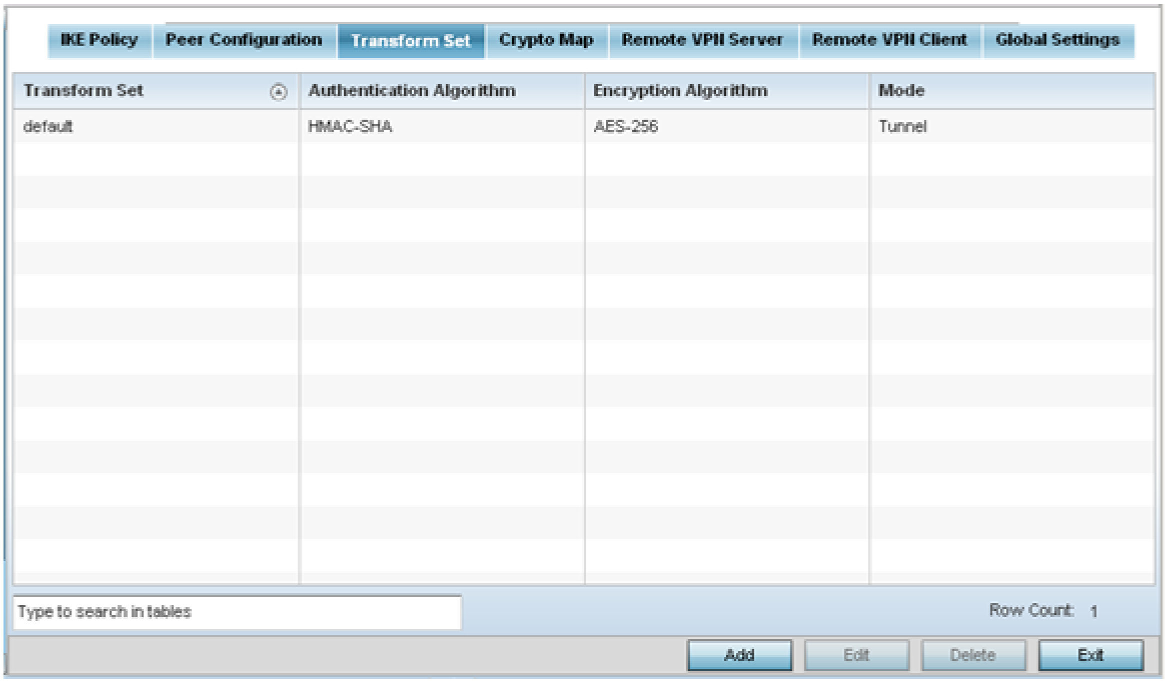
Transform Set

A *transform set* is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic.

To define a profile's VPN transform set:

1 Select the **Transform Set** tab.

Create or modify *Transform Set* configurations to specify how traffic is protected for profile utilizing devices.



Transform Set	Authentication Algorithm	Encryption Algorithm	Mode
default	HMAC-SHA	AES-256	Tunnel

2 Review the following attributes of existing **Transform Set** configurations:

Name	Lists the 32 character maximum name assigned to each listed transform set upon creation. Again, 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 options arer *HMAC-SHA,SHA256, AES-XCBC-MAC* 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 Select Add to define a new transform set configuration, Edit to modify an existing configuration or Delete to remove an existing transform set.

Adding and Editing a Transform Set

To add or edit a profile's VPN transform set:

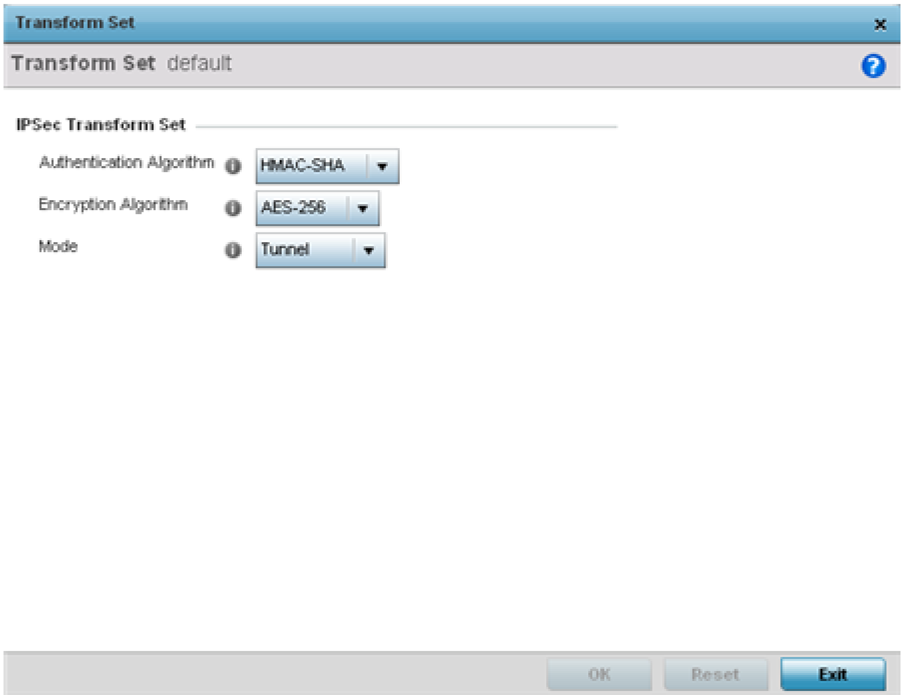
1 Go to **Configuration** → **Profiles** → **Manage Profiles** .

Select a target profile from those displayed on the screen.

2 Expand **Security** and select **VPN**..

3 Select the Transform Set tab.

4 Select Add to define a new transform set configuration, Edit to modify an existing configuration or Delete to remove an existing transform set.



Authentication Algorithm HMAC-SHA

Encryption Algorithm AES-256

Mode Tunnel

5 Define the following settings for the new or modified transform set configuration:

Name	If 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 pull-down menu to select either *HMAC-SHA* or *HMAC-MD5*. 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	Use the pull-down menu to select 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.

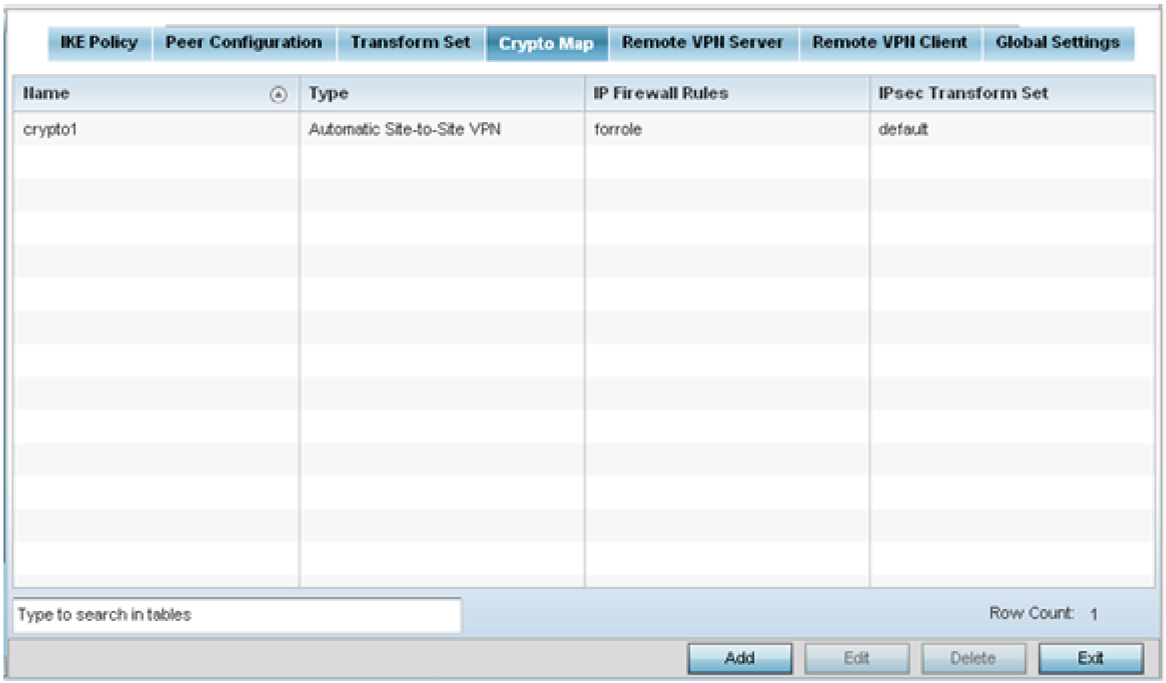
6 Select **OK** to save the changes made within the Transform Set screen. Select **Reset** to revert to the last saved configuration

Crypto Map

Use *crypto maps* (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).

To define a profile's VPN settings:

1 Select the **Crypto Map** tab.



Name	Type	IP Firewall Rules	IPsec Transform Set
crypto1	Automatic Site-to-Site VPN	forrole	default

2 Review the following Crypto Map configuration parameters to assess their 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.
Type	Displays the *site-to-site-manual*, *site-to-site-auto* or *remote VPN* configuration defined for each listed cyrpto map configuration. With site-to-site deployments, an IPSEC Tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point (located remotely) defines a tunnel with a security gateway. This facilitates the endpoints in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.
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.

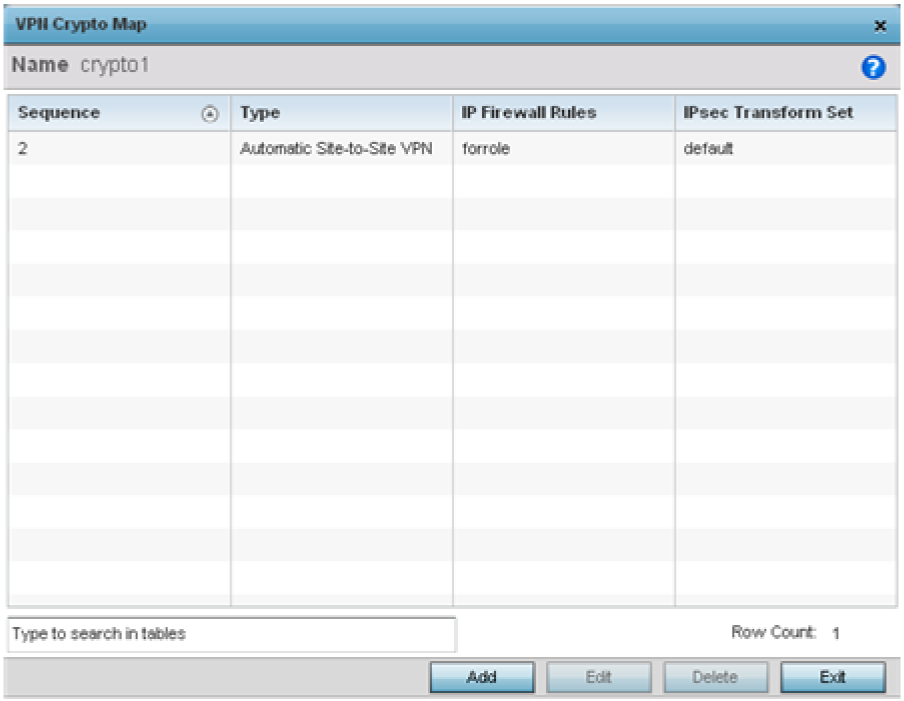
3. If requiring a new crypto map configuration, select the Add button. If updating the configuration of an existing crypto map, select it from amongst those available and select the Edit button.

Adding and Editing a Crypto Map

To add or edit a profile's VPN crypto map settings:

1. Go to **Configuration** → **Profiles** → **Manage Profiles** .

   Select a target profile from those displayed on the screen.
2. Expand **Security** and select **VPN**..
3. Select the VPN Crypto Map tab.
4. 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.
5. If adding a new crypto map, assign it a name up to 32 characters in length as a unique identifier. Select the Continue button to proceed to the VPN Crypto Map screen.



Sequence	Type	IP Firewall Rules	IPsec Transform Set
2	Automatic Site-to-Site VPN	forrole	default

6 Review the following before determining whether to add or modify a 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, provides the flexibility to connect to multiple peers from the same interface, based on the sequence number (from 1 - 1,000).
Type	Displays the *site-to-site-manual*, *site-to-site-auto* or *remote VPN* configuration defined for each listed crypto map configuration.
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 hash algorithms) applied to each listed crypto map configuration. Thus, each crypto map can be customized with its own data protection and peer authentication schemes.

7 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.

Crypto Map Settings

To define a profile's VPN crypto map settings:

1 Go to **Configuration** → **Profiles** → **Manage Profiles** .

Select a target profile from those displayed on the screen.

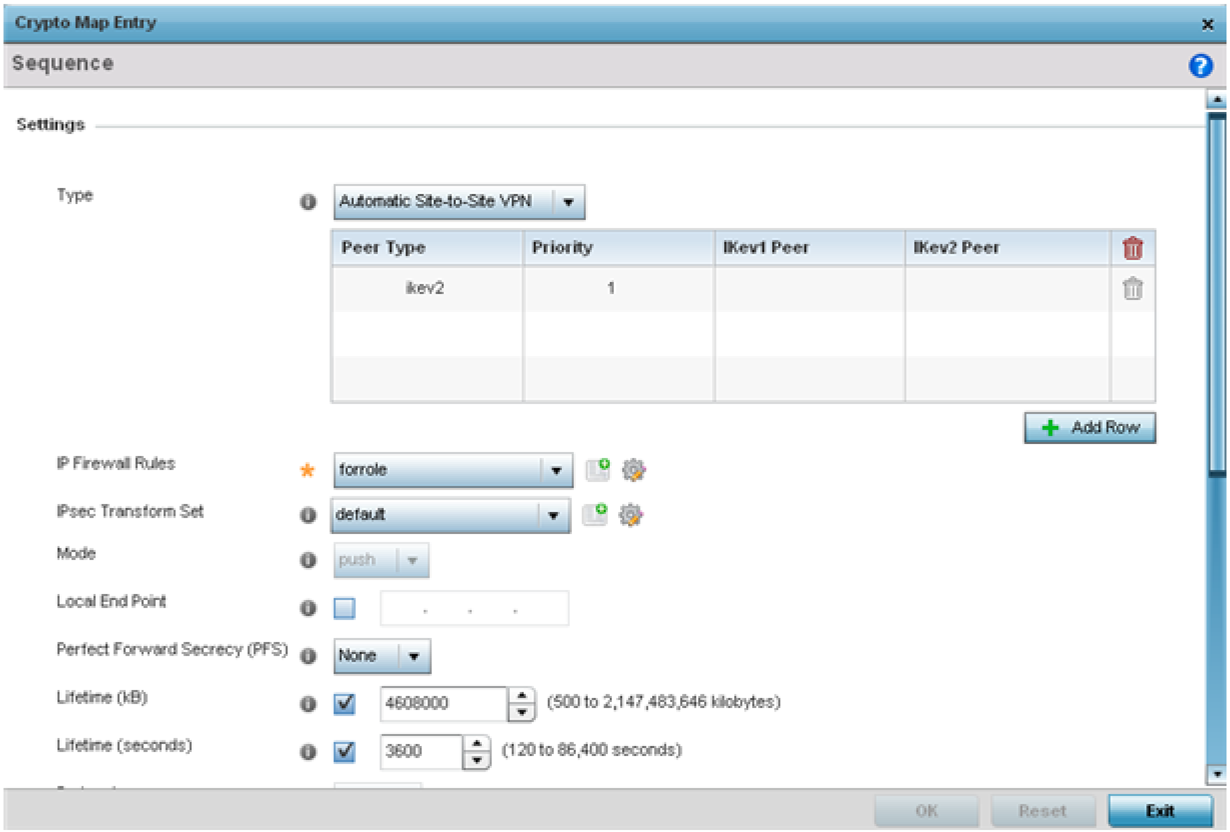
2 Expand **Security** and select **VPN**..

3 Select the Crypto Map tab.

4 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.

5 If adding a new crypto map, assign it a name up to 32 characters in length as an unique identifier. Select the Continue button to proceed to the VPN Crypto Map screen.

6 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.



Type: Automatic Site-to-Site VPN

Peer Type	Priority	IKev1 Peer	IKev2 Peer
ikev2	1		

IP Firewall Rules: forrole

IPsec Transform Set: default

Mode: push

Local End Point: ☐ . . .

Perfect Forward Secrecy (PFS): None

Lifetime (kB): ☑ 4608000 (500 to 2,147,483,646 kilobytes)

Lifetime (seconds): ☑ 3600 (120 to 86,400 seconds)

7 Define the following **Settings** 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 pull-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 pull-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 radio button 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 responds 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	Set an IPSec *security association* (SA) timeout in either *Seconds* (120 - 86,400), *Minutes* (2 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 15 minutes.
Enable NAT after IPSec	Enable this setting to utilize IP/Port NAT on the VPN tunnel. This setting is disabled by default.

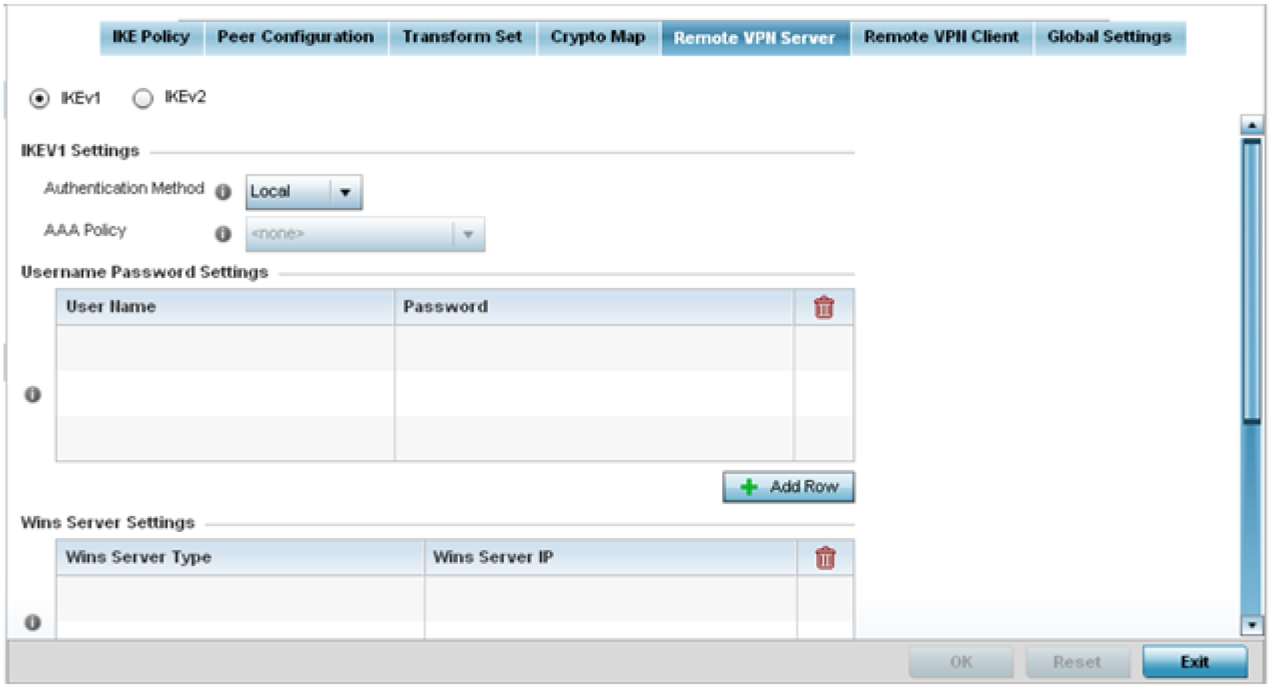
8. Select **OK** to save the updates made to the Crypto Map Entry screen. Selecting **Reset** reverts the screen to its last saved setting.

Remote VPN Server

To define a profile's 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.



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 IKEv1 or IKEv2 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. The default setting is Local. AP 6521 and AP 6511 model access points do not have a local RADIUS resource and must use an external RADIUS server resource.
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 and authentication data.

4 Refer to the **Username Password Settings** field and specify local user database user name and password credentials required for user validation when conducting authentication locally.

5 Refer to the **Wins Server Settings** field 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** field 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 these additional settings (required for IKEv2 only):

DHCP Server Type	Specify whether the DHCP server is specified as an *IP address*, *Hostname (FQDN)* or *None* (a different classification will be defined). *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.
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).
NetMask	Specify the netmask for remote VPN clients.
IP Local Pool	Define an IP address and mask for a virtual IP pool used to assign IP addresses to requesting remote VPN clients.
Relay Agent IP Address	Select this option to define DHCP relay agent IP address.

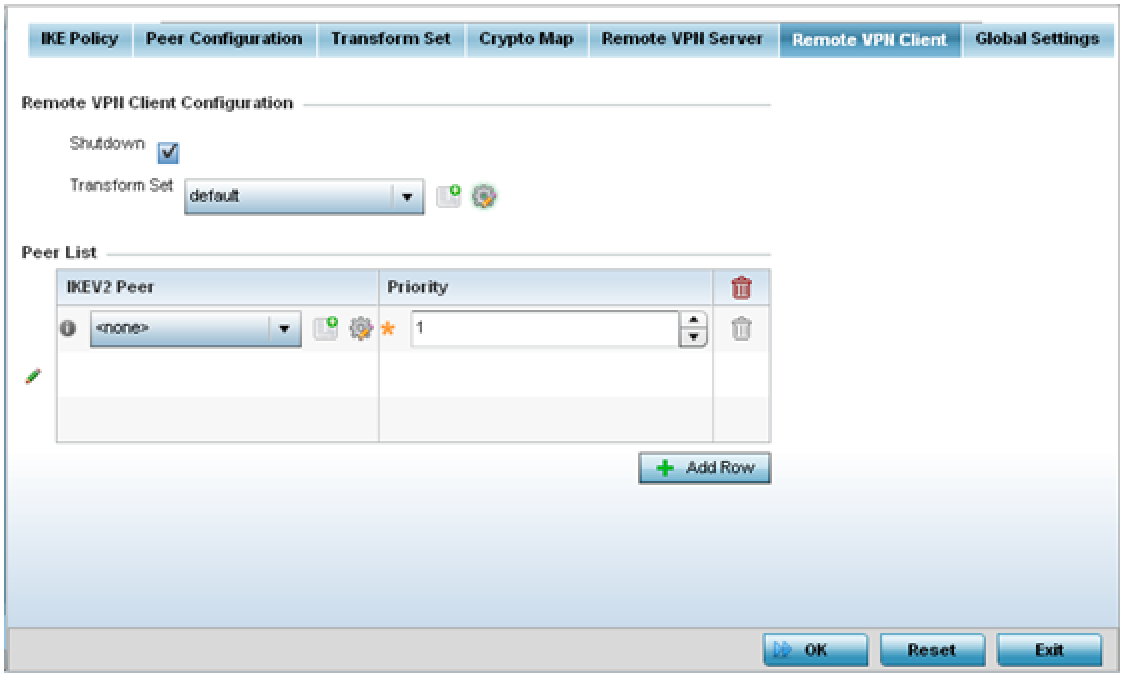
9 Select **OK** to save the updates made to the Remote VPN Server screen. Selecting **Reset** reverts the screen to its last saved configuration.

Remote VPN Client

To define a profile's remote VPN client connection settings:

1 Select **Remote VPN Client**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.



Shutdown ☑

Transform Set default

IKEV2 Peer	Priority
<none>	1

2 Set the following **Remote VPN Client Configuration** settings:

Shutdown	Select this option to disable the remote VPN client. The default is disabled.
Transform Set	Use the drop-down menu to select the transform set to apply to remote client VPN connections. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected client traffic.

3 Refer to the **Peer List** to select IKEV2 peer configurations and assign them priorities for utilization with Remote VPN client connections.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPsec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

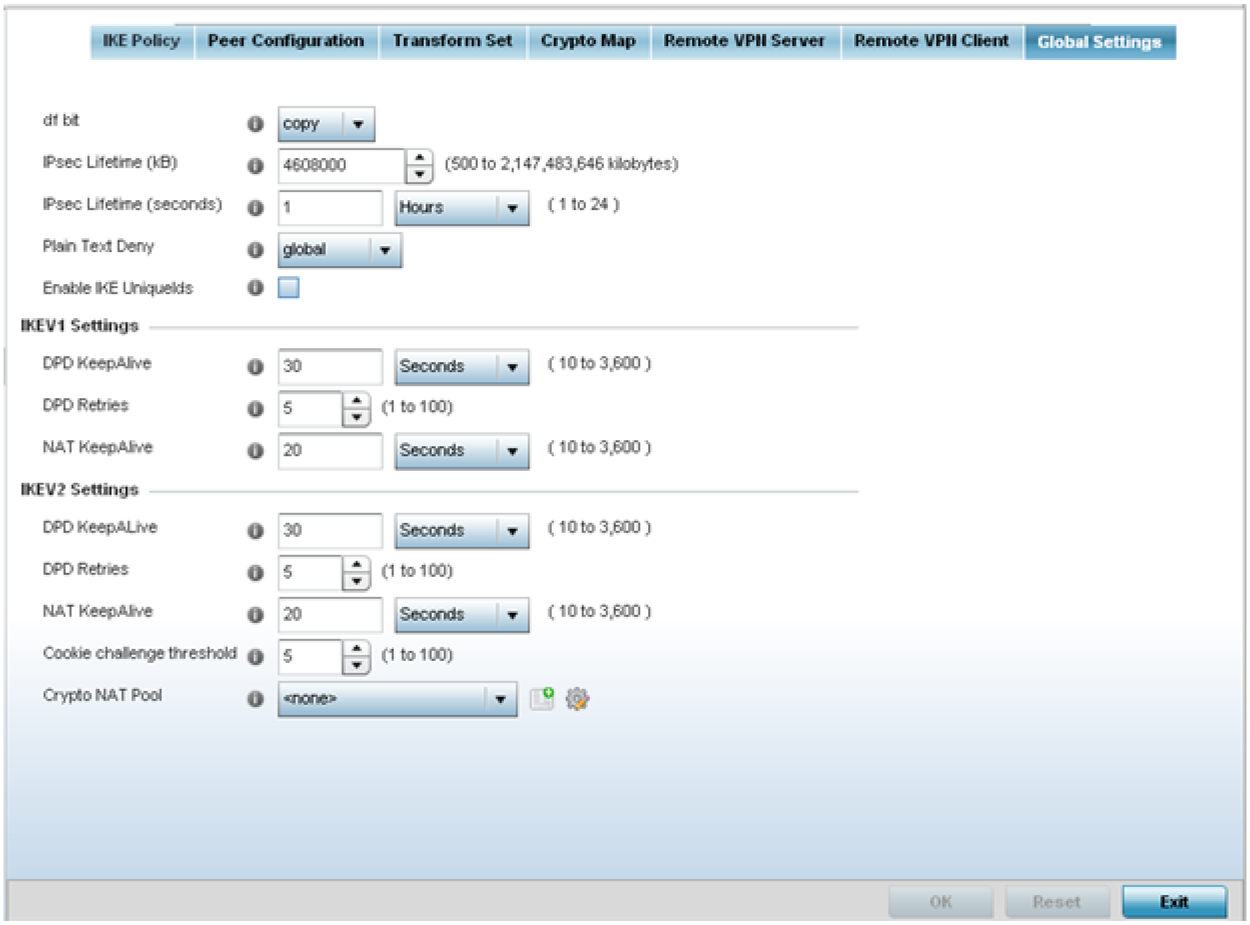
4 Select **OK** to save the updates made to the Remote VPN Client screen. Selecting **Reset** reverts the screen to its last saved configuration.

Global Settings

To define a profile's VPN global settings:

1 Select the **Global Settings** tab.

The **Global Settings** screen provides options for *Dead Peer Detection* (DPD). DPD represents the actions taken upon the detection of a dead peer within the IPSec VPN tunnel connection.



df bit: copy
IPsec Lifetime (kB): 4608000 (500 to 2,147,483,646 kilobytes)
IPsec Lifetime (seconds): 1 Hours (1 to 24)
Plain Text Deny: global
Enable IKE UniqueIds: ☐

IKEV1 Settings

DPD KeepAlive: 30 Seconds (10 to 3,600)
DPD Retries: 5 (1 to 100)
NAT KeepAlive: 20 Seconds (10 to 3,600)

IKEV2 Settings

DPD KeepALive: 30 Seconds (10 to 3,600)
DPD Retries: 5 (1 to 100)
NAT KeepAlive: 20 Seconds (10 to 3,600)
Cookie challenge threshold: 5 (1 to 100)
Crypto NAT Pool: <none>

2 Define the following **IPSec Global** 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. The available range either *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 setting is disabled by default.

3 Define the following **IKEV1 Settings**:

DPD Keep Alive	Define the interval (or frequency) for 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) for 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.

4 Define the following **IKEV2 Settings**:

DPD Keep Alive	Define the interval (or frequency) for 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) for 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 number of half open IKE *security associations* (SAs) (from 1 - 100) that, when exceeded, enables the cookie challenge mechanism. The is setting applies exclusively to IKEV2. The default setting is 5.
Crypto NAT Pool	Select the NAT pool used for internal source NAT on IPSec tunnels. NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

5 Select **OK** to save the updates made to the Global Settings screen. Selecting **Reset** reverts the screen to its last saved configuration.

Auto IPSec Tunnel

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated access points which are within a range of valid IP addresses. Administrators can define which packets are sent within the tunnel, and how they're 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 or associated access point

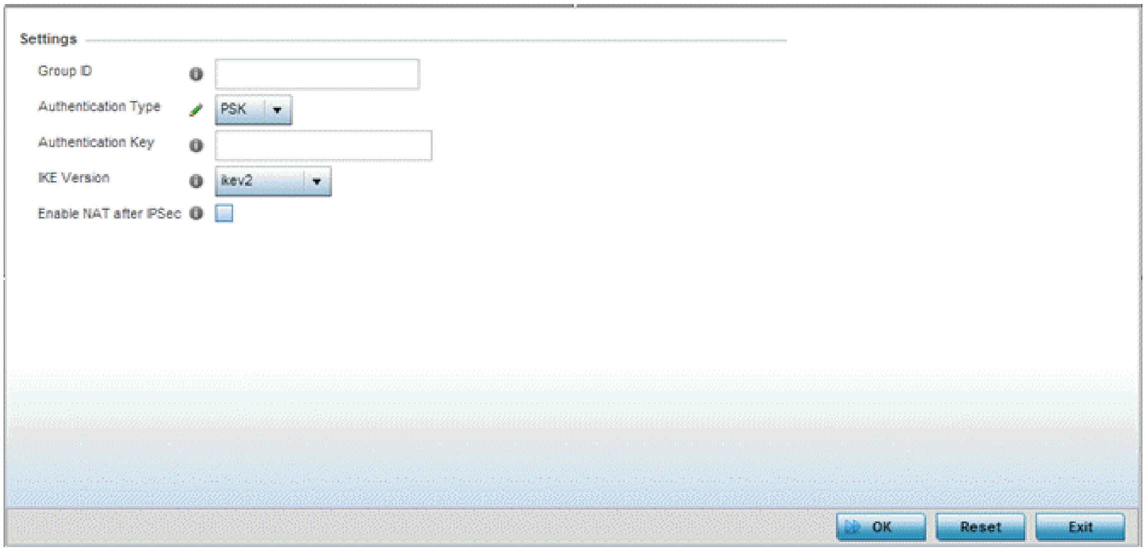
Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Internet Key Exchange (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 enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

To define an Auto IPSec Tunnel configuration or override that can be applied to a profile:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Expand Security and select Auto IPSec Tunnel.



3 The Settings field lists those Auto IPSec tunnel policies created thus far. Any of these policies can be selected and applied to a profile

Group ID	Define a 1 - 64 character identifier for an IKE exchange supporting auto IPSec tunnel secure peers.
Authentication Type	Use the drop-down menu to select either RSA or PSK (Pre Shared Key) as the authentication type for secure peer authentication on the auto IPSec secure tunnel. Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption. The default setting is RSA
Authentication Key	Enter the 8 - 21 character shared key (password) used for auto IPSec tunnel secure peer authentication.

IKE Version	Use the drop-down menu to select the IKE version used for auto IPSec tunnel secure authentication with the IPSec gateway.
Enable NAT after IPSec	Select this option to enable internal source port NAT on the auto IPSec secure tunnel.
Use Unique ID	Select this option to use a unique ID with auto IPSec secure authentication for the IPSec remote gateway (appending the MiNT ID). This setting is disabled by default.

4 Select OK to save the changes made to the auto IPSec tunnel configuration. Select Reset to revert to the last saved configuration.

Setting the Profile's NAT Configuration

Network Address Translation (NAT) is a technique to modify network address information within IP packet headers in transit across a traffic routing device. This enables mapping one IP address to another to protect 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 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.

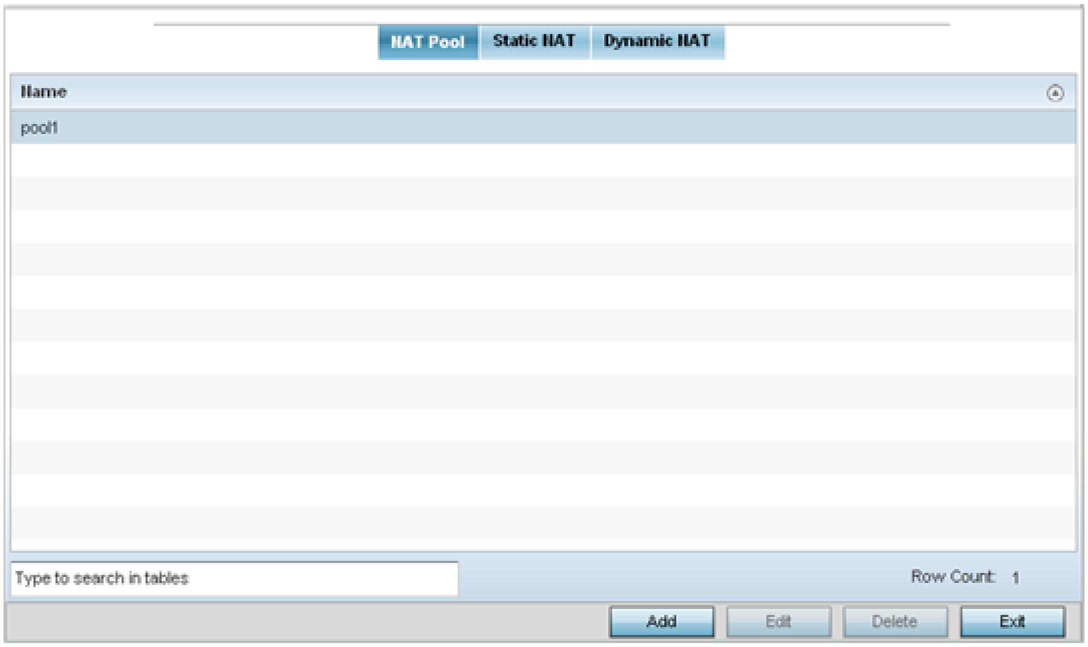
NAT can provide an profile outbound Internet access to wired and wireless hosts connected to a controller, service platform or access point. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows a controller, service platform or access point to translate 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.

NAT Pool

To define a NAT configuration that can be applied to a profile:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Expand Security and select NAT.



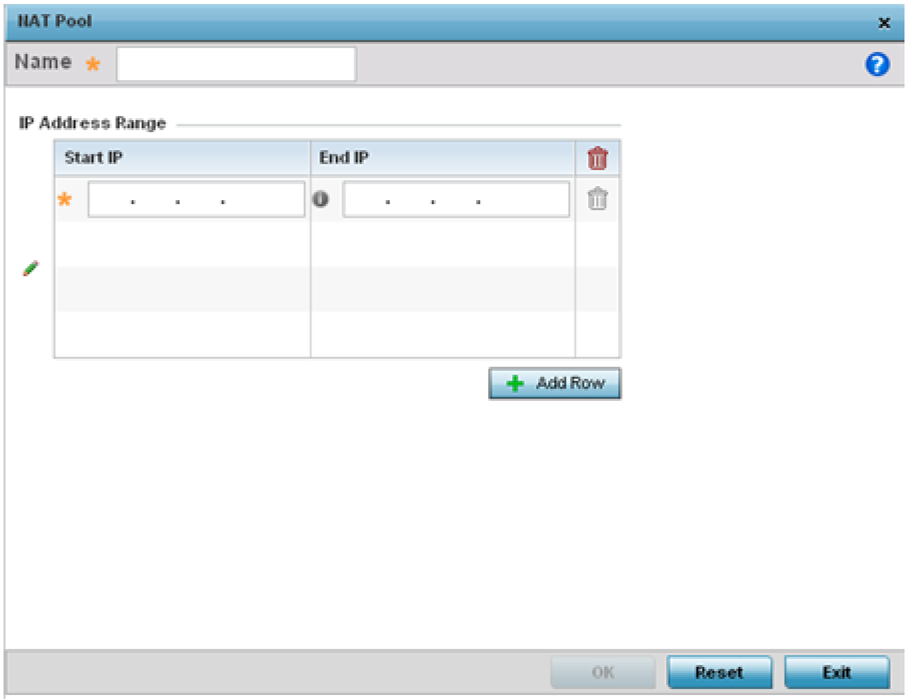
The **NAT Pool** displays by default. The NAT Pool screen lists those NAT policies created thus far. Any of these policies can be selected and applied to a profile.

3 Review existing NAT Pool policies created thus far to determine if a new policy warrants creation or an existing policy warrants modification or deletion.

Add

To add or edit a NAT configuration that can be applied to a profile:

1 Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify the attributes of a existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.



2 If adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

Name	If adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
IP Address Range	Define a range of IP addresses 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 being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

3 Select the + Add Row button as needed to append additional rows to the IP Address Range table.

4 Select OK to save the changes made to the profile's NAT Pool configuration. Select Reset to revert to the last saved configuration.

Static NAT

Static NAT maps a device's unregistered IP address to a registered IP address. It's useful when a device needs to be accessible from outside the network.

For more information, see:

- Source
- Destination

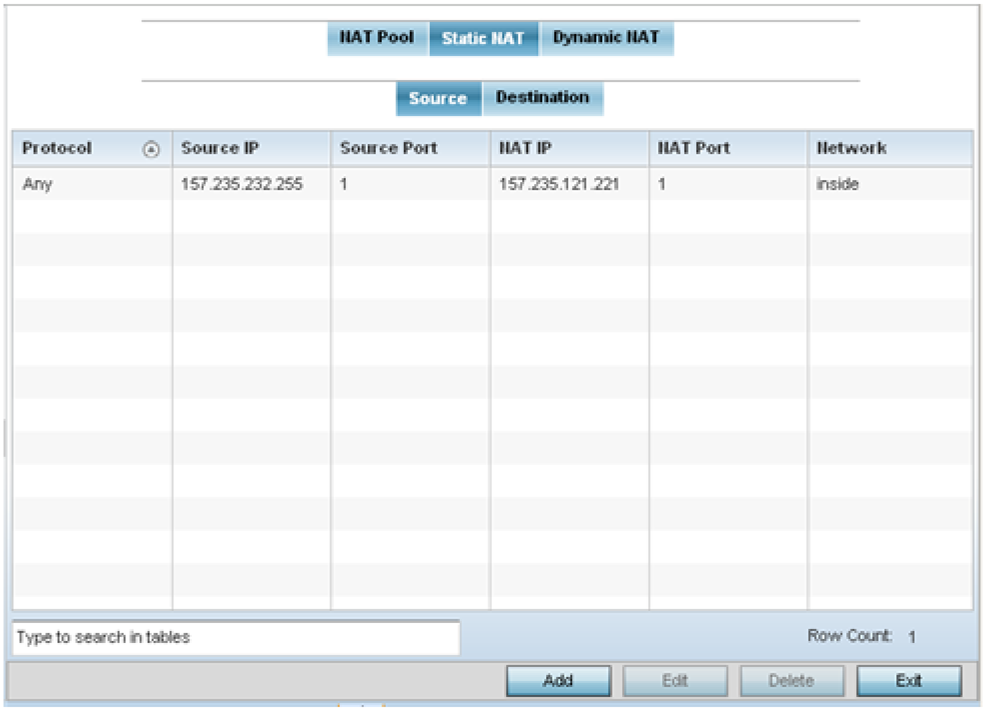
Source

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 define a static NAT configuration that can be applied to a profile:

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.



Protocol	Source IP	Source Port	NAT IP	NAT Port	Network
Any	157.235.232.255	1	157.235.121.221	1	inside

2 Select **Add** to create a new static NAT configuration. Existing NAT source configurations are not editable.

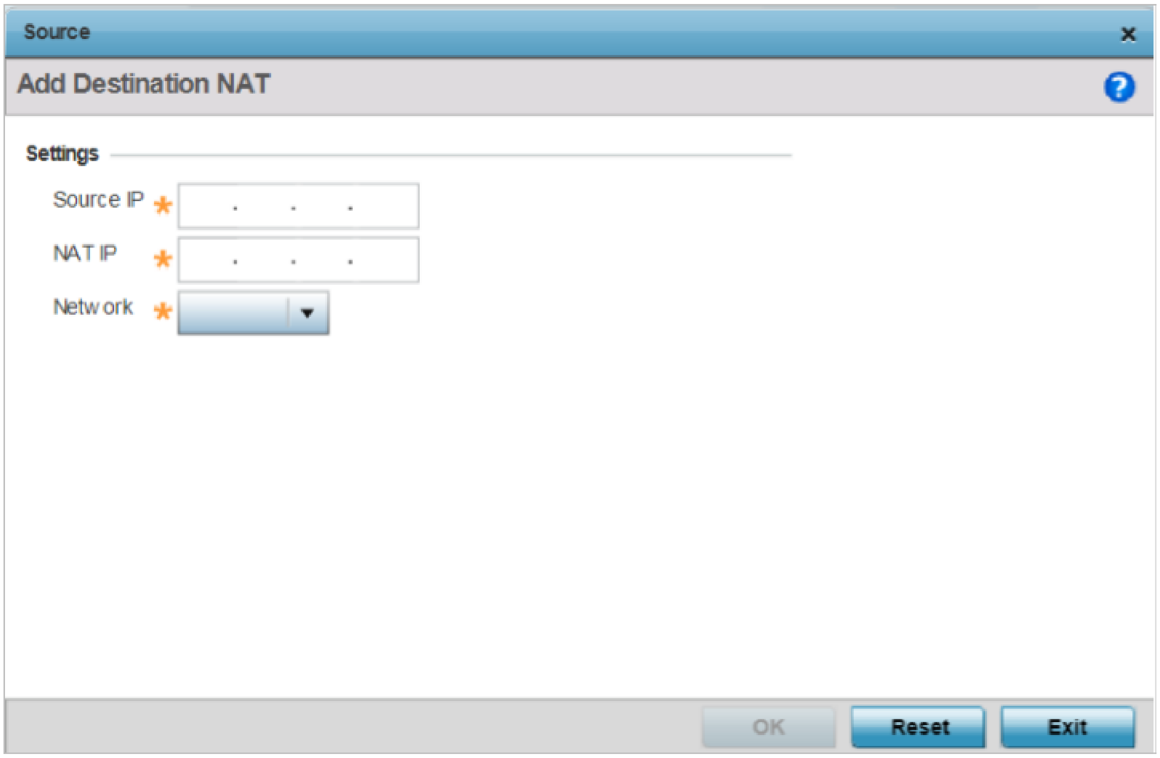


Figure 273: Static NAT Source Configuration Screen

3 Set or override the following Source configuration parameters:

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 time outs 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.
Source IP	Enter the local address used at the origination of the static NAT configuration. This address (once translated) is not exposed to the outside world when the translation address is used to interact with the remote destination.
Source Port	Use the spinner control to set the local port number used at the origination of the static NAT configuration. The default source 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	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. 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. Inside NAT is the default setting.Inside is the default setting.

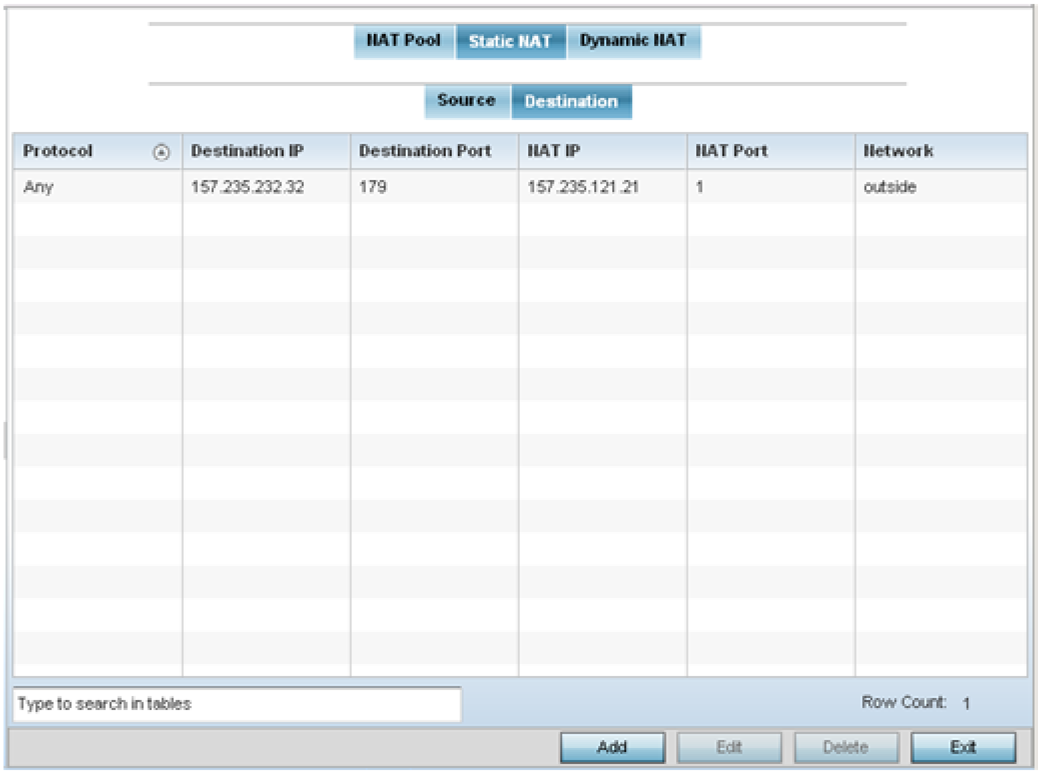
4 Select OK to save the changes or overrides made to the static NAT configuration. Select Reset to revert to the last saved configuration.

Destination

Static Destination NAT configurations ensure packets passing through the NAT back to the managed 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 set a NAT destination configuration that can be applied to a profile:

1 Select the Destination tab.



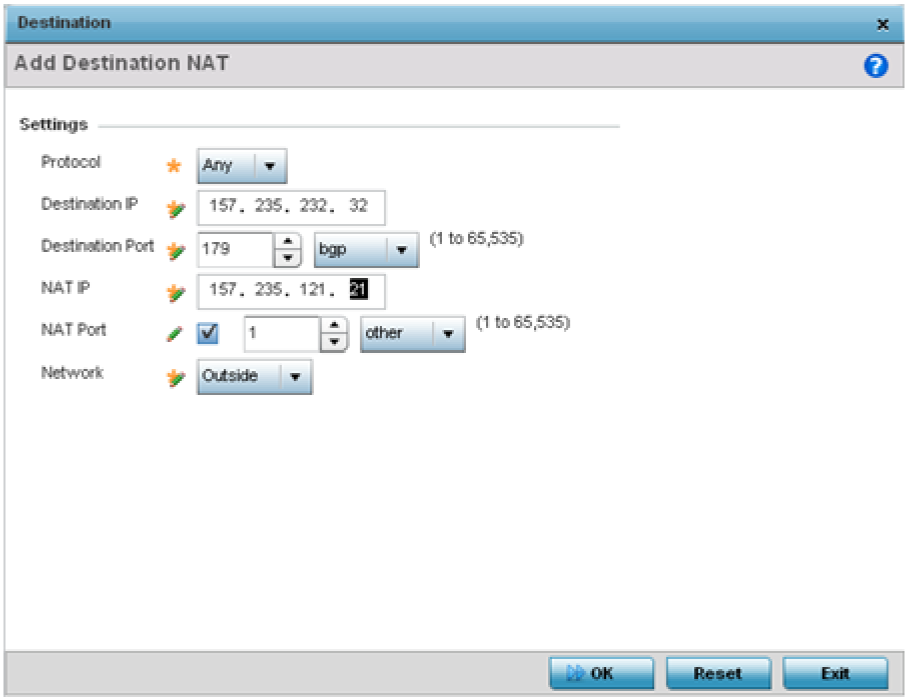
Protocol	Destination IP	Destination Port	NAT IP	NAT Port	Network
Any	157.235.232.32	179	157.235.121.21	1	outside

Row Count: 1

2 Review existing static Destination NAT configurations to determine if new configurations warrant creation or existing configurations warrant 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.

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.



Protocol: Any
Destination IP: 157. 235. 232. 32
Destination Port: 179 bgp (1 to 65,535)
NAT IP: 157. 235. 121. 21
NAT Port: ☑ 1 other (1 to 65,535)
Network: Outside

4 Set the following **Destination** configuration parameters:

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.

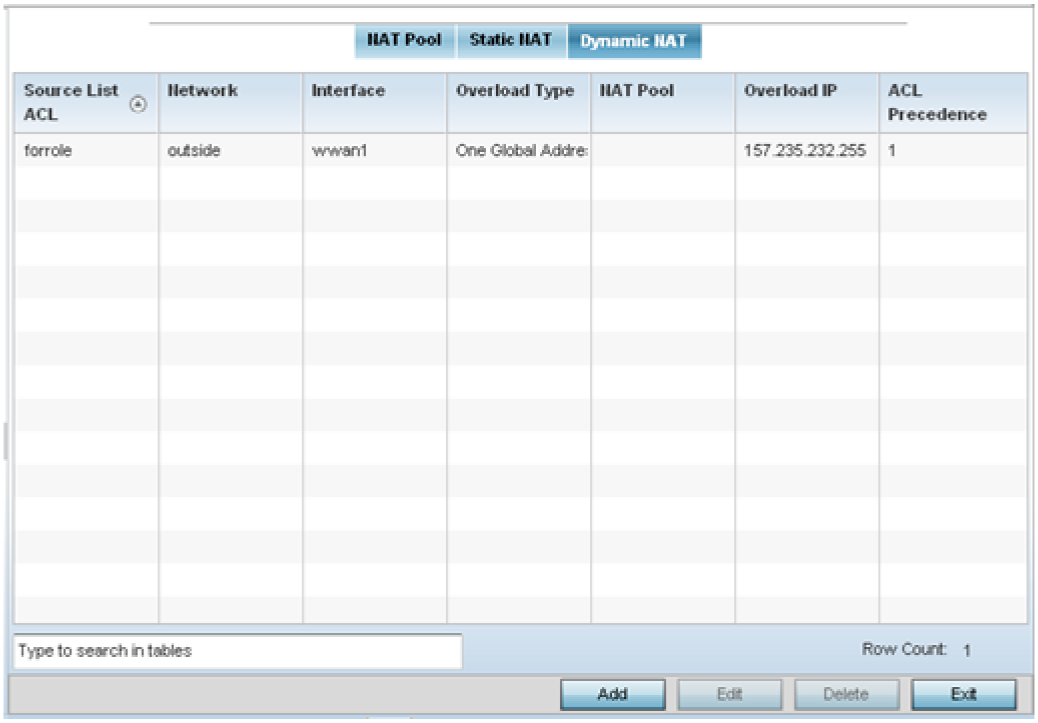
5 Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

Dynamic NAT

Dynamic NAT translates the IP address of packets 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 define a NAT configuration that can be applied to a profile:

1 Select the Dynamic NAT tab.



Source List ACL	Network	Interface	Overload Type	NAT Pool	Overload IP	ACL Precedence
forrole	outside	wwan1	One Global Addre:		157.235.232.255	1

Row Count: 1

2 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

Source List ACL	Lists an ACL name 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.
Interface	Lists the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.
Overload Type	Lists the 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	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
Overload IP	Enables the use of one global address for numerous local addresses.
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 these ACL rules.

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.

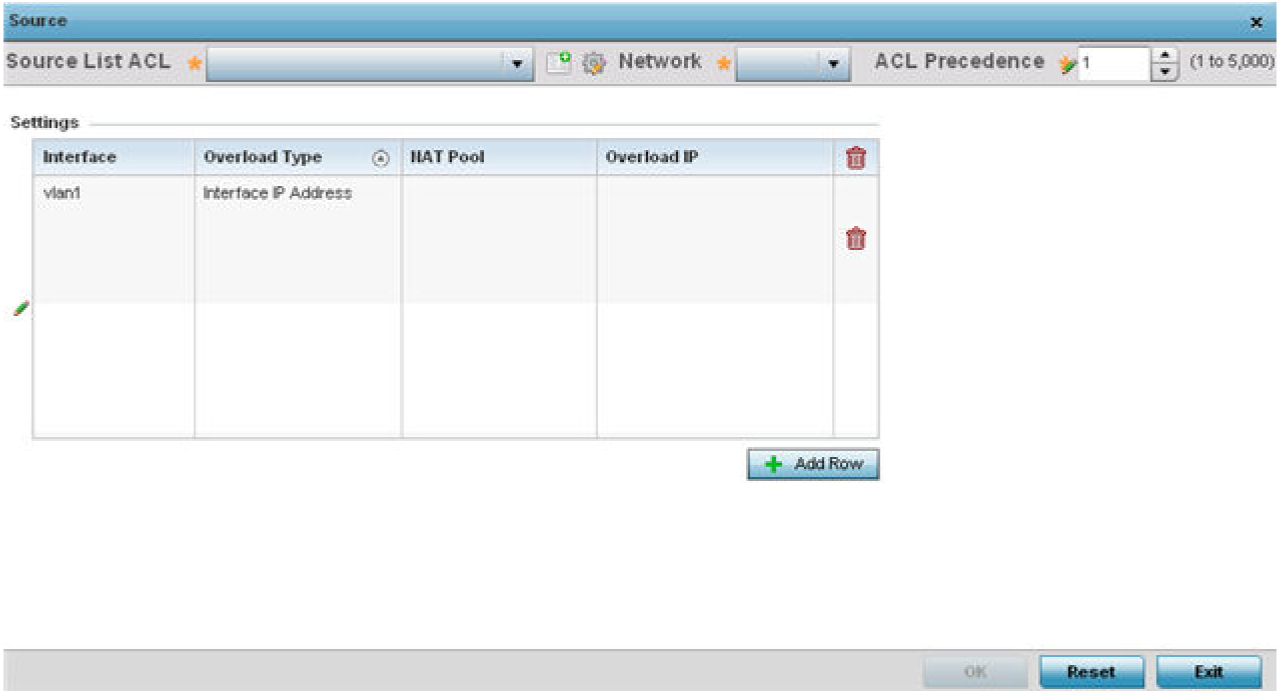


Figure 274: Profile Overrides - Security - NAT - Dynamic NAT - Source ACL List Screen

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.

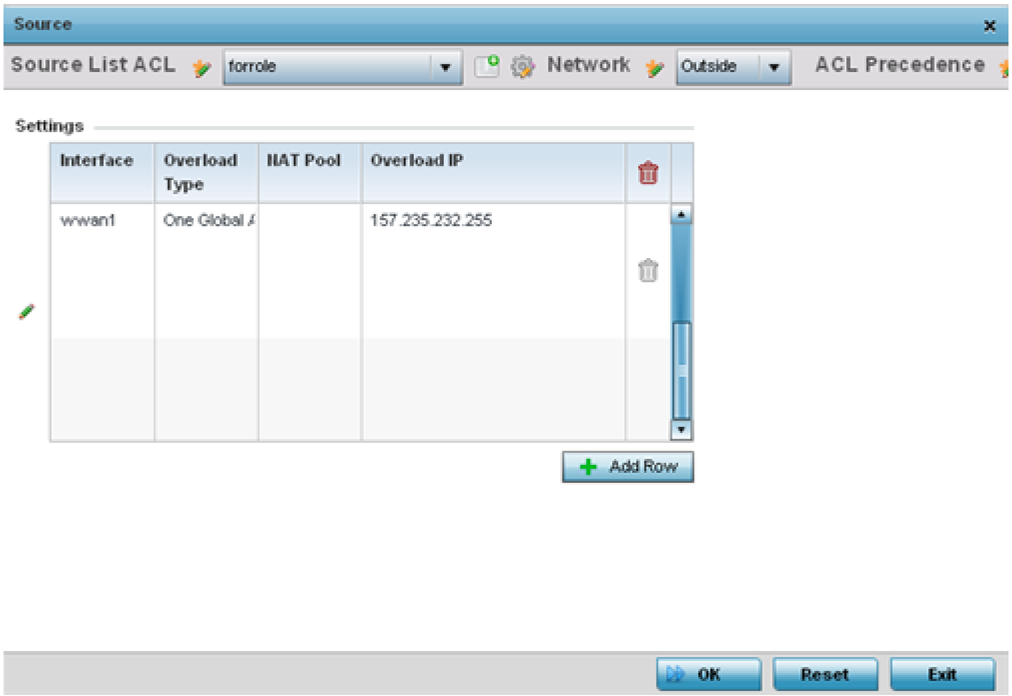
NAT Pool	Provide the name of an existing NAT pool for use with the dynamic NAT configuration. Note: This option is enabled only if the Overload Type is set or **`NAT Pool`**.
Overload IP	If **`One Global IP Address`** is selected as the **Overload Type**, define an IP address to use as a filter address for the IP ACL rule.

6 Select Add to create a new Dynamic NAT configuration, Edit to modify an existing configuration or Delete to permanently remove a configuration.

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.



Source List ACL: forrole

Network: Outside

Interface	Overload Type	NAT Pool	Overload IP
wwan1	One Global A		157.235.232.255

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, and matching packets are *NATed* to the WAN link instead of being bridged on their way to the router.

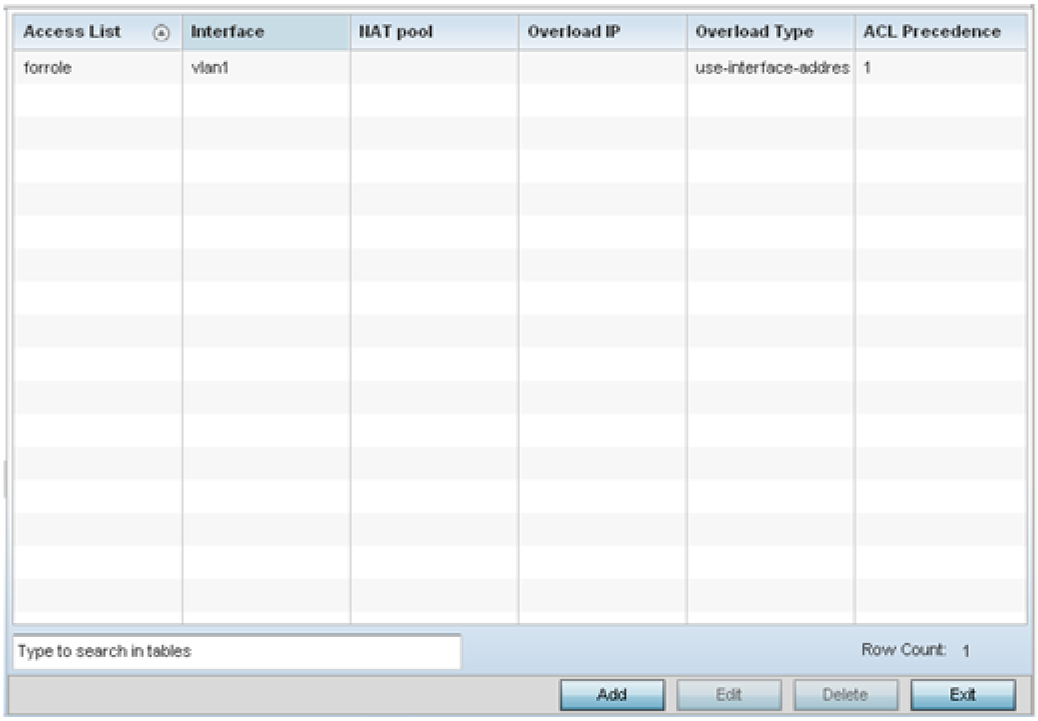
Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

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.

To define a NAT configuration that can be applied to a profile:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Expand Security and select Bridge NAT.



Access List	Interface	NAT pool	Overload IP	Overload Type	ACL Precedence
forrole	vlan1			use-interface-addres	1

Type to search in tables

Row Count: 1

3 Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration be 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 an 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* is NAT Pool.
Overload IP	Lists whether a single global address collectively supports 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.

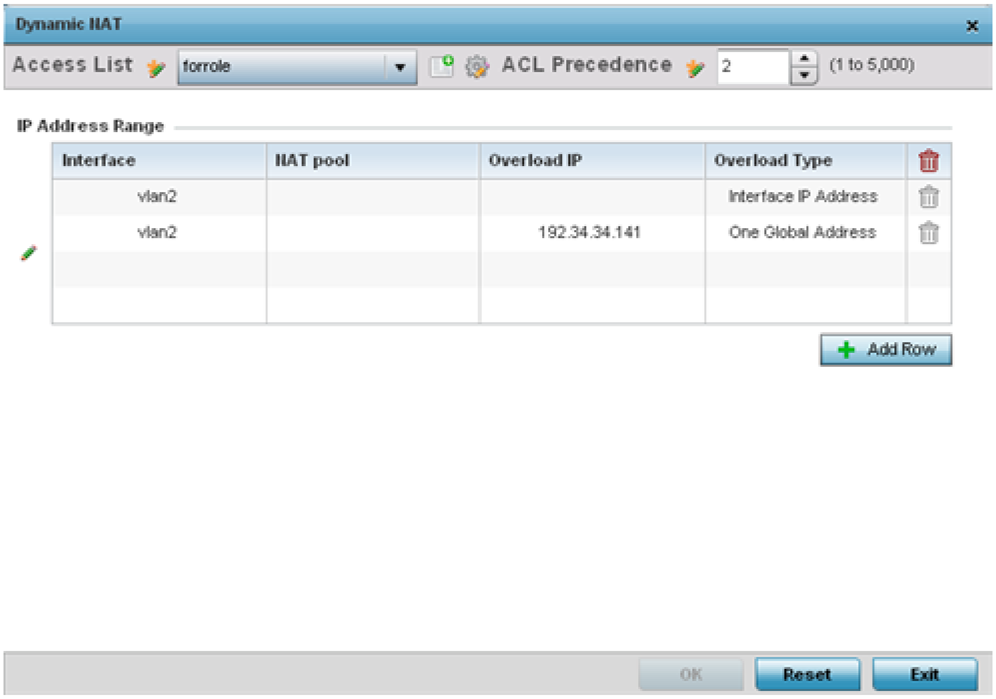
4 Select **Add** to create a new bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

Adding and Editing Bridge NAT Configurations

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 add or edit a bridge NAT configuration that can be applied to a profile:

1 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.



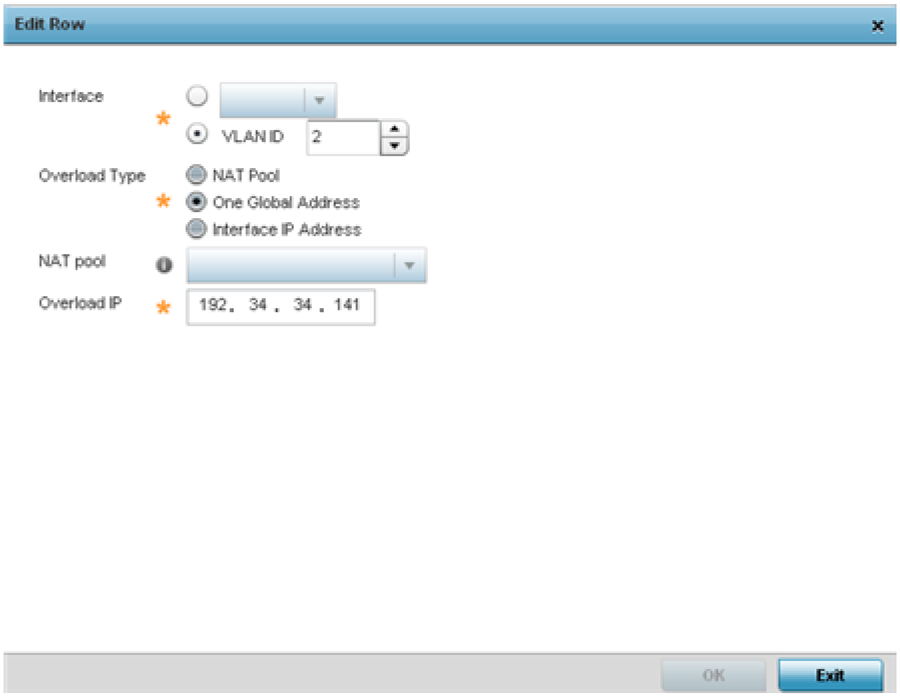
Interface	NAT pool	Overload IP	Overload Type
vlan2			Interface IP Address
vlan2		192.34.34.141	One Global Address

2 Select the ACL whose IP rules are 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 used to access the Internet.

ACL Precedence	Set the priority (from 1 - 5000) for the ACL. The lower the value, the higher the priority assigned to these ACL rules.
Interface	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an Access Point *wwan1* or *pppoe1* 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 whether the single global address supports numerous local addresses.
Overload Type	Displays the overload type for this policy based forwarding rule.

4 Select + Add Row to set IP address range settings for thebridge NAT configuration.



Interface ○ ● VLAN ID 2

Overload Type ○ NAT Pool ● One Global Address ○ Interface IP Address

NAT pool

Overload IP 192 . 34 . 34 . 141

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

Profile Security Configuration and Deployment Considerations

Before defining a profile's security configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Make sure the contents of the certificate revocation list are periodically audited to ensure revoked certificates remain quarantined or validated certificates are reinstated.
- A RFS 4000 model wireless controller ships with a baseline configuration supporting many-to-one NAT between devices connected to GE1 - GE5 ports on VLAN 1, and the UP1 port assigned to VLAN 2100. A RFS 4000 can be deployed within a small site using its default configuration, and then be connected to a Internet service providing instant access to the Internet.
- 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.
- A RFS 6000 model wireless controller ships with a minimum baseline configuration without NAT enabled. A RFS 6000 wireless controller requires VLAN configuration, IP addressing and NAT rules be created before many-to-one NAT services can be defined.
- WiNG managed controllers and service platforms can provide outbound NAT services for hosts connected to multiple VLANs. For small deployments, VLANs should be terminated within a RFS 4000 wireless controller providing site routing services. For medium-scale deployments, VLANs are typically terminated on a L3 (IP layer) or L2 (Ethernet layer).

VRRP Configuration

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. If WAN backhaul is available, and a router failure occurs, then the access point should act as a router and forward traffic on to its WAN link.

Define an external *Virtual Router Redundancy Protocol* (VRRP) configuration when router redundancy is required in a network requiring high availability.

Central to the configuration of VRRP is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

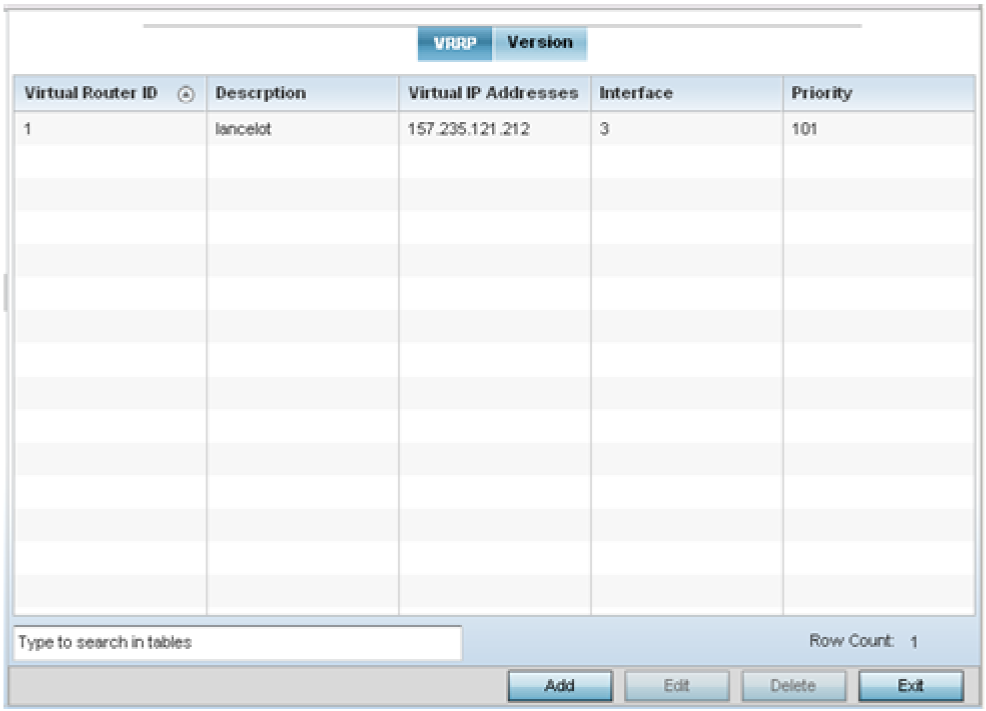
- *Responds to ARP requests*
- *Forwards packets with a destination link layer MAC address equal to the virtual router MAC address*
- *Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner*
- *Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.*

Those nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, 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.

VRRP

To define the configuration of a VRRP group:

1. Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.
2. Select VRRP.



Virtual Router ID	Description	Virtual IP Addresses	Interface	Priority
1	lancelot	157.235.121.212	3	101

Row Count: 1

3 Review the following VRRP configuration data to assess if a new VRRP configuration is required or if an existing VRRP configuration requires modification or removal:

Virtual Router ID	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.
Description	Displays 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	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
Interface	Displays the device interfaces selected to supply VRRP redundancy failover support.
Priority	Lists a numerical value (1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process.

4 Select Add button to create a new VRRP configuration. Select Edit to update an existing VRRP configuration.

Adding and Editing VRRP Configurations

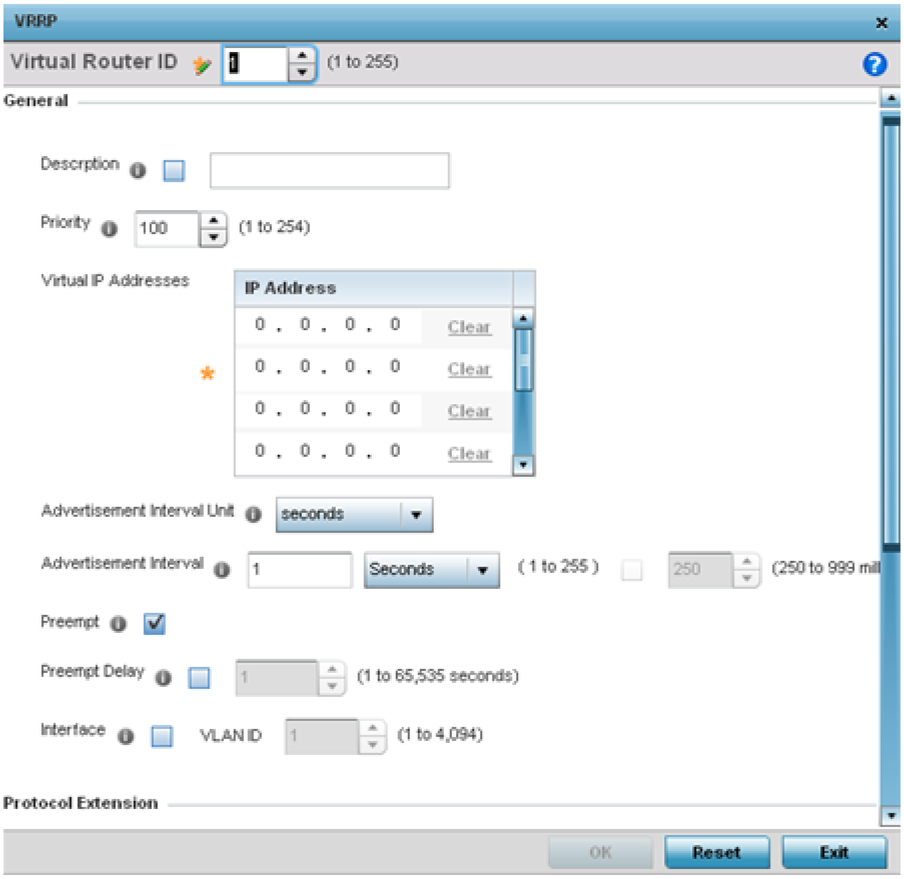
To define the configuration of a VRRP group:

1 Go to **Configuration** → **Profiles**.

2 Select VRRP.

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.

If adding or editing a VRRP configuration, the following screen displays:



Virtual Router ID 1 (1 to 255)

Description ☐

Priority 100 (1 to 254)

Virtual IP Addresses

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Advertisement Interval Unit seconds

Advertisement Interval 1 Seconds (1 to 255) ☐ 250 (250 to 999 mil

Preempt ☑

Preempt Delay ☐ 1 (1 to 65,535 seconds)

Interface ☐ VLAN ID 1 (1 to 4,094)

4 If creating a new VRRP configuration, assign a **Virtual Router ID** from (1 - 255). In addition to functioning as numerical identifier, the ID identifies the access point's virtual router a packet is reporting status for.

5 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 defined setting is used 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 8 IP addresses representing 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. Once an option is selected, the spinner control becomes enabled for that *Advertisement Interval* option. The default interval unit is seconds. If changing the VRRP group version from 2 to 3, ensure the advertisement interval is in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.
Advertisement Interval	Once a Advertisement Interval unit has been selected, use the spinner control to set the Interval at which 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 takeover 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 pre-emption.
Interface	Select this value to enable/disable VRRP operation and define the VLAN (1 - 4,094) interface where VRRP is running. These are the interfaces monitored to detect a link failure.

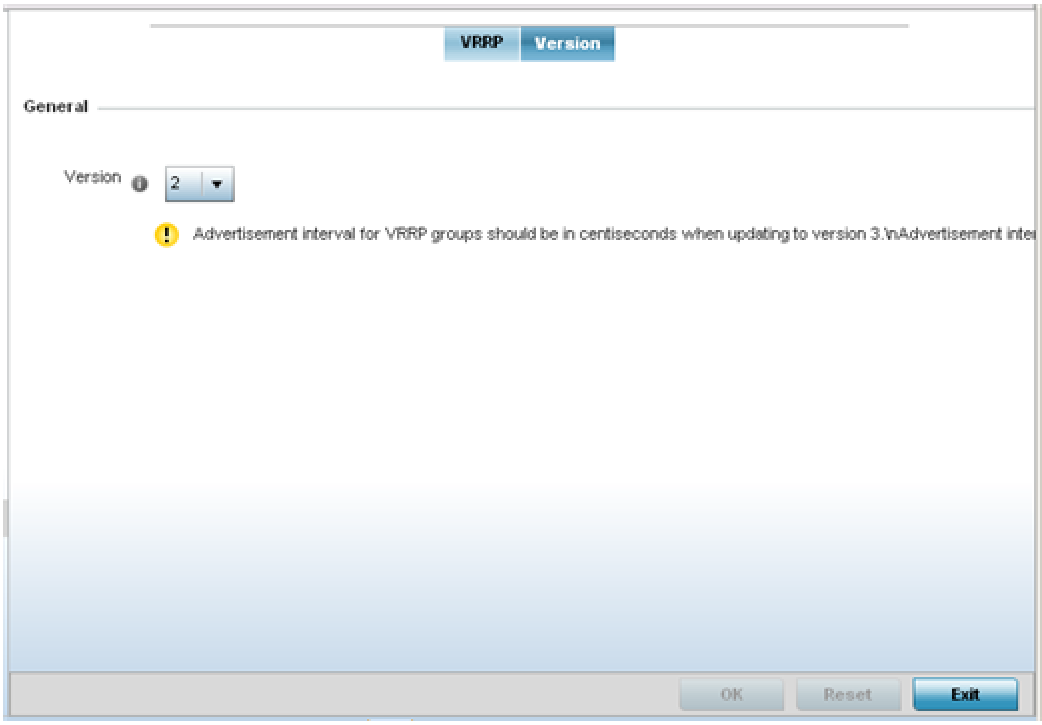
6 Refer to the **Protocol Extension** field to define the following:

Sync Group	Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled b y default.
Network Monitoring: Local Interface	Select the *wwan1*, *pppoe1* and *VLAN ID(s)* as needed to extend VRRP monitoring to these local interfaces. Once selected, these interfaces can be assigned an *increasing* or *decreasing* level or priority for virtual routing within the VRRP group.
Network Monitoring: Critical Resource Name	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 transition to the master state. 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 performing critical resource monitoring, the setting is incremented by the value defined.

7 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

Version

1 Select the **Version** tab to define the VRRP version scheme used with the configuration.



Version 2

Advertisement interval for VRRP groups should be in centiseconds when updating to version 3.\nAdvertisement inte

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.

Critical Resources Configuration

Critical resources are device IP addresses or interface destinations on the network defined as critical to the health of the controller, service platform or access point managed 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, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they're discovered. For example, a critical resource on the same subnet as an AP 8132 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 controllers, service platforms and access points using their respective device model profiles.

List of Critical Resources

A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy and one needs to be created and implemented.

To set a list of critical resources:

1 Select **Configuration** → **Profiles**.

A list of profiles (default and user-created) is displayed.

2 Select a profile from the displayed list.

The selected profile's configuration menu is displayed.

3 Select **Critical Resources**.

The List of Critical Resources screen displays.

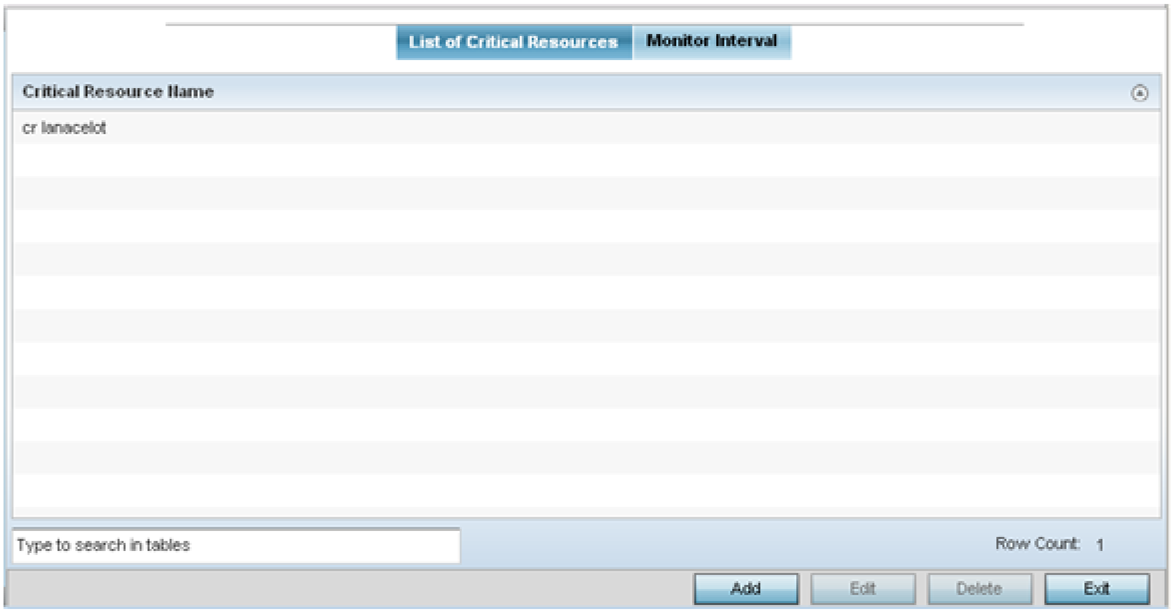


Figure 275: Configuration - Profiles - Critical Resources - List of Critical Resources Screen

4 Review existing CR configuration.

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, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5 Click **Add** to add a new critical resource and connection method, or select and existing resource and select to update the resource's configuration.

Adding and Editing Critical Resources

To add or edit a critical resource configuration:

1 Click the Add button at the bottom of the screen to add a new critical resource and connection method, or select and existing resource and select Edit to update the resource's configuration.

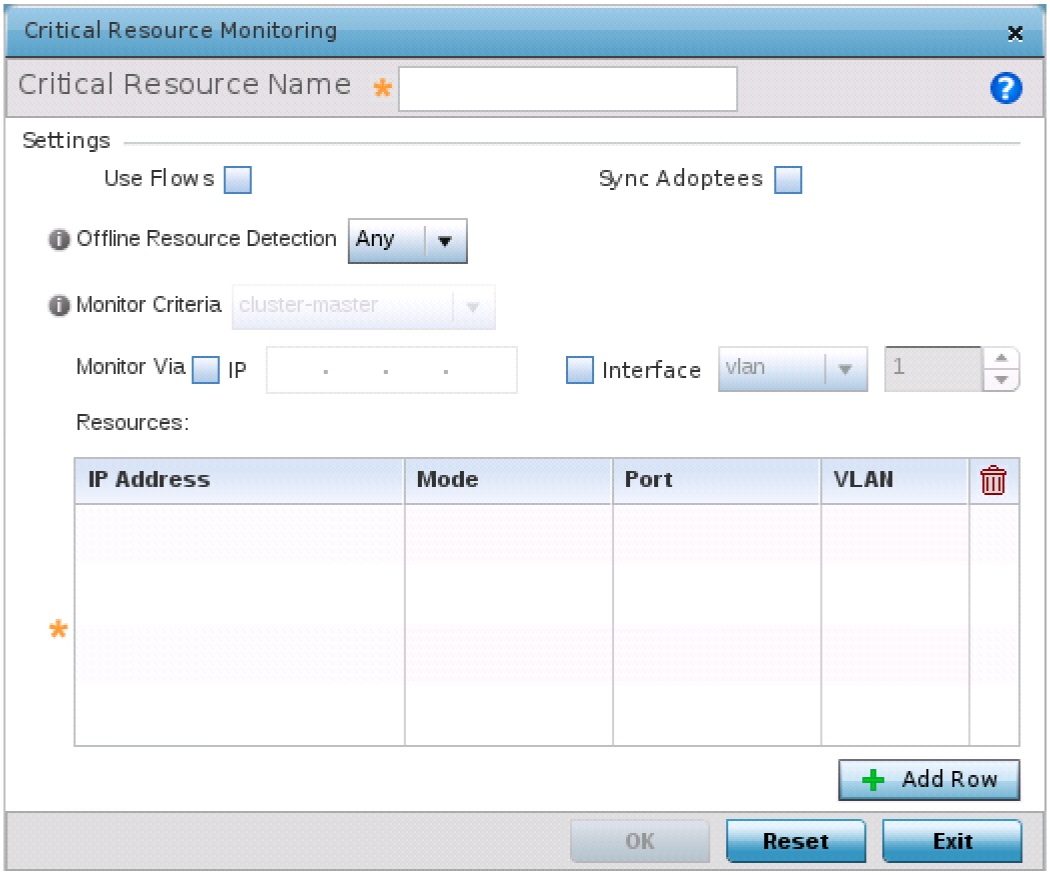


Figure 276: Critical Resources Screen - Adding a Critical Resource

2 Use the Offline Resource Detection drop-down menu to define how critical resource event messages are generated. Options include *Any* and *All*. If selecting Any, an event is generated when the state of any single critical resource changes. If selecting All, an event is generated when the state of all monitored critical resources change.

3 Select the IP checkbox (within the Monitor Via field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided critical resource IP address as a network identifier.

4 Select the Interface checkbox (within the Monitor Via field at the top of the screen) to monitor a critical resource using either the critical resource's VLAN, WWAN1 or PPPoE1 interface. If VLAN is selected, a spinner control is enabled to define the destination VLAN ID used as the interface for the critical resource.

5 Use the Resource Detection drop-down menu to define how critical resource event messages are generated. Options include Any and All. If selecting Any, an event is generated when the state of any single critical resource changes. If selecting All, an event is generated when the state of all monitored critical resources change.

6 Select + Add Row to define the following for critical resource configurations:

IP Address	Provide the IP address of the critical resource. This is the address used 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 by the controller, service platform or access point. Select from: •*arp-only* – Use the *Address Resolution Protocol* (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known. •*arp-and-ping* – Use both ARP and *Internet Control Message Protocol* (ICMP) for pining the critical resource and sending control messages (device not reachable, requested service not available, etc.).
Port	Use the drop-down menu to provide the physical port for each critical resource. The ports available depend on the device in use.
VLAN	Define the VLAN on which the critical resource is available using the spinner control.

7. Select **OK** to save the changes to the critical resource configuration. Select **Reset** to revert to the last saved configuration.

Monitor Interval

To define a critical resource's monitoring interval:

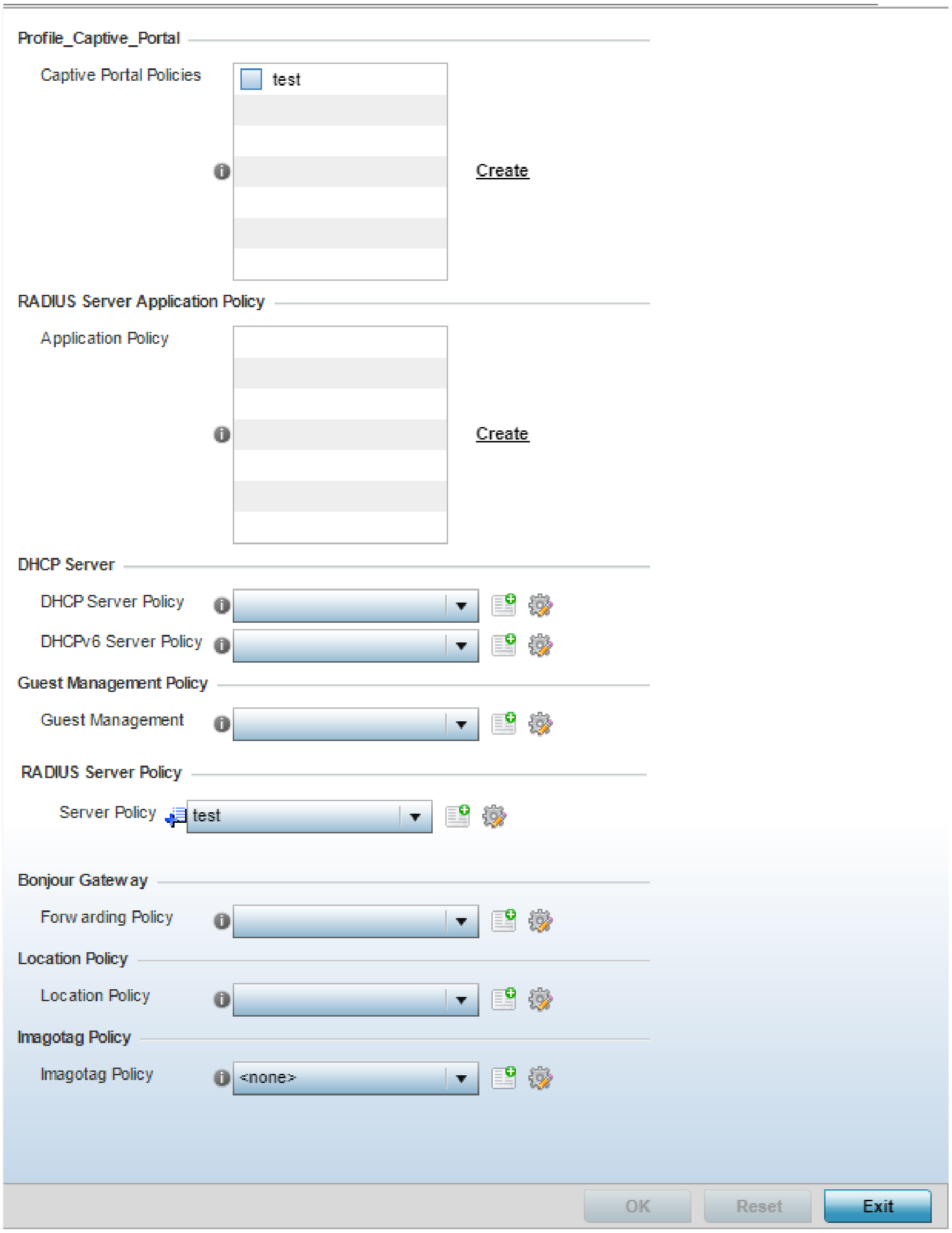
1. Select the **Monitor Interval** tab.
2. Set **Monitor Interval** as the duration between two successive pings to the critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.
3. Set the **Source IP for Port-Limited Monitoring** to define the IP address used 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 APR packets used to detect critical resources. However, some devices do not support the above 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. Set the **Monitoring Retries before Marking Resource as DOWN** for 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. Select **OK** to save the changes to the critical resource monitor interval. Select **Reset** to revert to the last saved configuration.

Profile Services Configuration

A profile can contain specific captive portal, DHCP server and RADIUS server configurations supported by a controller, service platform or access point's own internal resources. These captive portal, IP assignment and user authorization resources can be defined uniquely as profile requirements dictate.

To define a profile's services configuration:

1. Go to **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.
2. Select a target profile from the right-hand menu. The profile's configuration menu displays.
3. Select **Services.**



Profile_Captive_Portal

Captive Portal Policies: ☐ test — Create

RADIUS Server Application Policy

Application Policy — Create

DHCP Server

DHCP Server Policy

DHCPv6 Server Policy

Guest Management Policy

Guest Management

RADIUS Server Policy

Server Policy: test

Bonjour Gateway

Forwarding Policy

Location Policy

Location Policy

Imagotag Policy

Imagotag Policy: <none>

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 the **Clear Overrides** button. This removes all overrides from the device.

4 Refer to the Captive Portal Hosting section to select or set a guest access configuration (captive portal) for use with this profile.

A *captive portal* is guest access policy for providing guests temporary and restrictive access to the network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals capture and redirect 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 *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal that can be applied to the profile. For morel information, see Captive Portal Policies on page 834.

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, select 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, select the Create button to create a new policy configuration that can be applied to this profile.

   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 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 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).

   Either select an existing captive portal policy or select the **Create** button to create a new captive portal configuration that can be applied to this profile. Existing policies can be modified by selecting the **Edit** icon. For more information, see Setting the DHCP Configuration on page 858.
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, select the Create icon to create a new policy configuration that can be applied to this profile or 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 authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.

If an existing RADIUS server policy does not meet your requirements, select the **Create** button to create a new policy configuration that can be applied to this profile. Existing policies can be modified by selecting the **Edit** icon. For more information, see Setting the RADIUS Configuration on page 884.

9. Use the **Guest Management Policy** drop-down menu to select an existing Guest Management policy to use as a mechanism to manage guest users with this profile.
10. From the **Forwarding Policy** drop-down, select the Bonjour Gateway forwarding policy.

    Set **Bonjour Gateway** settings. 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 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 only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.
11. Use the **Location Policy** drop-down menu to select and apply a location policy to the controller/virtual controller. The location policy provides the ExtremeLocation server's hostname and ExtremeLocation tenant's location API key. This information is required by the controller to authenticate and authorize with the ExtremeLocation server. Use the **Create** or **Edit** icons to create a new policy or edit an existing policy.

    Note
    For information on creating location policies, see Location Policy on page 449.
12. 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** or **Edit** icons to create a new policy or edit an existing policy. The Imagotag feature is supported only on the AP-8432 model access point.

    For information on enabling support for SES-imagotag’s ESL tags on WiNG APs with USB interfaces, see Setting the Imagotag Policy on page 900.
13. Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

Profile Services Configuration and Deployment Considerations

Before defining a profile's captive portal, DHCP and RADIUS services 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 captive portal and the services provided, or if the profile should support captive portal access at all, since captive portals do increase the risk to the wireless network versus more secure access methods.
- 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 captive portals.
- 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 an internal DHCP resource is also provisioned with a strong user authorization and validation configuration.

Profile Management Configuration

Controllers, service platforms and access points have mechanisms to *allow* or *deny* management access to the network for different interfaces and protocols (*HTTP*, *HTTPS*, *Telnet*, *SSH* or *SNMP*). These management access configurations can be applied strategically to profiles as resource permissions dictate.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support. In a clustered environment, these operations can be performed on one member, then propagated to each cluster member and onwards to the devices managed by each cluster member.

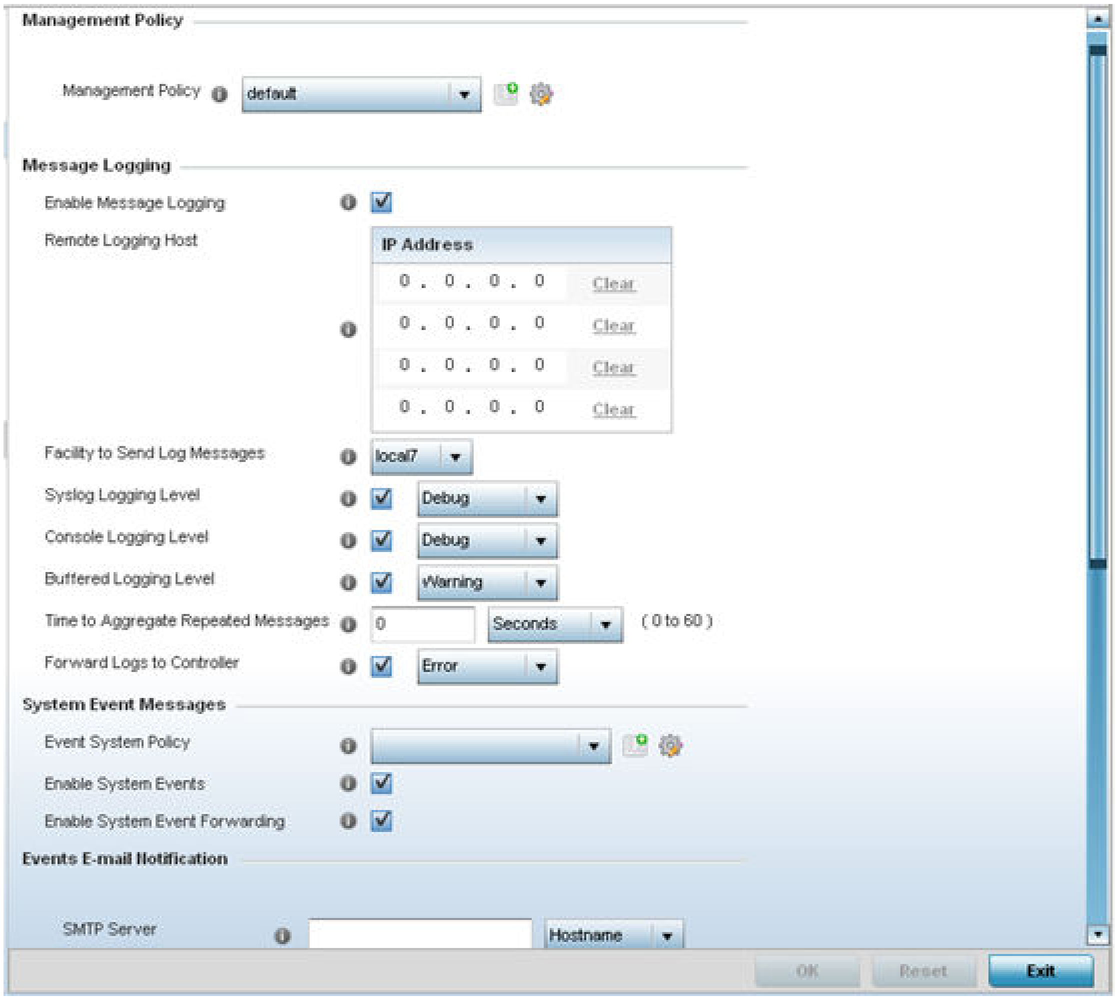
Management Settings

To define a profile's management configuration:

1. Select **Configuration** → **Profiles**.

   A list of profiles (default and user-created) is displayed.
2. Select a profile from the displayed list.

   The selected profile's configuration menu is displayed.
3. Expand the Management menu and select **Settings**.



Management Policy

Management Policy: default

Message Logging

Enable Message Logging ☑

Remote Logging Host

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Facility to Send Log Messages: local7

Syslog Logging Level ☑ Debug

Console Logging Level ☑ Debug

Buffered Logging Level ☑ Warning

Time to Aggregate Repeated Messages: 0 Seconds (0 to 60)

Forward Logs to Controller ☑ Error

System Event Messages

Event System Policy:

Enable System Events ☑

Enable System Event Forwarding ☑

Events E-mail Notification

SMTP Server: Hostname

Figure 277: Profiles Management Settings Tab

4 Refer to the **Management Policy** field to select or set a management configuration for use with this profile. A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If no management policies exist meeting the data access requirements of this profile, select the **Create** icon to access a series of screens used to define administration, access control and SNMP configurations. Select an existing policy and select the **Edit** icon to modify the configuration of an existing management policy.

5 Use to the **Critical Resource Policy** drop-down menu to set a critical resource policy for use with this profile. For more information on defining a critical resource policy, see Overriding a Critical Resource Configuration on page 287.

6 Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to determine an overall pattern that may be negatively impacting performance using the configuration defined for this profile.

Enable Message Logging	Select this option to enable the profile to log system events to a user defined 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.
Remote Logging Host	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select *Clear* as needed to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the local server facility (if used) for the profile event log transfer.
Syslog 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.
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.
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.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of this profile. 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 the checkbox to define a log level for forwarding event logs. 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** section to set how system messages are logged and forwarded on behalf of the profile.

Event System Policy	Select an Event System Policy from the drop-down menu. If an appropriate policy does not exist click the *Create* button to make a new policy.
Enable System Events	Select this option to allow the profile to capture system events and append them to a log file. It's important to log individual events to determine an overall pattern that may be negatively impacting performance. This setting is enabled by default.
Enable System Event Forwarding	Select the Enable System Event Forwarding box to enable the forwarding of system events to another cluster member. This setting is enabled by default.

8 Refer to the **Events E-mail Notification** section to define how system event notification emails are sent.

SMTP Server	Specify either the *Hostname* or *IP Address* of the outgoing SMTP server where notification emails will be originated.
Port of SMTP	If a non-standard SMTP port is use on the outgoing SMTP server check this box and specify a port between 1 and 65,535 for the outgoing SMTP server to use.
Sender Email Address	Specify the 64 character maximum email address from which notification emails are originated. This is the from address on notification emails.
Recipient’s E-mail Address	Specify up to 6 Email addresses to be the recipient’s 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 a *username* and *password* before sending email through the server.
Password for SMTP Server	Specify the password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a *username* and *password* before sending email through the server.

9 Refer to the **Persist Configurations Across Reloads** field to define how configuration settings are handled after reloads.

Use the drop-down menu to configure whether configuration updates should persist when the device configuration is reloaded. Available options are *Enabled*, *Disabled* and *Secure*.

10 Refer to the **External Analytics Engine** section to set analytics engine login information for an external host.

The Guest Access & Analytics software module is a site-wide Enterprise License available only on the NX9000 service platforms. When a customer visits a store, they connect to the Wireless LAN via guest access using a client device. The user needs to authenticate only on their first visit, and will automatically connect to the network for subsequent visits. The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors. The data can be exported for additional in-depth analysis.

Controller	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
URL	When using an external analytics engine with a NX9000 series service platform, enter the IP address or uniform resource locator (URL) for the system providing external analytics functions.
User Name	Enter the user name needed to access the external analytics engine
Password	Enter the password associated with the username on the external analytics engine.
Update Interval	Set the interval in either *Seconds* (1 - 3,600), *Minutes* (1 - 60) or *Hours* (1) to forward buffered information to an external server resource, even when the buffers are not full. The default setting in 1 minute.

11 Select **OK** to save the changes made to the profile's management settings. Select **Reset** to revert to the last saved configuration.

Firmware

An administrator can provide a profile with unique device configuration file and firmware upgrade support. In a clustered environment, these operations can be performed on one device, then propagated to each member of a cluster and onwards to devices managed by each cluster member. The number of concurrent device upgrades and their start times can be customized to ensure a sufficient number of devices remain in duty while upgrades are administered to others. Additionally, AP71XX and AP650 legacy access points can be updated from their legacy WiNG 4.x firmware baseline to the most recent 5.x firmware baseline to ensure they're operating with the most recent feature set.

To define a profile's access point upgrade configuration:

1 Select **Configuration** → **Profiles**.

A list of profiles (default and user-created) is displayed.

2 Select a profile from the displayed list.

The selected profile's configuration menu is displayed.

3 Expand **Management** and select **Firmware**.

4 Refer to the **Auto Install via DHCP Option** section to configure automatic configuration file and firmware updates.

Enable Configuration Update	Select the *Enable Configuration Update* radio button (from within the Automatic Configuration Update field) to enable automatic configuration file updates for the profile from an external location. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update.
Enable Firmware Upgrade	Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. This value is disabled by default.
Start Time (minutes)	Use the spinner control to set the number of minutes to delay the start of an auto upgrade operation. Stagger the start of an upgrade operation as needed in respect to allowing an access point to complete its current client support activity before being rendered offline during the update operation. The default setting is 10 minutes.

5 Refer to the parameters within the **Legacy Device Firmware Management** field to set legacy access point firmware provisions:

Migration Firmware from AP71xx 4.x path	Provide a path to a firmware image used to provision AP71xx model access points currently utilizing a 4.x version legacy firmware file. Once a valid path is provided, the update is enabled to the version maintained locally for AP71xx models.
Legacy AP650 Auto Update	Select this option to provision AP650 model access points from their legacy firmware versions to the version maintained locally for that model. This setting is enabled by default, making updates to AP650 models automatic if a newer AP650 image is maintained locally.

6 Use the parameters within the **Automatic Adopted AP Firmware Upgrade** section to define an automatic firmware upgrade from a local file.

Enable Controller Upgrade of AP Firmware	Select this radio button to enable adopted radios to upgrade to a newer firmware version using its associated controller's most recent resident firmware file for that access point model. This parameter is disabled by default.
Number of Concurrent Upgrades	Use the spinner control to define the maximum number (1 - 20) of adopted access points that can receive a firmware upgrade at the same time. Keep in mind, during a firmware upgrade, the access point is offline and unable to perform its normal wireless client support function until the upgrade process is complete and the access point rebooted.

7 Select the **Persist Image on Controller** button (from within the **Firmware Persistence for Adopted Devices** field) to enable a NX 4500, NX 6500, or NX 9000 series RF Domain manager to retain and store the new image of an access point selected for a firmware update. The image is only stored on the RF Domain manager when there's space to accommodate it.

The upgrade sequence is different depending on whether the designated RF Domain manager is a controller/service platform or access point.

- *When the RF Domain manager is an access point* - The NOC uploads a provisions an access point model's firmware on to the access point RF Domain manager. The NOC initiates an auto-update for access points using that model's firmware. If the **Persist Image on Controller** option is selected, the RF Domain manager retains the image for that model. The NOC then provisions the firmware of the next access point type to the RF Domain manager. The auto-update process is then repeated for that model. Once all the selected models have been updated, the RF Domain manager's model is updated last.

- *When the RF Domain manager is a controller or service platform* - The NOC adopts controllers to the NOC's cluster within its RF Domain. The NOC triggers an update on active controllers or service platforms and reboots them as soon as the update is complete. As soon as the active nodes come back up, the NOC triggers an update on standby controllers or service platforms and reboots them as soon as the update is complete. When the standby controllers or service platforms come back up the following conditions apply: *If the reboot is not scheduled* - The access points adopted to RF Domain members are not updated. It's expected the controllers and service platforms have auto-upgrade enabled which will update the access points when re-adopted. *If the reboot is scheduled* - The NOC pushes the first access point model's firmware to the RF Domain manager. The NOC initiates an access point upgrade on all access points on the RF Domain manager for that model. If the Persist Image on Controller option is selected, the RF Domain manager retains the image for that model. The NOC then provisions the firmware of the next access point type to the RF Domain manager. This process is repeated until each selected access point model is updated.

The Persist Image feature is *enabled* for all controller and service platform RF Domain managers with the flash memory capacity to store firmware images for the selected access point models they provision. This feature is *disabled* for access point RF Domain managers that do not typically have the flash memory capacity needed.

8. Select OK to save the changes made to the profile's Management Firmware configuration. Select Reset to revert to the last saved configuration.

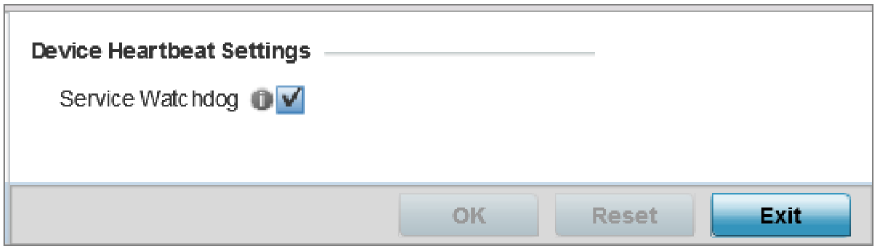
Overriding Management Heartbeat

To define or override a profile's management configuration:

1. Select **Configuration** → **Profiles**.

   A list of profiles (default and user-created) is displayed.
2. Select a profile from the displayed list.

   The selected profile's configuration menu is displayed.
3. Expand Management and select Heartbeat.



Device Heartbeat Settings

Service Watchdog ☑

Figure 278: Management - Heartbeat Configuration Screen

4. 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.

5 Click **OK** to save the changes and overrides made to the profile’s configuration.

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

Profile Management Configuration and Deployment Considerations

Before defining a profile's management configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Set profile management access configurations that provide both encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide data privacy and authentication.
- SNMPv3 should be used for management profile configurations, as it provides both encryption and authentication.

Profile Mesh Point Configuration

Mesh points are WiNG managed access points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere (including moving vehicles).

To set a profile's mesh point configuration:

1. Go to **Configuration** → **Profiles** → **Manage Profiles**.
2. Select a target profile from those listed on the screen
3. Select Mesh Point.
4. Refer to the Mesh Point screen to review existing mesh point configurations and determine whether a new mesh point configuration requires creation or an existing mesh point configuration requires modification.

MeshConnex Policy	Lists the administrator assigned name for the MeshConnex Policy, defined upon its creation. The name cannot be edited later with other parameters.
Is Root	Displays whether the mesh point is the root node in the mesh network or not. A green checkmark defines the mesh point as a root, a red X does not.
Preferred Root	Lists the MAC address of a preferred root device.
Preferred Neighbor	Lists the MAC address of the preferred neighbor within the mesh point's mesh topology.
Preferred Interface	Displays either *2.4GHz* or *5 GHz* as the preferred band of operation for the mesh point.
Monitor Critical Resources	When enabled (as defined by a green checkmark) you allow the dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.

Monitor Primary Port Link	When enabled (as defined by a green checfkmark) you allow the dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.
Path Method	Lists the method used for path selection in a mesh network. Available options include: *None* – No criteria used in root path selection. *uniform* – Indicates the path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). *mobile-snr-leaf* – The access point is mounted on a vehicle or a mobile platform (AP 7161 models only). The path to the route is selected based on the SNR *(Signal To Noise Ratio)* with the neighbor device. *snr-leaf* – Indicates the path with the best signal to noise ratio is always selected.

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 (car, train etc.). A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility.

5. If an existing mesh point does not meet your requirements, select the **Add** button to create a new configuration or the **Edit** button to modify the parameters of an existing configuration.
6. 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 when enabling VMM.
   - Set the RTS threshold value to 1 on all mesh devices. The default is 2347.
   - Use Opportunistic as the rate selection setting for the AP7161 radio. The default is Standard.
   - Disable Dynamic Chain Selection (radio setting). The default is enabled. This setting can be disabled in the CLI using the *dynamic-chain-selection* command, or in the UI.
   - Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph.
   - Consider setting a misconfiguration recovery time for the non-root AP profile. This configuration should delay the rejection of the newest configuration push from the controller, potentially causing adoption loss.

     The additional delay is to support cases when the new configuration from the controller causes the root AP to move from current channel to other channels, resulting in a mesh link going down, and in turn non-root APs losing adoption. This delay accommodates the time needed for the non-root AP to scan all channels and finding the best root node. The non-root AP can begin operating on the new channel, and establish the mesh link re-adopt to the controller. (For countries using DFS, the scan time is also factored in for the configured value). If the AP fails to find a suitable root node within this time, this new config is a misconfiguration and the device would reject the latest config.

     For outdoor APs, it is recommended the misconfiguration-recovery-time be disabled. This can be accomplished by setting the value to 0. Update non root ap71xx profiles on the controller to include this change.

     Using an appropriate console terminal and or connection to your device log on to the CLI and follow these steps:

     ```
     nx9500-xxxxxx>enable
     ```

```
nx9500-xxxxxx #configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

nx9500-xxxxxx (config)#profile ap71xx Non-Root AP71xx

nx9500-xxxxxx (config-profile-Non-Root-AP71xx)#misconfiguration-recovery-time 0

nx9500-xxxxxx (config-profile-Non-Root-AP71xx)
```

MeshConnex Policy Settings

To set a mesh point's policy setting configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Select **Manage Profiles** from the Configuration > Profiles menu.
4. Select **Mesh Point.**
5. Refer to the **Mesh Point** screen to review existing mesh point configurations and determine whether a new mesh point configuration requires creation or an existing mesh point configuration requires modification.
6. If an existing Mesh Point configuration does not meet your requirements, select the **Add** button to create a new configuration or **Edit** to modify the parameters of an existing configuration.

   The **Settings** tab displays by default.
7. Set the following **General** parameters:

MeshConnex Policy	If adding a new policy, specify a name for the MeshConnex Policy. The name cannot be edited later with other configuration parameters. Until a viable name is provided, the Settings tab cannot be enabled for configuration.
Is Root	Select the root behavior of this mesh point. Select *True* to indicate this mesh point is a root node for this mesh network. Select *False* to indicate this mesh point is not a root node for this mesh network.
Root Selection Method	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint.
Set as Cost Root	Select this option to set the mesh point as the cost root for meshpoint root selection. This setting is disabled by default.
Monitor Critical Resources	Enable this feature to allow dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.
Monitor Primary Port Link	Enable this feature to allow dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.

Wired Peer Excluded	Select this option to exclude a mesh from forming a link with another mesh device that's a wired peer. This option is disabled by default.
Path Method	Use the drop-down menu to select the method (criteria) used for selecting the root path. *None* – Select this to indicate no criteria used in root path selection. *uniform* – Select this to indicate that the path selection method is uniform. When selected, two paths will be considered equivalent if the average value is the same for these paths. *mobile-snr-leaf* – Select this if this access point is mounted on a vehicle or a mobile platform (AP 7161 models only). When selected, the path to the route will be selected based on the Signal To Noise Ratio (SNR) to the neighbor device. *snr-leaf* – Select this to indicate that the path with the best signal to noise ratio is always selected.

Note

When using 4.9GHz, the root preferences selection for the radio's preferred interface still displays as 5GHz.

1 Set the following **Root Path Preferences**:

Preferred Neighbor	Specify the MAC address of a preferred neighbor within the mesh topology.
Preferred Root	Specify the MAC address of a a preferred root device.
Preferred Interface	Use the drop-down menu to set the preferred mesh point interface to either *2.4GHz*, *4.9GHz* or *5.0GHz*.

2 Set the following **Root 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.
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.
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.
Root selection SNR Delta Range	Select the root selection method hysteresis (from 1 - 100dB) Root Selection Delta Range. The device must sustain a signal strength within the delta range to be considered a candidate. The default setting is 10 dB.

3 Select **OK** to save the updates to the Settings screen. Select **Reset** to revert to the last saved configuration.

Auto Channel Selection

The Auto Channel Selection screen is used to define the Dynamic Root Selection, Path Method SNR, and Path Method Root Path Metric.

Use the **Dynamic Root Selection** screen to refine channel scans, set the scan duration, whether scans are conducted off-channel, scan sample size and channel hold time.

Use the **Path Method SNR** screen to set a profile's mesh point channel width, mesh point priority and *signal to noise* (SNR) scan settings.

Use the **Path Method Root Path Metric** screen to set a profile's mesh point root path scan settings.

Dynamic Root Selection

Use the **Dynamic Root Selection** screen to refine channel scans, set the scan duration, whether scans are conducted off-channel, scan sample size and channel hold time.

To define a profile's mesh point dynamic root selection:

1. Select the **Configuration** tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Select **Manage Profiles** from the Configuration > Profiles menu.
4. Select **Mesh Point.**

   Refer to the Mesh Point screen to view existing Mesh Points. If an existing Mesh Point configuration does not meet your requirements, select the Add button to create a new mesh point configuration or the Edit button to modify the parameters of an existing mesh point configuration. The Mesh Point screen displays the Settings tab by default.
5. Select the **Auto Channel Selection** tab.

   The Dynamic Root Selection screen displays by default.
6. Set the following values (common to 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: *Automatic* – Defines the channel width is calculated automatically. This is the default value. *20 MHz* – Sets the width between two adjacent channels as 20 MHz. *40 MHz* – Sets the width between two adjacent channels as 40 MHz. *80 MHz* – Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
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.This setting is disabled by default
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) performed 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.

7. Select **OK** to save the updates to the Mesh Point's dynamic root selection configuration. Select **Reset** to revert to the last saved configuration.

Path Method SNR

Use the **Path Method SNR** screen to set a profile's mesh point channel width, mesh point priority and *signal to noise* (SNR) scan settings.

To define a profile's path method signal to noise ratio:

1. Select the **Configuration** tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Select **Manage Profiles** from the Configuration > Profiles menu.
4. Select **Mesh Point.**

   Refer to the Mesh Point screen to view existing Mesh Points. If an existing Mesh Point configuration does not meet your requirements, select the Add button to create a new mesh point configuration or the Edit button to modify the parameters of an existing mesh point configuration. The Mesh Point screen displays the **Settings** tab by default.
5. Select the **Auto Channel Selection** tab.
6. Select the **Path Method SNR** tab.
7. Set the following values (common to 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: *Automatic* – Defines the channel width is calculated automatically. This is the default value. *20 MHz* – Sets the width between two adjacent channels as 20 MHz. *40 MHz* – Sets the width between two adjacent channels as 40 MHz. *80 MHz* - Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
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.This setting is disabled by default.
SNR Delta	Set the *signal to noise* (SNR) ratio delta (from 1 - 100 dB) for mesh path selections. 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). 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	Configure the duration (from 20 - 250 milliseconds) for scan dwells on each channel, when performing an off channel scan. The default setting is 50 milliseconds.

8. Select **OK** to save the updates to the Mesh Point's path method SNR configuration. Select **Reset** to revert to the last saved configuration.

Path Method Root Path Metric

Use the **Path Method Root Path Metric** screen to set a profile's mesh point root path scan settings.

To define the path method root path metric:

1. Select the **Configuration** tab from the Web UI.
2. Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Mesh Point.**

Refer to the Mesh Point screen to view existing Mesh Points. If an existing Mesh Point configuration does not meet your requirements, select the Add button to create a new mesh point configuration or the Edit button to modify the parameters of an existing mesh point configuration. The Mesh Point screen displays the Settings tab by default.

5 Select the **Auto Channel Selection** tab.

6 Select the **Path Method Root Path Metric** tab.

7 Set the following values (common to both 2.4 GHZ and 5.0/4.9 GHz):

Channel Width	Set the channel width the mesh point's automatic channel scan assigns to the selected radio. Available options include: *Automatic* – Defines the channel width is calculated automatically. This is the default value. *20 MHz* – Sets the width between two adjacent channels as 20 MHz. *40 MHz* – Sets the width between two adjacent channels as 40 MHz. *80 MHz* - Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
Priority Meshpoint	Configure the mesh point monitored for automatic channel scans. This is the mesh point assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a mesh point is automatically selected.This setting is disabled by default.
Meshpoint: Path Minimum	Set the minimum path metric (from 100 - 20,000) for mesh connection establishment. The default setting is 1000.
Meshpoint: Path Metric Threshold	Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for mesh point selection. The default is 1500.
Meshpoint: Tolerance Period	Configure a duration to wait before triggering an automatic channel selection for the next mesh hop. The default is one 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 setting is 5.
Meshpoint Root: Off-channel Duration	Define the duration (from 20 - 250 milliseconds) for scan dwells on each channel, when performing an off channel scan. The default setting is 50 milliseconds.
Meshpoint Root: Channel Switch Delta	Configure the delta (from 5 - 35 dBm) that triggers a mesh point root automatic channel selection when exceeded. The default setting is 10 dBm.
Meshpoint Root Off-channel Scan Frequency	Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for mesh point 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.

8 Select **OK** to save the updates to the Mesh Point's path method SNR configuration. Select **Reset** to revert to the last saved configuration.

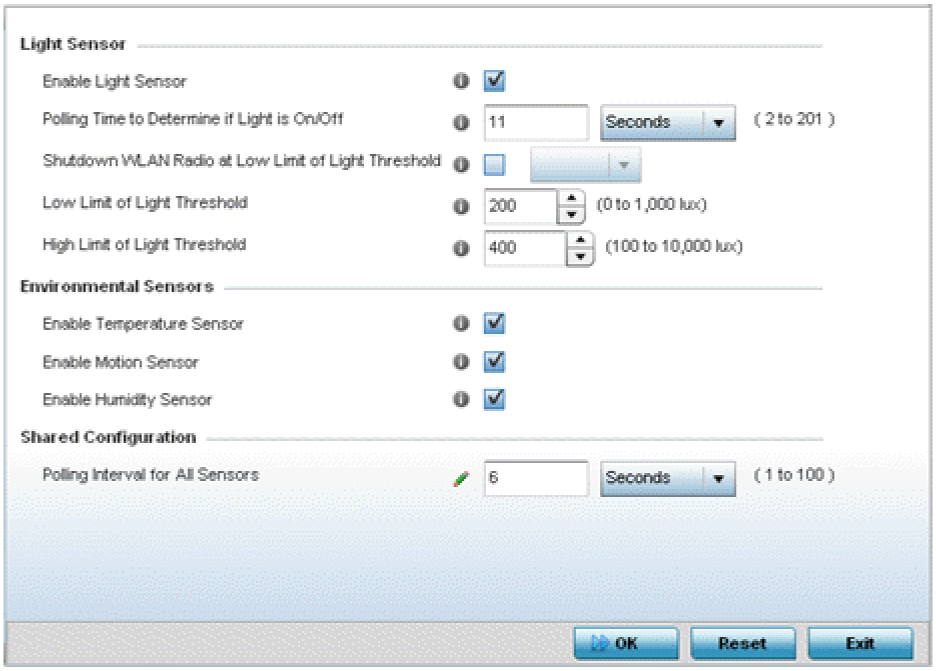
Environmental Sensor Configuration (AP8132 Only)

An AP 8132 sensor module is a USB environmental sensor extension to an <AP8132> model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the environmental conditions including temperature, humidity and light near 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 an environmental sensor configuration for an AP 8132 model access point:

1 Select the **Configuration** → **Profiles** → **Manage Profiles** tab from the Web UI.

2 Select Environmental Sensor.



Light Sensor

Enable Light Sensor ☑

Polling Time to Determine if Light is On/Off 11 Seconds (2 to 201)

Shutdown WLAN Radio at Low Limit of Light Threshold ☐

Low Limit of Light Threshold 200 (0 to 1,000 lux)

High Limit of Light Threshold 400 (100 to 10,000 lux)

Environmental Sensors

Enable Temperature Sensor ☑

Enable Motion Sensor ☑

Enable Humidity Sensor ☑

Shared Configuration

Polling Interval for All Sensors 6 Seconds (1 to 100)

3 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 <AP8132>'s deployment location has its lights powered on or off.
Polling Time to Determine if Light is On/Off	Define an interval in *Seconds* (10 - 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 10 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 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 200. In daytime, the light sensor's value is between 350-450. The default values for the low threshold is 200, i.e., the radio is turned off if the average reading value is lower than 200.
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 high threshold is 400. The radios are turned on when the average value is higher than 400.

4 Enable or disable the following AP 8132 Environmental Sensors:

Enable Temperature Sensor	Select this option to enable the module's temperature sensor. Results are viewable in 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 viewable in 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.

5 Define the following Shared Configuration settings:

Set a polling 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.

6 Select OK to save the changes made to the environmental sensor screen. Select Reset to revert to the last saved configuration.

Advanced Profile Configuration

A profile's advanced configuration is comprised its MINT protocol configuration, NAS identifier and port ID attributes. MINT provides secure profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. Therefore, MINT is well designed for profile support, wherein a group of controller, service platform or access point managed devices share the same configuration attributes.

Refer to the advanced profile's Miscellaneous menu item to set the profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected NAS *(network access server)* port.

To set a profile's advanced configuration:

1 Go to **Configuration** → **Profiles** → **Manage Profiles** .

Select a target profile from those displayed on the screen.

2 Select Advanced and expand the menu item.

The following sub menu items are available as advanced profile configuration options:

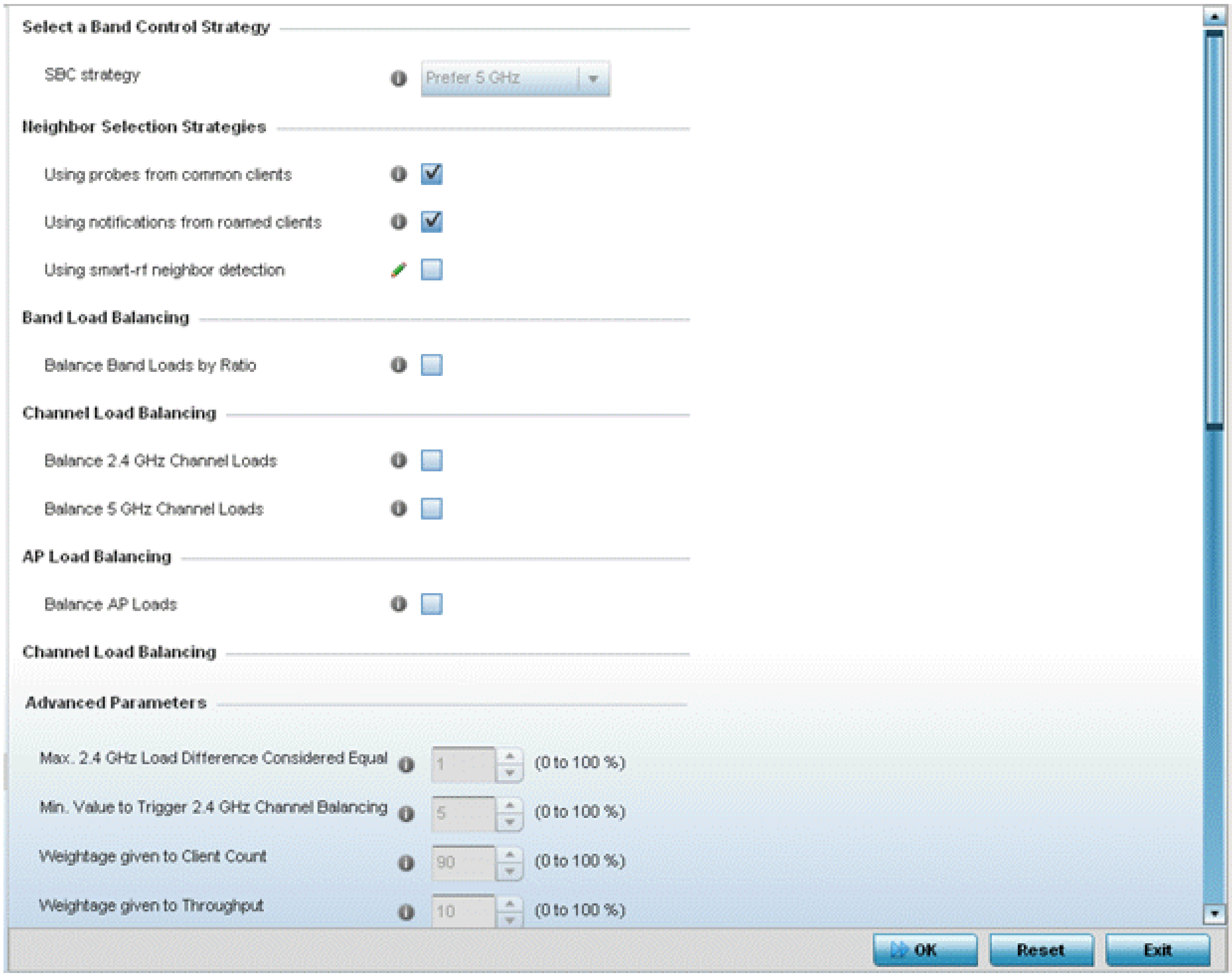
- Client Load Balancing
- Configuring MINT
- Advanced Profile Miscellaneous Configuration

Client Load Balancing

Set a the ratios and calculation values used by access points to distribute client loads both amongst neighbor devices and the 2.4 and 5 GHz radio bands.

To define access point client load balance algorithms:

1 Select **Client Load Balancing** from the Advanced menu item.



Select a Band Control Strategy

SBC strategy: Prefer 5 GHz

Neighbor Selection Strategies

Using probes from common clients ☑

Using notifications from roamed clients ☑

Using smart-rf neighbor detection ☐

Band Load Balancing

Balance Band Loads by Ratio ☐

Channel Load Balancing

Balance 2.4 GHz Channel Loads ☐

Balance 5 GHz Channel Loads ☐

AP Load Balancing

Balance AP Loads ☐

Channel Load Balancing

Advanced Parameters

Max. 2.4 GHz Load Difference Considered Equal: 1 (0 to 100 %)

Min. Value to Trigger 2.4 GHz Channel Balancing: 5 (0 to 100 %)

Weightage given to Client Count: 90 (0 to 100 %)

Weightage given to Throughput: 10 (0 to 100 %)

2 Select the **SBC strategy** from the drop-down menu to determine how band steering is conducted.

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 only associates in the 5 GHz band.

3 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 setting is enabled by default.
Using Notifications from roamed clients	Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This setting is enabled by default.
Using smart-rf neighbor detection	Select this option to select neighbors (peer devices) using Smart RF. This setting is enabled by default.

4 Enable **Balance Band Loads by Radio** to distribute an access points client traffic load across both the 2.4 and 5 GHz radio bands.

5 Set the following **Channel Load Balancing** settings:

Balance 2.4 GHz Channel Loads	Select this option to balance an access point's 2.4 GHz client load across all channels. This setting is enabled by default.
Balance 5 GHz Channel Loads	Select this option to balance an access point's 5 GHz client load across all channels. This setting is enabled by default.

6 Enable **Balance AP Loads** to distribute client traffic evenly amongst neighbor access points.

7 Set the following **Band Control** values:

Max. Band Load Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing band loads. The default setting is 1%.
Band Ratio (2.4 GHz)	Set the relative load for the 2.4 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
Band Ratio (5 GHz)	Set the relative load for the 5 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
5 GHz load at which both bands enabled	Define the 5 GHz radio load value (from 1 - 100%) above which the 5 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.
2.4 GHz load at which both bands enabled	Define the 2.4 GHz radio load value (from 1 - 100%) above which the 2.4 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.

8 Define the following **Neighbor Selection** settings:

Minimal signal strength for common clients	Define the minimum signal strength value (from -100 to 30 dBm) that must be exceeded for an access point's detected client to be considered a common client. the default setting is -100 dBi.
Minimum number of clients seen	Set the minimum number of clients (from 0 - 256) that must be common to two or more access points for the access points to regard one another as neighbors using the common client neighbor detection strategy. The default setting is 0.
Max confirmed neighbors	Set the maximum number (from 1 - 16) of neighbor access points that must be detected amongst peer access point to initiate load balancing. The default setting is 16.
Minimum signal strength for smart-rf neighbors	Set the minimal signal strength value (from -100 to 30 dBm) for an access point detected using Smart RF to qualify as a neighbor access point. the default setting is -65 dBm.

9 Set the following **Advanced Parameters** for client load balance values:

Max. 2.4 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 2.4 GHz client loads. The default setting is 1%.
Min. Value to Trigger 2.4 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 2.4 GHz radio band. The default setting is 5%.

Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 2.4 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 2.4 GHz radio band. The default setting is 10%.
Max. 5 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 5 GHz client loads. The default setting is 1%.
Min. Value to Trigger 5 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 5 GHz radio band. The default setting is 5%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 5 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 5 GHz radio band. The default setting is 10%.

10 Define the following **AP Load Balancing** settings:

Min. Value to Trigger Balancing	Set a value (from 1 - 100%) used to trigger client load balancing when exceeded. The default setting is 5%.
Max. AP Load Difference Considered Equal	Set the maximum load balance differential (from 1 - 100%) considered equal when comparing neighbor access point client loads. The default setting is 1%.
Weightage Given to Client Count	Set the weightage (from 1- 100%) applied to client count in an access point's overall load calculation. The default setting is 90%.
Weightage Given to Throughout	Set the weightage (from 1- 100%) applied to client throughput in an access point's overall load calculation. The default setting is 10%.

11 Select **OK** to save the changes made to the profile's client load balance configuration. Select **Reset** to revert to the last saved configuration.

Configuring MINT

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 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.

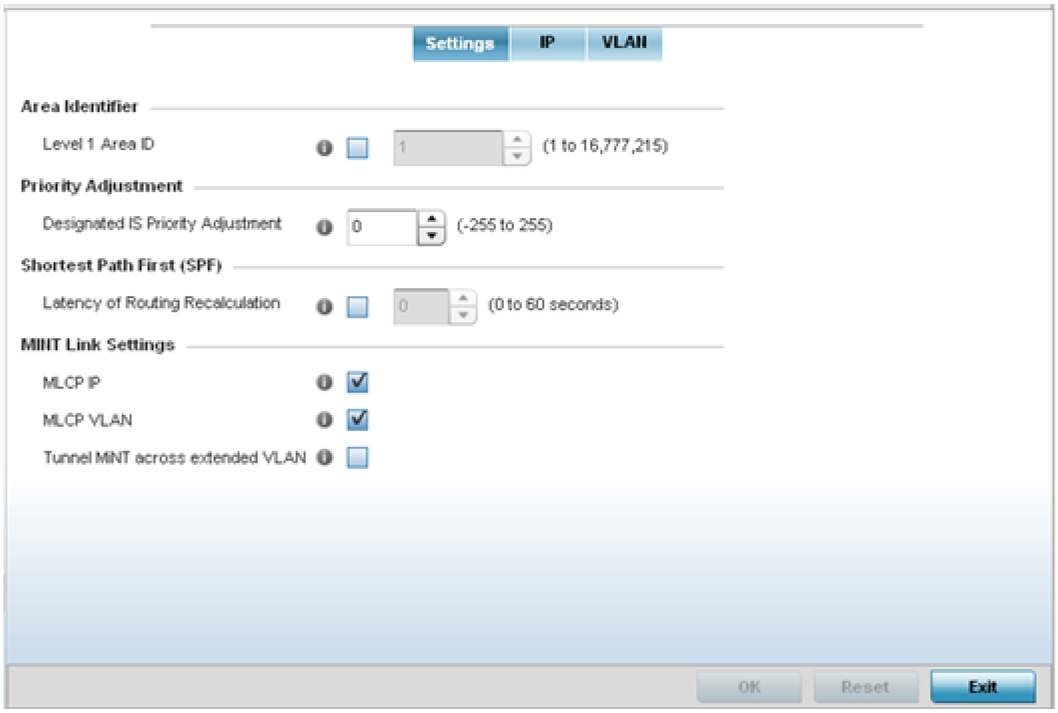
For more information, see:

- Settings
- IP
- VLAN

Settings

To define a profile's MiNT settings:

1 Select **MiNT Protocol** from the Advanced Profile's menu item.



Area Identifier

Level 1 Area ID ☐ 1 (1 to 16,777,215)

Priority Adjustment

Designated IS Priority Adjustment 0 (-255 to 255)

Shortest Path First (SPF)

Latency of Routing Recalculation ☐ 0 (0 to 60 seconds)

MINT Link Settings

MLCP IP ☑

MLCP VLAN ☑

Tunnel MINT across extended VLAN ☐

2 The **Settings** tab displays by default.

3 Refer to the **Area Identifier** field to define the Level 1 and Level 2 Area IDs used by the profile's MiNT configuration.

Level 1 Area ID	Select the check box to enable a spinner control for setting the Level 1 Area ID between 1 - 4,294,967,295. The default value is disabled.

4 Define the following **Device Heartbeat Settings** in respect to devices supported by the profile:

Designated IS Priority Adjustment	Set a **Designated IS Priority Adjustment** setting from -255 and 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.

5 Select the **Latency of Routing Recalculation** check box (within the **Shortest Path First (SPF)** field) to enable the spinner control used for defining a latency period from 0 - 60 seconds. The default setting has the check box disabled.

6 Define the following **MiNT Link Settings** in respect to devices supported by the profile:

MLCP IP	Check this box to enable *MiNT Link Creation Protocol* (MLCP) by IP Address. MLCP is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller, it can be another access point with a path to a controller.
MLCP VLAN	Check this box to enable MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. That neighboring device does not need to be a controller, it can be another access point with a path to a controller.

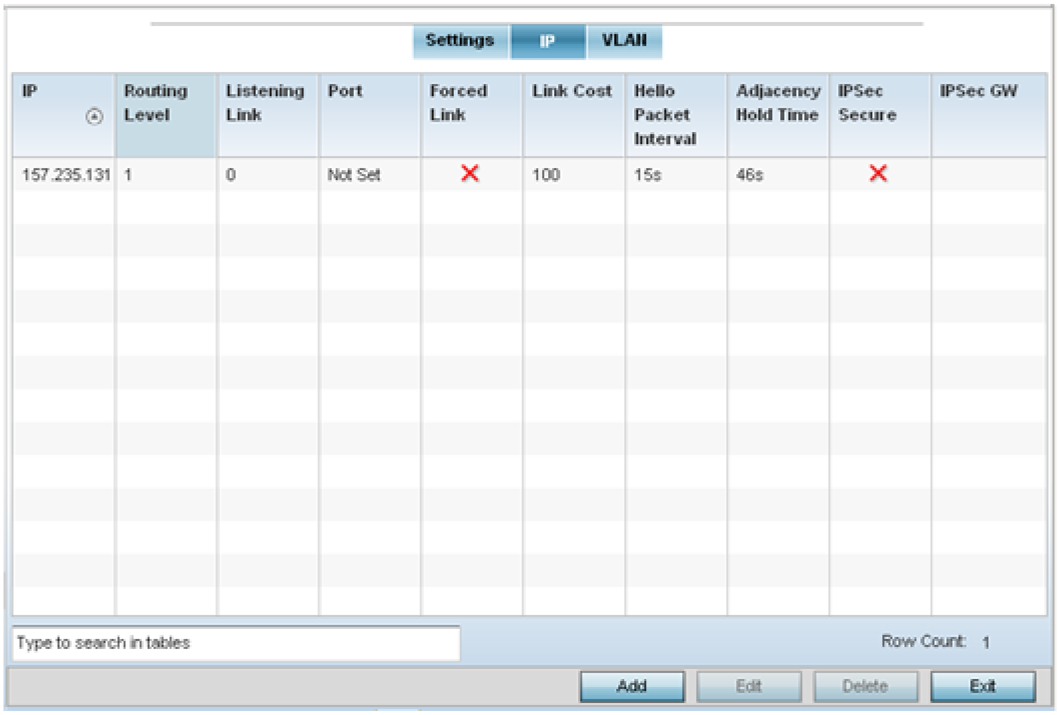
7 Select **Tunnel Controller Load Balancing (Level 1)** (if available to your controller) to enable load balancing through a WLAN tunnel controller.

8 If Tunnel Controller load balancing is enabled for your controller, enter the name of the designated WLAN tunnel controller.
9 Select **OK** to save the changes made to the Settings tab. Select **Reset** to revert to the last saved configuration.

IP

To define a profile's MiNT IP configuration:

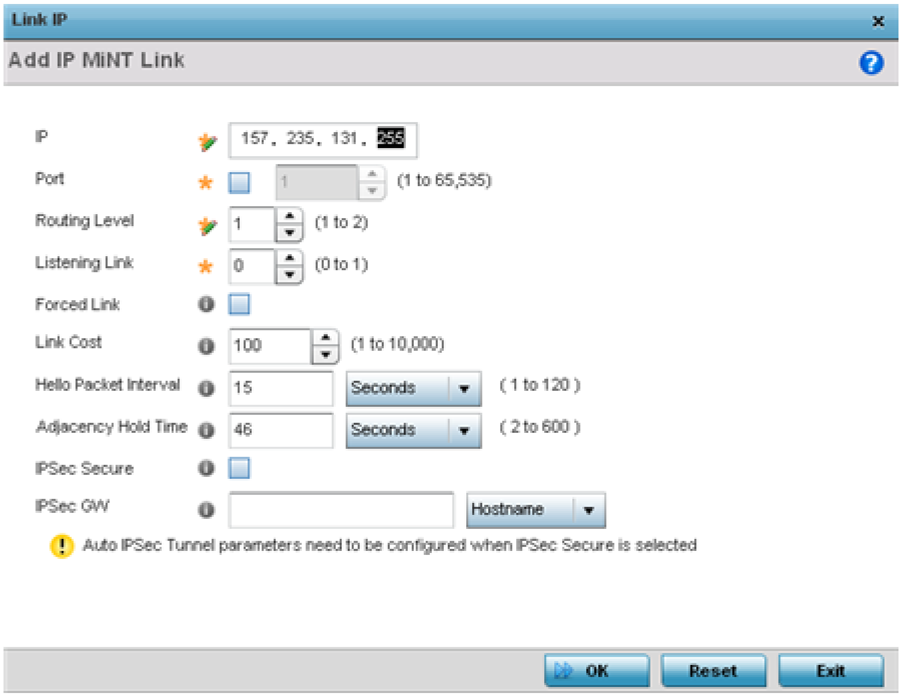
1 Select **MiNT Protocol** from the Advanced Profile's menu item.
2 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MiNT configuration.



IP	Routing Level	Listening Link	Port	Forced Link	Link Cost	Hello Packet Interval	Adjacency Hold Time	IPSec Secure	IPSec GW
157.235.131	1	0	Not Set	✗	100	15s	46s	✗	

Row Count: 1

3 The IP tab displays the IP address, routing level, link cost, hello packet interval and Adjacency Hold Time managed devices use to securely communicate amongst one another within the managed network. Select **Add** to create a new Link IP configuration or **Edit** to modify an existing MiNT configuration.



IP 157 . 235 . 131 . 255

Port ☐ 1 (1 to 65,535)

Routing Level 1 (1 to 2)

Listening Link 0 (0 to 1)

Forced Link ☐

Link Cost 100 (1 to 10,000)

Hello Packet Interval 15 Seconds (1 to 120)

Adjacency Hold Time 46 Seconds (2 to 600)

IPSec Secure ☐

IPSec GW Hostname

Auto IPSec Tunnel parameters need to be configured when IPSec Secure is selected

4 Set the following **Link IP** parameters to complete the MiNT network address configuration:

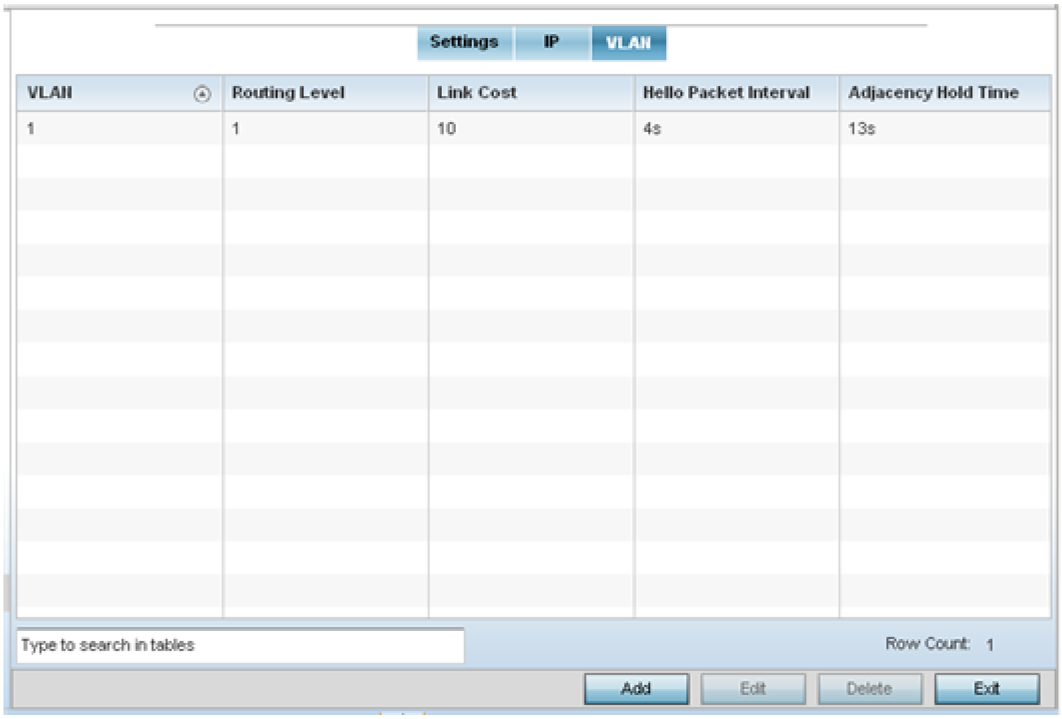
IP	Define the IP address used by peers for interoperation when supporting the MINT protocol.
Port	To specify a custom port for MiNT links, select this option and use the spinner control to define the port number between 1 and 65,535.
Routing Level	Use the spinner control to define a routing level of 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 doesn't scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted.
Forced Link	Check this box to specify the MiNT link as a forced link.
Link Cost	Use the spinner control to set a link cost between 1 - 10,000. The default value is 100.
Hello Packet Interval	Set 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 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	Enable this option to provide IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the IPSec gateway.

VLAN

To set a profile's MiNT VLAN configuration:

1 Select **MiNT Protocol** from the Advanced Profile's menu item.

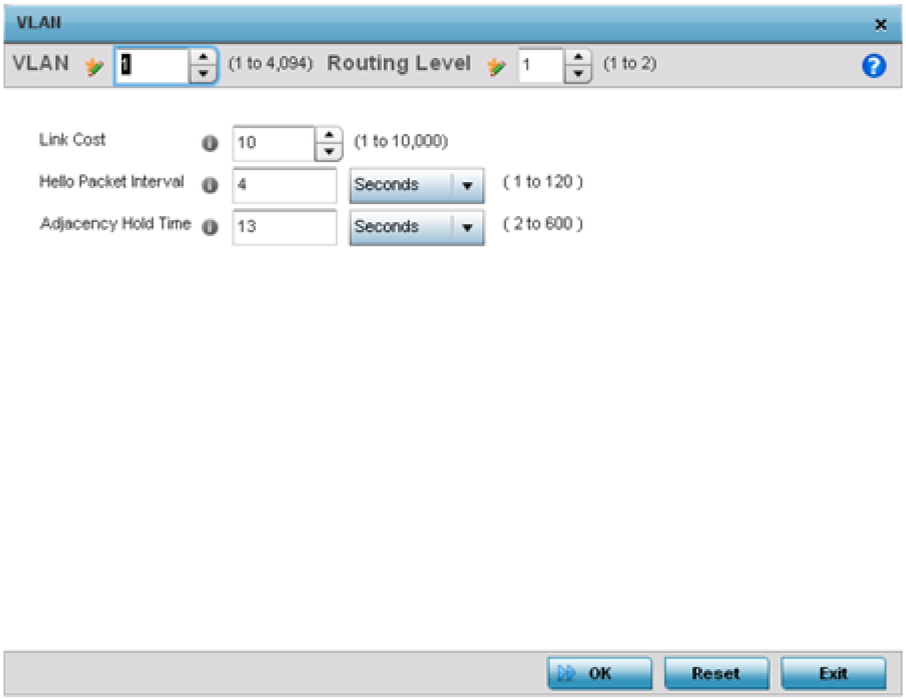
2 Select the **VLAN** tab to display the link IP VLAN information shared by the devices managed by the MiNT configuration.



VLAN	Routing Level	Link Cost	Hello Packet Interval	Adjacency Hold Time
1	1	10	4s	13s

Row Count: 1

3 The VLAN tab displays the **VLAN**, **Routing Level**, **Link Cost**, **Hello Packet Interval** and **Adjacency Hold Time** managed devices use to securely communicate amongst one another. Select **Add** to create a new VLAN link configuration or **Edit** to update an existing MiNT configuration.



VLAN: 1 (1 to 4,094) Routing Level: 1 (1 to 2)

Link Cost: 10 (1 to 10,000)

Hello Packet Interval: 4 Seconds (1 to 120)

Adjacency Hold Time: 13 Seconds (2 to 600)

4 Set the following **VLAN** parameters to complete the MiNT configuration:

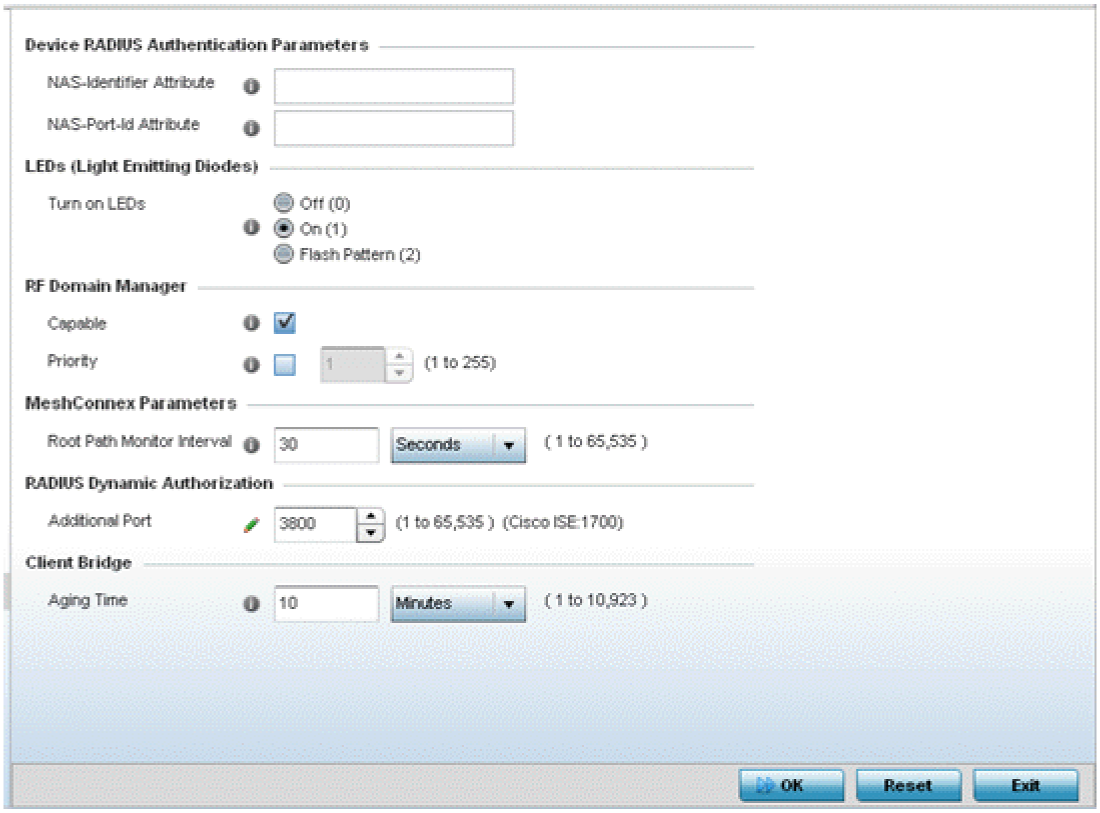
VLAN	Define a VLAN ID between 1 - 4,094 used by peers for interoperation when supporting the MiNT protocol.
Routing Level	Use the spinner control to define a routing level of either 1 or 2.
Link Cost	Use the spinner control to set a link cost between 1 - 10,000. The default value is 100.
Hello Packet Interval	Set 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 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.

5 Select **OK** to save the updates to the MiNT Protocol configuration. Select **Reset** to revert to the last saved configuration.

Advanced Profile Miscellaneous Configuration

Refer to the advanced profile's Miscellaneous menu item to set the 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. When users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection.

1 Select **Miscellaneous** from the Advanced Profile's menu item.



Device RADIUS Authentication Parameters
NAS-Identifier Attribute
NAS-Port-Id Attribute
LEDs (Light Emitting Diodes)
Turn on LEDs ○ Off (0) ● On (1) ○ Flash Pattern (2)
RF Domain Manager
Capable ☑
Priority ☐ 1 (1 to 255)
MeshConnex Parameters
Root Path Monitor Interval 30 Seconds (1 to 65,535)
RADIUS Dynamic Authorization
Additional Port 3800 (1 to 65,535) (Cisco ISE:1700)
Client Bridge
Aging Time 10 Minutes (1 to 10,923)

2 Set a **NAS-Identifier Attribute** up to 253 characters in length.

This is the RADIUS NAS-Identifier attribute that typically identifies the device where a RADIUS request originates.

3. 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.
4. Select the **Turn on LEDs** option (within the **LEDs (Light Emitting Diodes)** field) to enable the LEDs on an access point.

   Select the **Flash Pattern(2)** option (within the **LEDs (Light Emitting Diodes)** field) to flash an access point's LED's in a distinct manner (different from its operational LED behavior) to allow an administrator to validate an access point has received its configuration from its managing controller or service platform.

   Enabling this feature allows an administrator to validate an access point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.
5. Select the **Capable** option (within the **RF Domain Manager** section) to designate this specific profile managed device as being capable of being the RF Domain manager. The default value is enabled.
6. Select the **Priority** check box (within the **RF Domain Manager** section) to set a priority value for this specific profile managed device. Once enabled, use the spinner control to set a device priority between 1 - 255. The higher the number set, the higher the priority in the RF Domain manager election process.
7. Set the **Meshpoint Behavior** as either an **External (Fixed)** unit or a mobile **Vehicle Mounted** unit.
8. Configure a **Root Path Monitor Interval**, between 1 and 65,535 seconds, to specify how often to check if the meshpoint is up or down.
9. Set the **Additional Port** value for **RADIUS Dynamic Authorization** field. Set this value to 1700 to enable a CISCO Identity Services Engine (ISE) Authentication, Authorization and Accounting (AAA) server, when deployed in the network, to dynamically authenticate a client.

   When a client requests access to the network, the CISCO ISE RADIUS server presents the client with a URL where the device's compliance to the networks security such as validity of anti-virus or anti-spyware software is checked for the validity for their definition files (this checking is called posture). If the client device complies, then it is allowed access to the network.
10. Set the **Aging Time** value for a dedicated Client Bridge. Use the spinner control to set a value in *Days* (1 -8), *Hours* (1 - 183), *Minutes* (1 - 10, 923) and *Seconds* (10 - 655, 350). The aging time represents the time this MAC address is allowed to remain on the network since its last update. The default setting is 10 minutes.
11. Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

9 RF Domains

Managing RF Domains

A controller or service platform's configuration is composed of numerous elements including RF Domains, profiles, policies, WLANs and device specific configurations. RF Domains are used to assign regulatory, location and relevant policies to controllers and service platforms. RF Domains are required, and each controller or service platform must be assigned at least one default RF Domain.

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:

- Default RF Domain - Automatically assigned to each controller or service platform and associated access point by default.
- User Defined RF Domains - Created by administrators and manually assigned to individual controller or service platforms, but can be automatically assigned to access points using adoption policies.

Each controller and service platform is assigned to only one RF Domain at a time. However, a user defined RF Domain can be assigned to multiple controllers or service platforms as required. User defined RF Domains can be manually assigned or automatically assigned to access points using an AP provisioning policy.

Default RF Domains

Each controller and service platform utilizes a default RF Domain. Access points are assigned to this default RF Domain as they are discovered by the controller or service platform. The default RF Domain can be used for single site deployments, where regional, regulatory and RF policies are common between devices. When regional, regulatory or RF policies need to be device specific, user defined RF Domains are recommended.

A default RF Domain can also omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered by the controller or service platform. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.

User Defined RF Domains

Configure and deploy user defined RF Domains for single or multiple sites when controllers or service platforms require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User defined RF Domains can be used to:

- Assign unique Smart RF or WIPS policies to access points deployed on different floors or buildings within a site.
- Assign unique regional or regulatory configurations to access points deployed in different states or countries.
- Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

User defined RF Domains must be manually assigned to controllers or service platforms, but can be manually or automatically assigned to access points. Manual RF Domain assignment can be performed using the CLI or UI by modifying each device's individual configuration and assigning a specific RF Domain to the device. Automatic RF Domain assignments can be made using an AP provisioning policy which can assign specific RF Domains to access points based on an access point's model, serial number, VLAN, DHCP option, IP address or MAC address.

Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play access point deployments by automatically applying RF Domains to remote access points.

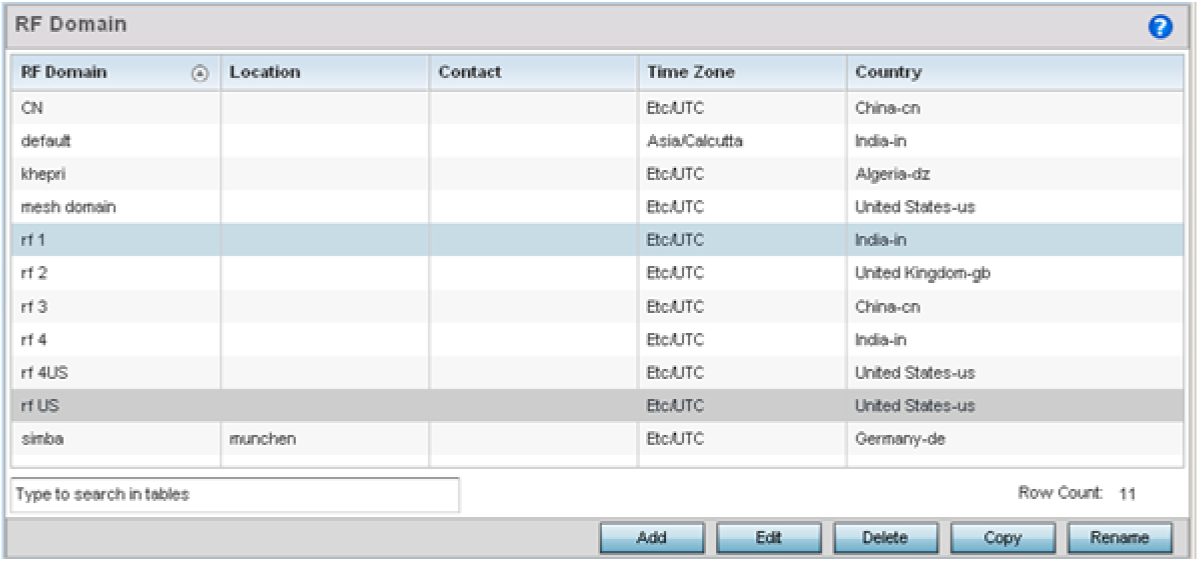
Managing RF Domains

Managing RF Domains entails setting individual RF Domain configurations and administrating them as a collective set. Remember that access points, unlike controllers and service platforms, use only a single RF Domain shared among peer access points of the same model.

To review the configurations of existing RF Domains:

1. Select **Configuration** > **RF Domains** from the Web UI. Access points select RF Domains using a path of **Configuration** > **Devices** > **RF Domains**.

   The RF Domain screen displays within the main portion of the Web UI, and the RF Domain Browser displays in the lower, left-hand, portion of the Web UI.
2. Refer to the RF Domain screen to review high-level configuration data for existing RF Domain policies.



RF Domain	Location	Contact	Time Zone	Country
CN			Etc/UTC	China-cn
default			Asia/Calcutta	India-in
khepri			Etc/UTC	Algeria-dz
mesh domain			Etc/UTC	United States-us
rf 1			Etc/UTC	India-in
rf 2			Etc/UTC	United Kingdom-gb
rf 3			Etc/UTC	China-cn
rf 4			Etc/UTC	India-in
rf 4US			Etc/UTC	United States-us
rf US			Etc/UTC	United States-us
simba	munchen		Etc/UTC	Germany-de

Type to search in tables

Row Count: 11

Figure 279: RF Domains Screen

3 Use the following (read-only) information to determine whether a new RF Domain policy requires creation, or an existing RF Domain requires edit or deletion:

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.

4 Refer to the RF Domain Browser to expand an existing policy and review the members of that controller, service platform or access point RF Domain.

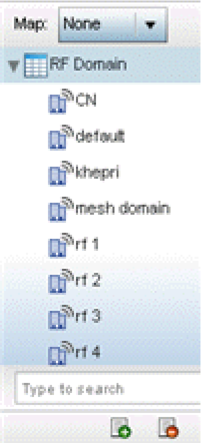


Figure 280: RF Domain Browser

5 Once the data within the RF Domain screen and RF Domain Browser is reviewed, determine whether a new policy requires creation, or if an existing policy requires edit or deletion. The management of RF Domains entails the following:
   - RF Domain Basic Configuration on page 750
   - RF Domain Sensor Configuration on page 753
   - RF Domain Client Name Configuration on page 755
   - Overriding RF Domain SSID and other Configurations on page 756
   - RF Domain Network Alias on page 762

RF Domain Basic Configuration

An administrator needs to set RD Domain deployment values, Smart RF policy and override settings, smart scan channel assignments, WIPS policy and stat fetching configuration as part of a RF Domain's unique basic configuration:

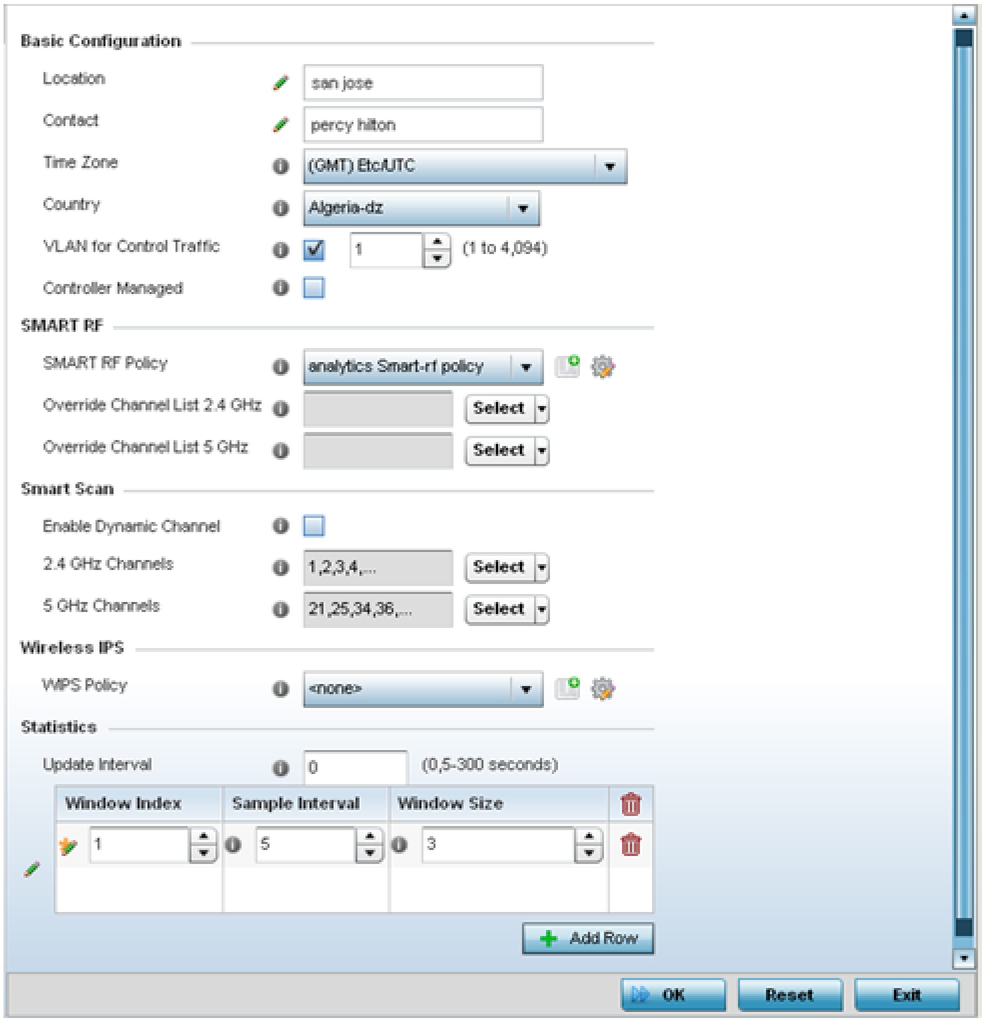
To set a RF Domain basic configuration:

1 Select **Configuration** → **RF Domains** from the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**. An RF Domain can be permanently removed by highlighting it from the list and selecting **Delete**.

   An existing RF Domain can also be modified by selecting it directly from the RF Domain Browser.

3 If you are adding or modifying an existing RF Domain, the RF Domain Basic Configuration screen displays by default.



Basic Configuration

Location: san jose

Contact: percy hilton

Time Zone: (GMT) Etc/UTC

Country: Algeria-dz

VLAN for Control Traffic: ☑ 1 (1 to 4,094)

Controller Managed: ☐

SMART RF

SMART RF Policy: analytics Smart-rf policy

Override Channel List 2.4 GHz: Select

Override Channel List 5 GHz: Select

Smart Scan

Enable Dynamic Channel: ☐

2.4 GHz Channels: 1,2,3,4,...

5 GHz Channels: 21,25,34,36,...

Wireless IPS

WIPS Policy: <none>

Statistics

Update Interval: 0 (0,5-300 seconds)

Window Index	Sample Interval	Window Size
1	5	3

Figure 281: RF Domain - Basic Configuration Screen

4 Define the following Basic Configuration parameters for the RF Domain:

RF Domain	If creating a new RF Domain, assign it a name representative of its intended function. The name cannot exceed 32 characters. The name cannot be changed as part of the edit process.
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 device configurations are deployed and managed by the RF Domain policy.
Contact	Provide the name of the contact (or administrator) assigned to respond to events created by or impacting the 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 to controllers, service platforms and 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 a device's illegal operation, as device radios transmit in specific channels unique to the country of operation.
Latitude Coordinate	Configures the of the RF Domain's latitude in order to fix its exact geographical location on a map. Use this option to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.
Longitude Coordinate	Configures the of the RF Domain's longitude in order to fix its exact geographical location on a map. Use this option to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.
VLAN for Traffic Control	Select the check box to enable a spinner control used for specifying the VLAN (within a range of 1 - 4,094) used for traffic control within this RF Domain.
Controller Managed	Select the check box to enable management of the RF Domain for adopted wireless clients by the controller or service platform. This option is disabled by default.

5 Define the following **SMART RF** parameters for the RF Domain:

When a radio fails or is faulty, a Smart RF policy can used provide automatic recovery by instructing neighboring access points to increase their transmit power to compensate for the coverage loss.

Once correct access point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events and can be used to ensure adequate detector coverage is available. Manual detector radio selection can also be made using visualizations from the LANPlanner tool.

For an overview of Smart RF and instructions on how to create a Smart RF policy that can be used with an RF Domain, see Smart RF Policies on page 406.

SMART RF Policy	Assign an existing Smart RF Policy to the RF Domain, or if none exist create a new one. Use the Smart RF Policy drop-down menu to navigate to existing Smart RF policies and select the one best suited to the function of the RF Domain. If none exist, select the Create icon and provide the required parameters to define a Smart RF configuration that can be used with the RF Domain. An existing policy can be edited by selecting the policy from the drop-down menu and selecting the Edit icon.
Override Channel List 2.4 GHz	Select an override list of channels Smart RF can use for channel compensations on 2.4 GHz radios.
Override Channel List 5 GHz	Select an override list of channels Smart RF can use for channel compensations on 5 GHz radios.

6 Define the following RF Domain **Smart Scan** values:

Enable Dynamic Channel	Enable this setting to configuration the dynamic channel listing mode for smart scans in the 2.4 and 5 GHz bands. This setting is disabled by default.
2.4 GHz Channels	Set the list of 2.4 GHz mode channels sent in smart scans responses to clients.
5 GHz Channels	Set the list of 5 GHz mode channels sent in smart scans responses to clients.

7 Assign an existing **Wireless IPS** (WIPS) policy to the RF Domain, or if none exist create a new one.

Use the **WIPS Policy** drop-down menu to navigate to existing WIPS policies and select the one best suited to the function of the RF Domain. If none exist, select the Create icon and provide the required parameters to define a WIPS configuration that can be used with the RF Domain. An existing policy can be edited by selecting the policy from the drop-down menu and selecting the **Edit** icon.

A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. a WIPS policy uses a dedicated sensor for actively detecting and locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

For an overview of WIPS and instructions on how to create a WIPS policy that can be used with a RF Domain, see Configuring a WIPS Policy on page 817.

8 Refer to the **Statistics** field to define how RF Domain stats and updated.

Update Interval	Set an interval of 0 or from 5-3600 seconds for update retrievals.
Window Index	Use the spinner control to set a numerical index used as an identifier for each RF Domain statistic defined.
Sample Interval	Use the spinner control to define the interval (in seconds) to capture windowed statistics supporting a RF Domain configuration. The default is 5 seconds.
Window Size	Use the spinner control to set the number of samples used to represent a RF Domain statistic. The default value is 6 samples.

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

RF Domain Sensor Configuration

The WIPS protects clients and access point radio traffic from attacks and unauthorized wireless network 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 wired and wireless device lockdowns upon threat acknowledgement.

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

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's able to scan (in sensor mode) across all legal channels within the 2.4 and 5.0 GHz radio bands. 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.

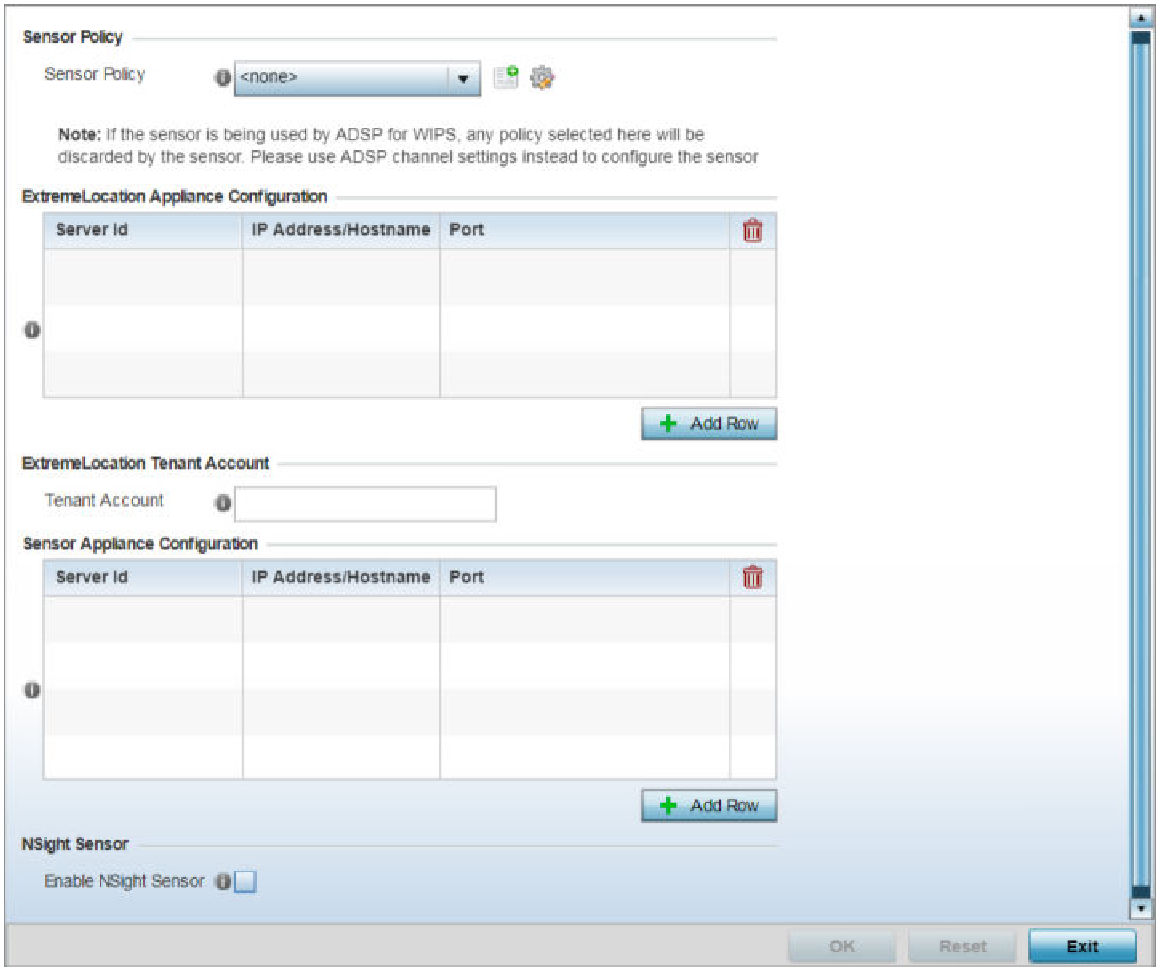
The AP-7522, AP 7532, vAP 7562, AP-8432 and AP-8533 model access points can also function as ExtremeLocation sensors. ExtremeLocation is a highly scalable indoor locationing platform that gathers location-related analytics, such as visitor trends, peak and off-peak times, dwell time, heat-maps, etc. to enable entrepreneurs deeper visibility at a venue. To enable the location tracking system, the ExtremeLocation server should be up and running and the RF Domain Sensor configuration should point to the ExtremeLocation server.

To define a WIPS server configuration used with a RF Domain:

1 From the RF Domain screen, either select the **Add** button or highlight an existing policy and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain Browser.

2 Select the **Sensor** item from within the RF Domain screen.



Sensor Policy

Sensor Policy <none>

Note: If the sensor is being used by ADSP for WIPS, any policy selected here will be discarded by the sensor. Please use ADSP channel settings instead to configure the sensor

ExtremeLocation Appliance Configuration

Server Id	IP Address/Hostname	Port

ExtremeLocation Tenant Account

Tenant Account

Sensor Appliance Configuration

Server Id	IP Address/Hostname	Port

NSight Sensor

Enable NSight Sensor ☐

Figure 282: RF Domain - Sensor Screen

3 Use the **Sensor Policy** drop-down menu to select a Sensor policy to send RSSI information to a dedicated system for device locationing calculations. If no Sensor policy exists, use the **Create** icon to create a new Sensor policy. Or, use the **Edit** icon to edit an existing Sensor policy if required.

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.

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.

4 Select the **+ Add Row** button to populate the ExtremeLocation Appliance Configuration table with up to one ExtremeLocation server credentials.

Server Id	Use the spinner control to assign a DNS hostname of the ExtremeLocation resource. As of now only one (1) ExtremeLocation sever can be configured. Note: The ExtremeLocation sensor capabilities are supported only on the AP-7522, AP 7532, AP 7562, AP 7602, AP-7612, AP 7622, AP-8432, and AP-8533model access points.
IP Address/Hostname	Provide the ExtremeLocation server's hostname. When configured, access points within the RF Domain post location-related analytics to the specified ExtremeLocation server. Note: Enter the 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 for the ExtremeLocation server. This is the port on which the ExtremeLocation server is reachable. The default port is 443.

5 Enter the ExtremeLocation Tenant’s account number in the Tenant Account field.

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. Including the Tenant account number reinforces the Tenant's identity.

6 Select the **+ Add Row** button to populate the Sensor Appliance Configuration table with up to three rows for server credentials:

Server Id	Use the spinner control to assign a numerical ID for up to three ADSP server resources. The server with the lowest defined ID is the first reached by the controller or service platform. The default ID is 1.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of each server used as a ADSP sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of each ADSP sensor server utilized by RF member devices. The default port is 443.

7 Select the **Enable NSight Sensor** option, within the NSight Sensor field, to enable the use of sensor module by NSight. This option is disabled by default.

8 Select **OK** to save the changes to the Sensor configuration, or select **Reset** to Revert to the last saved configuration.

RF Domain Client Name Configuration

The 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 a RF Domain:

1. From the RF Domain screen, either select the **Add** button or highlight an existing policy and select **Edit**.

   An existing policy can also be modified by selecting it directly from the RF Domain browser.
2. Select the **Client Name Configuration** item from within the RF Domain screen.

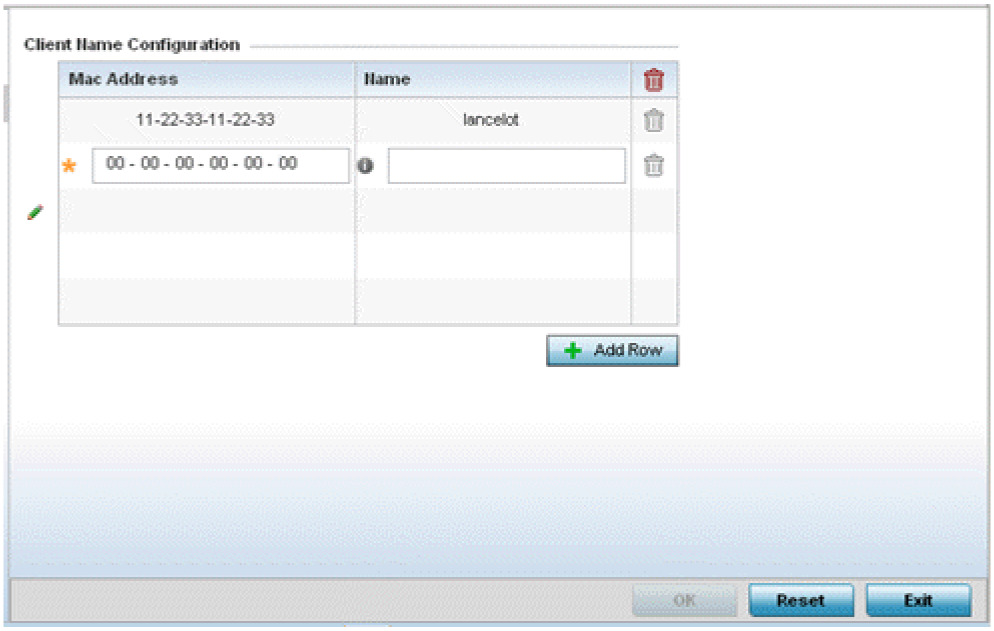


Figure 283: RF Domain Client Configuration Screen

3. 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.
4. Enter the client's factory coded MAC address.
5. Assign a **Name** to the RF Domain member access point's connected client to assist in its easy recognition.
6. Select **OK** to save the changes to the configuration, or select **Reset** to revert to the last saved configuration.

Overriding RF Domain SSID and other Configurations

Each WLAN provides associated wireless clients with a SSID *(Service Set Identifier)*. This has limitations, because it requires wireless clients associate with different SSIDs to obtain QoS and security policies. However, a WiNG managed RF Domain can have WLANs assigned and advertise a single SSID, but allow users to inherit different QoS or security policies. Use the Override SSID screen to assign WLANs an override SSID as needed for the RF Domain.

Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. When a wireless client associates with a WLAN, it is assigned a VLAN in such a way that users are load balanced across VLANs. The VLAN is assigned from the pool representative of the WLAN. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis.

To define an override SSID and override VLAN configuration used with a RF Domain:

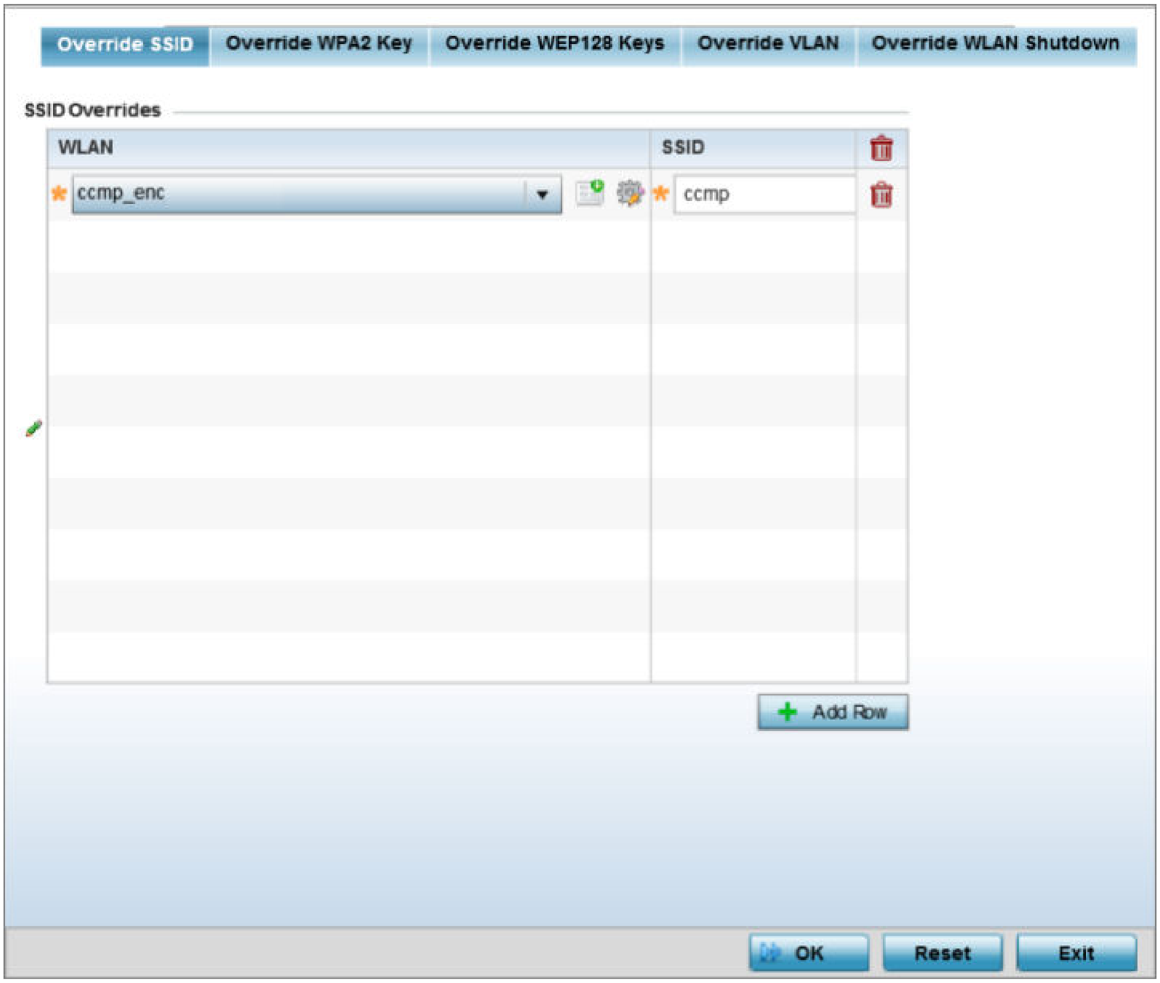
1 Go to **Configuration** → **RF Domain**. The RF Domain screen displays. This screen lists the RF Domains (default and user-created) witihin the network.

2 Double-click on the RF Domain to which SSID and VLAN overrides is to be applied.

The selected RF Domain's configuration menu displays.

3 Select **Overrides**.

The RF Domain overrides screen, with the Override SSID screen selected by default, displays.



WLAN: ccmp_enc
SSID: ccmp

Figure 284: RF Domain Override SSID Screen

4 Select the **+ Add Row** button to create a new Override SSID configuration.

To remove an existing Sensor Server Configuration from the table, highlight it and select the **Delete** icon.

5 Use the **WLAN** drop-down menu to select an existing WLAN to be supplied an override SSID.

If a WLAN configuration has not been defined, select the **Create** button and define at least one complete WLAN configuration. For detailed information on the steps required to create a WLAN, see Wireless LAN Policies on page 329.

6 Enter the name of the **SSID** to use with this WLAN.

7 Select **OK** to save the override SSID configuration changes, or select **Reset** to revert to the last saved configuration.

8 Select the **Override WPA2 Key** tab.

The Override WPA2 Key screen enables an administrator to override a WLAN's existing WPA2 PSK at the RF Domain level (not the profile level). WPA2 is a newer 802.11i standard that provides even stronger wireless security than WPA and WEP.

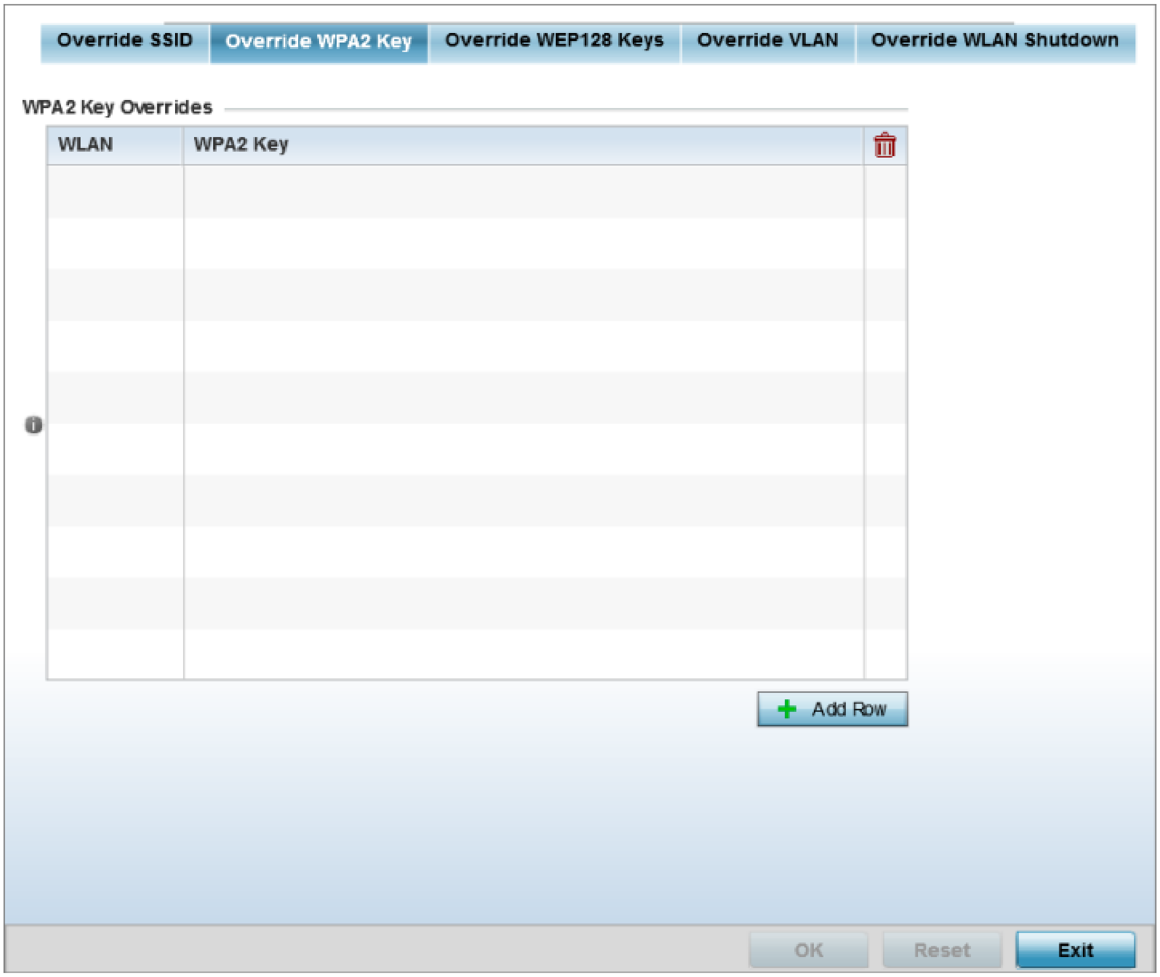


Figure 285: RF Domain Override WPA2 PSK Screen

9 Select the **+ Add Row** button to populate the screen with a row for selecting an existing WLAN to override with a new WPA2 key.

WLAN	Use the drop-down menu to selecting an existing WLAN whose key is to be overridden at the RF Domain level. A new WLAN configuration can be defined by selecting the **Create** icon, or an existing WLAN configuration can be modified by selecting the **Edit** icon.
WPA2 Key	Enter either an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

10 Select **OK** to save the changes to the Override WPA2 Key configuration, or select **Reset** to revert to the last saved configuration.

11 Select the **Override WEP128 Keys** tab.

The Override WEP128 Keys screen enables an administrator to override a WLAN's existing WEP 128 Keys at the RF Domain level (not the profile level). WEP 128 uses 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 on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if 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.

The screen displays existing WLANs whose WEP 128 key configuration can be overridden at the RF Domain level. Either select **Add** to create a new WEP 128 key configuration, or select an existing WEP 128 key and the **Edit** button to modify the selected key's existing key algorithm. The screen populates with the parameters required to override a WEP 128 configuration for the selected WLAN.

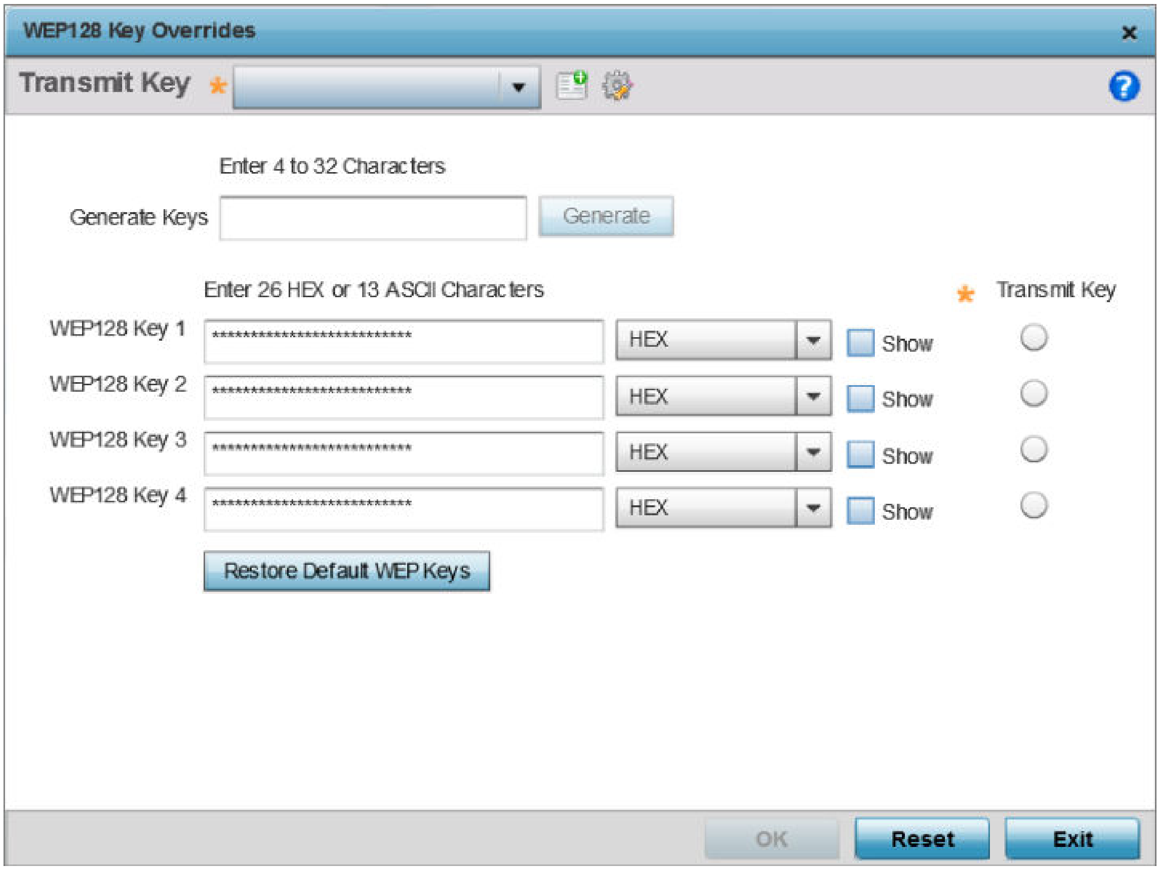


Figure 286: RF Domain Override WEP128 Keys Screen

12 Define the following settings for the WEP 128 key override:

Generate Keys	Specify a 4- to 32-character RF Domain override Pass Key and click the **Generate** button. The pass key can be any alphanumeric string. Wireless devices 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 areas 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	If you feel it necessary to restore the WEP algorithm back to its default settings, click the Restore Default WEP Keys button. Default WEP 128 keys are as follows: • Key 1 101112131415161718191A1B1C • Key 2 202122232425262728292A2B2C • Key 3 303132333435363738393A3B3C • Key 4 404142434445464748494A4B4C

13 Select **OK** to save the override WEP 128 Key configuration changes, or select **Reset** to revert to the last saved configuration.

14 Select the **Override VLAN** tab.

The Override VLAN screen lists those WLANs available for override.

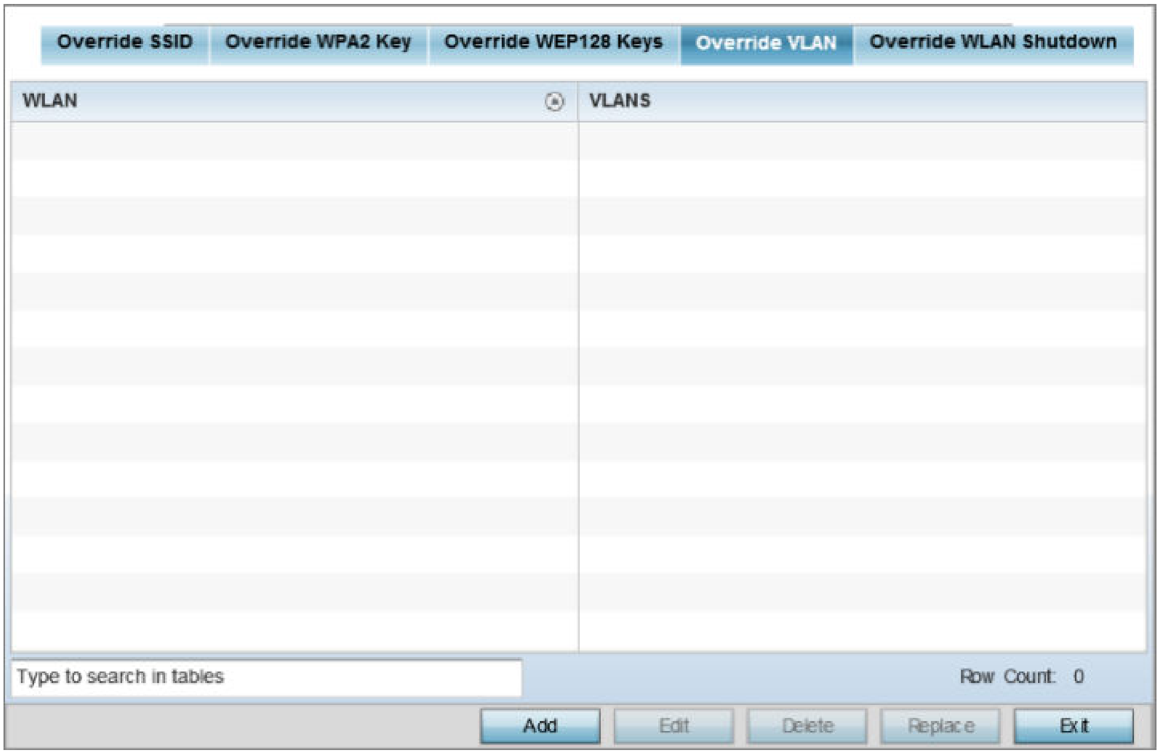
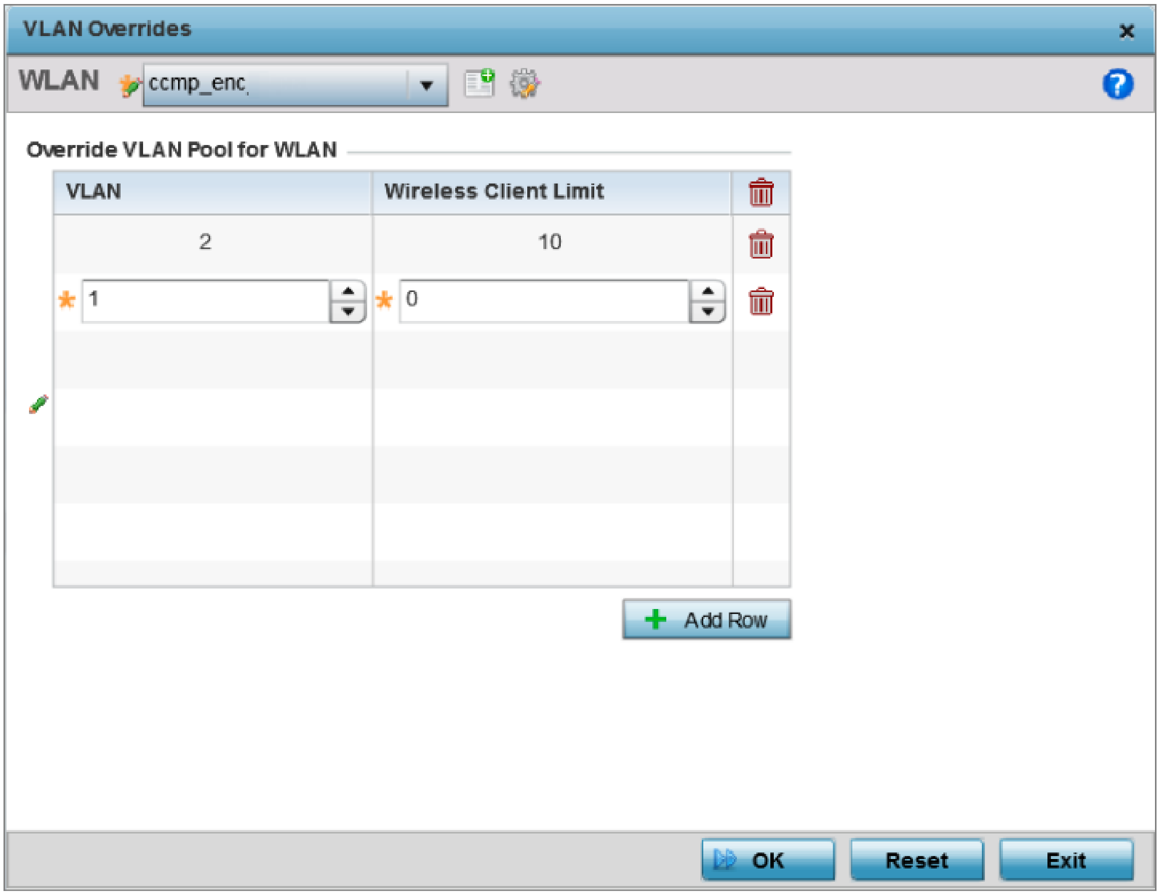


Figure 287: RF Domain Override VLAN screen

15 Select **Add** to define a new VLAN override configuration, choose an existing WLAN and select **Edit** to change the override VLAN and limit, or select **Delete** to remove a WLAN's override VLAN configuration



VLAN	Wireless Client Limit
2	10
1	0

Figure 288: RF Domain Override VLAN Add screen

16 Use the VLAN spinner control to change the VLANs for an existing WLAN client connection, or select the **+ Add Row** button to add additional VLANs for WLAN client connection.

17 Use the Wireless Client Limit spinner control to set the client user limit for the VLAN.

The maximum allowed client limit is 8192 per VLAN. VLANs can be defined from 1 - 4094. The default setting is 0.

18 Select **OK** to save the override VLAN configuration changes, or select **Reset** to revert to the last saved configuration.

19 Select the **Override WLAN Shutdown** tab.

20 Select the **+ Add Row** button to populate the screen with a row for selecting an existing WLAN to override the WLAN mode of operation.

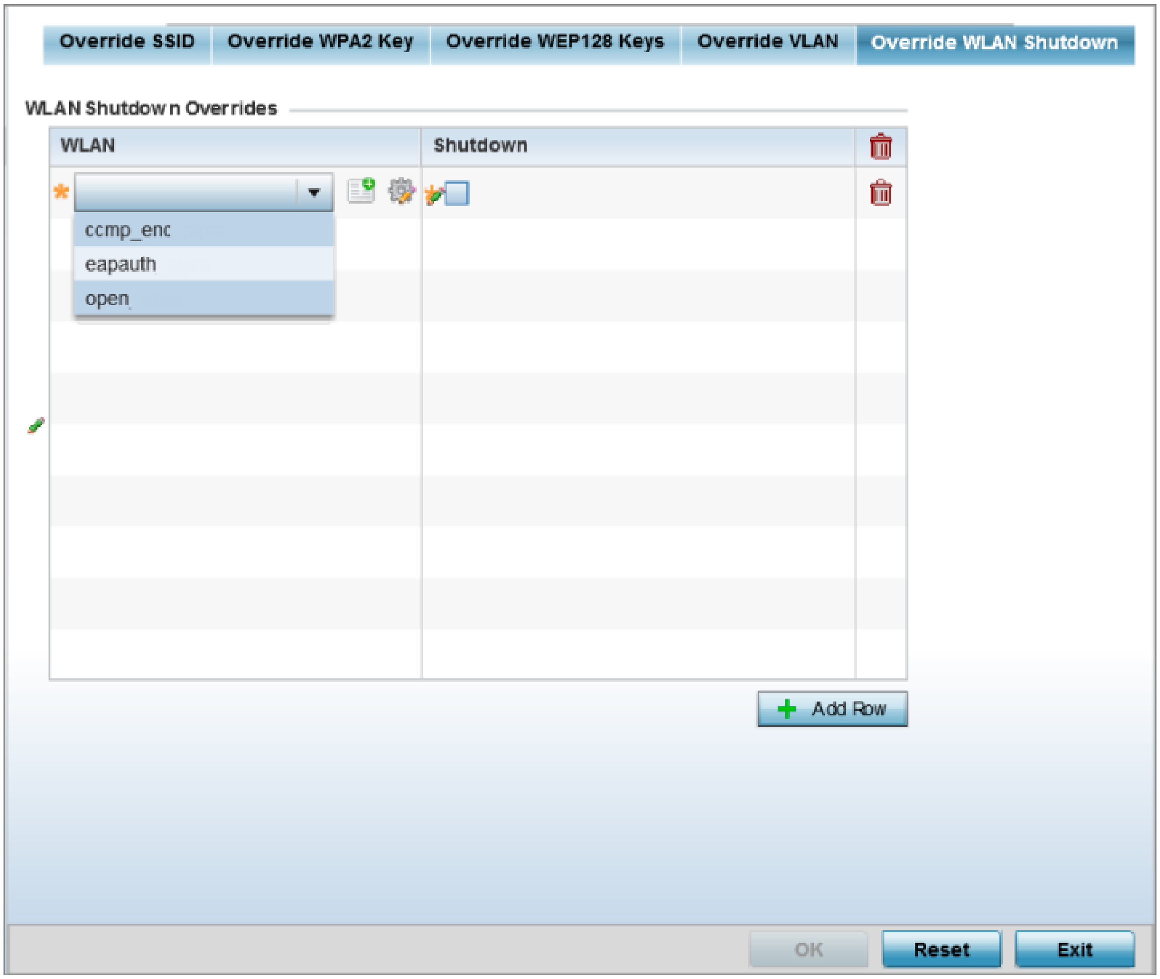


Figure 289: RF Domain Override Override WLAN Shutdown Add Screen

Configure the following parameters:

WLAN	Use the drop-down menu to select an existing WLAN whose mode of operation is to be overridden at the RF Domain level.
Shutdown	Select to shut down the WLAN operation on all mapped radios. When selected, the RF Domains access points, mapped to the selected WLAN, stop beaconing the WLAN's SSID.

21 Select **OK** to save the override VLAN shutdown configuration changes, or select **Reset** to revert to the last saved configuration.

RF Domain Network 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:

- RF Domain Basic Alias
- RF Domain Network Group Alias
- RF Domain Network Service Alias

RF Domain Basic Alias

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 for a RF Domain:

1 Select **Configuration** > **RF Domains** from the Web UI.

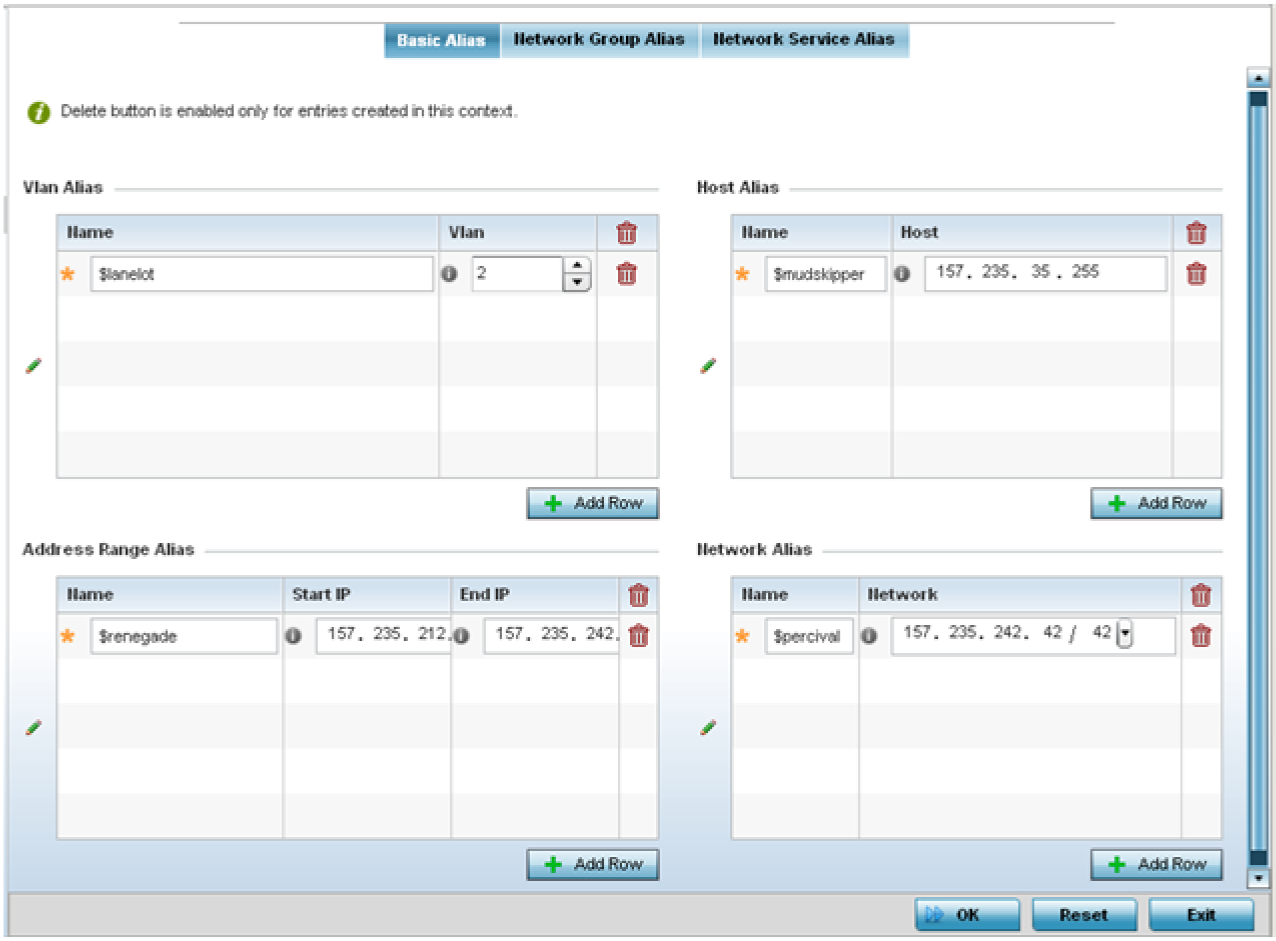
The RF Domain screen displays within the main portion of the Web UI, and the RF Domain Browser displays in the lower, left-hand portion of the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain Browser.

3 Expand the **Network** menu item and select **Alias**.

The Alias screen displays with the Basic Alias tab displayed by default.



Delete button is enabled only for entries created in this context.

Vlan Alias

Name	Vlan
$lanelot	2

Host Alias

Name	Host
$mudskipper	157 . 235 . 35 . 255

Address Range Alias

Name	Start IP	End IP
$renegade	157 . 235 . 212.	157 . 235 . 242.

Network Alias

Name	Network
$percival	157 . 235 . 242 . 42 / 42

Figure 290: RF Domain Network Basic Alias Screen

4 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 you are adding a new VLAN Alias, give 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.

5 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 you are adding a new Address Alias, give 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.

6 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 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 255 character maximum string value to use in the alias.

7 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 you are adding a new Host Alias, give it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Lists the numeric IP address set for the host.

8 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 you are adding a new Network Alias, give 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.

9 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen to its last saved configuration.

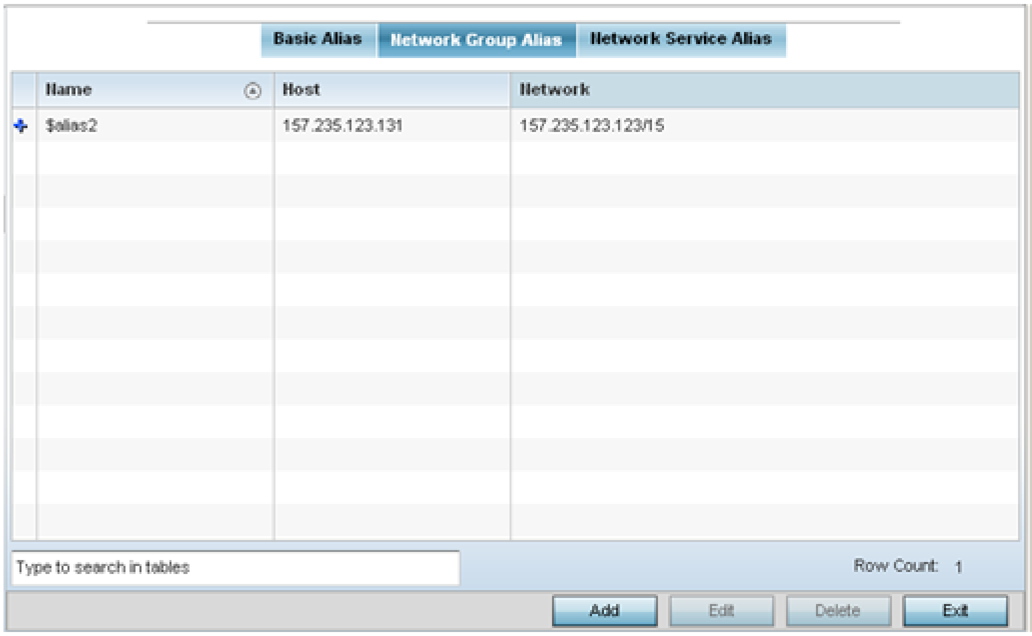
RF Domain Network Group Alias

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 edit or delete a network alias configuration:

1 Select the **Network Group** Alias tab. The screen displays the attributes of existing network group alias configurations.



Name	Host	Network
$alias2	157.235.123.131	157.235.123.123/15

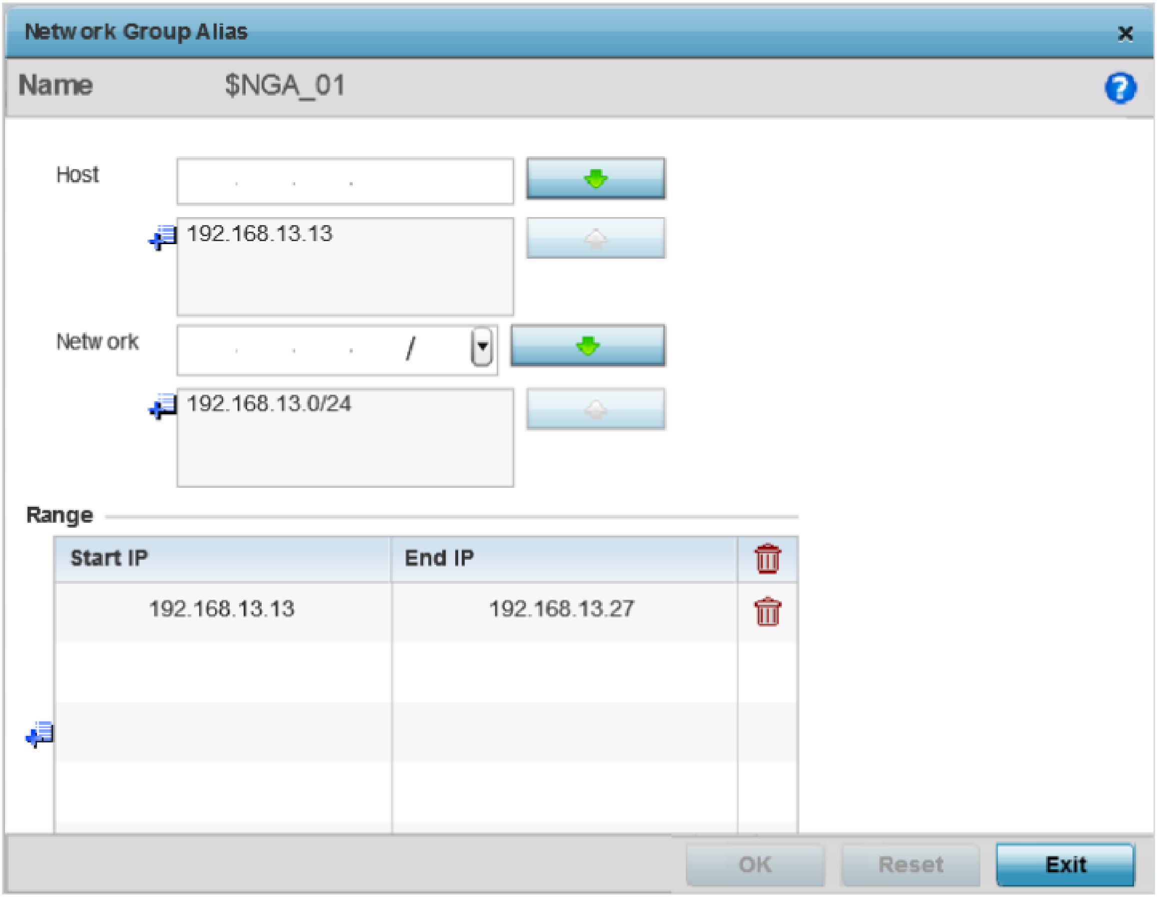
Figure 291: RF Domain Network Group Alias Screen

2 Review existing Network Group alias configurations.

Name	Displays the administrator assigned name assigned 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.

3 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

4 Select the added row to expand it into configurable parameters for defining the network alias rule.



Name $NGA_01

192.168.13.13

192.168.13.0/24

Start IP	End IP
192.168.13.13	192.168.13.27

Figure 292: RF Domain Network Group Alias Add Screen

5 If adding a new Network Alias Rule, give it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

6 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.

7 In 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 an existing alias range entry to edit it.

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

RF Domain 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 a RF Domain:

1 Select the **Network Service Alias** tab. The screen displays the attributes of existing network group alias configurations.

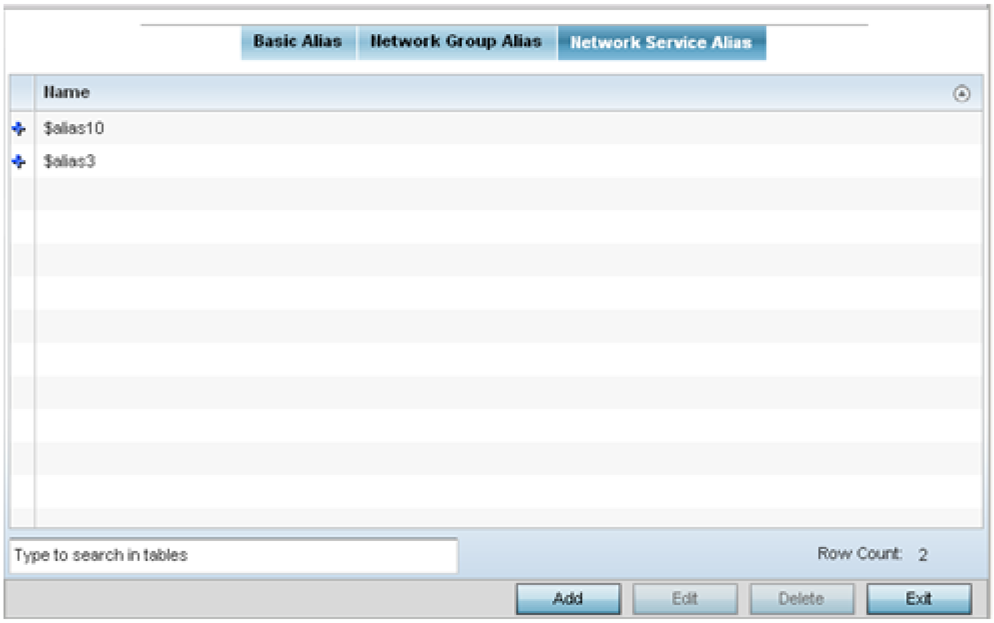


Figure 293: RF Domain Network Service Alias Screen

2 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

3 Select the added row to expand it into configurable parameters for defining the service alias rule.

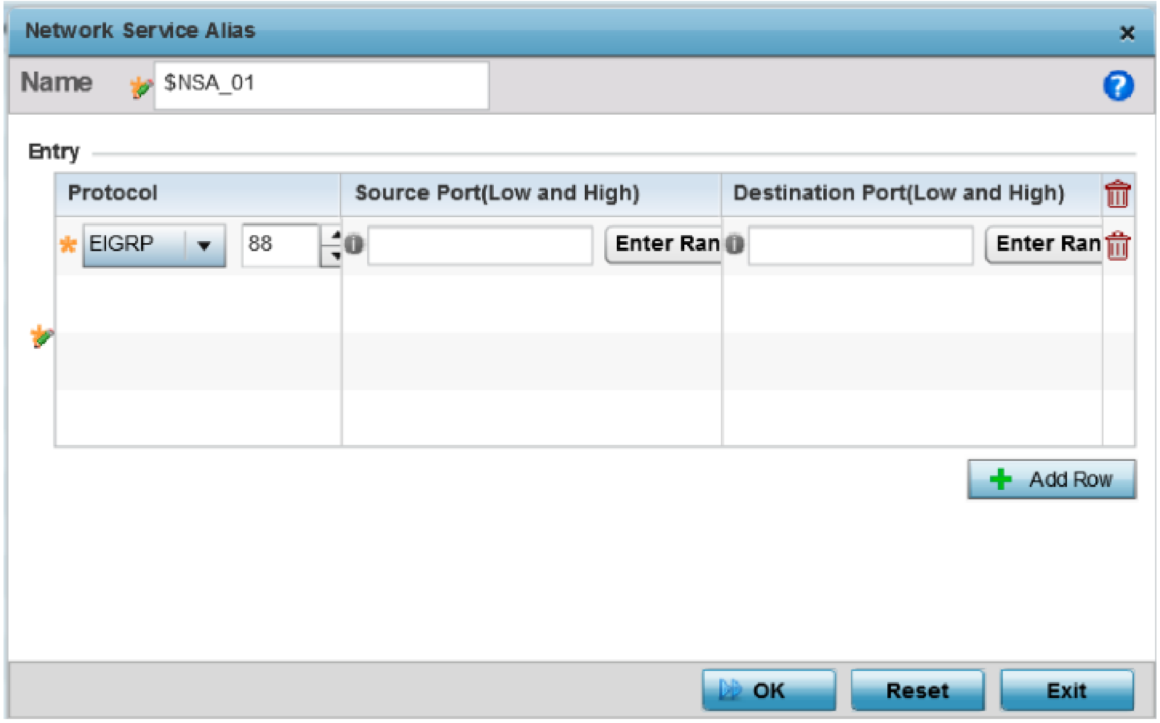


Figure 294: RF Domain Network Service Alias Add Screen

4 If adding a new Network Service Alias Rule, give it a name up to 32 characters. Ensure a $ precedes the name.

5 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias has to be 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 either `tcp` or `udp`. 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) such ranges can be specified.
Destination Port (Low and High)	This field is relevant only if the protocol is either `tcp` or `udp`. 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.

6 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 an existing service alias range entry to edit it.

7 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen to its last saved configuration.

RF Domain Deployment Considerations

Before settings RF Domains for controllers, service platforms and access points, refer to the following deployment guidelines to ensure the configurations are optimally effective:

- Each controller utilizes a default RF Domain. Access points are assigned to this default RF Domain as they are discovered. The default RF Domain can be used for single site deployments, where regional, regulatory and RF policies are common between devices.
- User defined RF Domains must be manually assigned to controllers, but can be manually or automatically assigned to access points.
- A Rogue AP detection configuration is a central component of an RF Domain policy, as it provides the RF Domain policy with the means to filter potentially threatening devices from operating with devices approved within the managed network.
- WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the radio(s) available to each WLAN.
- When planning sensor coverage, a minimum of 1 detector radio is recommended per 4 access points. To ensure effective placement, LANPlanner can be used to provide predictive planning services and visualization to ensure adequate radio coverage is provided based on site application and device requirements. LANPlanner provides visualization tools ensuring adequate radio coverage for client radios and sensors. A physical site survey should also be performed to verify client radio coverage, before a final deployment.
- Both default and user defined RF Domains contain policies and configuration parameters. Changes made to policies or configuration parameters are automatically inherited by all the controllers and access points assigned to the RF Domain.

10 Security Configuration

Wireless Firewall
Configuring IP Firewall Rules
Wireless Client Roles
Device Fingerprinting
Intrusion Prevention
EX3500 Time Range

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 771
- Configuring IP Firewall Rules on page 789
- Wireless Client Roles on page 803
- Device Fingerprinting on page 811
- Intrusion Prevention on page 816
- EX3500 Time Range on page 830

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.

For more information, refer to the following:

- Configuring a Firewall Policy on page 772
- Configuring MAC Firewall Rules on page 784
- Firewall Deployment Considerations on page 788

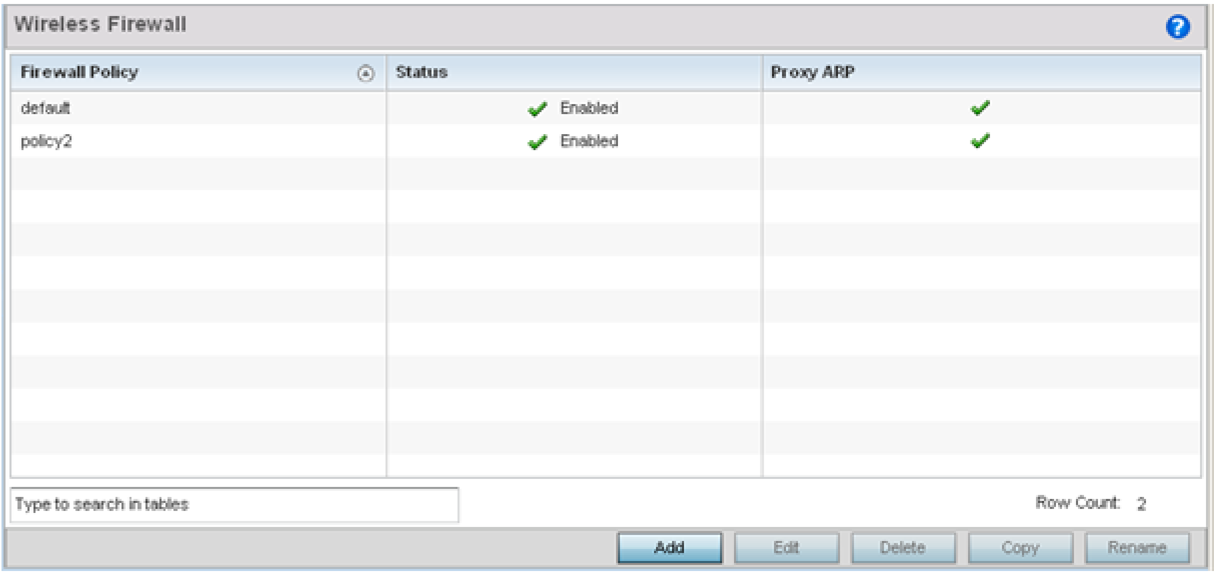
Configuring a Firewall Policy

Firewall configurations can be defined as separate policies available to the administrator for specific controller, service platform or access point deployments.

To define a firewall configuration:

1 Select **Configuration** > **Security** > **Wireless Firewall** > **Firewall Policy** to display existing firewall policies.

   The Wireless Firewall screen lists existing firewall policies. An existing policy can be selected and applied. The user has the option of displaying the configurations of each policy, or referring to the Wireless Firewall Browser and selecting individual polices for review.



Firewall Policy	Status	Proxy ARP
default	✓ Enabled	✓
policy2	✓ Enabled	✓

Row Count: 2

Figure 295: Wireless Firewall Policy Screen

2 Refer to the following configuration data for existing wireless firewall policies:

Firewall Policy	Displays the name assigned to the policy when created. The name cannot be modified as part of the edit process.
Status	Displays a green check mark if the policy has been enabled. A red "X" designates the policy as disabled.
Proxy ARP	Displays a green check mark if Proxy ARP routing has been enabled. A red "X" designates Proxy ARP as disabled.

3 Select **Add** to create a new wireless firewall policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available.

When adding a new firewall policy, begin by entering a name for the policy (not to exceed 64 characters). Then click **OK** to enable the other parameters within the screen.

The Wireless Firewall Policy configuration is divided into the following tabs:

- Firewall Policy Denial of Service on page 773 (displayed by default)
- Firewall Policy Storm Control on page 777
- Firewall Policy Advanced Settings on page 779

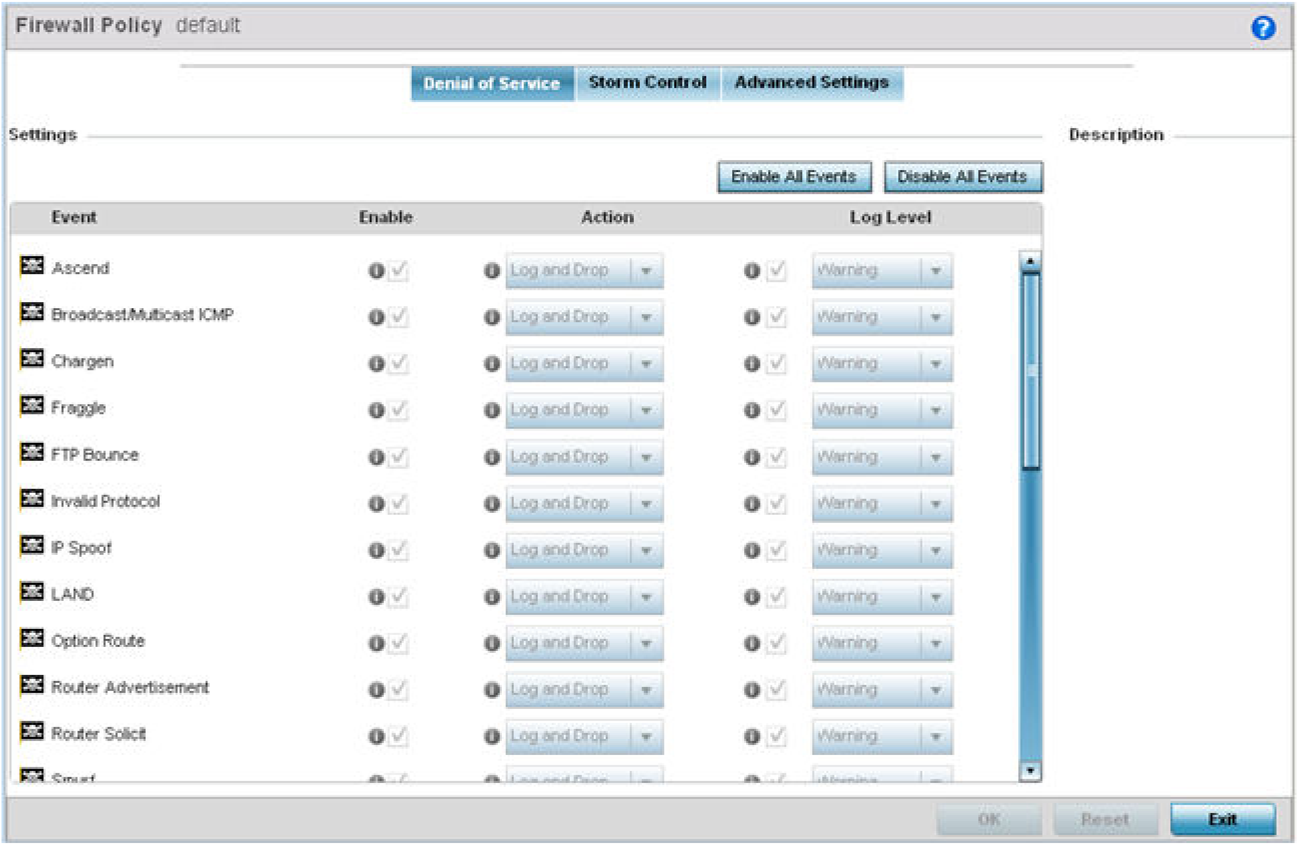
Firewall Policy Denial of Service

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 define a denial of service configuration for a Firewall policy:

1 Select the Denial of Service tab from the **Firewall Policy** configuration page.



Event	Enable	Action	Log Level
Ascend	✓	Log and Drop	✓ Warning
Broadcast/Multicast ICMP	✓	Log and Drop	✓ Warning
Chargen	✓	Log and Drop	✓ Warning
Fraggle	✓	Log and Drop	✓ Warning
FTP Bounce	✓	Log and Drop	✓ Warning
Invalid Protocol	✓	Log and Drop	✓ Warning
IP Spoof	✓	Log and Drop	✓ Warning
LAND	✓	Log and Drop	✓ Warning
Option Route	✓	Log and Drop	✓ Warning
Router Advertisement	✓	Log and Drop	✓ Warning
Router Solicit	✓	Log and Drop	✓ Warning

Figure 296: Wireless Firewall - Add/Edit - Denial of Service Screen

2 The **Settings** window contains a list of all of the Denial of Service (DoS) attacks for which the wireless controller's firewall has filters.

Each DoS filter contains the following items:

Event	Lists the name of each DoS attack.
Enable	Checking the **Enable** box sets the firewall policy to filter the associated DoS attack based on the selection in the Action column.
Action	If a Denial of Service filter is enabled, chose an action from the drop-down menu to determine how the firewall policy treats the associated DoS attack. • Log and Drop - An entry for the associated DoS attack is added to the log and then the packets are dropped. • Log Only - An entry for the associated DoS attack is added to the log. No further action is taken. • Drop Only - The DoS packets are 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.

3 Refer to the following for a summary of each Denial of Service attack the firewall can filter.

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. 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). 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. 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. 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. 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. 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. 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. Events can be individually enabled or collectively enabled/disabled using the **Enable All Events** and **Disable All Events** buttons.
5. Select **OK** to update the Denial of Service settings.

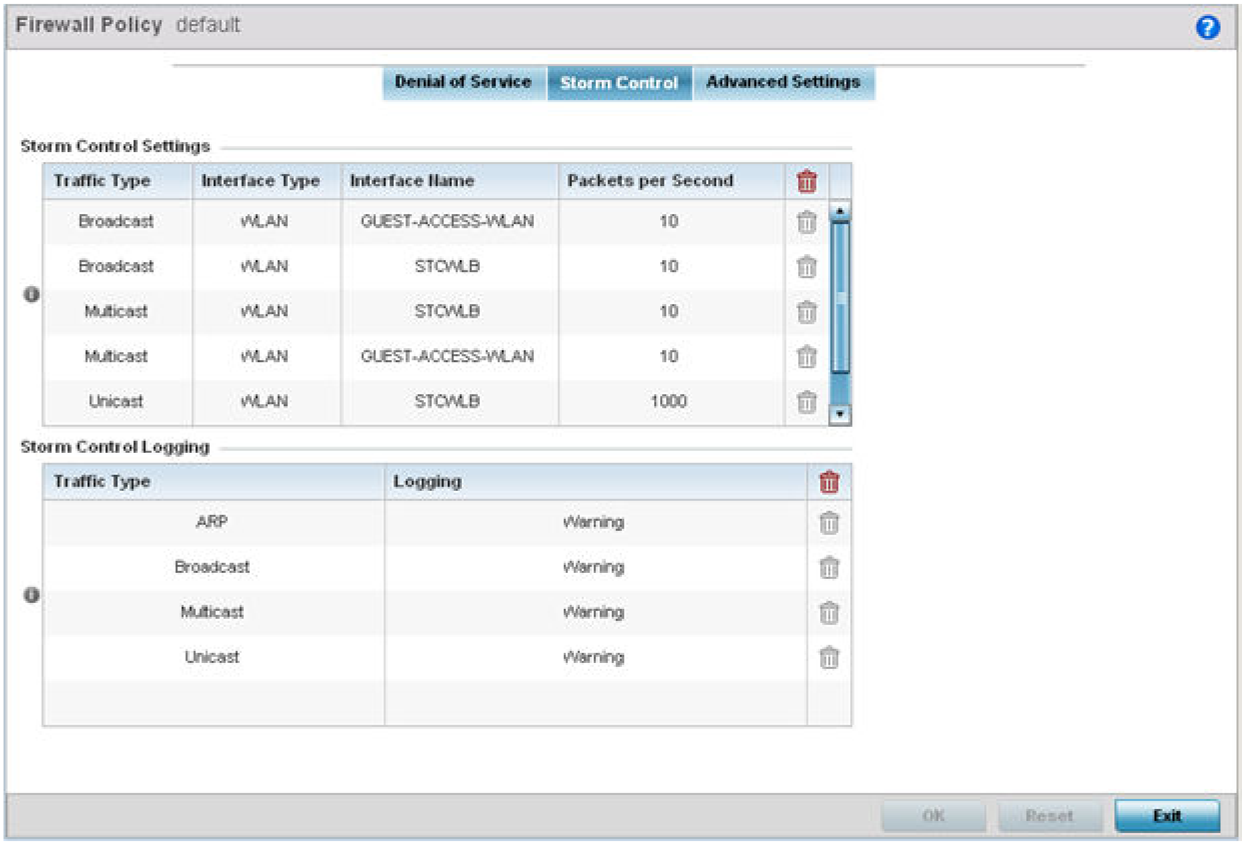
   Select **Reset** to revert to the last saved configuration.

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.



Traffic Type	Interface Type	Interface Name	Packets per Second
Broadcast	WLAN	GUEST-ACCESS-WLAN	10
Broadcast	WLAN	STCWLB	10
Multicast	WLAN	STCWLB	10
Multicast	WLAN	GUEST-ACCESS-WLAN	10
Unicast	WLAN	STCWLB	1000

Traffic Type	Logging
ARP	Warning
Broadcast	Warning
Multicast	Warning
Unicast	Warning

Figure 297: 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.

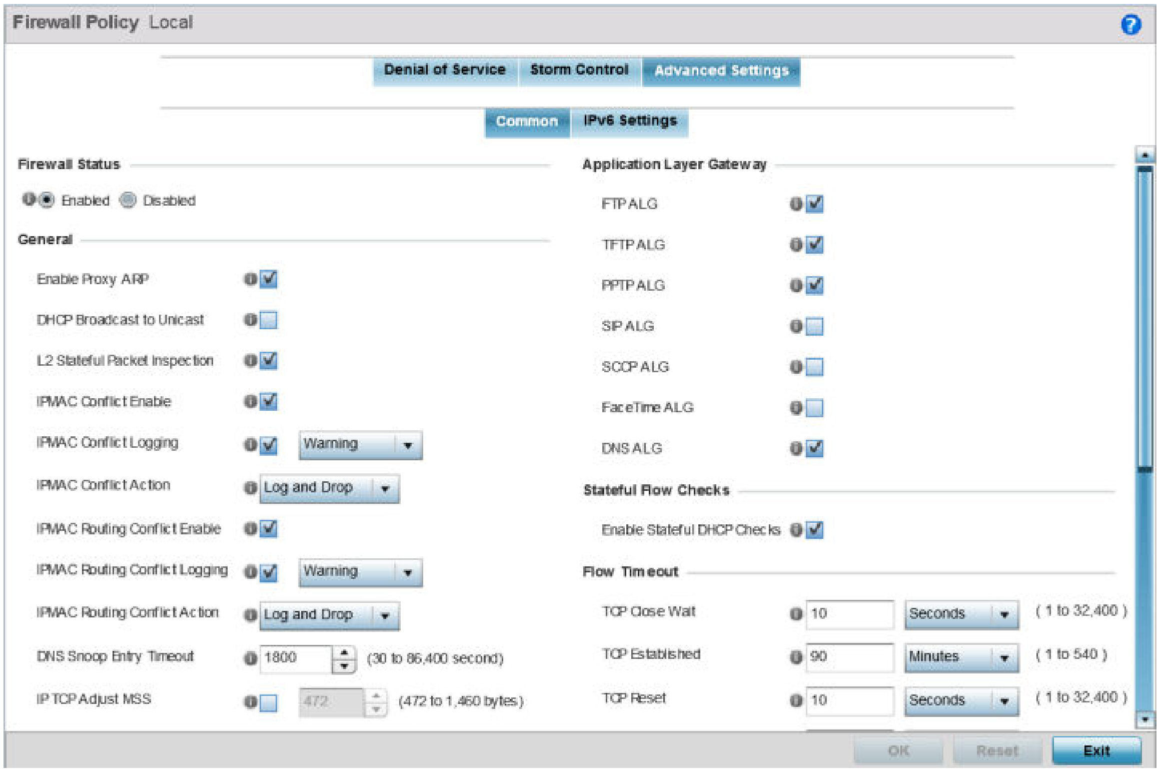
Firewall Policy Advanced Settings

To define a firewall policy Advanced Configuration:

1 Select the Advanced Settings tab from the **Firewall Policy** configuration page.

The **Advanced Settings** screen displays Common and IPv6 Settings tabs with the Common displayed by default. Use these screens to define common IPv4 settings and settings unique to an IPv6 firewall.

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.



Firewall Status
● Enabled ○ Disabled

General
Enable Proxy ARP ☑
DHCP Broadcast to Unicast ☐
L2 Stateful Packet Inspection ☑
IPMAC Conflict Enable ☑
IPMAC Conflict Logging ☑ Warning
IPMAC Conflict Action Log and Drop
IPMAC Routing Conflict Enable ☑
IPMAC Routing Conflict Logging ☑ Warning
IPMAC Routing Conflict Action Log and Drop
DNS Snoop Entry Timeout 1800 (30 to 86,400 second)
IP TCP Adjust MSS ☐ 472 (472 to 1,460 bytes)

Application Layer Gateway
FTP ALG ☑
TFTP ALG ☑
PPTP ALG ☑
SIP ALG ☐
SCCP ALG ☐
FaceTime ALG ☐
DNS ALG ☑

Stateful Flow Checks
Enable Stateful DHCP Checks ☑

Flow Timeout
TCP Close Wait 10 Seconds (1 to 32,400)
TCP Established 90 Minutes (1 to 540)
TCP Reset 10 Seconds (1 to 32,400)

Figure 298: Wireless Firewall - Add/Edit - Advanced Settings - Common Tab

2 Refer to the **Firewall Status** radio buttons to define the firewall as either enabled or disabled.

The firewall is enabled by default.

If you are disabling the firewall, a confirmation prompt displays stating NAT, wireless hotspot, proxy ARP, deny-staticwireless- client and deny-wireless-client sending not permitted traffic excessively will be disabled.

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.

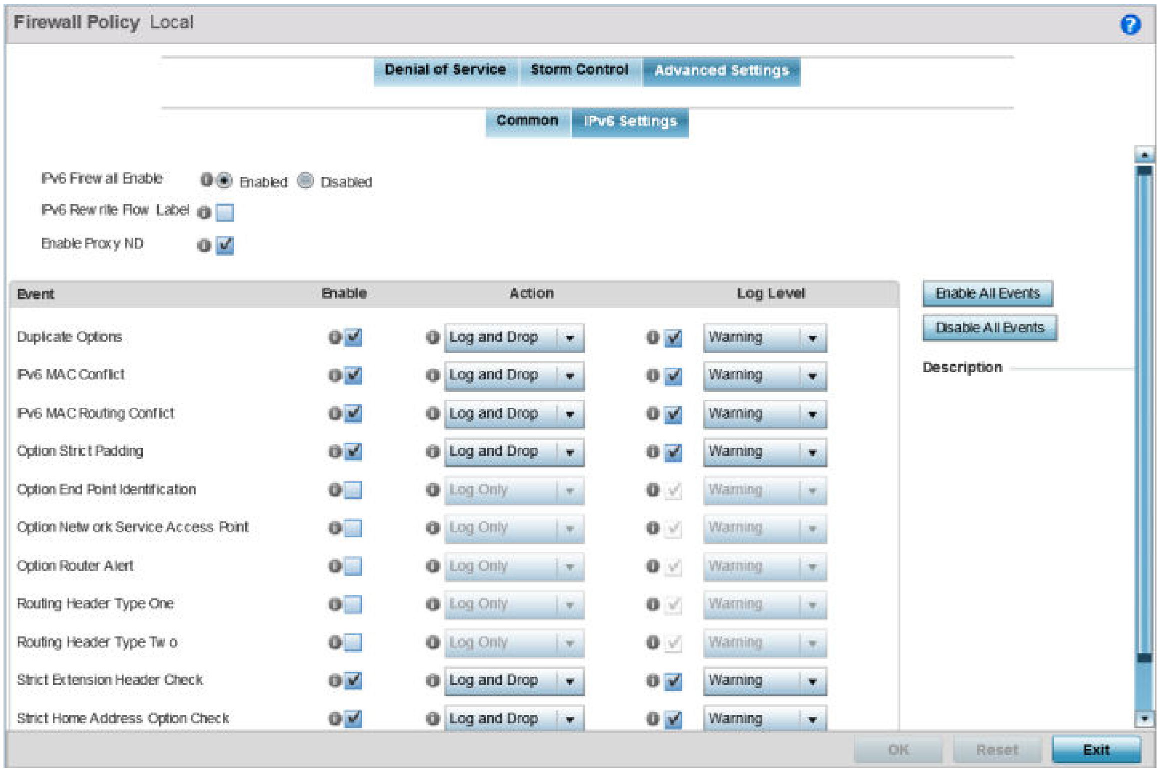
8 Refer to the **TCP Protocol Checks** field to set the following parameters:

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.

10 Select the IPv6 Settings tab.



IPv6 Firewall Enable ● Enabled ○ Disabled

IPv6 Rewrite Flow Label ☐

Enable Proxy ND ☑

Event	Enable	Action		Log Level
Duplicate Options	☑	Log and Drop	☑	Warning
IPv6 MAC Conflict	☑	Log and Drop	☑	Warning
IPv6 MAC Routing Conflict	☑	Log and Drop	☑	Warning
Option Strict Padding	☑	Log and Drop	☑	Warning
Option End Point Identification	☐	Log Only	☑	Warning
Option Network Service Access Point	☐	Log Only	☑	Warning
Option Router Alert	☐	Log Only	☑	Warning
Routing Header Type One	☐	Log Only	☑	Warning
Routing Header Type Two	☐	Log Only	☑	Warning
Strict Extension Header Check	☑	Log and Drop	☑	Warning
Strict Home Address Option Check	☑	Log and Drop	☑	Warning

Figure 299: Wireless Firewall - Add/Edit - Advanced Settings - IPv6 Settings Tab

11 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.

12 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.

13 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.

14 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. • Log and Drop - An entry for the associated IPv6 event is added to the log and then the packets are dropped. • Log Only - An entry for the associated IPv6 event is added to the log. No further action is taken. • 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.

15 Select **OK** to update the firewall policy's advanced IPv6 settings.

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

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.

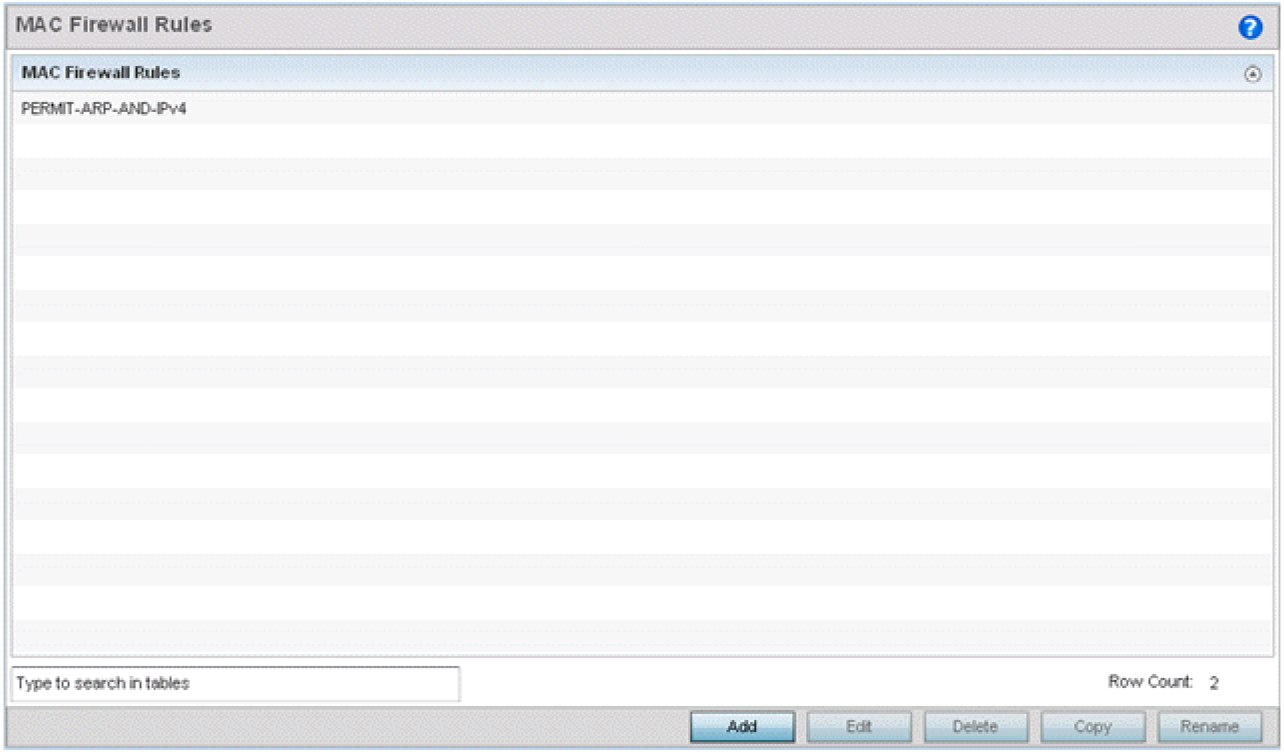
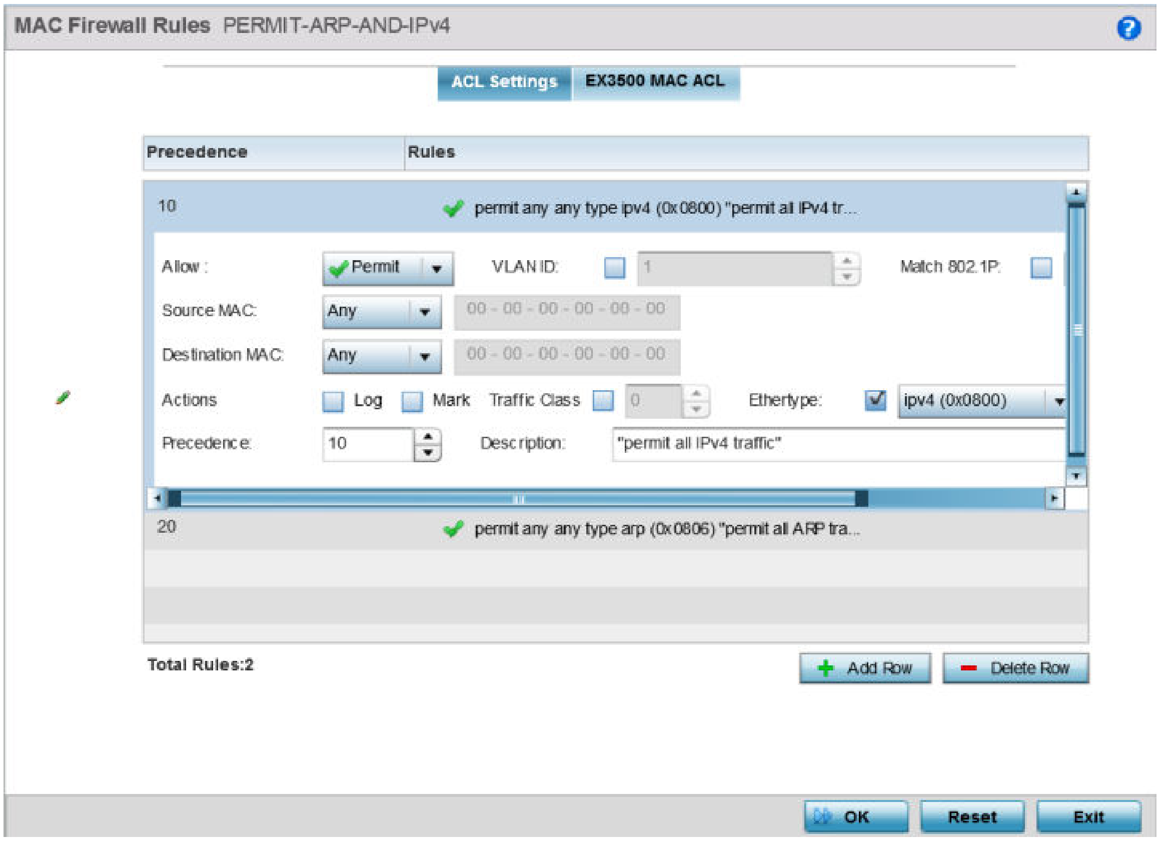


Figure 300: MAC Firewall Rules Screen

2 Select **+ Add Row** 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.



Precedence	Rules
10	✓ permit any any type ipv4 (0x0800) "permit all IPv4 tr...
20	✓ permit any any type arp (0x0806) "permit all ARP tra...

Allow : Permit
VLAN ID: ☐ 1
Match 802.1P: ☐
Source MAC: Any 00 - 00 - 00 - 00 - 00 - 00
Destination MAC: Any 00 - 00 - 00 - 00 - 00 - 00
Actions ☐ Log ☐ Mark Traffic Class ☐ 0 Ethertype: ☑ ipv4 (0x0800)
Precedence: 10 Description: "permit all IPv4 traffic"

Total Rules:2

Figure 301: MAC Firewall Rules - Add/Edit screen

4 If adding a new **MAC Firewall Rule**, provide a name up to 32 characters to help describe its filtering configuration.

5 Select a rule to modify it.

Set 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: • Deny - Instructs the firewall to prevent a packet from proceeding to its destination when filter conditions are met. • Permit - Instructs the firewall to allow a packet to proceed to its destination when filter conditions are met.
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 between 1 and 4094.
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.
Source and Destination MAC	Enter both source and destination MAC addresses. The source MAC address and destination MAC address are used as basic matching criteria. Provide a subnet mask if using a mask.

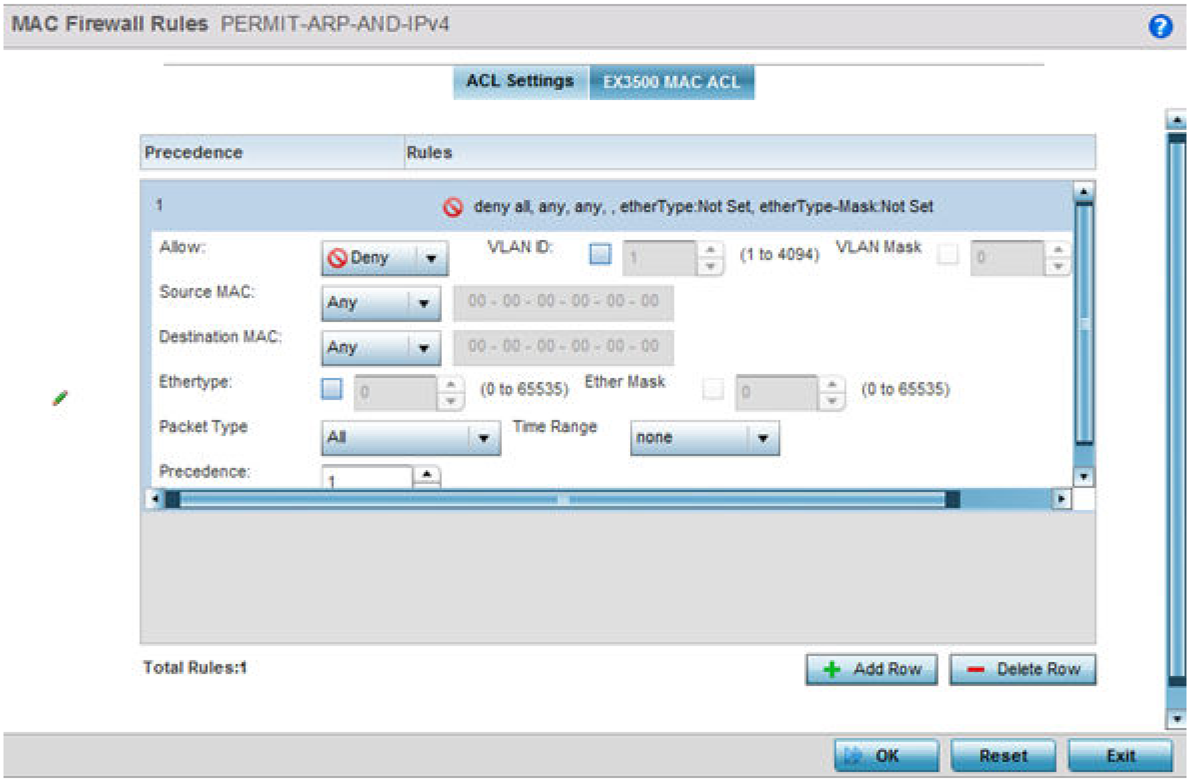
Action	The following actions are supported: • Log - Events are logged for archive and analysis. • Mark - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. • VLAN 802.1p priority. • DSCP bits in the IP header. • TOS bits in the IP header. • Mark, Log - Conducts both mark and log functions.
Traffic Class	Select this option to enable a spinner control for traffic class prioritization. Devices that originate a packet must identify a class or priority for packets. Devices use the traffic class field in the MAC header to set this priority.
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.
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.
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 the EX3500 MAC ACL tab to define MAC firewall rules specific to the EX3500 switch.

Select the added row to expand it into configurable parameters for defining the MAC based firewall rule for this model switch.



MAC Firewall Rules PERMIT-ARP-AND-IPv4

Precedence	Rules
1	deny all, any, any, , etherType:Not Set, etherType-Mask:Not Set

Allow: Deny

VLAN ID: ☐ 1 (1 to 4094)

VLAN Mask ☐ 0

Source MAC: Any 00 - 00 - 00 - 00 - 00 - 00

Destination MAC: Any 00 - 00 - 00 - 00 - 00 - 00

Ethertype: ☐ 0 (0 to 65535)

Ether Mask ☐ 0 (0 to 65535)

Packet Type All

Time Range none

Precedence: 1

Total Rules:1

Figure 302: EX3500 MAC ACL Add/Edit Screen

8 Select a rule to modify it.

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: • Deny - Instructs the firewall to prevent a packet from proceeding to its destination. • Permit - Instructs the firewall to allow a packet to proceed to its destination.
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 between 1 and 4094.
VLAN Mask	Enter a VLAN ID bit mask value.
Source and Destination MAC	Enter both source and destination MAC addresses. The source MAC address and destination MAC address are used as basic matching criteria. Provide a subnet mask if using a mask.
Ethertype	Use the spinner control to specify an Ethertype. 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. Select a value in the range 0 - 65535. This field is enabled by default. The default value is 1.
Ethertype Mask	Use the spinner control to specify the Ethertype Mask. Select a value in the range 0 - 65535. This field is enabled by default. The default value is 1.
Packet Type	Use the drop-down menu to select the packet type. Packet type can be one of all, tagged-eth2, or untagged-eth2.
Time Range	Use this field to select a time range when this ACL will be enabled. For more information, see EX3500 Time Range on page 830.
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.

9 Select **OK** when completed to update the MAC firewall Rules.

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

Firewall Deployment Considerations

Before defining a unique controller, service platform or access point Firewall access policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Firewalls implement access control policies, so if you don't have an idea of what kind of access to allow or deny, a Firewall is of little value.
- It is 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
- 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 network access. Firewall policies should be applied to captive portal enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.

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 IP SNMP ACL Policy on page 794
- Setting a Network Service Alias on page 797
- EX3500 ACL Standard on page 799

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:

1 Select **Configuration** > **Security** > **IP Firewall**.

2 Expand the **IP Firewall** menu item and select either the **IPv4 ACL** or **IPv6 ACL** menu option.

Either the IPv4 Firewall Rules screen or the IPv6 Firewall Rules screen displays the existing polices defined thus far.

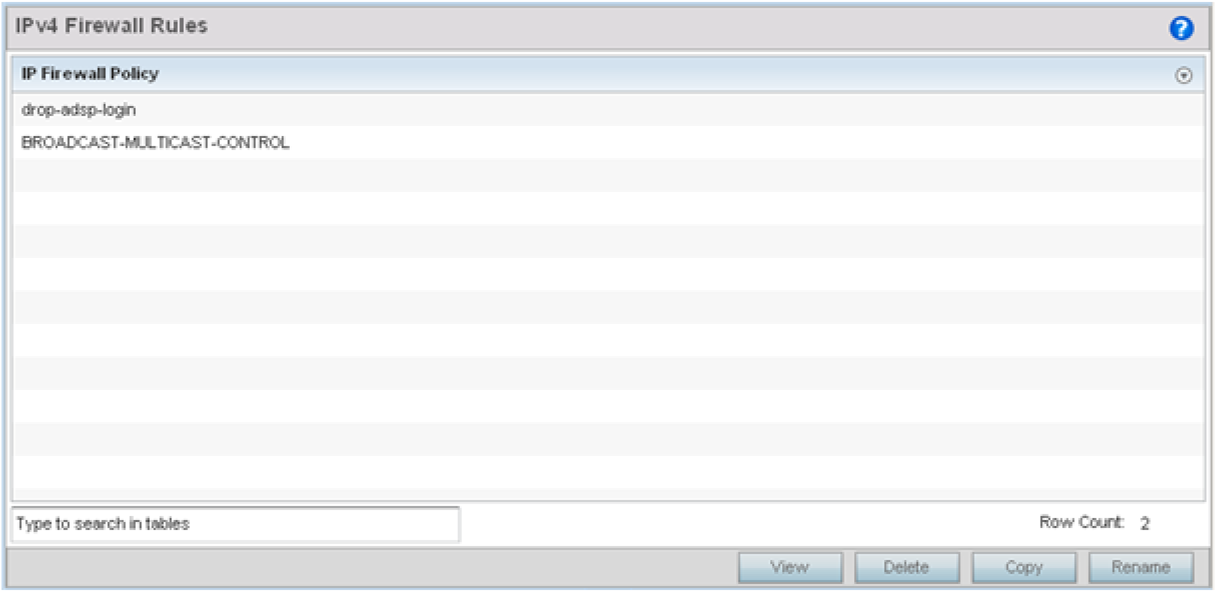
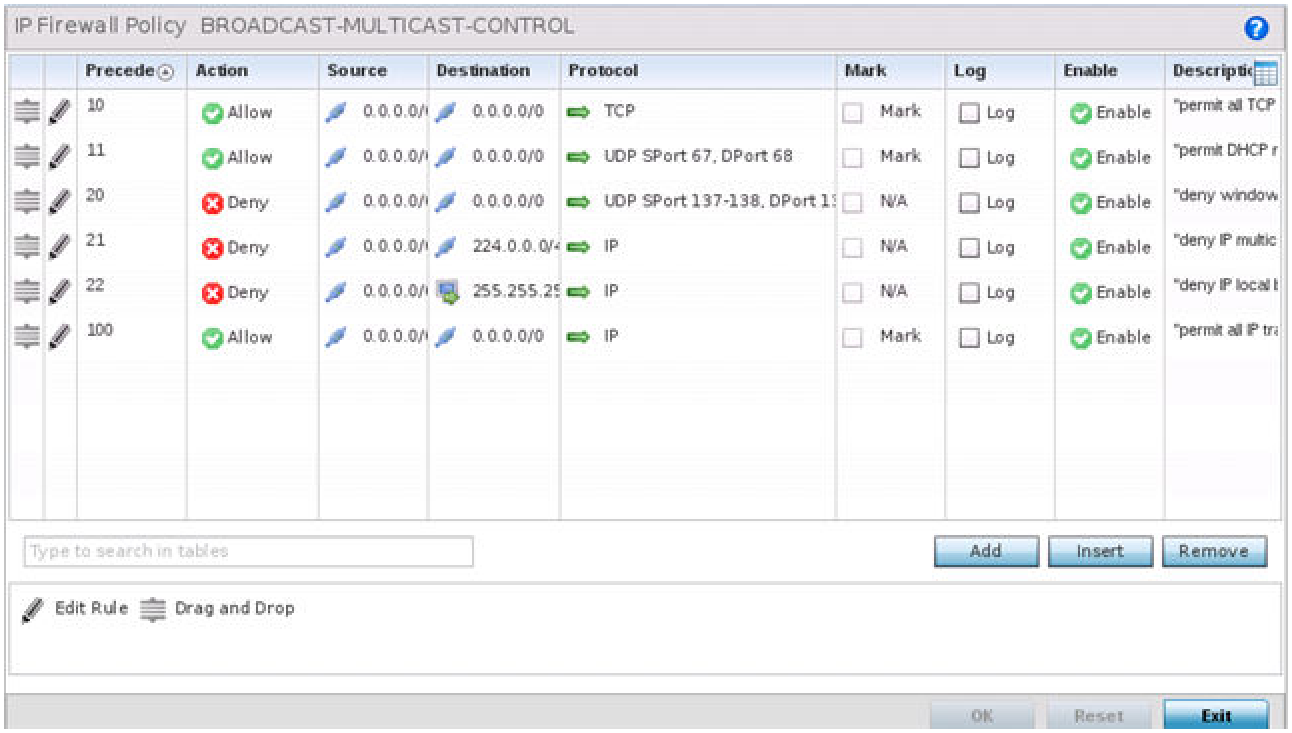


Figure 303: IP Firewall Rules Screen

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.

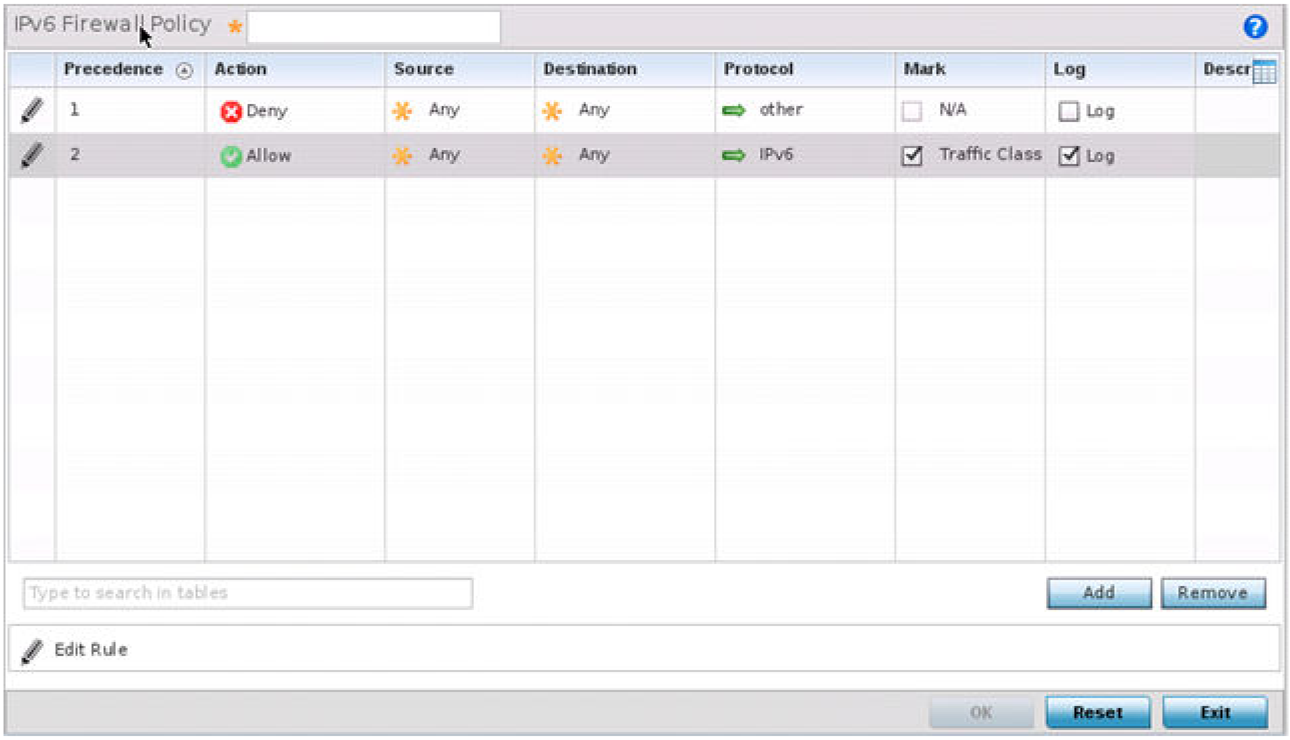
4 Select the added row to expand it into configurable parameters for defining the IPv4 or IPv6 based firewall policy.



IP Firewall Policy BROADCAST-MULTICAST-CONTROL

Precede	Action	Source	Destination	Protocol	Mark	Log	Enable	Descriptio
10	Allow	0.0.0.0/	0.0.0.0/0	TCP	☐ Mark	☐ Log	Enable	"permit all TCP
11	Allow	0.0.0.0/	0.0.0.0/0	UDP SPort 67, DPort 68	☐ Mark	☐ Log	Enable	"permit DHCP r
20	Deny	0.0.0.0/	0.0.0.0/0	UDP SPort 137-138, DPort 1	☐ N/A	☐ Log	Enable	"deny window
21	Deny	0.0.0.0/	224.0.0.0/	IP	☐ N/A	☐ Log	Enable	"deny IP multic
22	Deny	0.0.0.0/	255.255.25	IP	☐ N/A	☐ Log	Enable	"deny IP local I
100	Allow	0.0.0.0/	0.0.0.0/0	IP	☐ Mark	☐ Log	Enable	"permit all IP tr

Figure 304: IPv4 Firewall Rules - Add/Edit Screen



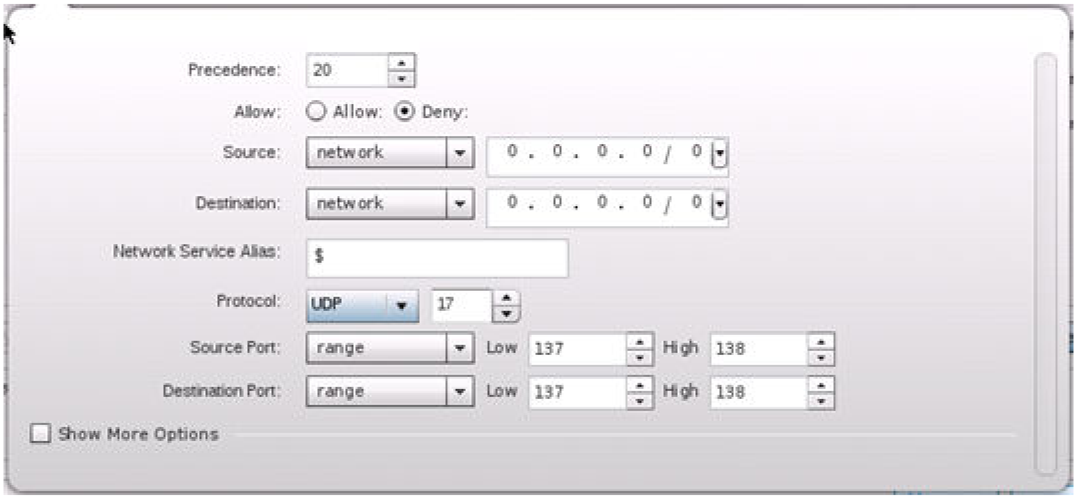
IPv6 Firewall Policy *

Precedence	Action	Source	Destination	Protocol	Mark	Log	Descr
1	Deny	Any	Any	other	☐ N/A	☐ Log	
2	Allow	Any	Any	IPv6	☑ Traffic Class	☑ Log	

Figure 305: IPv6 Firewall Rules - Add/Edit Screen

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.

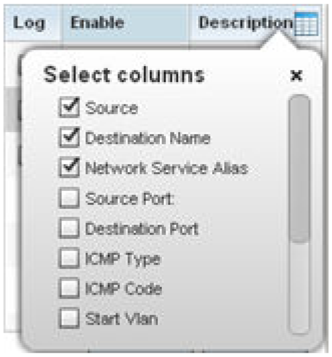
a Select the Edit Rule icon to the left of a particular IP firewall rule configuration to update its parameters collectively.



Precedence: 20
Allow: ○ Allow: ● Deny:
Source: network 0 . 0 . 0 . 0 / 0
Destination: network 0 . 0 . 0 . 0 / 0
Network Service Alias: $
Protocol: UDP 17
Source Port: range Low 137 High 138
Destination Port: range Low 137 High 138
☐ Show More Options

Figure 306: IP Firewall Rules - Add Criteria Screen

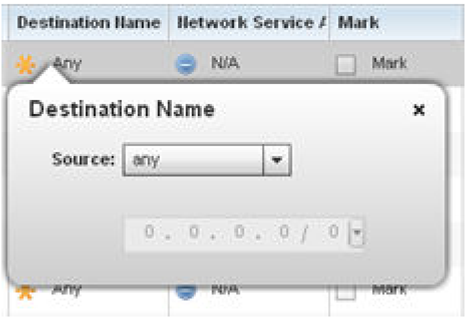
b Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.



Log Enable Description

Select columns ×
☑ Source
☑ Destination Name
☑ Network Service Alias
☐ Source Port
☐ Destination Port
☐ ICMP Type
☐ ICMP Code
☐ Start Vlan

Figure 307: IP Firewall Rules - Select Columns Pop-up



Source: any

Figure 308: 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.

5 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: • Deny - Instructs the firewall to restrict a packet from proceeding to its destination. • Permit - Instructs the firewall to allow a packet to proceed to its destination.
Source	Select the source IP address used as basic matching criteria for this IP ACL rule.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (any), are designated as a set of configurations consisting of protocol and port mappings (an alias), set as a numeric IP address (host) or defined as network IP and mask. Selecting alias requires a destination network group alias be available or created.
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.
Mark	Select an IP firewall rule's **Mark** check box to enable or disable event marking and set the rule's 8021p or dscp level (from 0 - 7).
Log	Select an IP firewall rule's **Log** check box to enable or disable event logging for this rule's usage.
Enable	This option displays for IPv4 based firewalls only. Select an IPv4 firewall rule's Enable or Disable icon to determine this rule's inclusion with the IP firewall policy.
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.

6 Select **Add** to add additional IP firewall rule configurations.

Select **Remove** to remove selected IP firewall rules as they become obsolete for filtering network access permissions.

7 Select **OK** when completed to update the IP firewall rules.

Select **Reset** to revert the screen to its 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**.

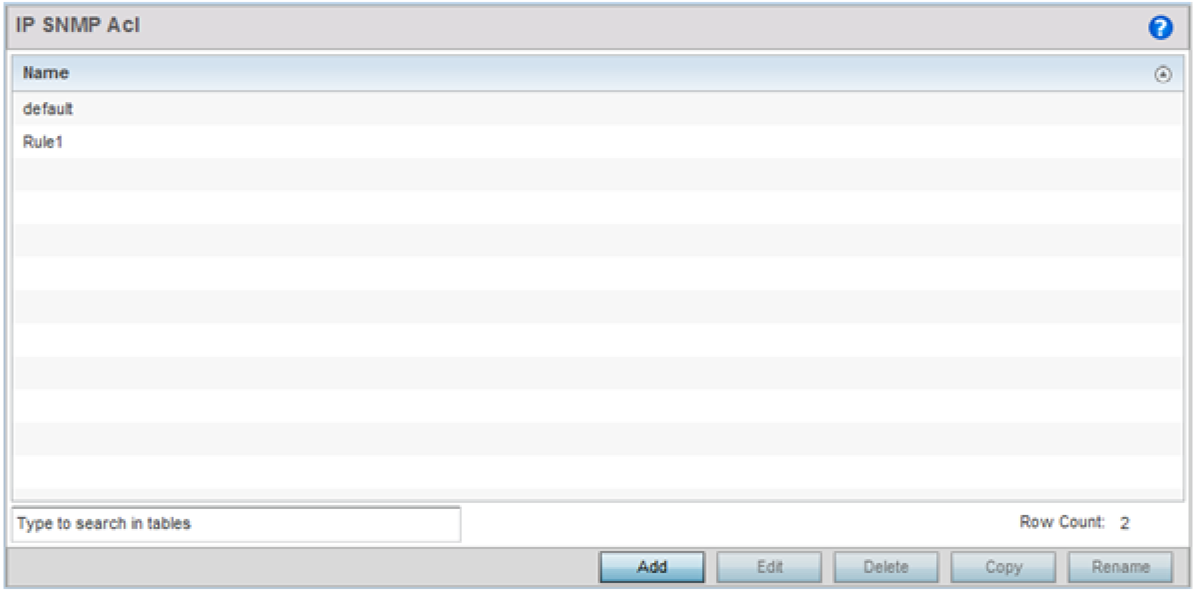
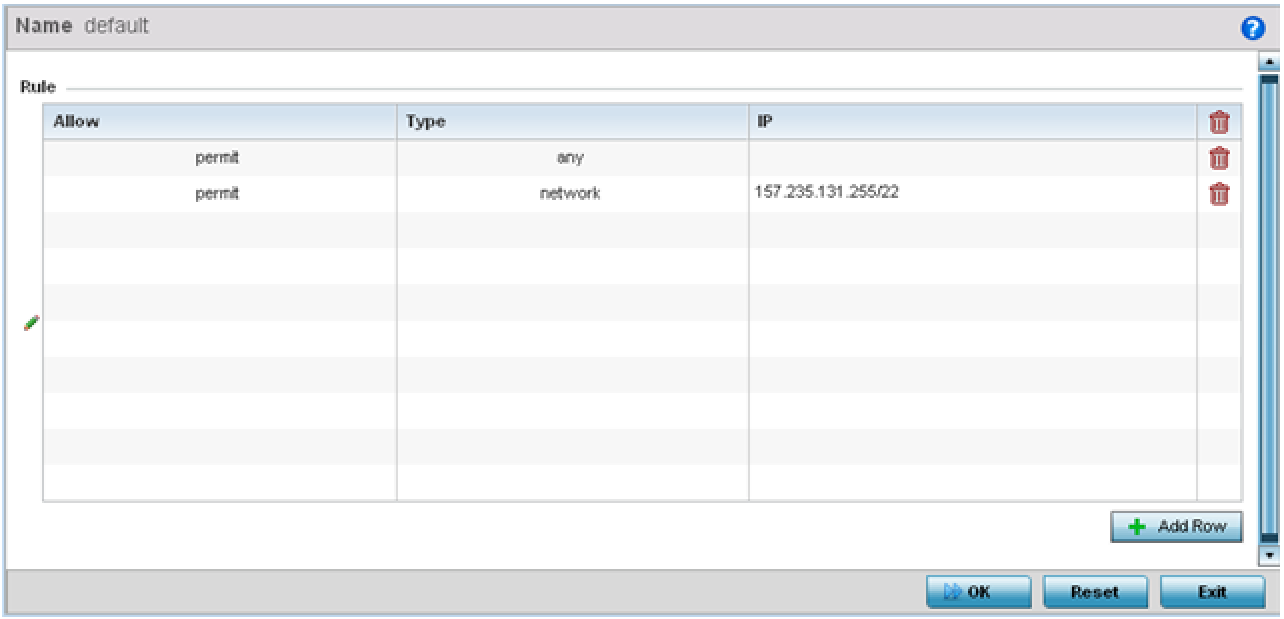


Figure 309: IP SNMP ACL Screen

3 Select **Add** to create a new SNMP firewall rule.

Select an existing policy and click **Edit** to modify the attributes of that policy's configuration. Existing policies can be removed by highlighting them and selecting **Delete**.



Allow	Type	IP
permit	any	
permit	network	157.235.131.255/22

Figure 310: IP SNMP ACL - Add/Edit screen

4 Provide a new IP SNMP ACL **Name** up to 32 characters in length to help distinguish this ACL from others with similar rules.

5 Select **+ Add Row** to launch a sub-screen where the ACL's permit/deny and network type rules can be applied.

Allow	Select this option to allow the SNMP MIB object traffic. The default setting is to permit SNMP traffic.
Type	Define whether the permit or deny ACL rule applied to the ACL is specific to a **`Host`** IP address, is applied to a **`Network`** address and subnet mask, or is applied to **`Any`**. The default setting is **`Network`**.

6 Select **Add** to add additional IP firewall rule configurations.

Select **Remove** to remove selected IP firewall rules as they become obsolete for filtering network access permissions.

7 Select **OK** when completed to update the IP firewall rules.

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

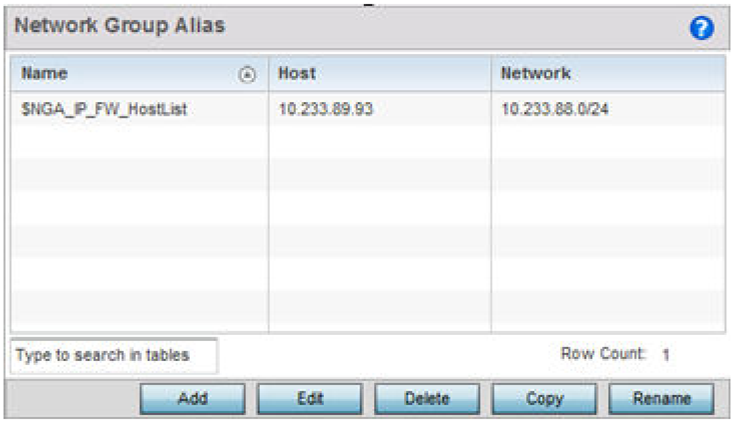
Setting a Network Group Alias

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** > **IP Firewall** > **Network Group Alias** from the Web UI.
2 Select **Add**, or highlight an existing network group alias and select **Edit**.



Name	Host	Network
$NGA_IP_FW_HostList	10.233.89.93	10.233.88.0/24

Figure 311: IP Firewall Network Group Alias Screen

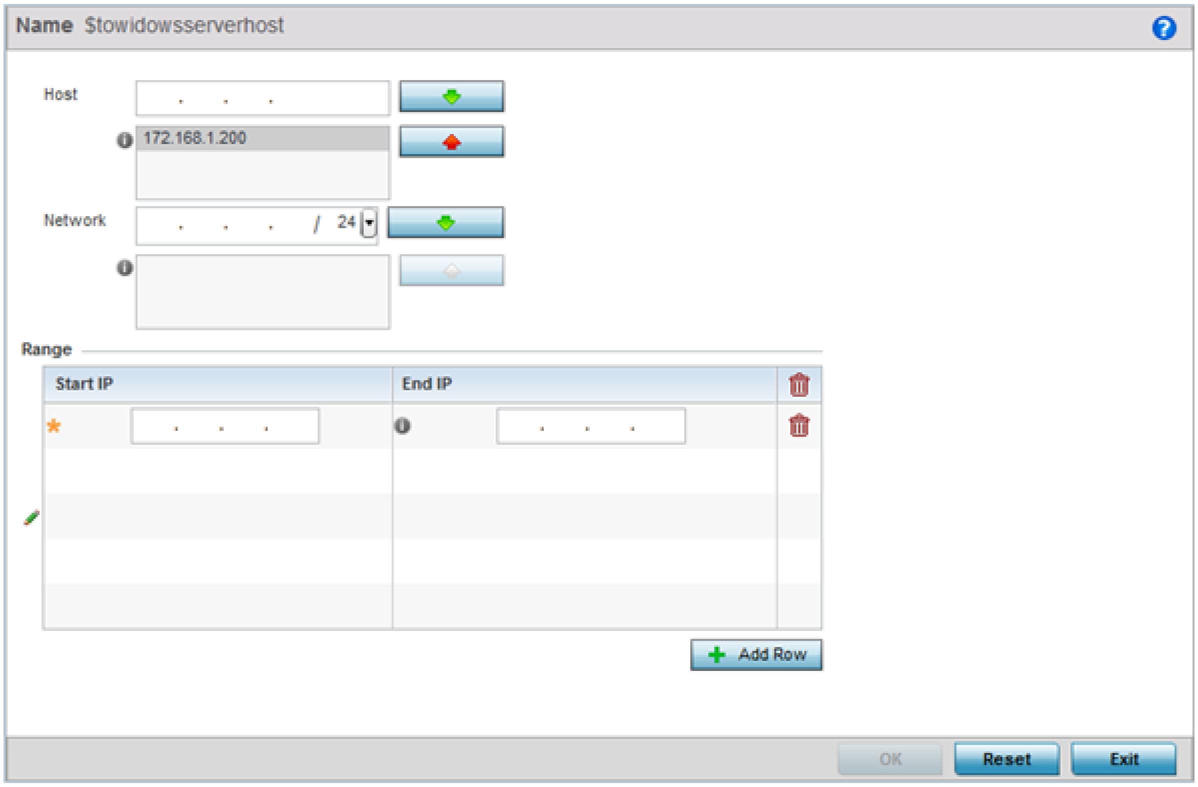
3 Review the existing Nertwork Group alias configurations.

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.

4 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy, or **Delete** to remove obsolete policies.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

5 Click **Add** to create a new network group alias, or select an existing network group alias and click **Edit**.


Name $towidowsserverhost

Host

172.168.1.200

Network

24

Figure 312: Network Group Alias - Add/Edit Screen

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 ($).

6 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.

7 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.

8 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

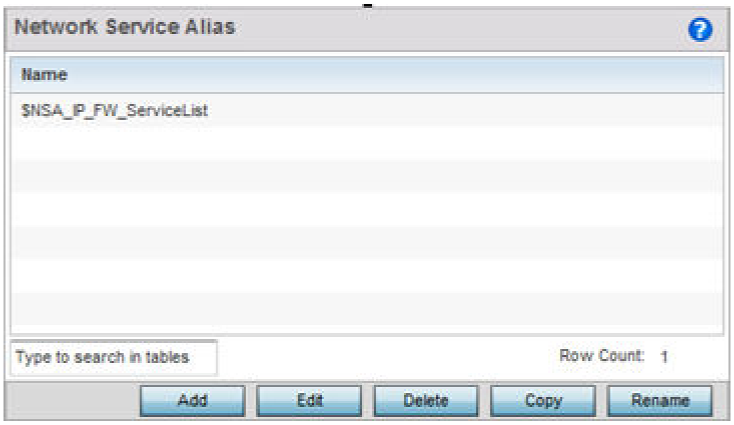
A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to two source port ranges and up to two destination port ranges can be configured. A maximum of four protocol entries can be configured 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.



Name
$NSA_IP_FW_ServiceList

Row Count: 1

Figure 313: IP Firewall Network Service Alias Screen

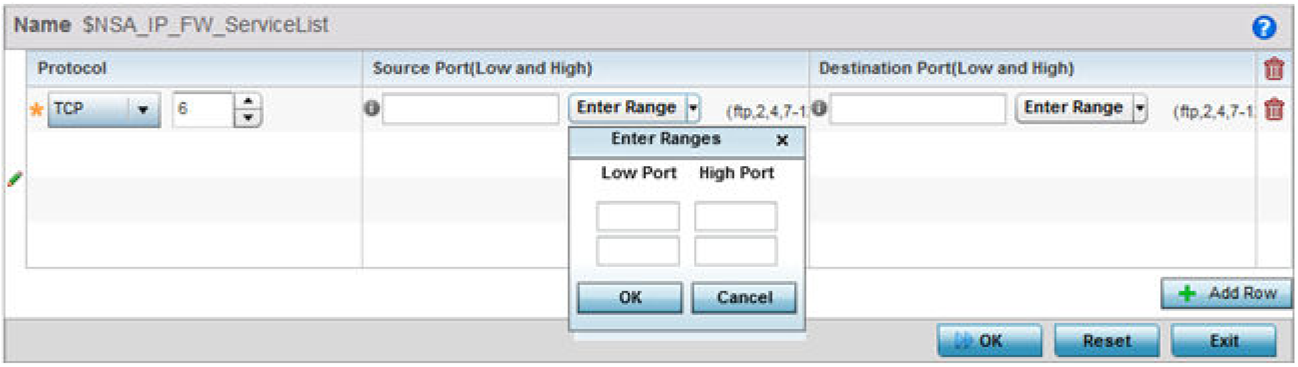
2 Select **Add** to create a new network service alias.

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 ($).



Name $NSA_IP_FW_ServiceList

Protocol: TCP 6

Figure 314: 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. 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. 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.

EX3500 ACL Standard

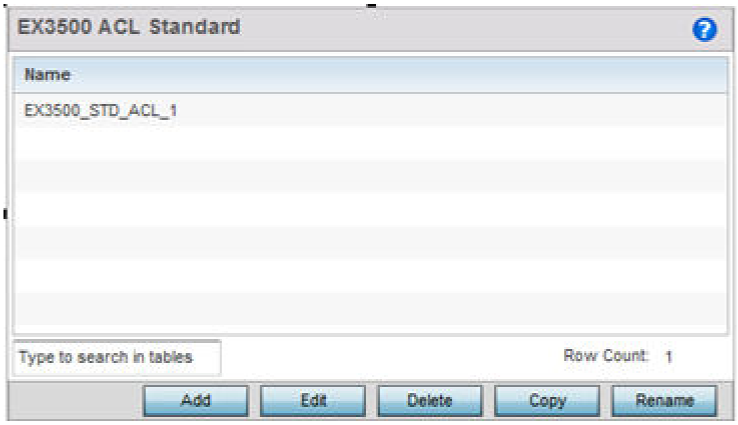
A Standard ACL for EX3500 is a policy-based ACL that either prevents or allows specific clients from using the device.

An ACL affords a system administrator the ability to grant or restrict client access by specifying that traffic from a specific host or a specific network to either be denied or permitted.

To define a standard ACL for EX3500:

1 Select **Configuration** > **Security** > **IP Firewall** > **EX3500 ACL Standard** from the Web UI.

The EX3500 ACL Standard screen displays within the main portion of the Web UI.



EX3500 ACL Standard

Name
EX3500_STD_ACL_1

Type to search in tables

Row Count: 1

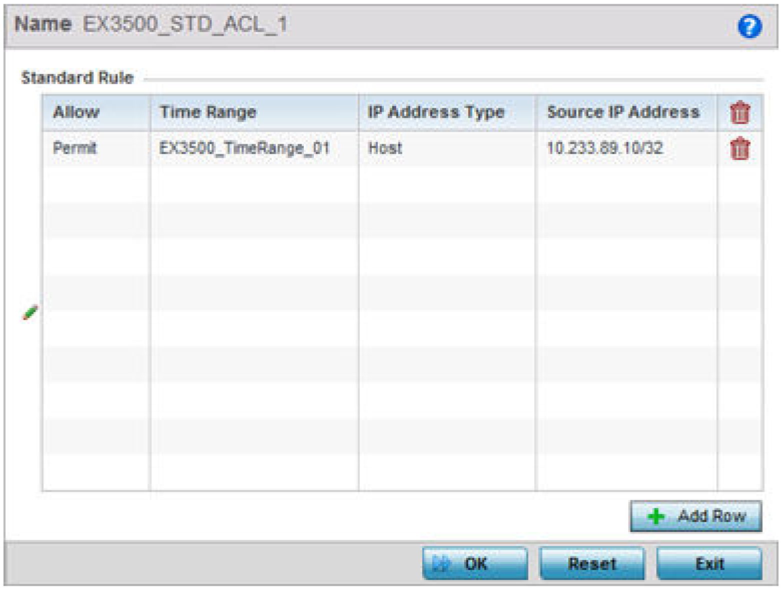
Figure 315: EX3500 ACL Standard Screen

2 Select **Add** to create a new ACL, **Edit** to modify the attributes of an existing ACL, or **Delete** to remove obsolete ACLs.

Use **Copy** to create a copy of the selected ACL and modify it for further use. Use **Rename** to rename the selected ACL.

3 Either use **Add** to create a new EX3500 Standard ACL, or select an existing ACL and click **Edit** to edit it.

The following screen displays.



Name EX3500_STD_ACL_1

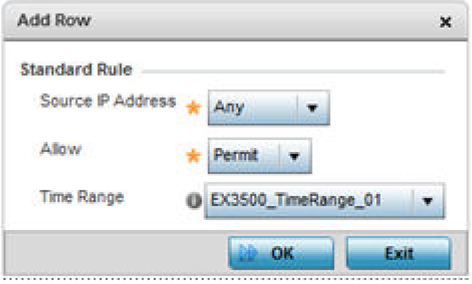
Standard Rule

Allow	Time Range	IP Address Type	Source IP Address
Permit	EX3500_TimeRange_01	Host	10.233.89.10/32

Figure 316: EX3500 ACL Standard - Add/Edit Screen

4 If you are adding a new **EX3500 ACL Standard**, provide it a name with up to 32 characters.

5 To add a new standard rule, click **Add Row**.



Add Row

Standard Rule

Source IP Address: Any

Allow: Permit

Time Range: EX3500_TimeRange_01

Figure 317: EX3500 ACL Standard - Add/Edit - Standard Rule Screen

6 Provide the following details:

Source IP Address	Use this drop-down menu to provide the source information. Source IP address can be one of Any, Host or Network. When selecting Host provide the IP address of the host device. When selecting Network, provide the IP address of the network along with the mask.
Allow	Use this drop-down menu to indicate the action to be performed. Select from **Permit** or **Deny**.
Time Range	From the drop-down menu select the preconfigured time range to use for this ACL. Select None to indicate no preference. For more information on time ranges, see EX3500 Time Range on page 830.

7 Select **OK** when completed to update the EX3500 Standard ACL.

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

EX3500 ACL Extended

An extended ACL is comprised of access control entries (ACEs). Each ACE specifies a source and destination for matching and filtering traffic to the EX3500 switch.

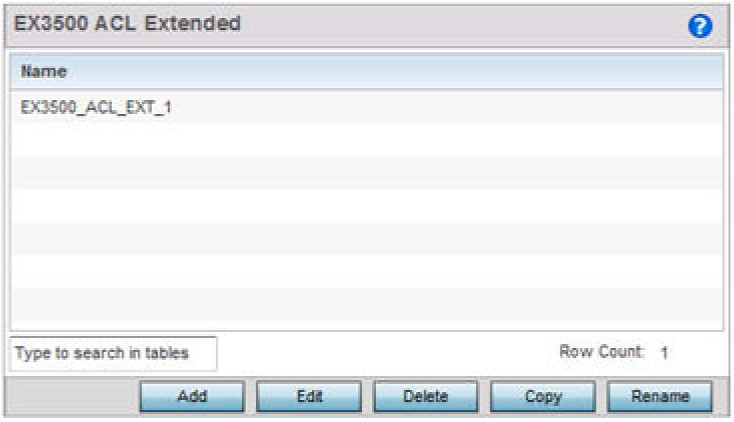
An ACL affords a system administrator the ability to grant or restrict client access by specifying that traffic from a specific host or a specific network to either be denied or permitted.

IP based firewalls function like Access Control Lists (ACLs) to filter/mark packets, 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.

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 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.

To configure an extended ACL on EX3500:

1 Select **Configuration** > **Security** > **IP Firewall** > **EX3500 ACL Extended** from the Web UI.



EX3500 ACL Extended

Name
EX3500_ACL_EXT_1

Row Count: 1

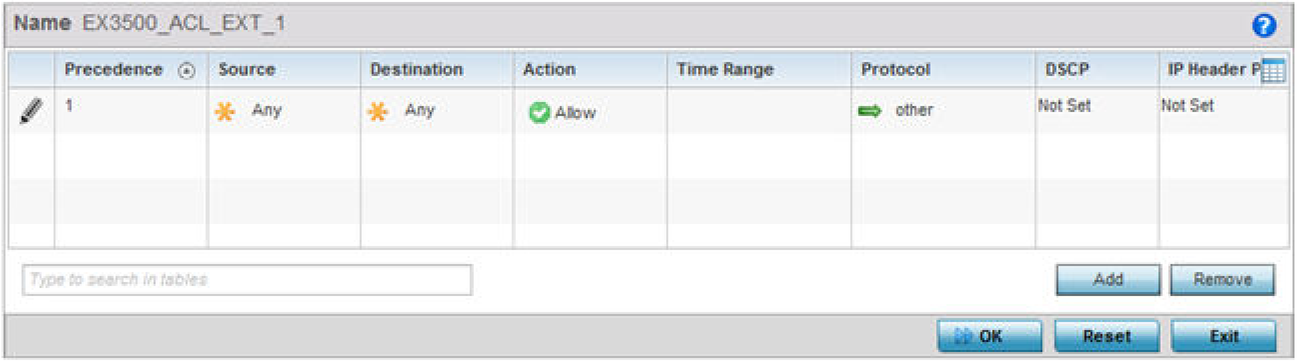
Figure 318: EX3500 ACL Extended Screen

2 Select **Add** to create a new ACL, **Edit** to modify the attributes of an existing ACL, or **Delete** to remove obsolete ACLs.

Use **Copy** to create a copy of the selected ACL and modify it for further use. Use **Rename** to rename the selected ACL.

3 Either use **Add** to create a new EX3500 Extended ACL, or select an existing ACL and click **Edit** to edit it.

The following screen displays.



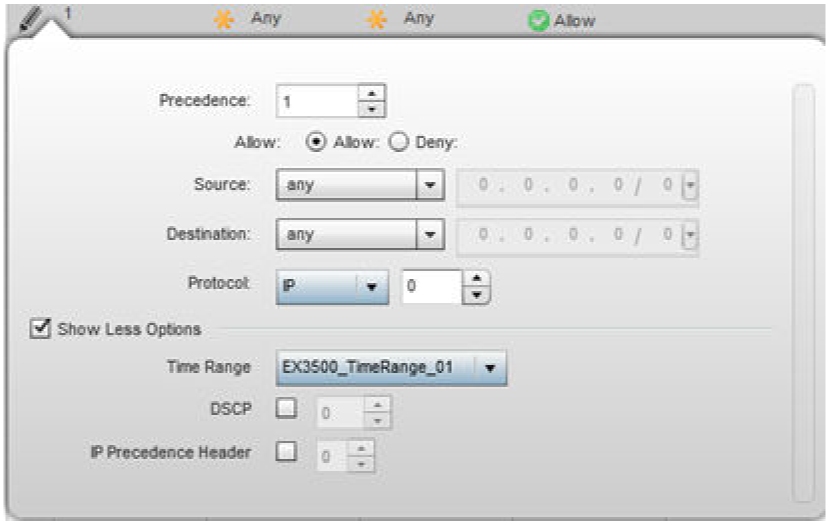
Name EX3500_ACL_EXT_1

	Precedence	Source	Destination	Action	Time Range	Protocol	DSCP	IP Header P
✎	1	Any	Any	Allow		other	Not Set	Not Set

Figure 319: EX3500 ACL Extended - Add/Edit Screen

EX3500 extended ACL configurations can either be modified as a collective group of variables or selected and updated individually if 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.



1 Any Any Allow

Precedence: 1

Allow: ● Allow: ○ Deny:

Source: any 0 . 0 . 0 . 0 / 0

Destination: any 0 . 0 . 0 . 0 / 0

Protocol: IP 0

☑ Show Less Options

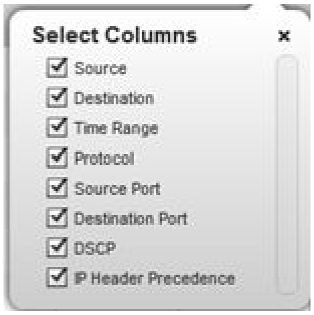
Time Range EX3500_TimeRange_01

DSCP ☐ 0

IP Precedence Header ☐ 0

Figure 320: EX3500 ACL Extended - Add/Edit - Add Criteria Screen

b Click the icon located at the top right-hand side of the screen and select the values as needed to add/hide criteria to the configuration of the extended ACL.



Select Columns

- ☑ Source
- ☑ Destination
- ☑ Time Range
- ☑ Protocol
- ☑ Source Port
- ☑ Destination Port
- ☑ DSCP
- ☑ IP Header Precedence

Figure 321: EX3500 ACL Extended - Select Fields Screen

4 Define the following Extended ACL rule settings as required:

Precedence	Specify or modify a precedence for this ACL between 1-128. 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 ACL rule is made up of matching criteria rules. The action defines the action to be performed if it matches the specified criteria. The following actions are supported: • Deny - Instructs the firewall to restrict a packet from proceeding to its destination. • Permit - Instructs the firewall to allow a packet to proceed to its destination.
Source	Use this drop-down menu to provide the source information. Source IP address can be one of Any, Host, or Network. When selecting Host provide the IP address of the host device. When selecting Network, provide the IP address of the network along with the mask.
Destination	Use this drop-down menu to provide the destination information. Destination IP address can be one of Any, Host or Network. When selecting Host provide the IP address of the host device. When selecting Network, provide the IP address of the network along with the mask.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Depending on the selected protocol, other fields might become visible and can be configured.
Time Range	Use the drop-down menu to configure a time range when this ACL is applicable. For more information on configuring time ranges, see EX3500 Time Range on page 830.
DSCP	*Differentiated Services Code Point* is a mechanism that specifies a simple mechanism for classifying and manage network traffic and provide a QoS mechanism. Use the spinner to select a value in the range 0-63. Use this value to classify and mark packets that match the criteria specified in this extended ACL rule. Either **DSCP** or **IP Header Precedence** can be configured. The two fields cannot be configured together.
IP Header Precedence	Use this field to set the precedence value in the IP Header. Use the spinner to select a value in the range 0-7. Use this value to classify and mark packets that match the criteria specified in this extended ACL rule. Either **DSCP** or **IP Header Precedence** can be configured. The two fields cannot be configured together.

5 Select **OK** when completed to update the EX3500 Extended ACL.

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 Select **Configuration** > **Security** > **Wireless Client Roles**.

The Wireless Client Roles screen displays the name of those client role policies created thus far.

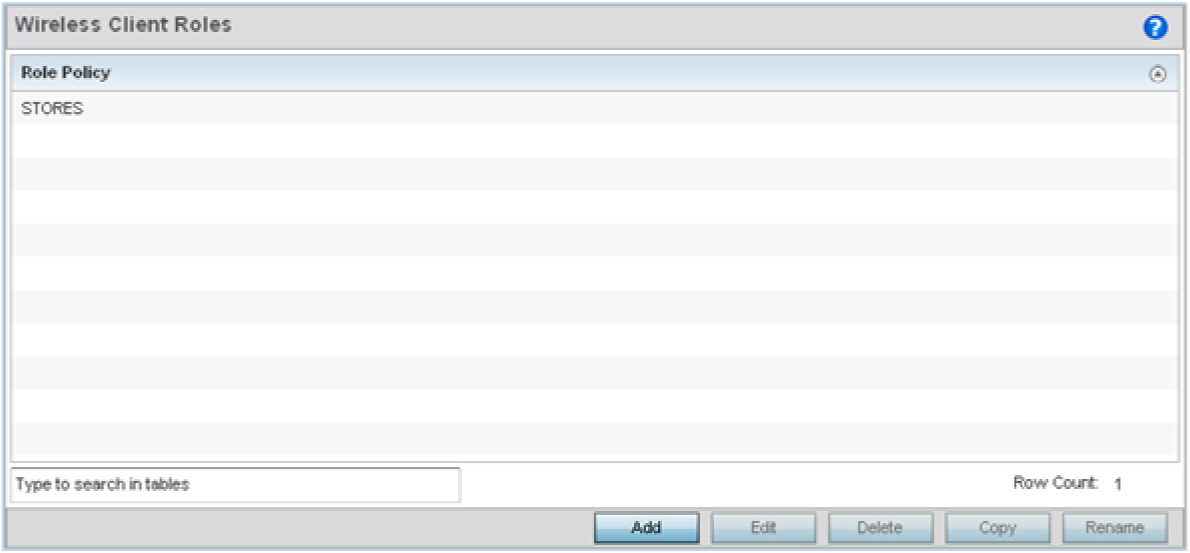
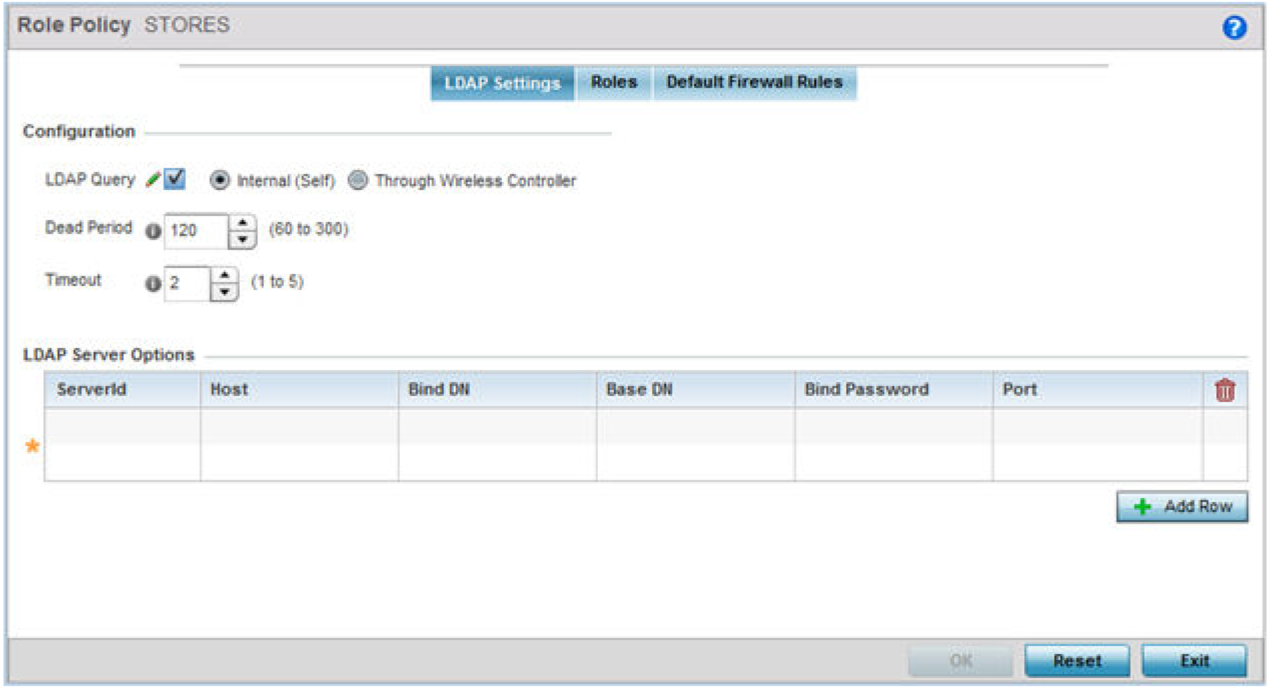


Figure 322: Wireless Client Roles Screen

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.



Role Policy STORES

Configuration

LDAP Query ☑ ● Internal (Self) ○ Through Wireless Controller

Dead Period 120 (60 to 300)

Timeout 2 (1 to 5)

LDAP Server Options

ServerId	Host	Bind DN	Base DN	Bind Password	Port

Figure 323: 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.

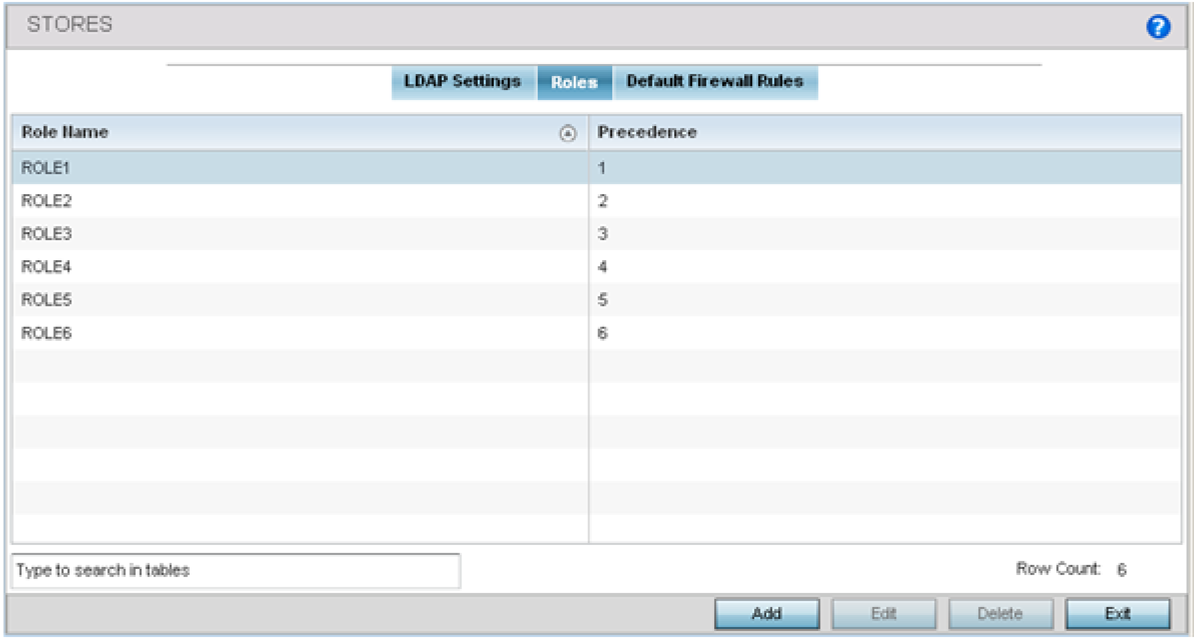
When adding or editing the LDAP server options, define the following parameters:

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.



Role Name	Precedence
ROLE1	1
ROLE2	2
ROLE3	3
ROLE4	4
ROLE5	5
ROLE6	6

Row Count: 6

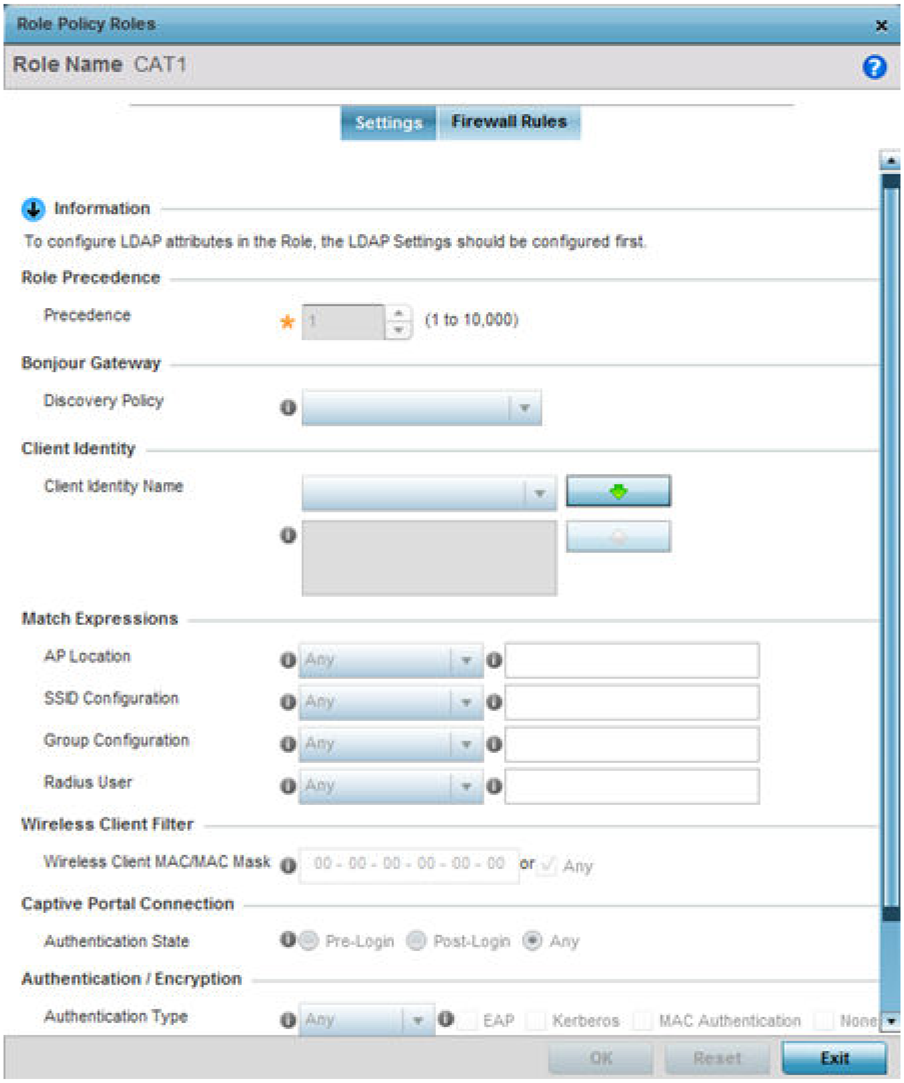
Figure 324: Wireless Client Roles - Add/Edit - Roles Tab

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.



Role Name CAT1

To configure LDAP attributes in the Role, the LDAP Settings should be configured first.

Precedence 1 (1 to 10,000)

AP Location Any

SSID Configuration Any

Group Configuration Any

Radius User Any

Wireless Client MAC/MAC Mask 00 - 00 - 00 - 00 - 00 - 00 or ☑ Any

Authentication State ○ Pre-Login ○ Post-Login ● Any

Authentication Type Any ☐ EAP ☐ Kerberos ☐ MAC Authentication ☐ None

Figure 325: 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 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.

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: • Exact - The role is applied only to access points with the exact location string specified in the role. • Contains - The role is applied only to access points whose location contains the location string specified in the role. • Does Not Contain - The role is applied only to access points whose location does not contain the location string specified in the role. • 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: • Exact - The role is applied only when the exact SSID string is specified in the role.. • Contains - The role is applied only when the SSID contains the string specified in the role. • Does Not Contain - The role is applied when the SSID does not contain the string specified in the role. • 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: • Exact - The role is applied only when the exact RADIUS Group Name string is specified in the role.. • Contains - The role is applied when the RADIUS Group Name contains the string specified in the role. • Does Not Contain - The role is applied when the RADIUS Group Name does not contain the string specified in the role. • 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: • Exact - The role is applied only when the exact RADIUS user string is specified in the role.. • Contains - The role is applied when the RADIUS user starts with the string specified in the role. • Does Not Contain - The role is applied when the RADIUS user does not contain the string specified in the role. • 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.

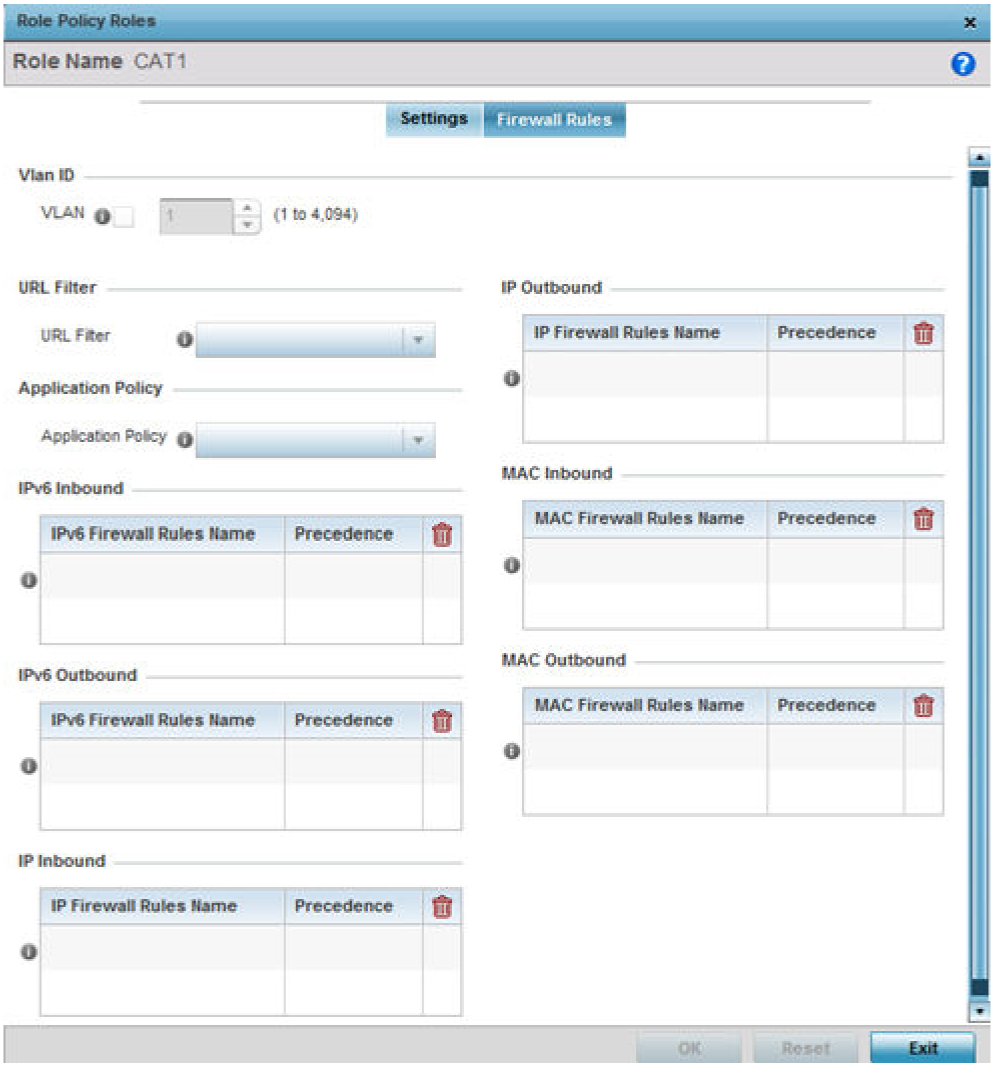


Figure 326: Wireless Client Roles - Add/Edit - Roles - Firewall Rules Tab

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. For more information on creating IPv6 ACL, refer to Setting an IPv4 or IPv6 Firewall Policy on page 789.
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. For more information on creating IP ACL, refer to Setting an IPv4 or IPv6 Firewall Policy on page 789.
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. For more information on creating MAC ACL, refer to Configuring MAC Firewall Rules on page 784.
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 assists administrators by controlling how BYOD devices access a corporate wireless domain.

Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

Note
Ensure DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

To define a device fingerprinting configuration on controllers, service platforms and Access Points:

1. Select **Configuration**.
2. Select **Security**.

3 Select **Device Fingerprinting**.

The Client Identity screen displays, populated by default with existing client identity configurations.

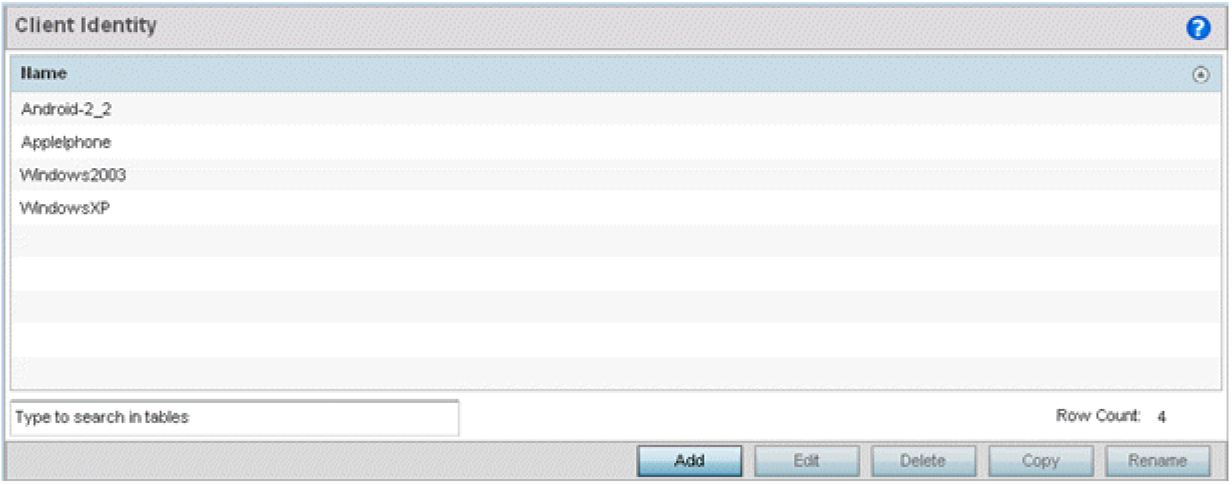


Figure 327: Device Fingerprinting - Client Identity Screen

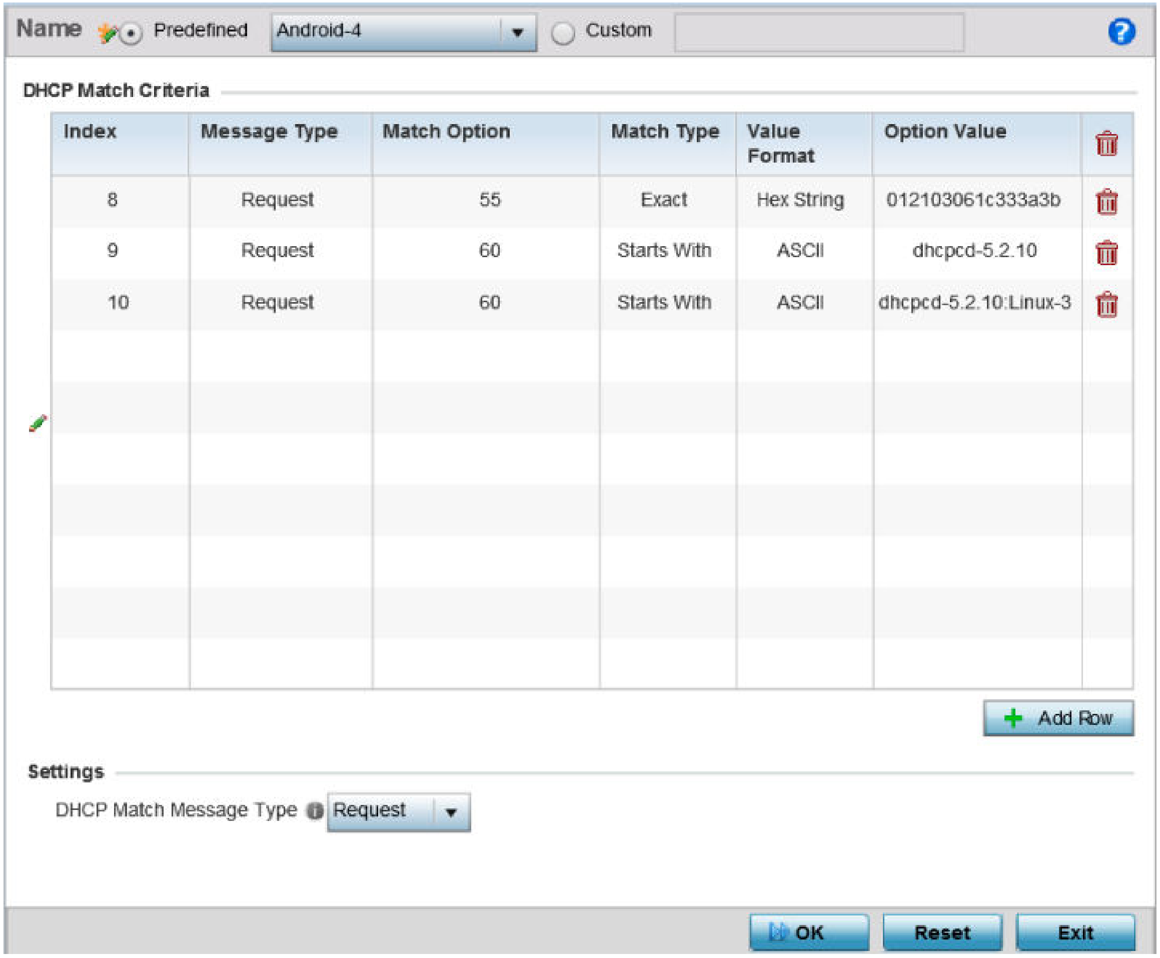
4 Select **Add** to create a new client identity policy, **Edit** to modify a selected policy, or **Delete** to remove obsolete policies from the list of those available.

Use **Rename** to change the name of an existing client identity policy, or **Copy** a policy to a different location.

Client identity policies use *signatures* to identify and group clients. Signatures are sets of attributes unique to the device model and manufacturer. Once identified, signatures classify and assign network access permissions collectively without having to administer multiple devices individually.

5 If you are adding a new client identity configuration, define a 32-character maximum name and select the **OK** button at the bottom of the screen to enable the remainder of the screen's editable parameters.

6 Select the **+ Add Row** button to add a new signature in the client identity.



Name ● Predefined Android-4 ○ Custom

DHCP Match Criteria

Index	Message Type	Match Option	Match Type	Value Format	Option Value
8	Request	55	Exact	Hex String	012103061c333a3b
9	Request	60	Starts With	ASCII	dhcpcd-5.2.10
10	Request	60	Starts With	ASCII	dhcpcd-5.2.10:Linux-3

Settings

DHCP Match Message Type: Request

Figure 328: Device Fingerprinting - Add/Edit - Client Signature Screen

7 Optionally, select **Pre-defined** and choose from a list of pre-defined client identities.

Once selected, the **DHCP Match Criteria** field is populated with fingerprints for the selected client identity.

8 To create a custom identity configuration, select **Custom** and provide a name in the adjacent field.

Select the **OK** button at the bottom of the screen.

9 Provide the following information for each device signature configuration:

Index	Use the spinner control to assign an index (numeric identifier) for this signature. A maximum of 16 signatures can be created.
Message Type	Use the drop-down menu to designate the DHCP message type matched for signatures. • Request – Looks for a signature in DHCP request messages. This is the default value. • Discover – Looks for a signature in DHCP discover messages.

Match Option	Options are passed in DHCP discover and request messages as Option Code, Option Type, and Option Value sets. When **Option Codes** is selected, the Option Code passed in the DHCP discover/request is extracted and a fingerprint is derived. The derived fingerprint is used to identify the device. • Option – Indicates a specific DHCP Option is used to identify a device. When selected, a text box is enabled to input the DHCP Option used for fingerprinting. • Option Codes – Indicates the Option Code passed in the DHCP request and discover message is used for matching.
Match Type	Use the drop-down menu to select how signatures are matched. Available options include: • Exact – The complete signature string matches the string specified in the **Option Value** field. • Starts-with – The signature is checked if it starts with the string specified in the **Option Value** field. • 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 being checked. The value can be either ASCII or Hexadecimal.
Option Value	Use this text box to set the 64-character maximum DHCP option value to match.

10 Use the **DHCP Match Message Type** drop-down menu (from the **Settings** field at the bottom of the screen) to specify the DHCP message type configured option values are matched against.

The following options are available:

Discover	Looks for a signature in DHCP discover messages.
Request	Looks for a signature in DHCP request messages. This is the default value.
Any	The fingerprint is checked with either the DHCP request or the DHCP discover message.
All	The fingerprint is checked with both the DHCP request and the DHCP discover message.

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

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

12 Expand the **Device Fingerprinting** menu item on the left-hand side of the screen and select **Client Identity Group**.

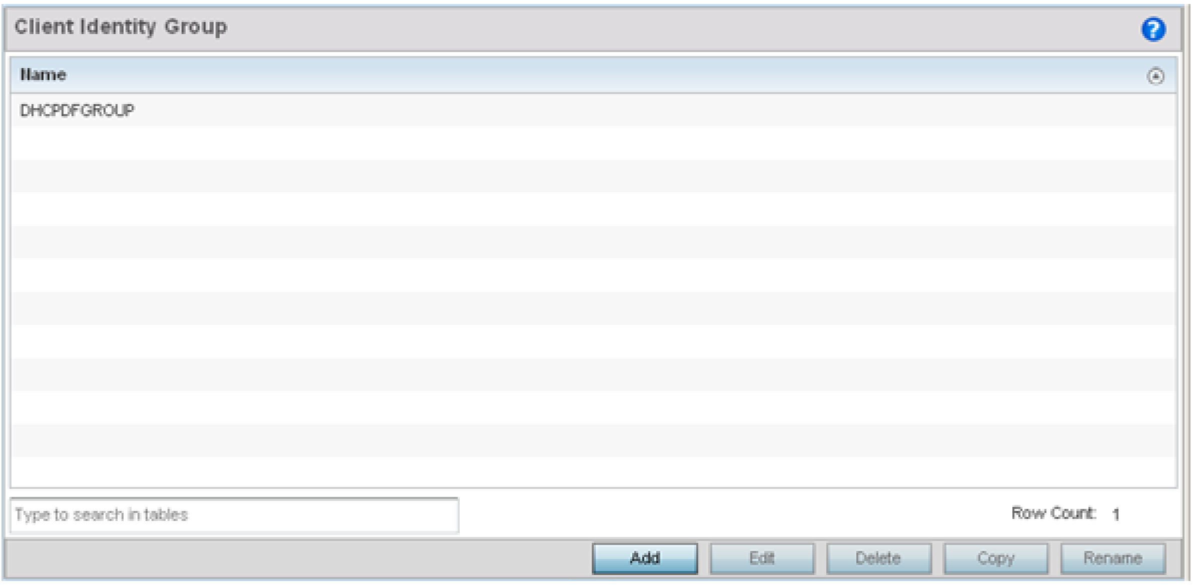


Figure 329: Device Fingerprinting - Client Identity Group Screen

An *identity group* is a collection of client identity variables. Each client identity in the group is set a value indicating its priority 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 signature specific to a device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each class.

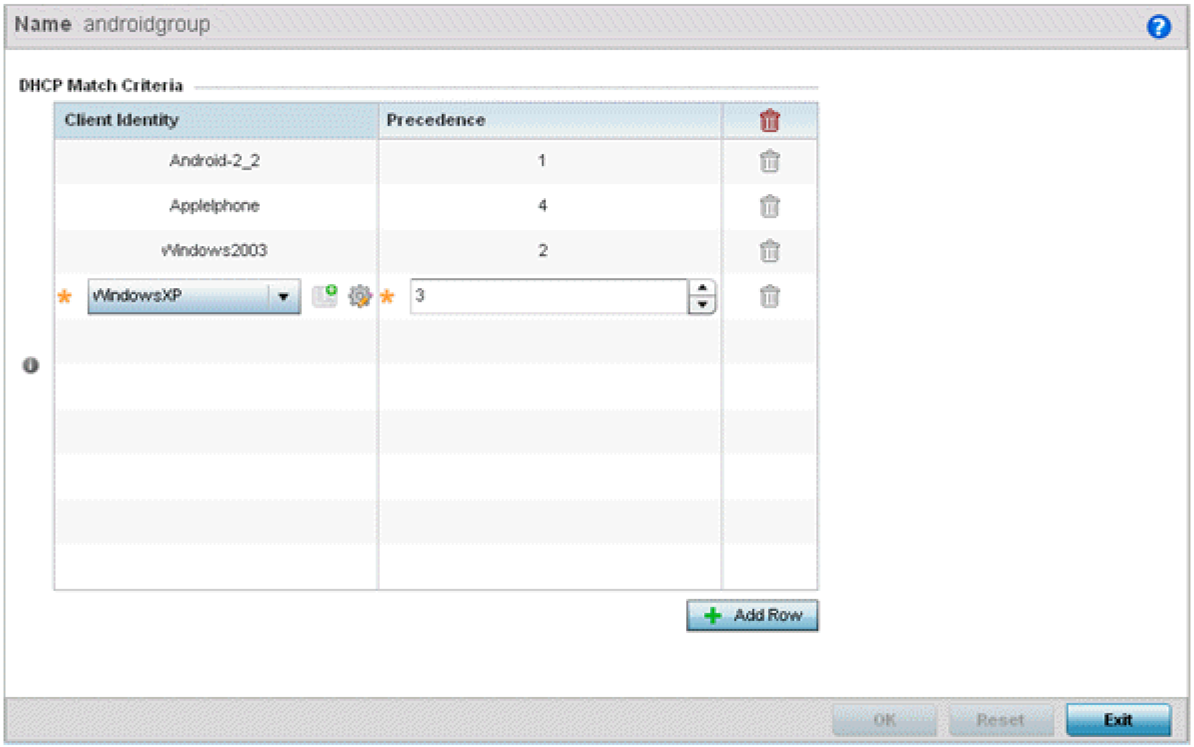
13 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy, or **Delete** to remove obsolete policies from the list of those available.

Use **Rename** to change the name of an existing policy, or **Copy** a policy to a different location.

Client identity group policies configure the signatures used to identify clients and use the signatures to classify and assign network access permissions.

14 If you are adding a new client identity group, provide a 32-character maximum name and select the **OK** button at the bottom of the screen.

15 Select the **+ Add Row** button to populate the screen's **Client Identity** and **Precedence** parameters.



Name androidgroup

DHCP Match Criteria

Client Identity	Precedence
Android-2_2	1
Applelphone	4
Windows2003	2
WindowsXP	3

Figure 330: Device Fingerprinting - Add/Edit - Client Identity Group Screen

16 Select the **Client Identity** policy to include in this group from the drop-down menu.

17 Use the **Precedence** spinner control to set the sequence (or priority) each listed client identity is checked or matched.

Lower integers are assigned the highest priority.

18 Select **OK** to save the changes.

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

Intrusion Prevention

The *Wireless Intrusion Protection System* (WIPS) provides continuous protection against wireless threats and acts as an additional layer of security complementing VPNs and encryption and authentication policies. WIPS is supported through the use of dedicated sensor devices (access point radios) designed to detect and locate unauthorized devices. After detection, unauthorized devices are blocked by manual termination or air lockdown.

Unauthorized APs are untrusted 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 an 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.

WiNG managed controllers, service platforms and access points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed as a dedicated solution within a separate enclosure. A WIPS deployment provides the following enterprise class security management features and functionality:

- *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 a controller, service platform or access point managed network.
- *Rogue Detection and Segregation* - WIPS 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 in order for administrators to act promptly against rogues and not invest in a manual search of neighboring access points to isolate the few attached to the network.
- *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. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. WEP Cloaking module enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in mobile devices.

Configuring a WIPS Policy

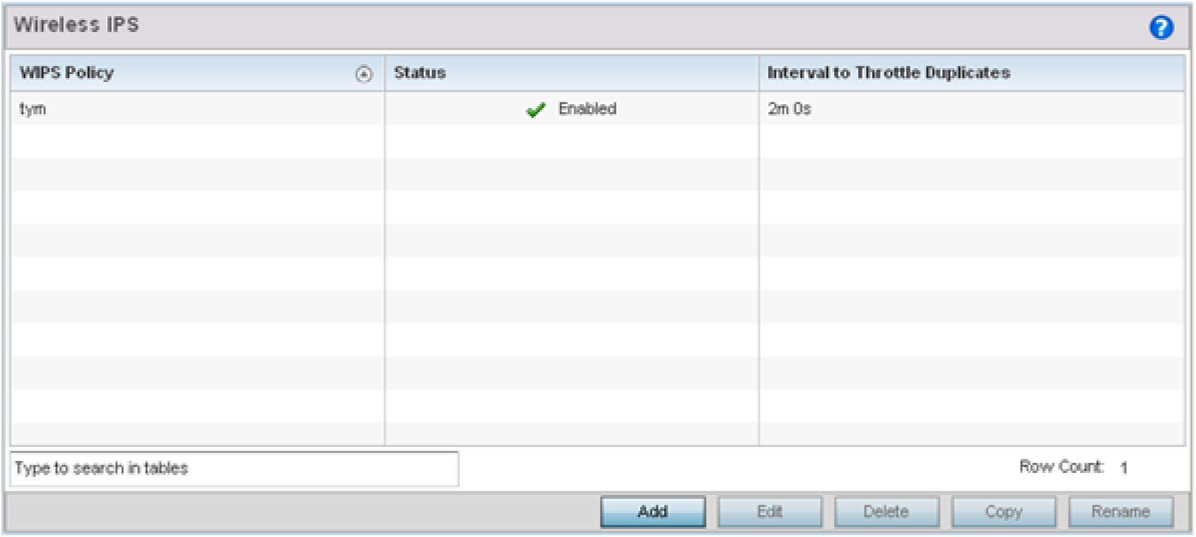
Unauthorized device detection needs to be enabled for each WIPS policy (it's disabled by default). Whether currently enabled or disabled, A WIPS policy can have specific categorization policies defined and specific events enabled for detection. Once defined, a WIPS policy is available for use with controller, service platform or Access Point device profile.

To configure a WIPS policy:

1 Select **Configuration** > **Security** > **Intrusion Prevention**.

2 Expand the Intrusion Prevention option within the **Configuration** > **Security** menu to display the **WIPS Policy, Advanced WIPS Policy** and **Device Categorization** items available.

The Wireless IPS screen displays by default. It lists existing WIPS policies if any are configured. Any of these existing WIPS policies can be selected and applied.



WIPS Policy	Status	Interval to Throttle Duplicates
tym	✓ Enabled	2m 0s

Figure 331: Wireless IPS Screen

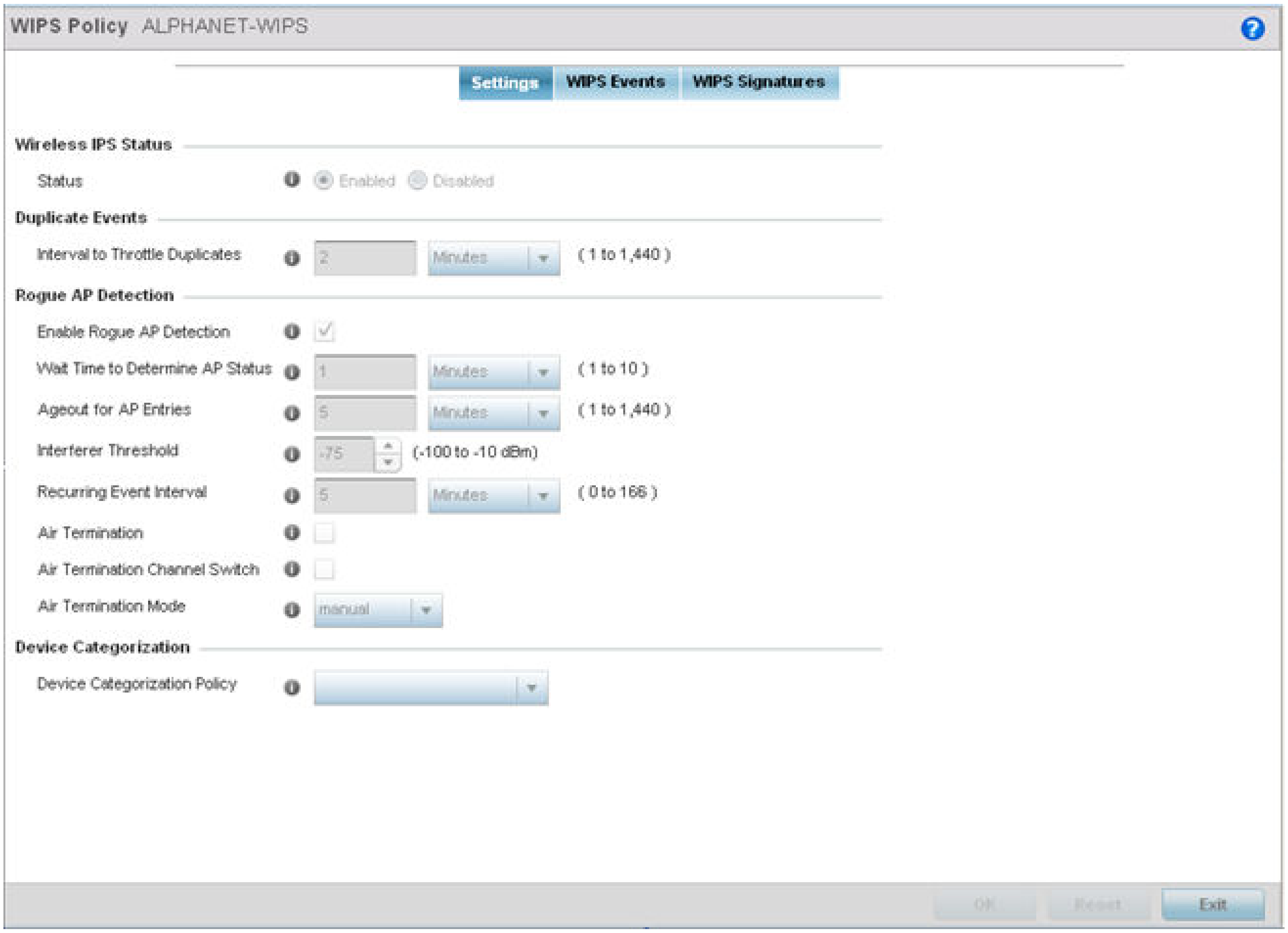
3 Refer to the following for existing WIPS policies:

WIPS Policy	Displays the name assigned to the WIPS policy when it was initially created. The name cannot be modified as part of the edit process.
Status	Displays a green check mark if the listed WIPS policy is enabled and ready for use with a profile. A red “X” designates the listed WIPS policy as disabled.
Interval to Throttle Duplicates	Displays the duration when event duplicates (redundant events) are not stored in event history.

4 Select **Add** to create a new WIPS policy, **Edit** to modify the attributes of a selected policy, or **Delete** to remove obsolete policies from the list of those available.

Use **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

If you are adding or editing an existing WIPS policy, the WIPS Policy screen displays with the Settings tab displayed by default.



WIPS Policy ALPHANET-WIPS

Wireless IPS Status

Status ● Enabled ○ Disabled

Duplicate Events

Interval to Throttle Duplicates 2 Minutes (1 to 1,440)

Rogue AP Detection

Enable Rogue AP Detection ☑

Wait Time to Determine AP Status 1 Minutes (1 to 10)

Ageout for AP Entries 5 Minutes (1 to 1,440)

Interferer Threshold -75 (-100 to -10 dBm)

Recurring Event Interval 5 Minutes (0 to 168)

Air Termination ☐

Air Termination Channel Switch ☐

Air Termination Mode manual

Device Categorization

Device Categorization Policy

Figure 332: WIPS Policy Screen - Add/Edit - Settings Tab

5 If you are creating a new WIPS Policy, assign it name to help differentiate it from others that may have a similar configuration.

The policy name cannot exceed 64 characters. The name cannot be modified as part of the edit process.

6 Within the **Wireless IPS Status** field, select either **Enabled** or **Disabled** to activate or deactivate the WIPS policy.

The default setting is **Enabled**.

7 Enter the **Interval to Throttle Packets** 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 2 minutes.

8. 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 unauthorized (unsanctioned) devices for 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 (1 - 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 age out rogue devices. Set the policy in either seconds (30 - 86,400), minutes (1- 1,440), hours (1 - 24) or days (1). The default setting is 5 minutes.
Interferer Threshold	Specify an 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 points 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.

9. Use the **Device Categorization Policy** drop-down menu to select a policy describing whether a device is filtered as sanctioned, a client or access point, and the MAC and SSID addresses used as filtering mechanisms.

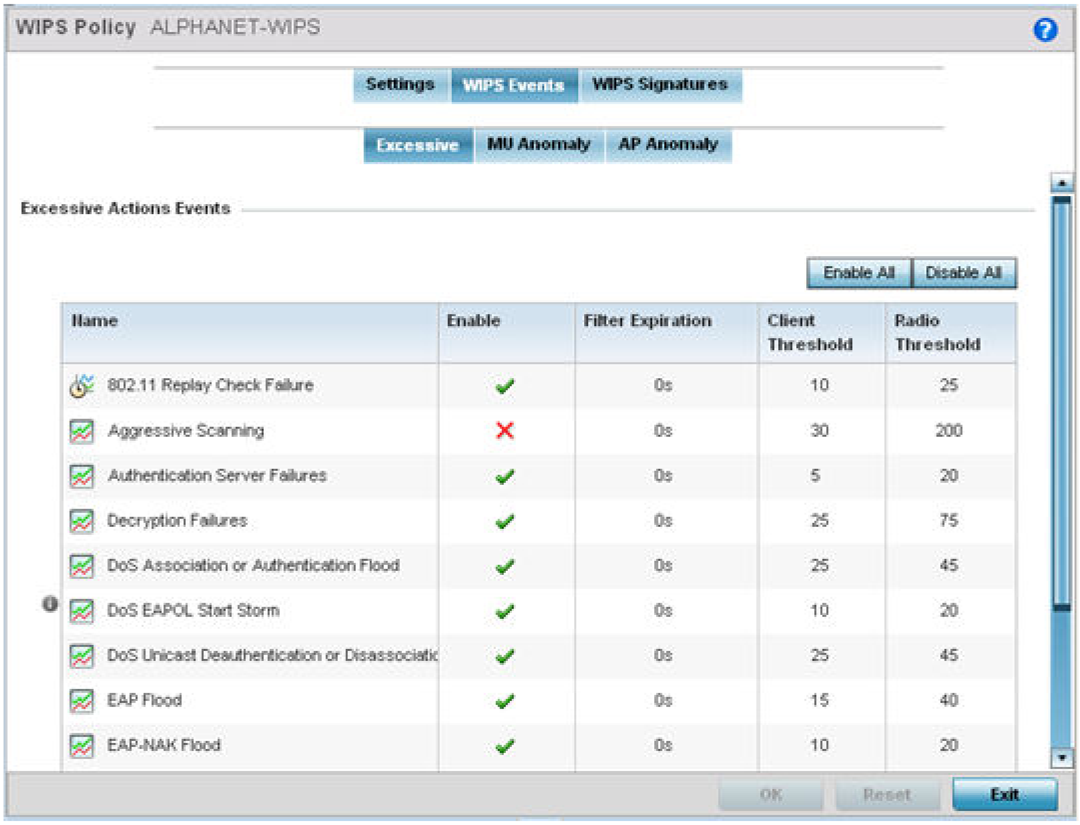
   If a policy requires creation, select **Create**. If an existing policy requires modification, select **Edit** and update the device categorization policy as needed.

10. Select **OK** to update the settings.

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

11 Select the WIPS Events tab to enable events, filters and threshold values for this WIPS policy.

The Excessive tab displays by default.



Name	Enable	Filter Expiration	Client Threshold	Radio Threshold
802.11 Replay Check Failure	✓	0s	10	25
Aggressive Scanning	✗	0s	30	200
Authentication Server Failures	✓	0s	5	20
Decryption Failures	✓	0s	25	75
DoS Association or Authentication Flood	✓	0s	25	45
DoS EAPOL Start Storm	✓	0s	10	20
DoS Unicast Deauthentication or Disassociatic	✓	0s	25	45
EAP Flood	✓	0s	15	40
EAP-NAK Flood	✓	0s	10	20

Figure 333: WIPS Events Screen - Add/Edit - Excessive Tab

The Excessive tab lists a series of events that can impact the performance of the network. 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.

An Excessive Action Event is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the Excessive Action Events table to select and configure the action taken when events are triggered.

AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

12 Set the configurations of the following **Excessive Action Events**:

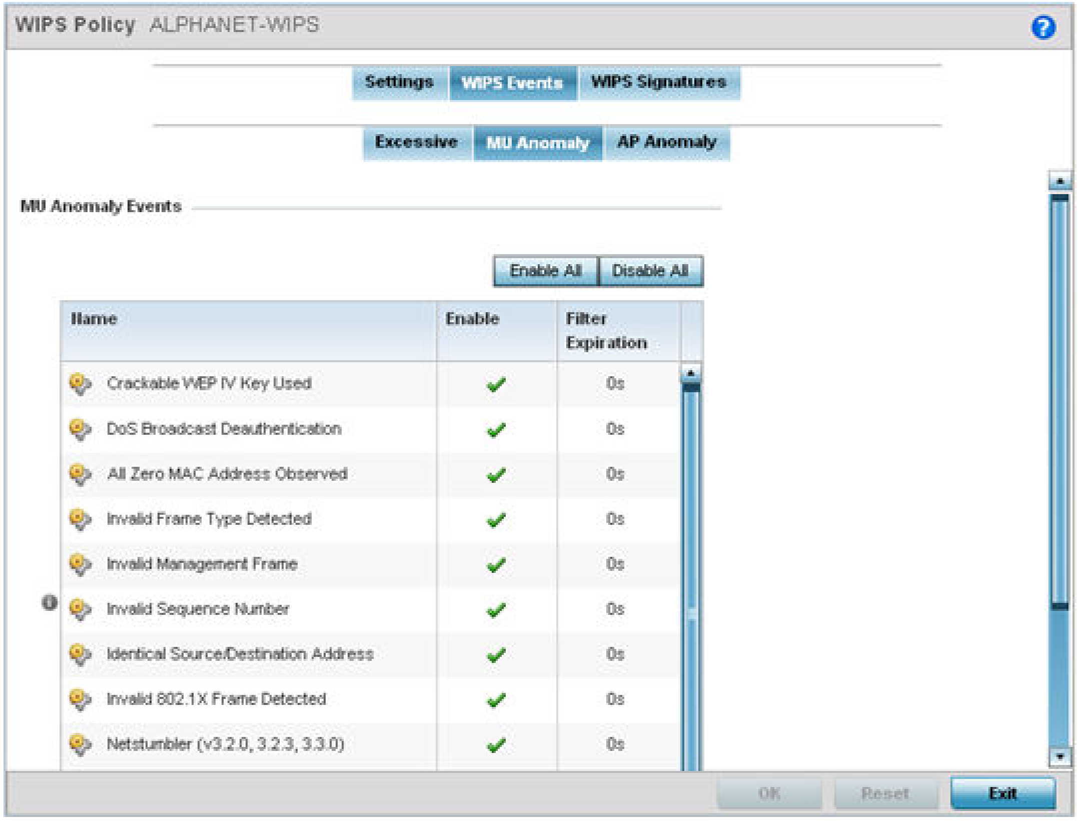
Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each Excessive Action 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. Events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

Filter Expiration	Set the duration the anomaly causing client is filtered. This creates a special ACL entry and frames coming from the client are silently 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 one of the APs, the information is passed to the domain controller or service platform. The domain controller or service platform then propagates this information to all APs 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 events history.

13 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.

14 Select the MU Anomaly tab:



Name	Enable	Filter Expiration
Crackable WEP IV Key Used	✓	0s
DoS Broadcast Deauthentication	✓	0s
All Zero MAC Address Observed	✓	0s
Invalid Frame Type Detected	✓	0s
Invalid Management Frame	✓	0s
Invalid Sequence Number	✓	0s
Identical Source/Destination Address	✓	0s
Invalid 802.1X Frame Detected	✓	0s
Netstumbler (v3.2.0, 3.2.3, 3.3.0)	✓	0s

Figure 334: WIPS Events Screen - Add/Edit - MU Anomaly Tab

MU anomaly events are suspicious events by wireless clients that can compromise the security and stability of the network. Use this MU anomaly screen to configure the intervals clients can be filtered upon the generation of each defined event.

MU events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

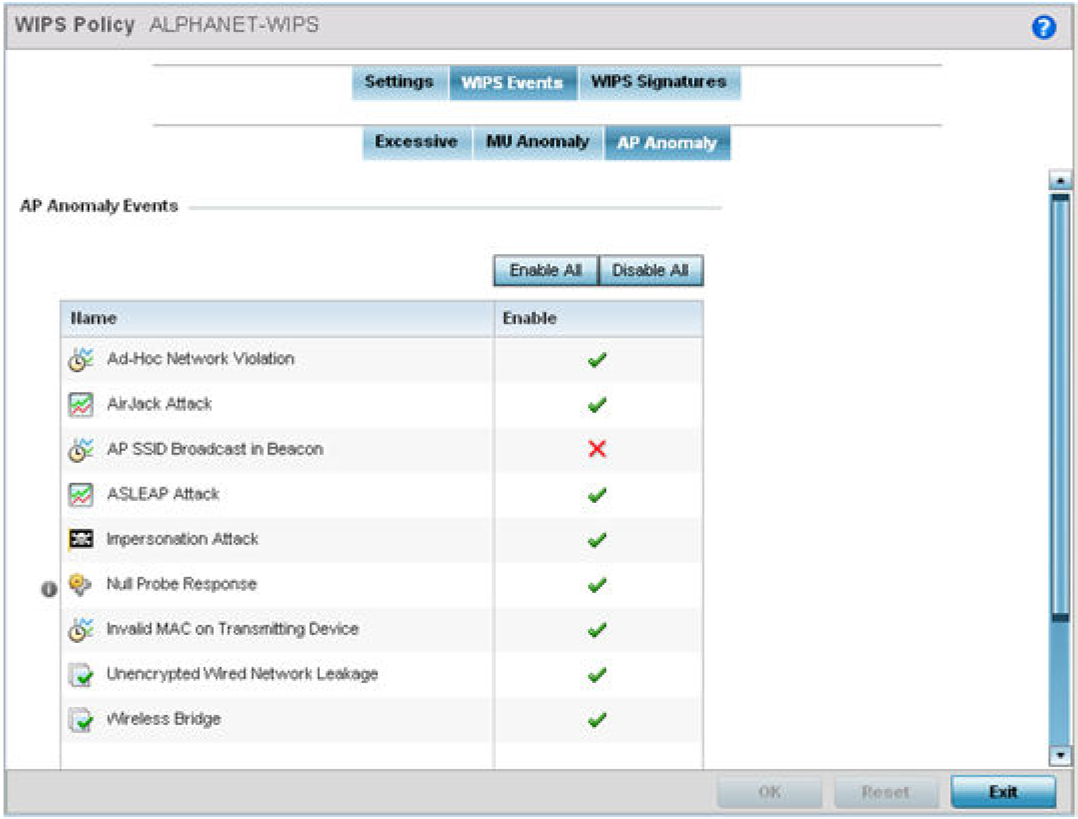
15 Set the following **MU Anomaly Events** configurations:

Name	Displays the name of the MU anomaly 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 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. MU events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.
Filter Expiration	Set the duration the anomaly causing 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.

16 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.

17 Select the AP Anomaly tab:



Name	Enable
Ad-Hoc Network Violation	✓
AirJack Attack	✓
AP SSID Broadcast in Beacon	✗
ASLEAP Attack	✓
Impersonation Attack	✓
Null Probe Response	✓
Invalid MAC on Transmitting Device	✓
Unencrypted Wired Network Leakage	✓
Wireless Bridge	✓

Figure 335: WIPS Events screen - Add/Edit - AP Anomaly Tab

AP anomaly events are suspicious frames sent by a neighboring APs. Use this screen to determine whether an event is enabled for tracking.

AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

18 Set the following **AP Anomaly Events** configurations:

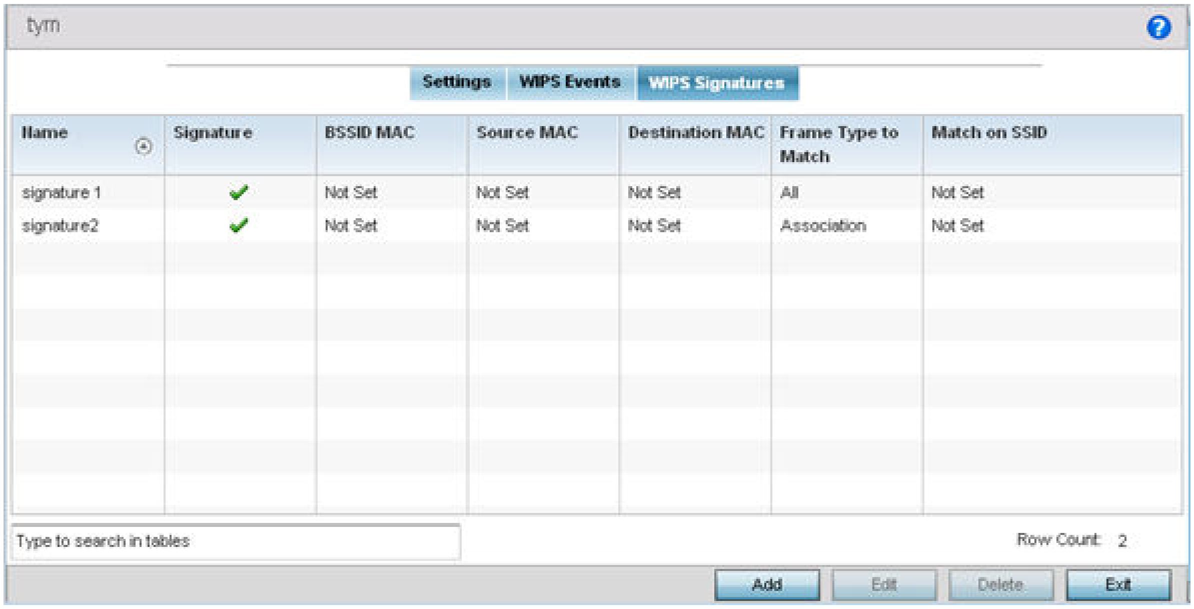
Name	Displays the name of the AP anomaly event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each AP anomaly event. Use 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. AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

19 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.

20 Select the WIPS Signatures tab.

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.



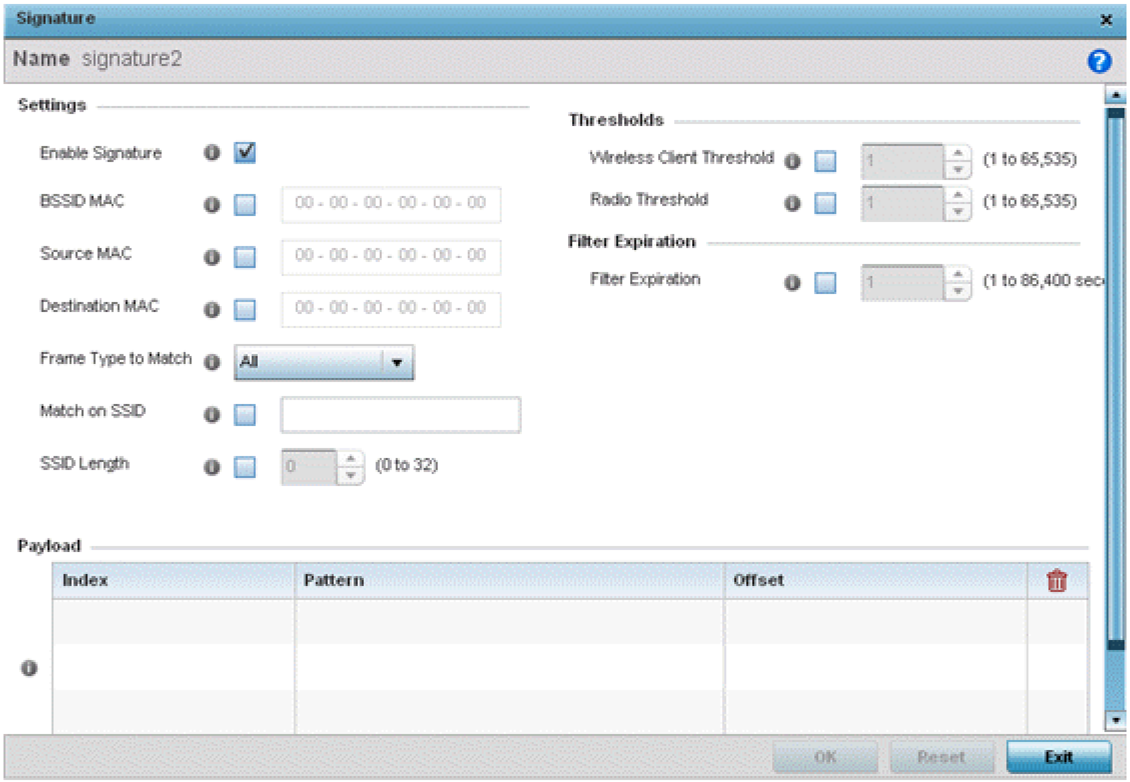
Name	Signature	BSSID MAC	Source MAC	Destination MAC	Frame Type to Match	Match on SSID
signature 1	✓	Not Set	Not Set	Not Set	All	Not Set
signature2	✓	Not Set	Not Set	Not Set	Association	Not Set

Figure 336: WIPS Signatures Screen

21 The WIPS Signatures screen displays the following read-only data:

Name	Lists the name (in the top left-hand corner) 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 check mark 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 and potential device exclusion.
Source MAC	Displays each source MAC address of the packet examined for matching purposes and potential device exclusion.
Destination MAC	Displays each destination MAC address of the packet examined for matching purposes and potential device exclusion.
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.

22 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.



Name signature2

Enable Signature ☑

BSSID MAC ☐ 00 - 00 - 00 - 00 - 00 - 00

Source MAC ☐ 00 - 00 - 00 - 00 - 00 - 00

Destination MAC ☐ 00 - 00 - 00 - 00 - 00 - 00

Frame Type to Match All

Match on SSID ☐

SSID Length ☐ 0 (0 to 32)

Wireless Client Threshold ☐ 1 (1 to 65,535)

Radio Threshold ☐ 1 (1 to 65,535)

Filter Expiration ☐ 1 (1 to 86,400 sec

Figure 337: WIPS Signatures Screen - Add/Edit - Signature Screen

23 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.

24 Set the following network address information for a new or modified WIPS Signature:

Enable Signature	Select the check box 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 packets examined for matching, filtering and potential device exclusion using the signature.
Destination MAC	Set a destination MAC address for the packet examined for matching, filtering and potential device exclusion with the signature.
Frame Type to Match	Use the drop-down menu to select a frame type for matching and filtering with the WIPS signature.
Match on SSID	Set the SSID used for matching and filtering with the signature. Ensure that it is specified properly, or the SSID will not be properly filtered.
SSID Length	Set the character length of the SSID used for matching and filtering with this signature. The maximum length is 32 characters.

25 Refer to the **Thresholds** field to set signature threshold limitations 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.

26 Set a **Filter Expiration** (from 1 - 86,400 seconds) that specifies the duration a client is excluded from RF Domain manager radio association when responsible for triggering a WIPS event.

27 Refer to the **Payload** table to set a numerical index pattern and offset for the WIPS signature.

Select **+ Add Row** and provide **Index**, **Pattern**, and **Offset** variables for the payload.

28 Select **OK** to save the updates to the WIPS Signature configuration.

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

Configuring a Device Categorization Policy

Having devices properly classified can help suppress unnecessary unsanctioned AP alarms and allow an administrator to focus on the alarms and devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization while appearing to be legitimate. WIPS enables devices to be categorized as access points, then defined as *sanctioned* or *unsanctioned* within the network.

Sanctioned access points are generally known to you and conform with your organization's security policies. Unsanctioned devices have been detected as interoperating within the managed network, but are not approved. These devices should be filtered to avoid jeopardizing data.

To categorize access points as sanctioned or unsanctioned:

1 Select **Configuration** > **Security** > **Intrusion Prevention**.

2 Expand the Intrusion Prevention option within the **Configuration** > **Security** menu and select **Device Categorization**.

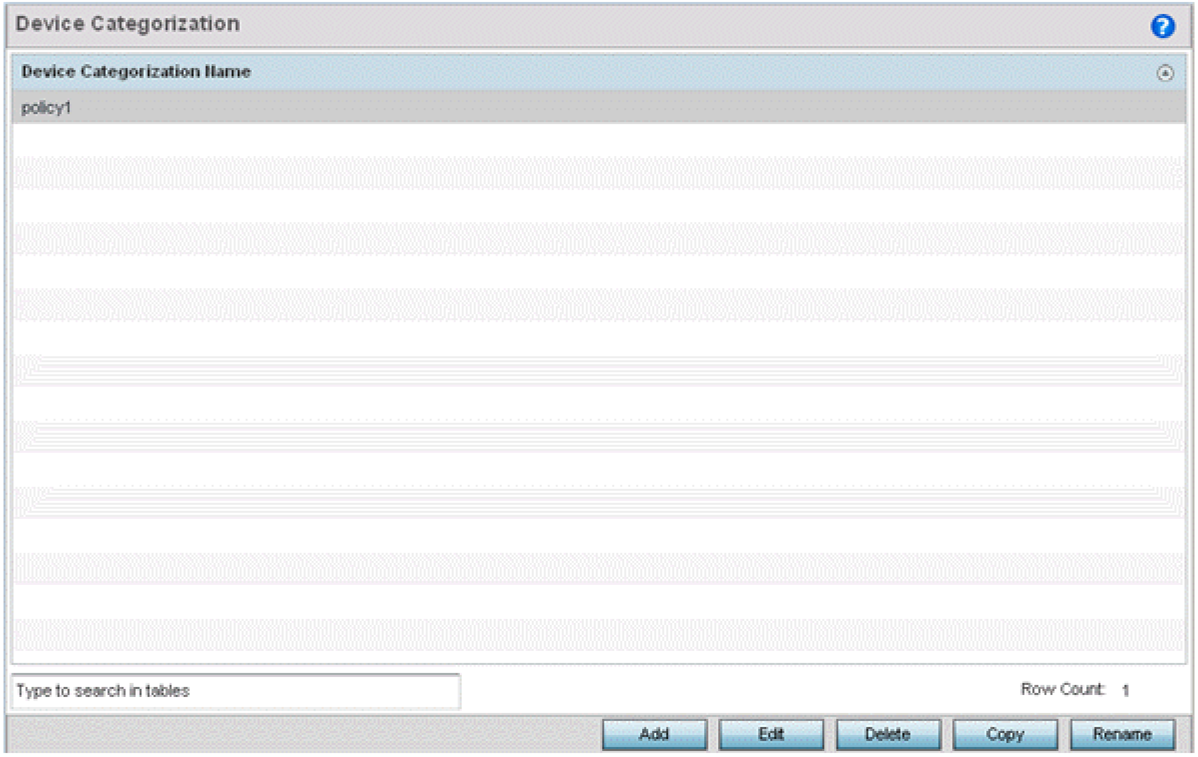
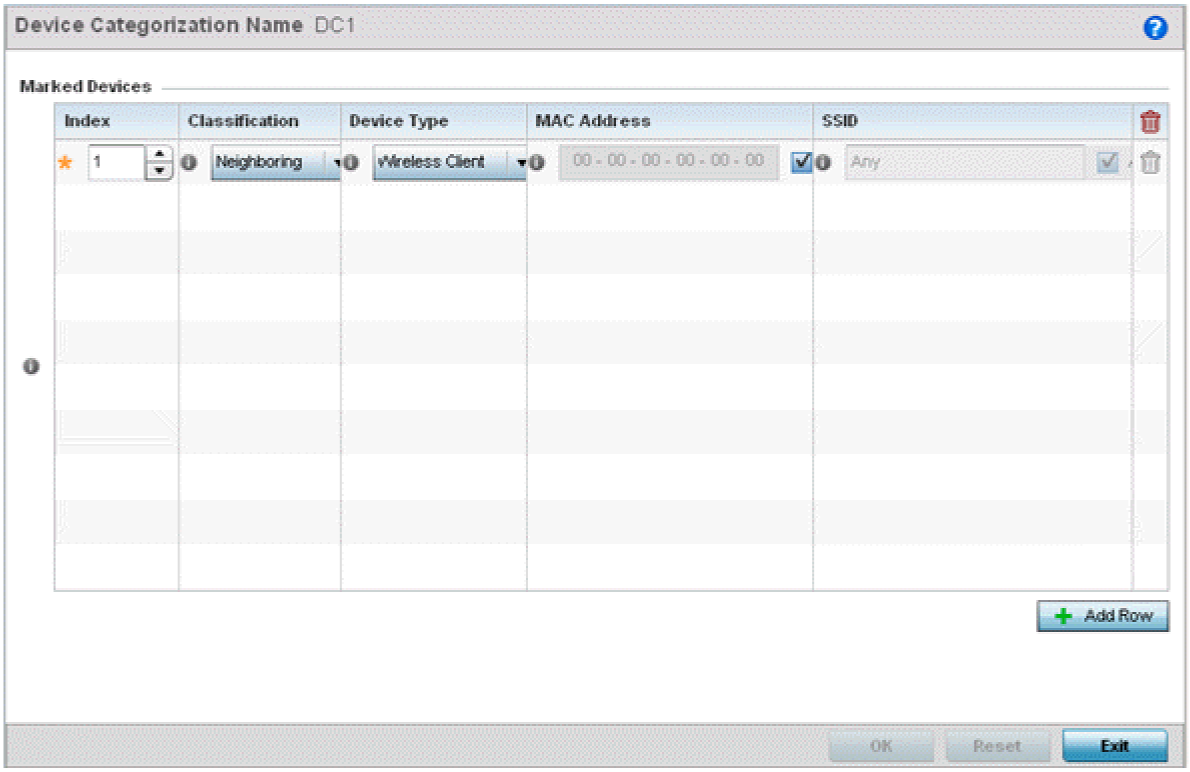


Figure 338: WIPS Device Categorization Screen

The Device Categorization screen lists those device authorization policies defined thus far.

3 Select **Add** to create a new policy, **Edit** to modify the attributes of a selected existing policy, or **Delete** to remove obsolete policies from those available.

Select **Rename** to change the name of a policy or **Copy** a policy to a different location.



Device Categorization Name DC1

Marked Devices

Index	Classification	Device Type	MAC Address	SSID
1	Neighboring	Wireless Client	00 - 00 - 00 - 00 - 00 - 00	Any

Figure 339: WIPS Device Categorization - Configuration Screen

4 If you are creating a new Device Categorization policy, provide it a name (up to 64 characters) to distinguish this policy from others with similar configurations.

Select **OK** to save the name and enable the remaining parameters on the screen.

5 Select **+ Add Row** to populate the **Marked Devices** field with parameters for adding an access point's MAC address, SSID, access point designation, and network authorization.

Select the red **(-) Delete Row** icon as needed to remove an individual table entry.

6 Define the following parameters to add a device to a list of devices categorized as sanctioned or unsanctioned for network operation:

Index	Use the spinner controls to set the Index number for each Device Categorization Name.
Classification	Use the drop-down menu to designate the target device as either sanctioned (True) or unsanctioned (False). The default setting is False, categorizing this device as unsanctioned. Thus, each added device requires authorization. A green check mark designates the device as sanctioned, while a red "X" defines the device as unsanctioned.
Device Type	Use the drop-down menu to designate the target device as either an access point (True) or other (False). The default setting is False, categorizing this device as other than an access point. A green check mark designates the device as an access point, while a red "X" defines the categorized device as other than an access point.

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. The MAC address will be defined as sanctioned or unsanctioned as part of the device categorization process.
SSID	Enter the SSID of the target device requiring categorization. The SSID cannot exceed 32 characters.

7 Select **OK** to save the updates to the **Marked Devices** list.

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

Intrusion Detection Deployment Considerations

Before configuring WIPS support on a controller, service platform or access point, 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 administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be 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?
- Controller or service platform visibility to all deployed VLANs is recommended. If an external L3 device has been deployed for routing services, each VLAN should be 802.1Q tagged to the controller or service platform to allow the detection any unsanctioned APs physically connected to the network.
- Trusted and known access points should be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.

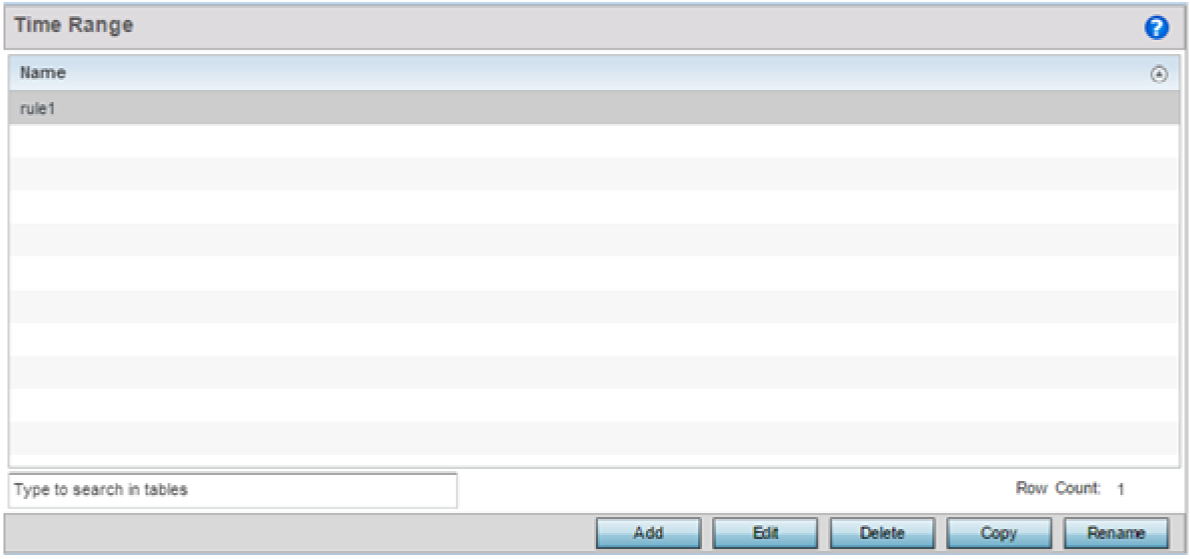
EX3500 Time Range

An *EX3500 time range* is a set of configurations consisting of periodic and absolute time ranges. Periodic time ranges can be configured to reoccur daily, weekly, weekends and on specific weekdays, such as Sunday. Absolute time ranges can be configured for a range of days during a particular period. Absolute time ranges do not reoccur.

The EX3500 time ranges are used when configuring EX3500 MAC ACL firewall rules. For more information, see Configuring MAC Firewall Rules on page 784.

To set an EX3500 switch periodic or absolute time ranges:

1 Select **Configuration** > **Security** > **EX3500 Time Ranges**.



Name
rule1

Row Count: 1

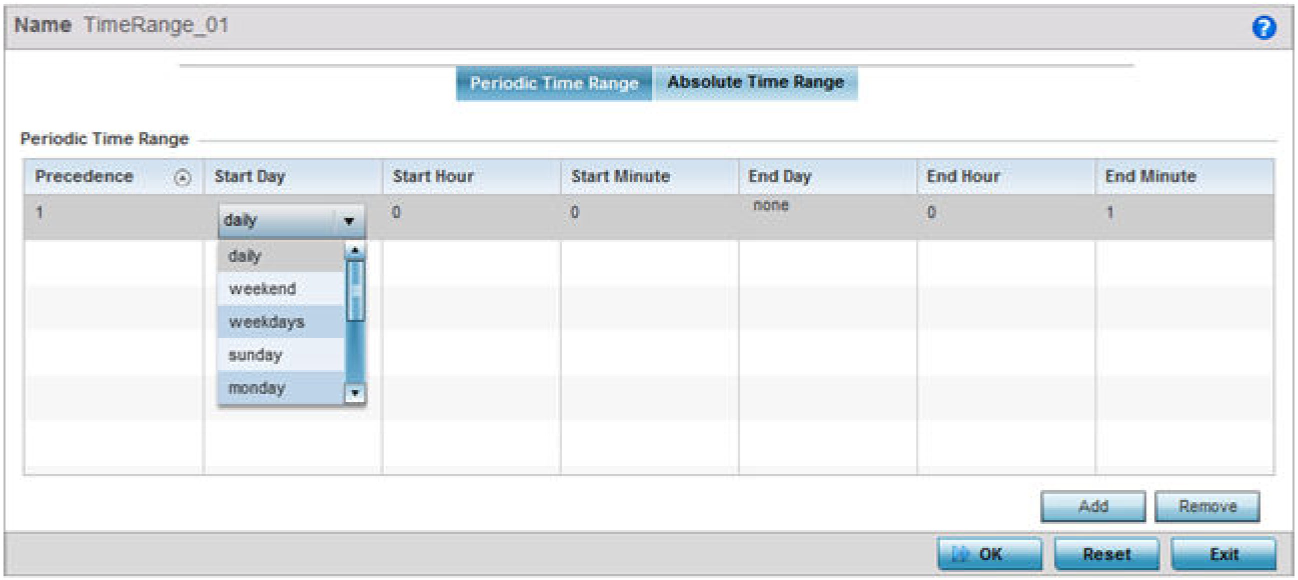
Figure 340: EX3500 Time Range Screen

The Time Range screen displays within the main portion of the Web UI.

2 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing time range, or **Delete** to remove obsolete time ranges.

Use **Copy** to create a copy of the selected time range and modify it for further use. Use **Rename** to rename the selected time range.

3 Either use the **Add** button to create an new EX3500 time range or select an existing range and click **Edit** to modify it.



Name TimeRange_01

Precedence	Start Day	Start Hour	Start Minute	End Day	End Hour	End Minute
1	daily	0	0	none	0	1

Figure 341: EX3500 Time Range - Periodic Time Range Screen

The Periodic Time Range tab displays by default.

4 If you are adding a new EX3500 time range, give it a name up to 32 characters.

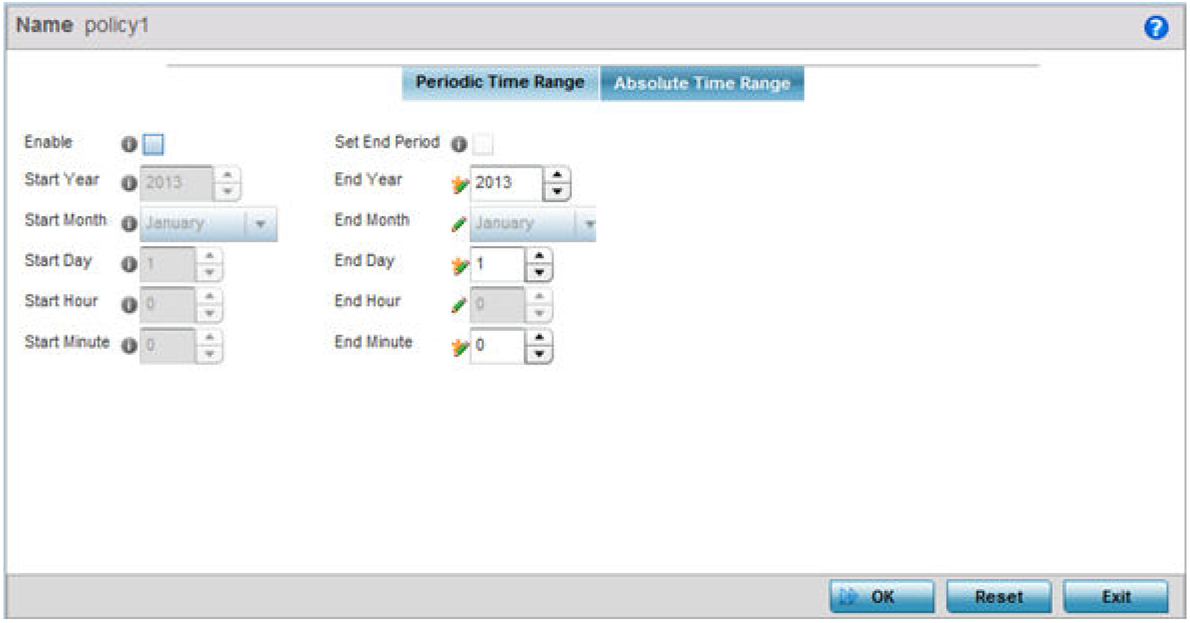
5 Select **Add** to provide the following parameters:

Precedence	Specify or modify a precedence value for this periodic time range policy. Rules with lower precedence are always applied first. If modifying a precedence to apply a higher integer, it moves down the table to reflect its lower priority. Select a precedence value in the range 1-7.
Start Day	Specify the periodic time range's start day. Day value can be one of daily, weekend, weekdays, sunday, monday, tuesday, wednesday, thursday, friday or saturday. Specify a start day from one of the above values.
Start Hour	Specify the periodic time range's start hour. Hours are specified in 24-hour format. Use the spinner to select the appropriate hour.
Start Minute	Specify the periodic time range's start minute. Use the spinner to select the appropriate minute.
End Day	Specify the periodic time range's end day. End day is the day when the time period ends. The options available for this field changes depending on the choice made in the **Start Day** field.
End Hour	Specify the periodic time range's end hour. Hours are specified in 24 hour format. In most cases, this value cannot be lower than the value specified in the **Start Hour** field. Use the spinner to select the correct end hour value.
End Minute	Specify the periodic time range's end minute. In most cases, this value cannot be lower than the value specified in the **Start Minute** field. Use the spinner to select the correct end.

6 Select **OK** to save the updates.

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

7 Select the **Absolute Time Range** to configure a time range that is absolute and occurs only once.



Name policy1

Enable ☐
Start Year 2013
Start Month January
Start Day 1
Start Hour 0
Start Minute 0

Set End Period ☐
End Year 2013
End Month January
End Day 1
End Hour 0
End Minute 0

Figure 342: EX3500 Time Range - Absolute Time Range Screen

8 Select **Enable** to enable this feature.

Absolute time range can be configured only when enabled.

9 Configure the following parameters:

Start Year	Specify the absolute time range's start year. Use the spinner control to select the year. Select a year in the range 2013-2037.
Start Month	Specify the absolute time range's start month. Use the drop-down menu to select the month.
Start Day	Specify the absolute time range's start day. Day value can be one of daily, weekend, weekdays, sunday, monday, tuesday, wednesday, thursday, friday or saturday. Specify a start day from one of the above values.
Start Hour	Specify the absolute time range's start hour. Hours are specified in 24 hour format. Use the spinner to select the appropriate hour.
Start Minute	Specify the absolute time range's start minute. Use the spinner to select the appropriate minute.
End Period	Select the option to set specific end periods for each of the Year, Month, Day, Hour and Minute values available for start time definitions.
End Year	Specify the absolute time range's end year. Use the spinner control to select the year. Select a year in the range 2013-2037. End year cannot be earlier than the value specified in the **Start Year** field.
End Month	Specify the absolute time range's end month. Use the drop-down menu to select the month.
End Day	Specify the absolute time range's end day. End day is the day when the time period ends. The options available for this field changes depending on the choice made in the **Start Day** field.
End Hour	Specify the absolute time range's end hour. Hours are specified in 24 hour format. In most cases, this value cannot be lower than the value specified in the **Start Hour** field. Use the spinner to select the correct end hour value.
End Minute	Specify the absolute time range's end minute. In most cases, this value cannot be lower than the value specified in the **Start Minute** field. Use the spinner to select the correct end.

10 Select **OK** when completed to update the EX3500 time range.

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

11 Services Configuration

Captive Portal Policies
Setting the Guest Management Configuration
Setting the DHCP Configuration
Setting the Bonjour Gateway Configuration
Setting the DHCPv6 Server Policy
Setting the RADIUS Configuration
Setting the URL List
Setting the Imagotag Policy

Controllers, service platforms and access points natively support guest and temporary user access policies, lease DHCP IP addresses to requesting clients and authenticate requesting clients.

For more information, refer to the following:

- Captive Portal Policies on page 834
- Setting the Guest Management Configuration on page 848
- Setting the DHCP Configuration on page 858
- Setting the Bonjour Gateway Configuration on page 874
- Setting the DHCPv6 Server Policy on page 878
- Setting the RADIUS Configuration on page 884
- Setting the Imagotag Policy on page 900
- Setting the URL List on page 899

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.

Refer to the following sections for configuring Captive Portal Policy parameters:

- Captive Portal Policy Basic Configuration on page 835
- Configuring DNS Whitelists on page 847
- Captive Portal Deployment Considerations on page 847

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.

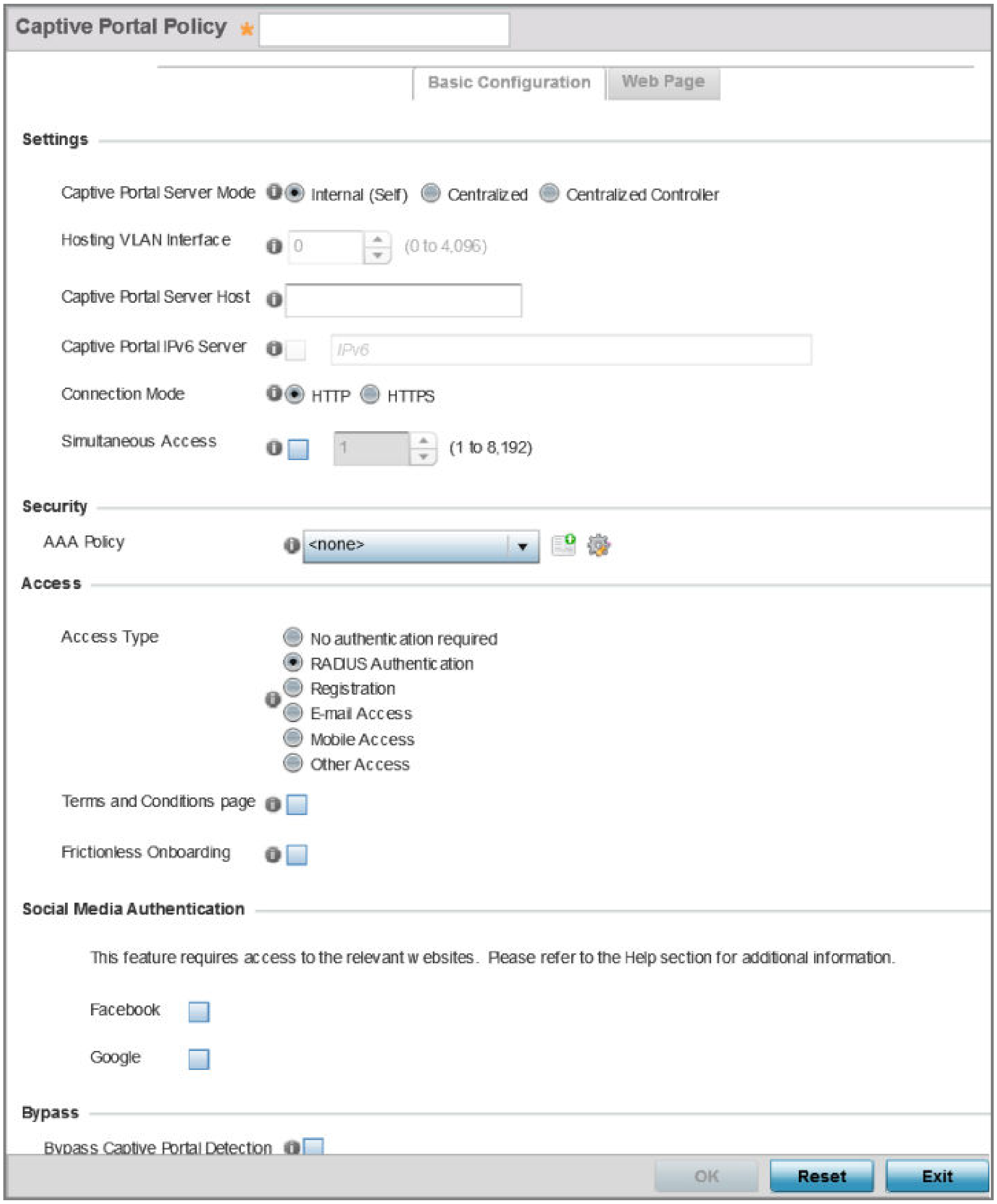

Captive Portal Policy
Basic Configuration
Web Page
Settings
Captive Portal Server Mode
● Internal (Self) ○ Centralized ○ Centralized Controller
Hosting VLAN Interface
0
(0 to 4,096)
Captive Portal Server Host
Captive Portal IPv6 Server
IPv6
Connection Mode
● HTTP ○ HTTPS
Simultaneous Access
1
(1 to 8,192)
Security
AAA Policy
<none>
Access
Access Type
○ No authentication required
● RADIUS Authentication
○ Registration
○ E-mail Access
○ Mobile Access
○ Other Access
Terms and Conditions page ☐
Frictionless Onboarding ☐
Social Media Authentication
This feature requires access to the relevant w ebsites. Please refer to the Help section for additional information.
Facebook ☐
Google ☐
Bypass
Bypass Captive Portal Detection ☐
OK
Reset
Exit

Figure 343: 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. 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	When using `Centralized` mode, select this option to define an IPv6 formatted address of the controller, service platform or Access Point resource hosting the captive portal.
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.

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: • **No authentication required** - Requesting clients are redirected to the captive portal Welcome page without authentication. • **RADIUS Authentication** - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting. • **Registration** - A requesting client's user credentials require authentication through social media credential exchange. • **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. • **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. • **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. It also provides an integration API, as a means of on-boarding guest users through a loyalty application. 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. 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 client VLAN assignments using the RADIUS server. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.
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 509.

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*.

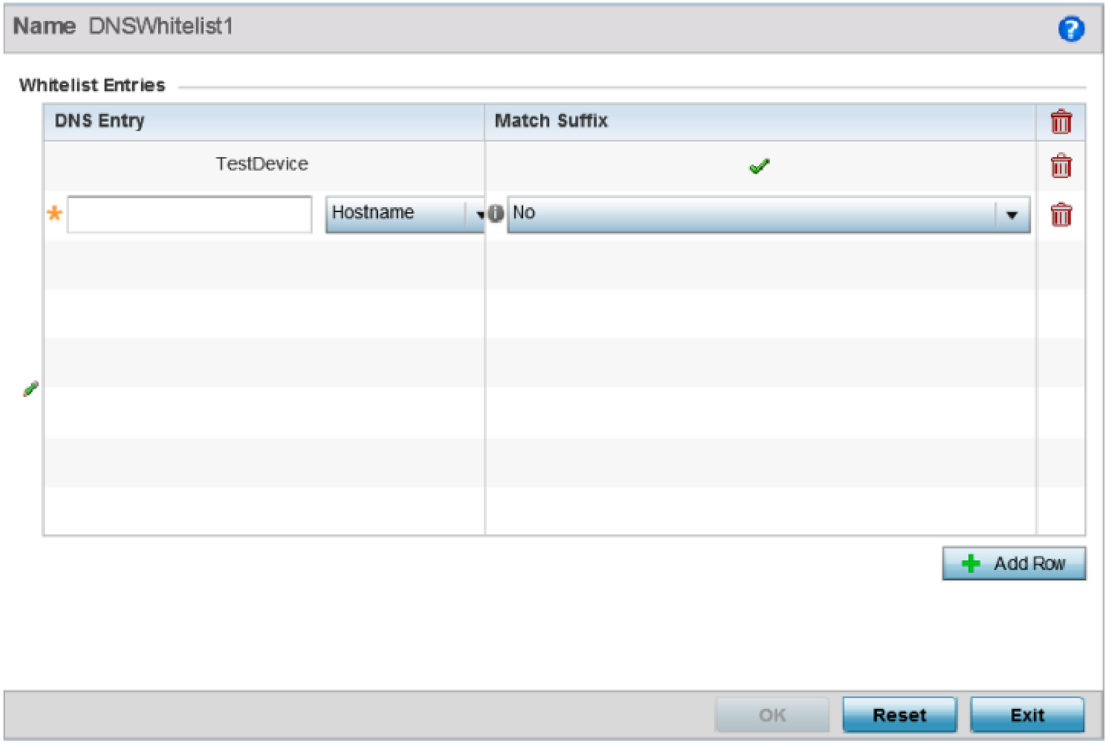
To effectively host captive portal pages on an external web server, the IP addresses of the destination web servers should be in the whitelist.

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.

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.



Name DNSWhitelist1

Whitelist Entries

DNS Entry	Match Suffix
TestDevice	✓
Hostname	No

Figure 344: 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.

Hostnames cannot contain underscores.

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. A hostname cannot contain an underscore.
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. When a user reaches this threshold, from 1 and 102,400 megabytes, it triggers the specified action.
Action	When a captive portal client reaches its data usage limit, a specified log action is executed. Choose from one of the following: • **`Log Only`** — Logs the event • **`log-and-disconnect`** — Logs the event and disconnects the user When **`Log Only`** is selected, an entry is added to the log file whenever a captive portal client exceeds the data limit. When **`log-and-disconnect`** is selected, an entry is added to the log file when the data limit is exceeded and the client is disconnected from the captive portal.

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.

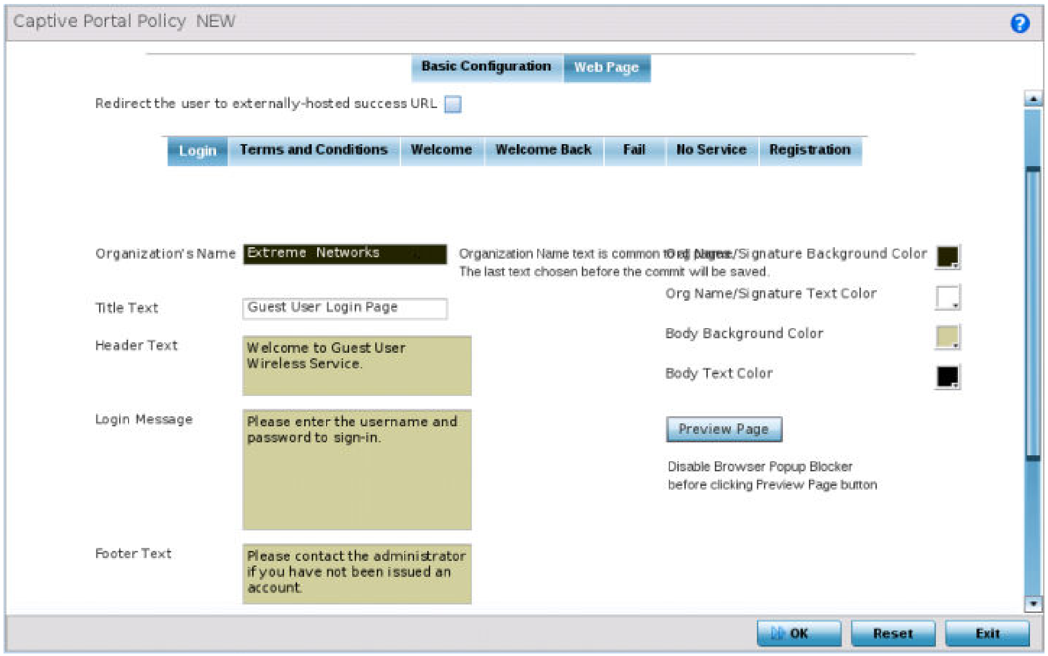
15 Select **OK** to save the changes made within the Basic Configuration screen.

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



Redirect the user to externally-hosted success URL ☐

Organization's Name: Extreme Networks

Organization Name text is common to all pages. The last text chosen before the commit will be saved.

Org Name/Signature Background Color ■

Org Name/Signature Text Color □

Body Background Color ■

Body Text Color ■

Title Text: Guest User Login Page

Header Text: Welcome to Guest User Wireless Service.

Login Message: Please enter the username and password to sign-in.

Footer Text: Please contact the administrator if you have not been issued an account.

Disable Browser Popup Blocker before clicking Preview Page button

Figure 345: Captive Portal Policy - Web Page - Internal Option Screen

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.

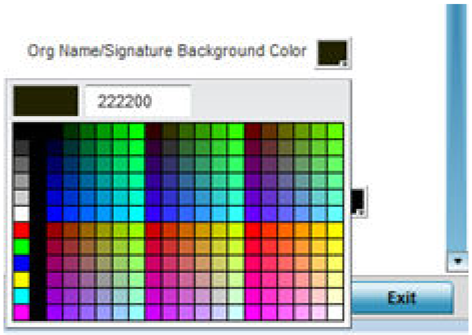
2 Select the location where the captive portal Login, Terms and Conditions, Welcome, Fail, No Service and Registration Web pages are hosted.

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.

3 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.



Org Name/Signature Background Color

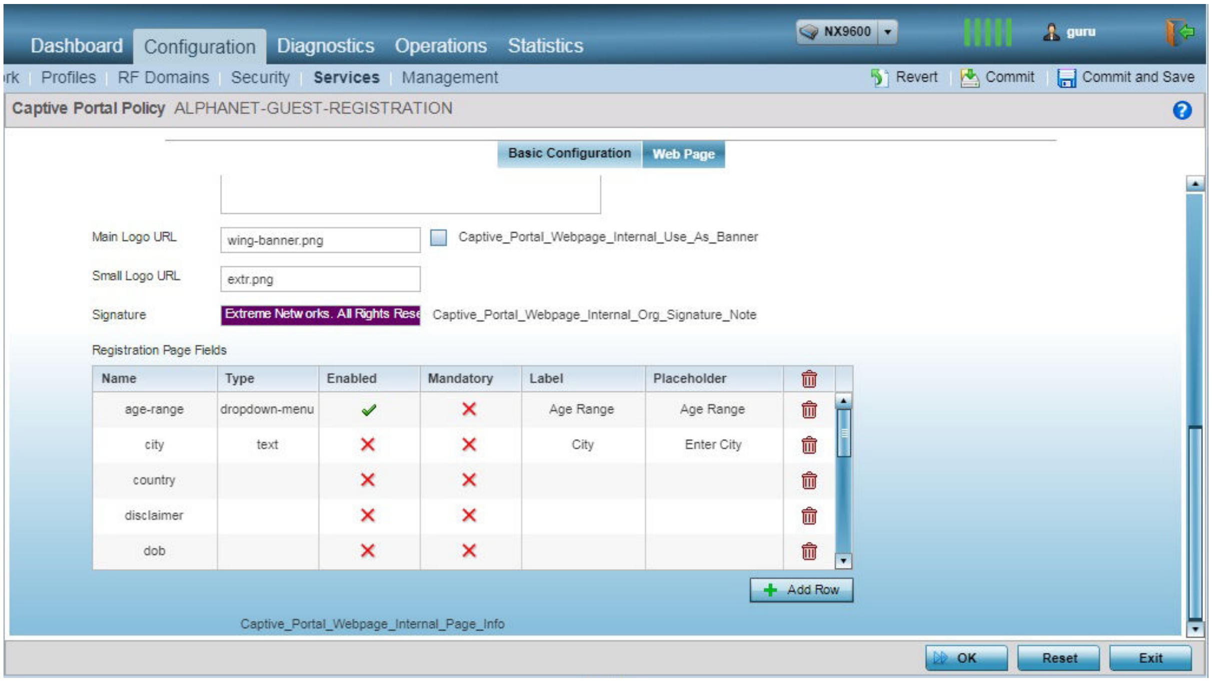
222200

Figure 346: Captive Portal Policy - Web Page - Color Palette Menu

4 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.



Captive Portal Policy ALPHANET-GUEST-REGISTRATION

Main Logo URL: wing-banner.png ☐ Captive_Portal_Webpage_Internal_Use_As_Banner

Small Logo URL: extr.png

Signature: Extreme Netw orks. All Rights Rese Captive_Portal_Webpage_Internal_Org_Signature_Note

Registration Page Fields

Name	Type	Enabled	Mandatory	Label	Placeholder
age-range	dropdown-menu	✓	✗	Age Range	Age Range
city	text	✗	✗	City	Enter City
country		✗	✗		
disclaimer		✗	✗		
dob		✗	✗		

Captive_Portal_Webpage_Internal_Page_Info

Figure 347: Captive Portal Policy - Web Page - Internal - Registration - Registration Page Fields Table

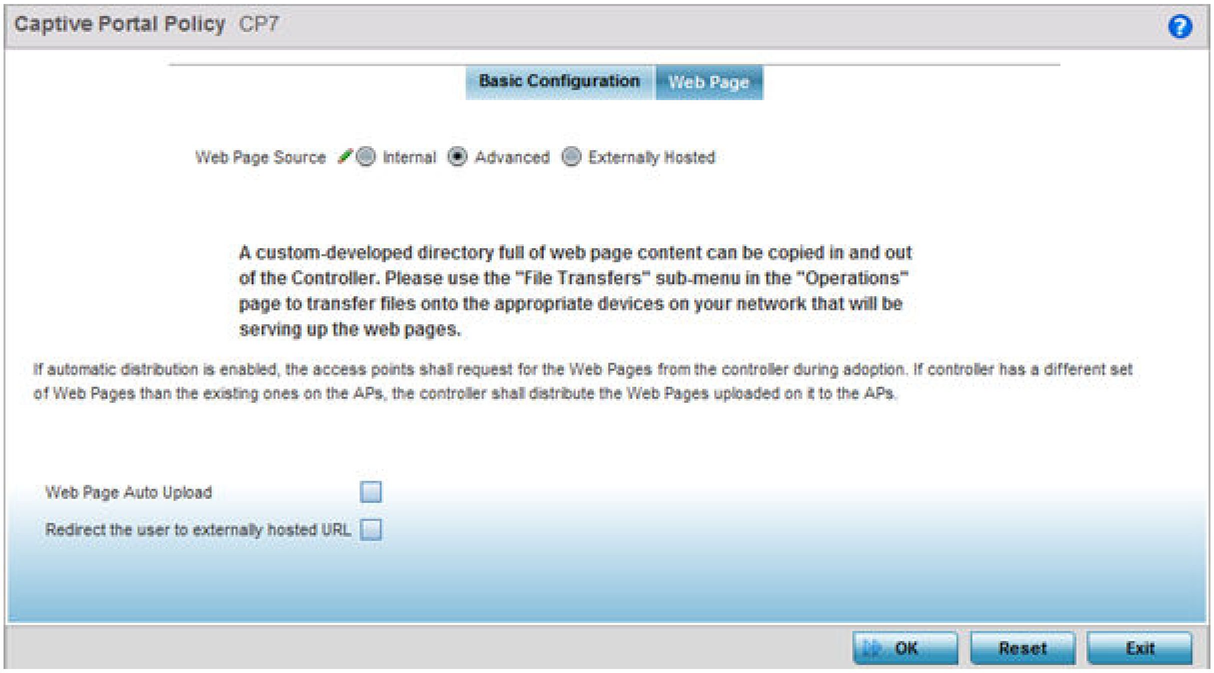
5 Click **OK** to save the changes made within any of the Internal Page screens.

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

6 Select **Advanced** to use a custom-developed directory of web pages.

Web pages in the directory can be copied to and from the controller or service platform, to support the captive portal.

Use the File Transfers sub-menu in the **Operations** page to transfer files to the appropriate devices serving up the web pages.



Captive Portal Policy CP7

Web Page Source ○ Internal ● Advanced ○ Externally Hosted

A custom-developed directory full of web page content can be copied in and out of the Controller. Please use the "File Transfers" sub-menu in the "Operations" page to transfer files onto the appropriate devices on your network that will be serving up the web pages.

If automatic distribution is enabled, the access points shall request for the Web Pages from the controller during adoption. If controller has a different set of Web Pages than the existing ones on the APs, the controller shall distribute the Web Pages uploaded on it to the APs.

Web Page Auto Upload ☐

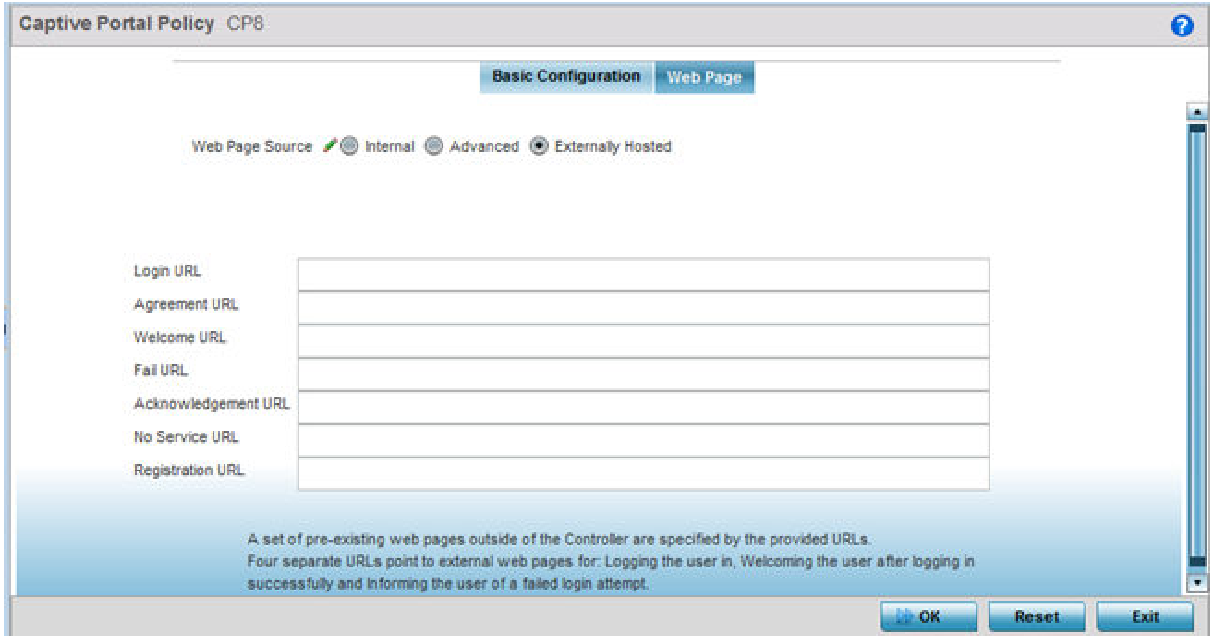
Redirect the user to externally hosted URL ☐

Figure 348: Captive Portal Policy - Web Page Screen - Advanced Option

7 Select the **Externally Hosted** radio button if hosting the captive portal on an external server resource.

Select to automatically launch the advanced pages for requesting clients upon association. This setting is disabled by default.

Select **Redirect the user to externally hosted URL** to use an externally hosted server resource and its login permissions for logging into the advanced page. This setting is disabled by default.



Web Page Source ○ Internal ○ Advanced ● Externally Hosted

A set of pre-existing web pages outside of the Controller are specified by the provided URLs. Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

Figure 349: Captive Portal Policy - Web Page - Externally Hosted Option

Login URL	Define the complete URL for the location of the Login screen. The Login screen prompts the user for a username and password to access either 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 network 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. The client needs to provide correct login information to regain access.
Acknowledgement URL	Define the complete URL to the location of the Acknowledgement page. The Acknowledgement URL is needed by returning users whose MAC addresses has been validated previously, but must accept the conditions of the captive portal again.
No Service URL	Define the complete URL to the location of the No URL 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 URL is supported by NX9500, NX9600 and NX75XX service platform models as an adopting controller verifying (registering) user information before client access is provided to captive portal managed Internet resources.

8 Click **OK** when completed to update the captive portal's advanced configuration.

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

Configuring DNS Whitelists

A DNS whitelist is used in conjunction with a captive portal to provide access services to wireless clients. Use the whitelist to create a set of allowed destination IP addresses within the captive portal. To effectively host hotspot pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist.

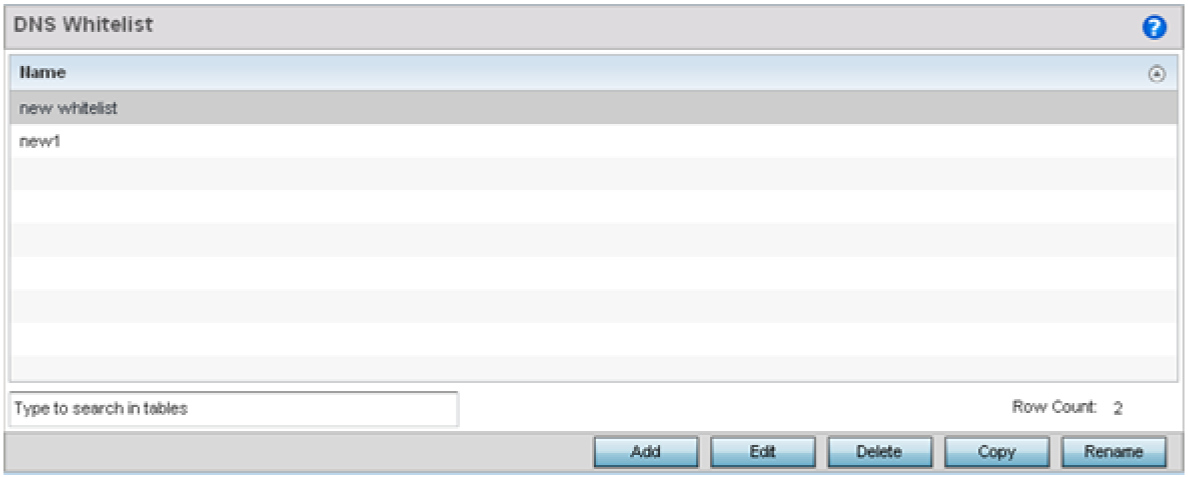
To define the whitelist:

1 Go to **Configuration** → **Services**.

The upper, left-hand, side of the user interface displays a Services menu pane where Captive Portal, DHCP and RADIUS configuration options can be selected.

2 Expand the **Captive Portals** node and select DNS Whitelist.

The DNS Whitelist screen displays.



Name
new whitelist
new1

Row Count: 2

Figure 350: Captive Portal DNS Whitelist Screen

3 Review the names of existing whitelists. Click **Add** to create a new whitelist entry, or select an existing whitelist and click **Edit** to modify it.

Captive Portal Deployment Considerations

Before defining a captive portal configuration for a controller, service platform or access point, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The architecture should consider the number of wireless clients allowed and the services provided. Each topology has benefits and disadvantages which should taken into consideration to meet each deployment's requirements.
- Captive portal authentication uses secure HTTPS to protect user credentials, but does not typically provide encryption for user data once they have been authenticated. For private access applications, WPA2 (with a strong passphrase) should be enabled to provide strong encryption.
- Guest user traffic should be assigned a dedicated VLAN, separate from other internal networks.
- Guest access configurations 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.

- Guest access services should be defined in a manner whereby end-user traffic does not cause network congestion.
- A valid certificate should be issued and installed on all devices providing captive portal access to the WLAN and wireless network. The certificate should be issued from a public certificate authority ensuring guests can access the captive portal without browser errors.

Setting the Guest Management Configuration

Establish a guest management configuration to redirect guest users to a registration portal upon association to the captive portal SSID, The guest users are redirected to an internally (or) externally hosted registration page (registration.html) where the guest user can complete the registration process if not previously registered. The internal captive portal adds a new registration page that's customizable based on business requirement.

A guest management policy is for configuration of E-mail host and SMS gateway related commands along with the credentials required for sending passcode to guest via email and SMS. Configure up to 32 different guest management policies. Each guest management policy allows an administrator to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. At any point of time, there can be only one guest management policy active per device.

Guest registration is supported on NX9000 series service platforms as an adopting controller with up to 2 million user identity entries. Guest registration is supported on NX 7500 series service platforms as an adopting controller with up to 1 million user identity entries. Guest management and registration is not supported on all other WiNG supported platforms.

Note

An option to backup the guest registration configuration is not available in the user interface. To backup the guest user database, a guest-databasebackup command must be invoked using the CLI. For more information, refer to the *WiNG CLI Reference Guide*.

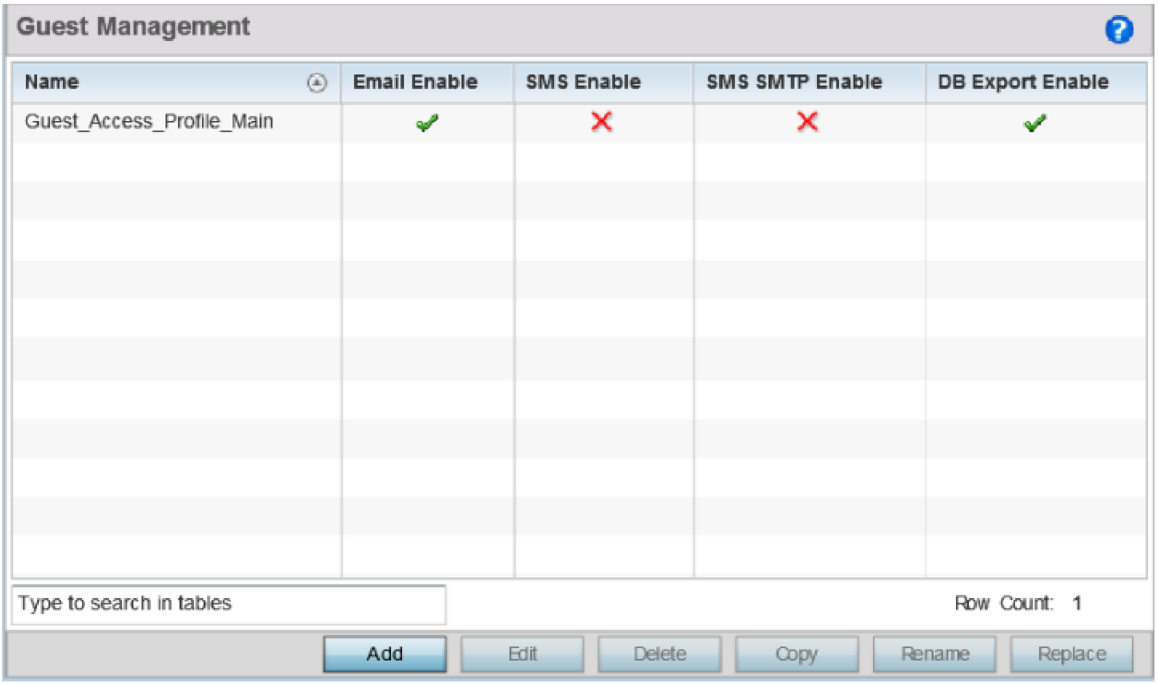
Refer to the following sections for configuring Guest Management parameters:

- Email on page 850
- SMS on page 852
- SMS SMTP on page 854
- DB Export on page 856

To set the guest management configuration:

1 Select **Configuration** > **Services** > **Guest Management**.

The Guest Management screen displays.



Name	Email Enable	SMS Enable	SMS SMTP Enable	DB Export Enable
Guest_Access_Profile_Main	✓	✗	✗	✓

Figure 351: Guest Management Screen

2 Review the following (at a high level) to determine if a new guest management requires creation, an existing guest management configuration requires modification, or an existing configuration needs to be deleted.

Name	Lists the name(s) of up to 32 guest user policies created on the service platform for registering guest user credentials.
Email Enable	A green check mark defines Email as enabled for guest management, a red X defines Email as disabled. Guest users can register themselves with their E-mail credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/member id and the received pass code for further login to the captive portal.
SMS Enable	A green check mark defines SMS as enabled for guest management, a red X defines SMS as disabled. SMS enables guest users to registers themselves with their E-mail or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered E-mail or mobile device ID and received passcode for login to the captive portal.
SMS SMTP Enable	A green check mark defines SMS SMTP as enabled for guest management, a red X defines SMS SMTP as disabled. Optionally configure an E-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway E-mail address to which the message is E-mailed. The gateway server converts the E-mail into SMS and sends the message to the guest user's mobile device.
DB Export Enable	A green check mark indicates that exporting the guest user database is enabled for this device. When enabled, the list of guest users on the captive portal can be periodically exported to an external server.

3. Click **Add** to create a new guest management configuration, choose an existing configuration and click **Edit** to modify its properties, or choose an existing guest management and click **Delete** to remove it from those available.

   Click **Rename** to change the name of an existing guest management configuration or copy a configuration to a different location. Click **Replace** to replace an existing Guest Management policy with a new policy.

Email

Guest users can register themselves with their email credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/ member id and the received pass code for further login to the captive portal.

To define a guest management configuration using email as the primary key for authentication:

1. Select **Configuration** > **Services** > **Guest Management**.

   Review existing guest management configurations to determine whether new email configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **Email** tab.

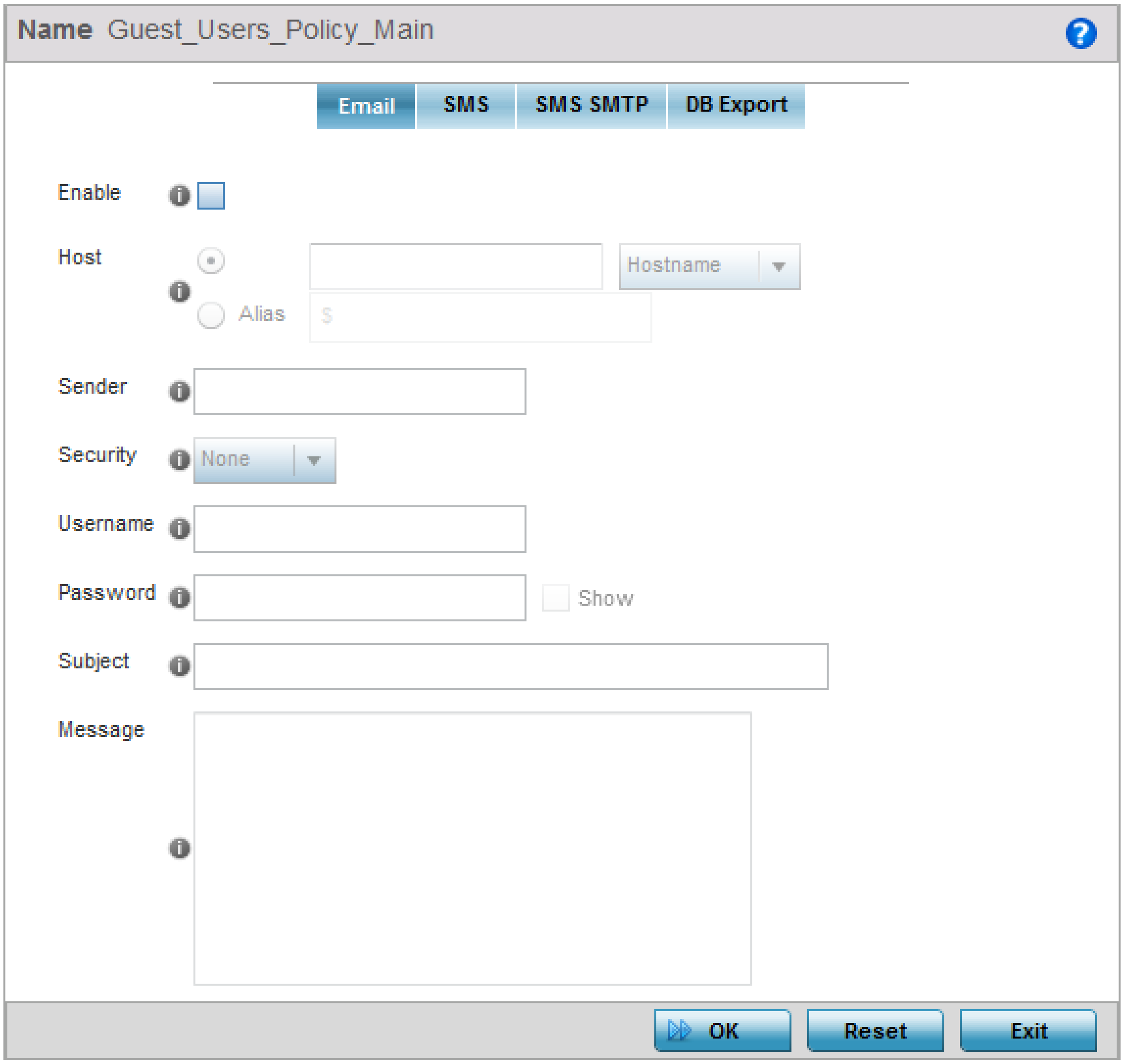


Figure 352: Guest Management - Add/Edit - Email Tab

3 Set the following email guest user network address and message content information required for notifying a guest with a passcode using email:

Enable	Enable this option so guest users can register themselves with their email credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered Email/ mobile/ member id and the received pass code for further login to the captive portal. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMTP server resource used for guest management email traffic, guest user credential validation and passcode reception. Optionally create an alias to define the host once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest email credentials.

Security	Use the drop-down menu to select ssl or starttls as the email host server user authentication validation scheme for this particular username and password combination. Optionally select None to apply to no additional user authentication beyond the required username and password combination.
Username	Provide a unique 100 character maximum username unique to this guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest email credentials.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest email credentials.
Subject	Enter the 100 character maximum email subject for the email message sent to the guest user along with the required passcode. You can use the tag 'GM_NAME' in the subject which is replaced by the guest user's name.
Message	Create the 1024 character maximum message content for the email sent to the guest user along with the passcode. You can use the following tags in the message body. • GM_NAME – indicates the guest user's name in the message. This tag is replaced by the guest user's name when the email is created. • GM_PASSCODE - indicates the password assigned to the user. The tag is replaced by the actual password when the email is created. • CR-NL - indicates a line break. When used, the word next to this tag starts on a new line when the email is created.

4 Click **OK** to save the updates to the guest management Email configuration.

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

SMS

SMS enables guest users to registers themselves with their email or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered email or mobile device ID and received passcode for login to the captive portal.

Note

When utilizing SMS, the WLAN's authentication type should be None and the registration type should be enabled as user registration. Captive portal authentication must always enforce guest registration.

SMS is similar to MAC address based self registration, but in addition a captive portal sends a SMS message to the user on the mobile phone number provided at registration containing an access code. The user then inputs the access code on the user screen. The captive portal verifies the code, returns the Welcome page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is Clickatell. A passcode can be sent with SMS to the guest user directly using Clickatell, or the passcode can be sent via email to the SMS Clickatell gateway server, and Clickatell sends the passcode SMS to the guest user.

To define a guest management configuration using SMS:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **SMS** tab.

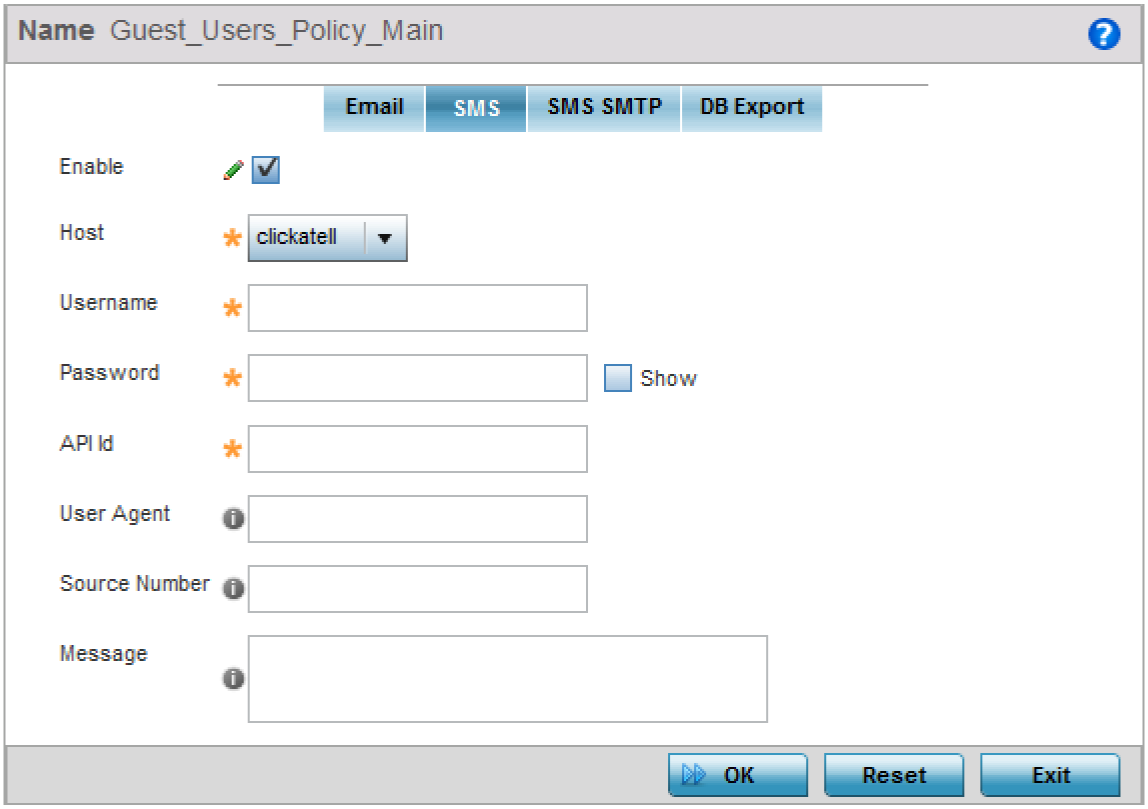


Figure 353: Guest Management - Add/Edit - SMS Tab

3 Set the following SMS guest user network address and message content information required for notifying a guest with a passcode:

Enable	Select this option to enable guest users to registers themselves with their email or mobile device ID as the primary key for authentication. This setting is disabled by default and must be enabled to define the required settings.
Host	By default, *clickatell* is the only host SMS gateway server resource. Upon receiving the passcode email, the SMS gateway sends the actual notification passcode SMS to the guest user.
Username	Provide a unique 32 character maximum username unique to this SMS guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest user credentials with SMS.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMS.
API Id	Set a 32 character maximum API Id for the configuration of the clickatell api_id (http/smtp api_id).

User Agent	Select the user agent for configuring the clickatell SMS gateway server and its related credentials for sending the passcode to guests.
Source Number	Set a 32 character maximum source-address from the number associated with clickatell. It can be a large integer or short code. The source number is only applicable to certain countries (like the United States).
Message	Create the 1024 character maximum message content for the SMS based request sent to the guest user along with the passcode.

4 Click **OK** to save the updates to the guest management SMS configuration.

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

SMS SMTP

Optionally configure an email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway email address to which the message is emailed. The gateway server converts the email into SMS and sends the message to the guest user's mobile device.

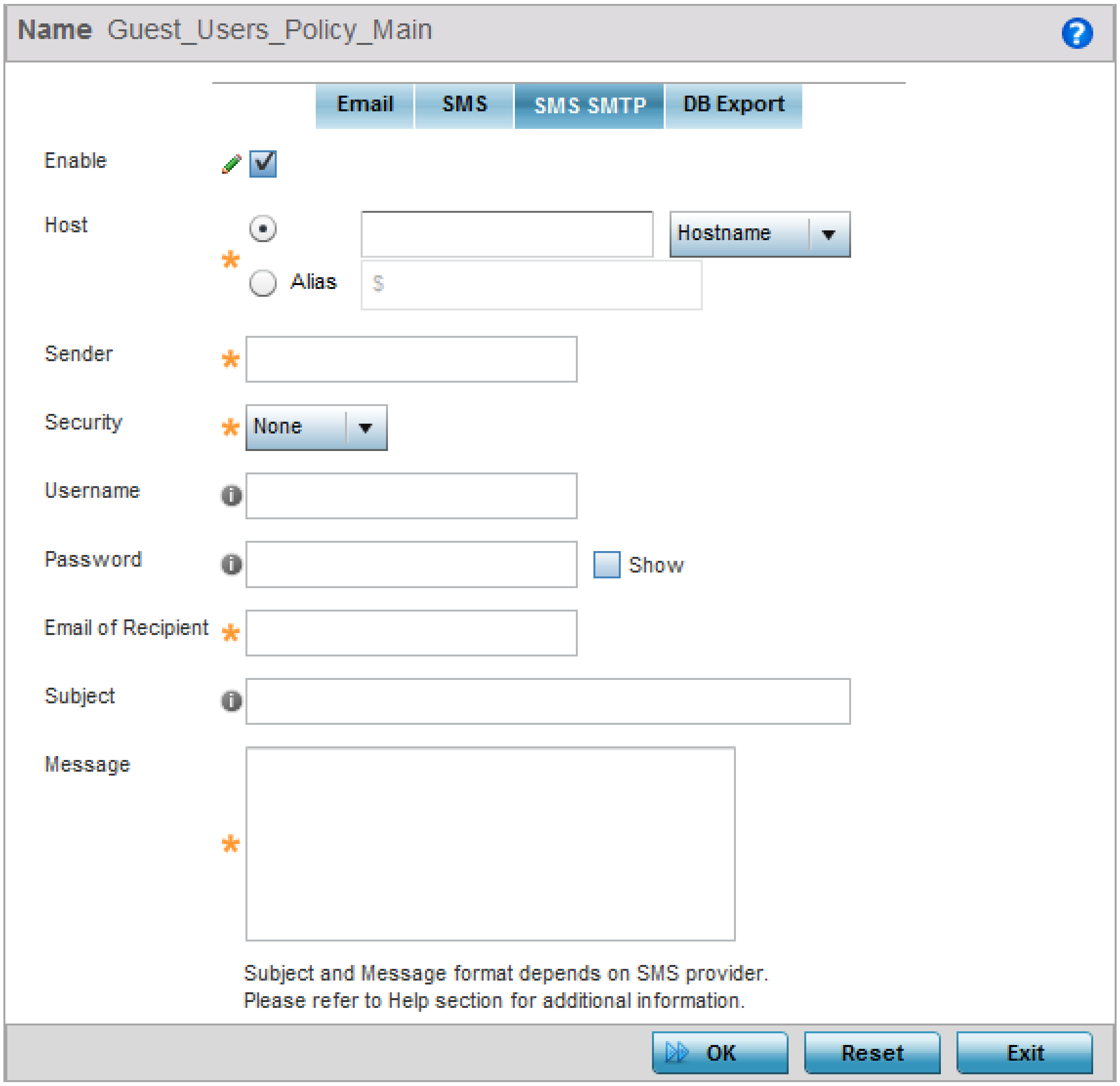
When sending an email, the email client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the Email.

To define a guest management configuration using SMS SMTP:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **SMS SMTP** tab.



Subject and Message format depends on SMS provider.
Please refer to Help section for additional information.

Figure 354: Guest Management - Add/Edit - SMS SMTP Tab

3 Set the following SMS SMTP guest user network and message content information required for notifying a guest with a passcode:

Enable	Enable this setting to configure an email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway Email address to which the message is emailed. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMS gateway server resource used for guest management email traffic, guest user credential validation and passcode reception. Consider providing the host as an alias. An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest email credentials using SMTP.

Security	Use the drop-down menu to select `ssl` or `starttls` as the SMTP server user authentication validation scheme for this particular username and password combination. Optionally select None to apply to no additional user authentication beyond the required username and password combination. The default value is `ssl`.
Username	Provide a unique 64 character maximum username unique to this SMTP guest management configuration. This username requires its own password and must be correctly provided to receive the required passcode for registering guest user credentials.
Password	Define a 64 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMTP.
Email of Recipient	Enter a 64 character maximum email address for the recipient of guest management email traffic.
Subject	Enter a 100 character maximum email subject for the email message sent to the guest user along with the required passcode.
Message	Enter a 1024 character maximum email message per the message format required by the gateway server. The sms-over-smtp message format is the required format from clickatell while sending email to the SMS gateway server.

4. Click **OK** to save the updates to the guest management SMS SMTP configuration.

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

DB Export

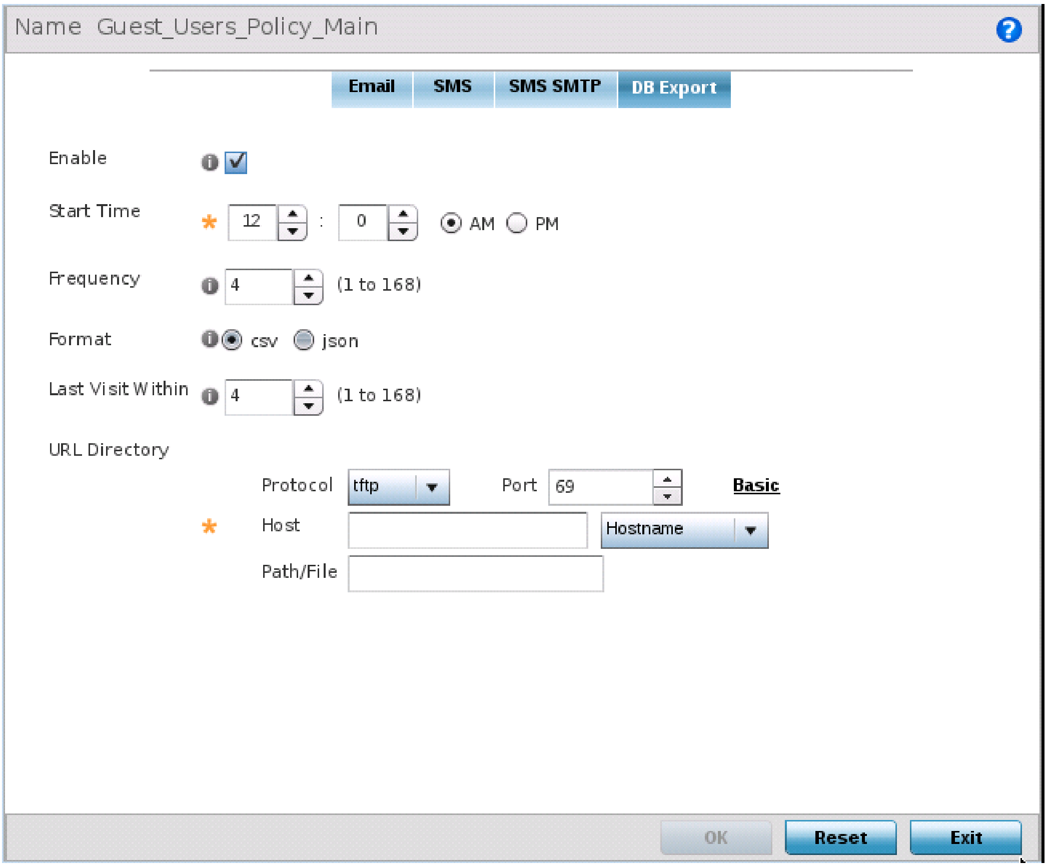
Optionally configure the guest user database export parameters. The guest user database can be periodically exported to an external server for backup and analysis.

To define the database export parameters:

1. Select **Configuration** > **Services** > **Guest Management**.

   Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **DB Export** tab.



Name Guest_Users_Policy_Main

Enable ☑

Start Time * 12 : 0 ● AM ○ PM

Frequency 4 (1 to 168)

Format ● csv ○ json

Last Visit Within 4 (1 to 168)

URL Directory

Protocol tftp Port 69

* Host Hostname

Path/File

Figure 355: Guest Management - Add/Edit - DB Export Tab

3 Set the following DB Export parameters:

Enable	Enable this setting to configure the guest user database to an external server for backup and analysis. This setting is disabled by default and must be enabled to define the required settings.
Start Time	Define the start time when the first database backup occurs. The first run of the guest user database backup is always the current day. Use the spinner controls to set the start hour and minute. Use the AM/PM options to configure the exact hour. The default value is 12:00 AM.
Frequency	Define the backup frequency. This is the time interval between two consecutive backups. Use the spinner control to set the value between 1 hour and 168 hours. The default frequency is 4 hours.
Format	The guest user database can be exported in the following formats: • CSV • JSON Select the appropriate export format. The default export format is CSV.
Last Visit Time	Use this field to filter or restrict the amount of data that is exported. Use the spinner to set a value in the range 1 - 168 hours. When set, any data that is older than the set period - from when the database is being backed up - is not exported. The default value is 4 hours.

URL Directory	Use the field to provide the URL to which the guest user database is exported. Select the Advanced link to expose fields for setting the remote server’s URL.
Protocol	Select the protocol used for exporting the guest user database. Available options include: • tftp • ftp • sftp • http • cf • usb1-4
Port	Use the spinner control to 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 to export the guest user database to. Hostnames cannot include an underscore character. This option is not valid for cf and usb1-4. 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 on the remote server where the guest user database file is copied to. Enter the complete relative path to the file on the remote server.

4 Click **OK** to save the updates to the guest management DB Export configuration.

Click **Reset** to revert the screen back 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.

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.

Numerous DHCP network address credentials can have an alias applied. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values. 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. An alias name always starts with a dollar sign ($) and should not exceed 32 characters. An alias that's applied to a DHCP configuration can be either a Global, Profile, RF Domain or Device alias. For more information on aliases and their application, Alias Configuration on page 666.

Note
DHCP server updates are implemented only when the controller or service platform is restarted.

Refer to the following sections for more information on configuring DHCP parameters:

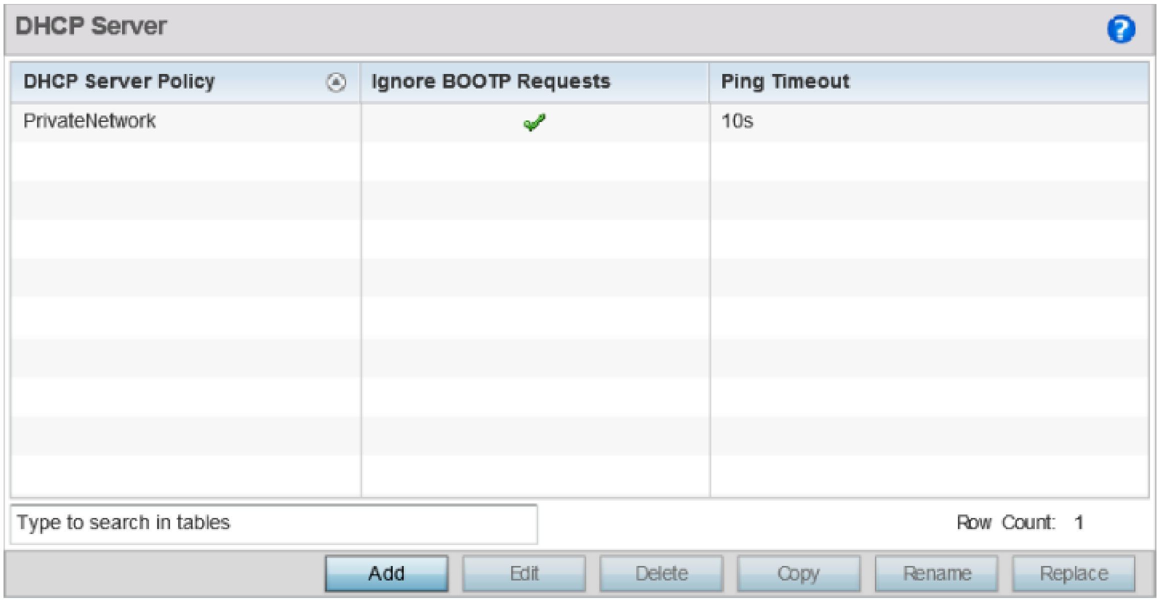
- Defining DHCP Pools on page 860
- Defining DHCP Server Global Settings on page 869
- DHCP Class Policy Configuration on page 871
- DHCP Deployment Considerations on page 873

To access and review the local DHCP server configuration:

1 Select **Configuration** > **Services** > **DHCP Server Policy**.

Review existing guest management configurations to determine whether new email configuration requires creation or an existing guest user configuration requires modification or deletion.

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.



DHCP Server

DHCP Server Policy	Ignore BOOTP Requests	Ping Timeout
PrivateNetwork	✓	10s

Type to search in tables

Row Count: 1

Figure 356: 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.

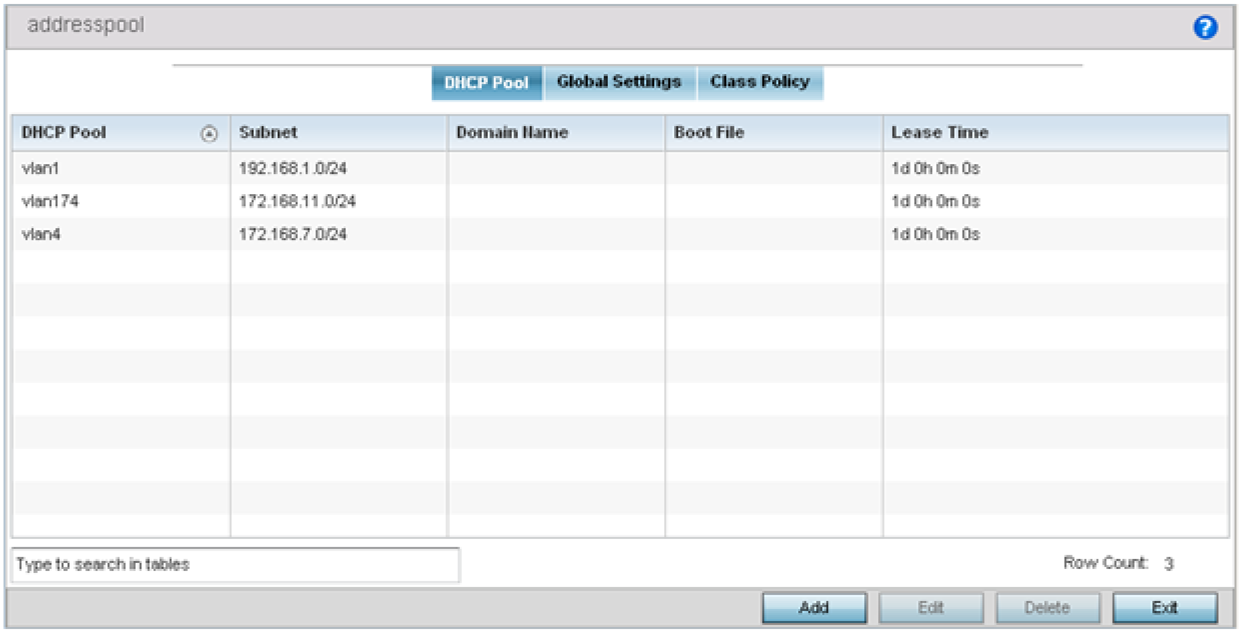
To define the parameters of a DHCP pool:

1 Select **Configuration** > **Services**.

The upper, left-hand, side of the user interface displays a Services menu pane where *Captive Portal*, *DHCP* and *RADIUS* configuration options can be selected.

2 Select **DHCP Server Policy**.

The DHCP Server Policy screen displays the DHCP Pool tab by default.



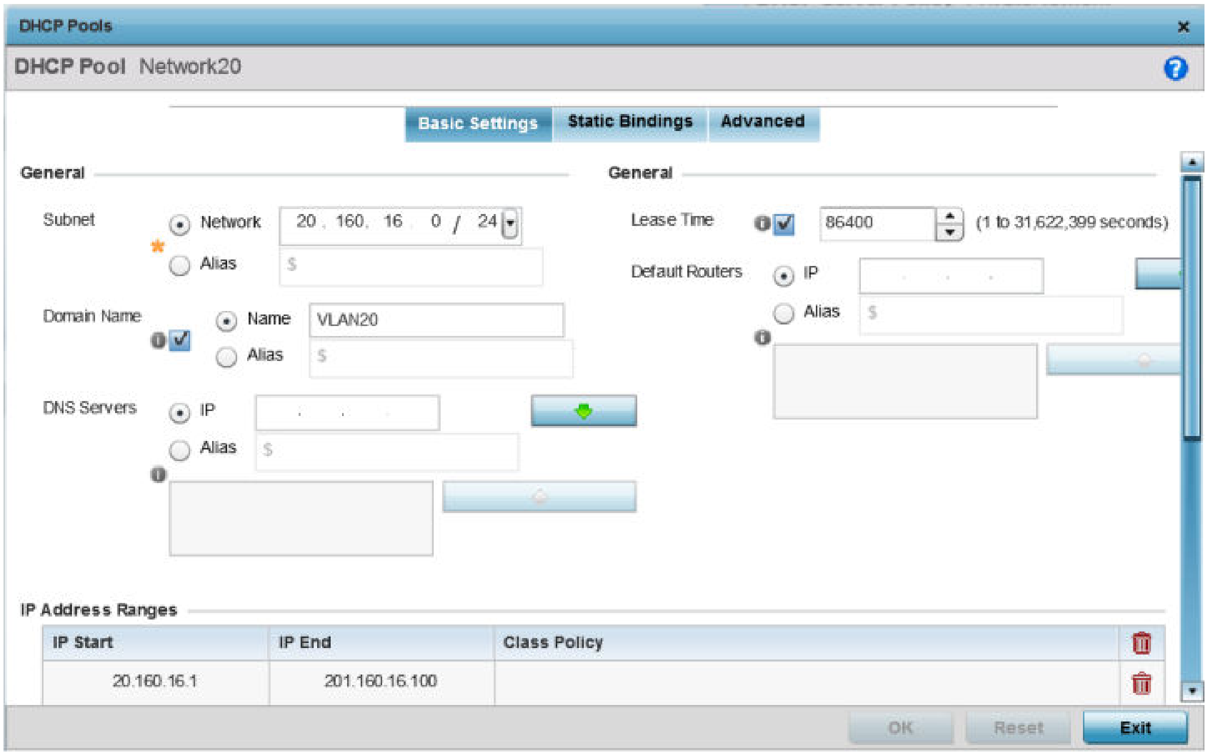
DHCP Pool	Subnet	Domain Name	Boot File	Lease Time
vlan1	192.168.1.0/24			1d 0h 0m 0s
vlan174	172.168.11.0/24			1d 0h 0m 0s
vlan4	172.168.7.0/24			1d 0h 0m 0s

Figure 357: 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 - 31,622,399 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.



DHCP Pool Network20

Subnet ● Network 20 . 160 . 16 . 0 / 24 ○ Alias $

Domain Name ☑ ● Name VLAN20 ○ Alias $

DNS Servers ● IP ○ Alias $

Lease Time ☑ 86400 (1 to 31,622,399 seconds)

Default Routers ● IP ○ Alias $

IP Address Ranges

IP Start	IP End	Class Policy
20.160.16.1	201.160.16.100	

Figure 358: 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.

An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

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. If you are setting a subnet IP alias, ensure that it begins with a dollar sign ($) and does not exceed 32 characters. A numeric IP address is the default setting, not an alias.

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*. If you are setting a domain name alias, ensure that it begins with a dollar sign ($) and does not exceed 32 characters. A numeric IP address is the default setting, not an alias.
DNS Servers	Define one (or a group) of Domain Name Servers (DNS) to translate domain names to IP addresses. An alias can alternatively be applied for a DNS server IP address. Up to 8 IP addresses can be supported. If you are setting a DNS IP alias, ensure that it begins with a dollar sign ($) and does not exceed 32 characters. An actual DNS IP address is the default setting, not an alias.
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 ($) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias. If you are setting a default router IP alias, ensure that it begins with a dollar sign ($) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias.

6. Define the range of included (starting and ending IP addresses) addresses for this particular pool.

   Use the **IP Address Ranges** field 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.

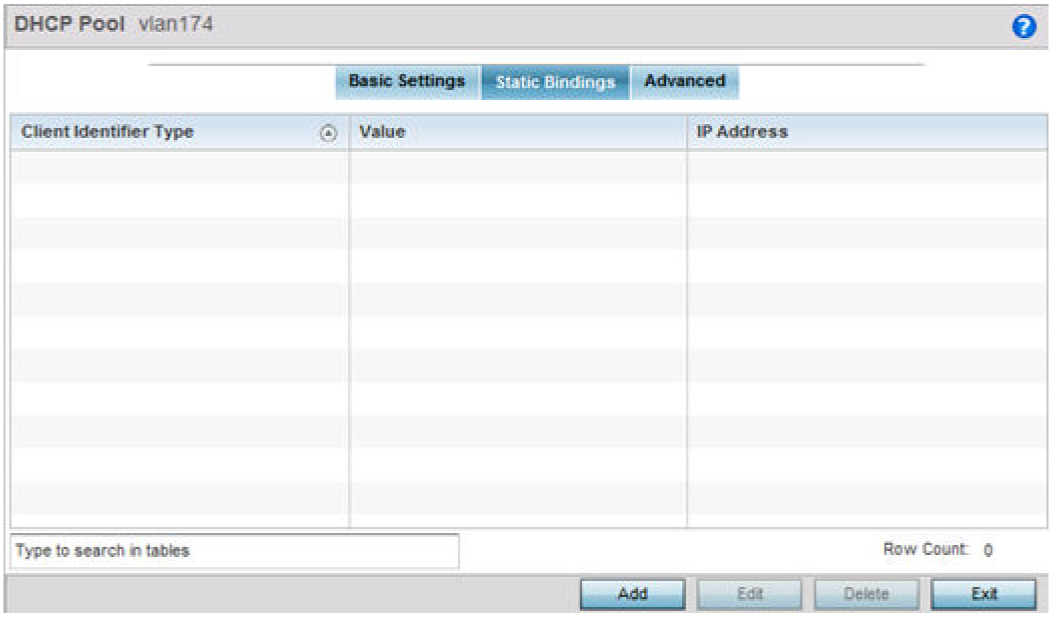


Figure 359: DHCP Pools - Add/Edit - Static Bindings Tab

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.

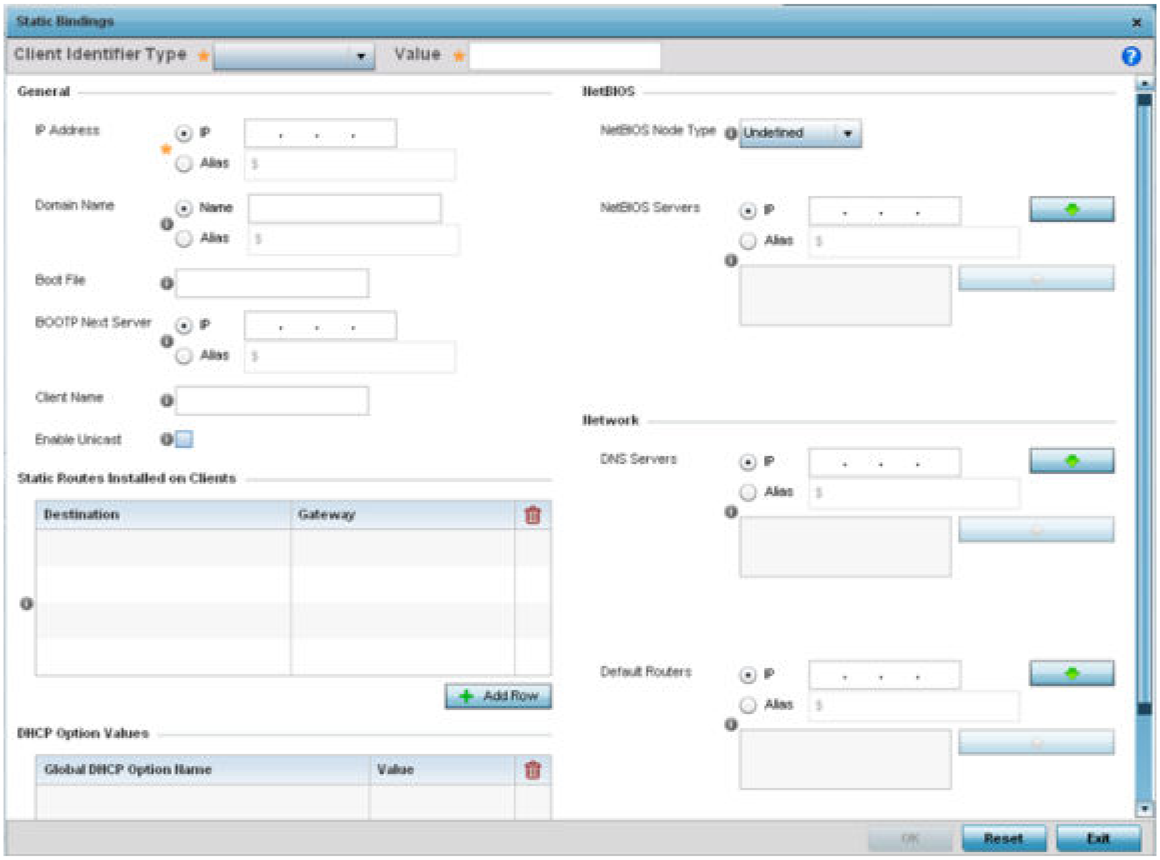


Figure 360: DHCP Pools - Add/Edit - Static Bindings - Add Screen

12 Set the following **General** parameters or aliases to complete the creation of the static binding configuration.

An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

IP Address	Set an IP address of the client using this host pool for DHCP resources. The IP option is selected by default. Optionally select **Alias** to provide an IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
Domain Name	Provide a domain name for the current interface. Domain names are not case sensitive and can contain letters, numbers, and hyphens. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com*. The Name option is selected by default. Optionally select **Alias** to provide a domain name alias beginning with a dollar sign ($) and not exceeding 32 characters.
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. The IP option is selected by default. Optionally select **Alias** to provide a boot file IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

BOOTP Next Server	Provide the numerical IP address or alias of the server providing BOOTP resources. 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. The IP option is selected by default. Optionally select Alias to provide a next BOOTP server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
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: • Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name. • 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. • Mixed - A mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address. • Hybrid - A combination of two or more nodes. • Undefined - 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. The IP option is selected by default. Optionally select Alias to provide a NetBIOS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

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.

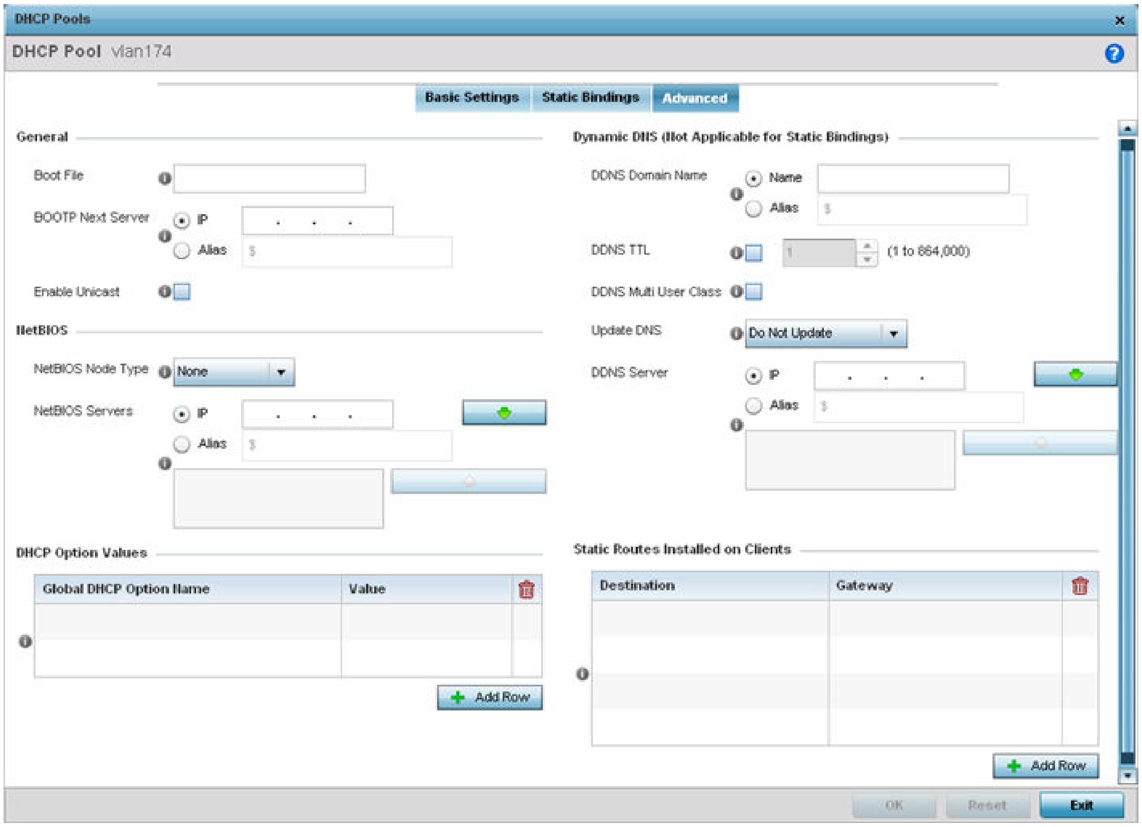
Up to eight IP addresses can be provided. The IP option is selected by default for both DNS Servers and Default Routers. foo

Optionally, select **Alias** to provide an IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

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.



DHCP Pool vlan174

BOOTP Next Server: ● IP ○ Alias

Enable Unicast: ☐

NetBIOS Node Type: None

NetBIOS Servers: ● IP ○ Alias

DDNS Domain Name: ● Name ○ Alias

DDNS TTL: ☐ 1 (1 to 864,000)

DDNS Multi User Class: ☐

Update DNS: Do Not Update

DDNS Server: ● IP ○ Alias

Figure 361: 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. BOOTP 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. The IP option is selected by default. Optionally select Alias to provide a next BOOTP server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
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: • Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name. • 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. • Mixed - Mixed uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address. • Hybrid - A combination of two or more nodes. • Undefined - 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. The IP option is selected by default. Optionally select Alias to provide a NetBIOS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

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

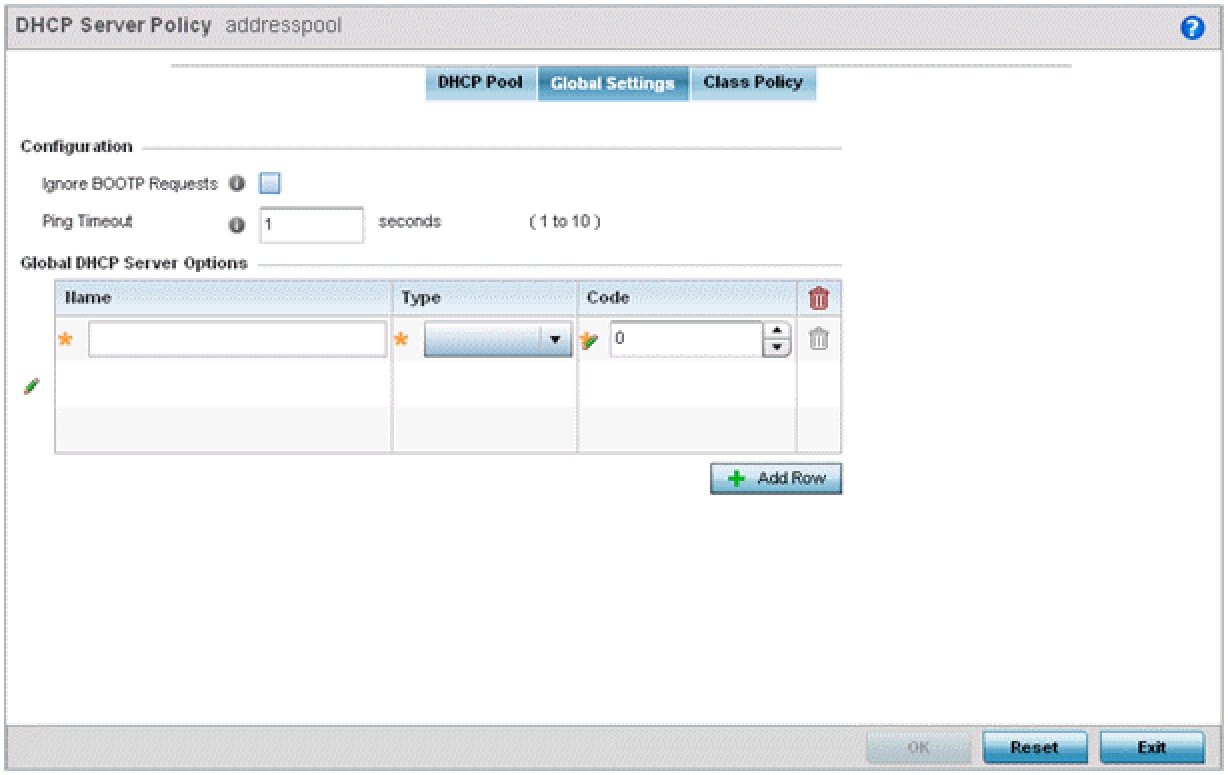
Set a DHCP server global configuration by defining whether BOOTP requests are ignored and by defining DHCP global server options.

To define DHCP server global settings:

1. Select **DHCP Server Policy** from within the Services menu pane.

   Add or **Edit** an existing policy.

2 Select the **Global Settings** tab.



Ignore BOOTP Requests ☐

Ping Timeout 1 seconds

Code 0

Figure 362: DHCP Server Policy - Add/Edit - Global Settings Tab

3 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.

4 Set the **Activation Criteria** for the DHCP server policy:

Select the **Criteria** option to invoke a drop-down menu to determine when the DHCP daemon is invoked. Options include `vrrp-master`, `cluster-master` or `rf-domain-manager`.

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 of the RF Domain capable of storing and provisioning configuration and firmware images for other members of the RF Domain.

5. 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.
6. 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 **DHCP Server Policy** from within the Services menu pane.

   Add or **Edit** an existing policy.

2 Select the **Class Policy** tab.

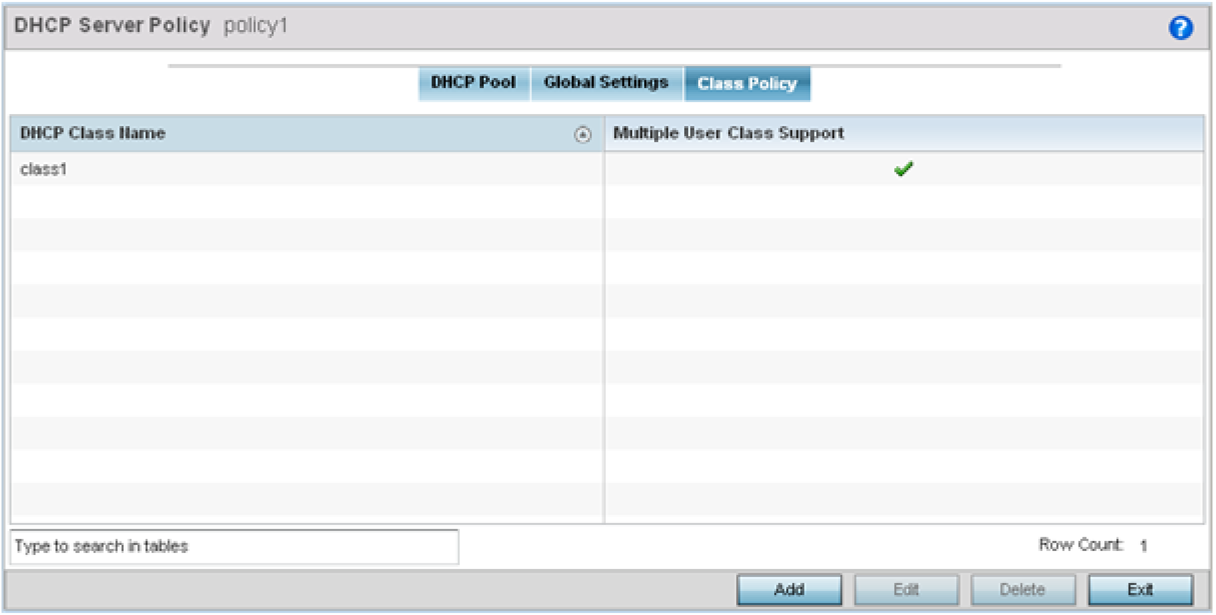
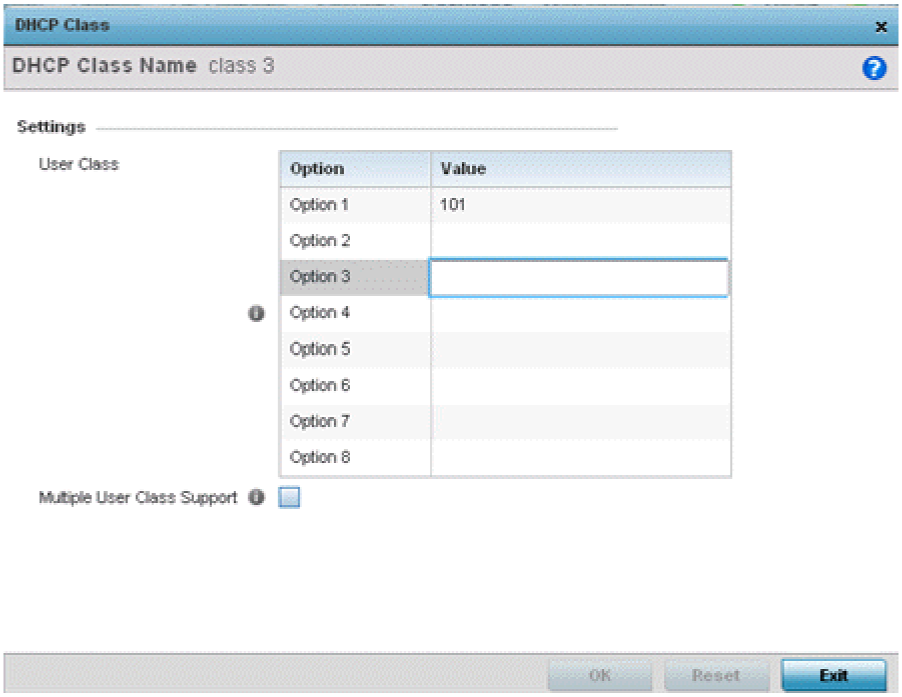


Figure 363: DHCP Server Policy - Class Policy Tab

3 Refer to the following to determine whether a new class policy requires creation, an existing class policy requires edit or an existing policy requires deletion:

DHCP Class Name	Displays client names grouped by the class name assigned when the class policy was created.
Multiple User Class	A green check mark in this column defines multiple user class support as enabled from the listed DHCP class name. A red "X" defines multiple user class support as disabled. Multiple user class support can be *enabled* or *disabled* for existing class names by editing the class name's configuration.

4 Click **Add** to create a new DHCP class policy, **Edit** to update an existing policy or **Delete** to remove an existing policy.



DHCP Class

DHCP Class Name class 3

Settings

User Class

Option	Value
Option 1	101
Option 2	
Option 3	
Option 4	
Option 5	
Option 6	
Option 7	
Option 8	

Multiple User Class Support ☐

Figure 364: DHCP Class Name Add Screen

5 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.

6 Select a row within the **Value** column to enter a 32-character maximum value string.

7 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.

8 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

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.

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.

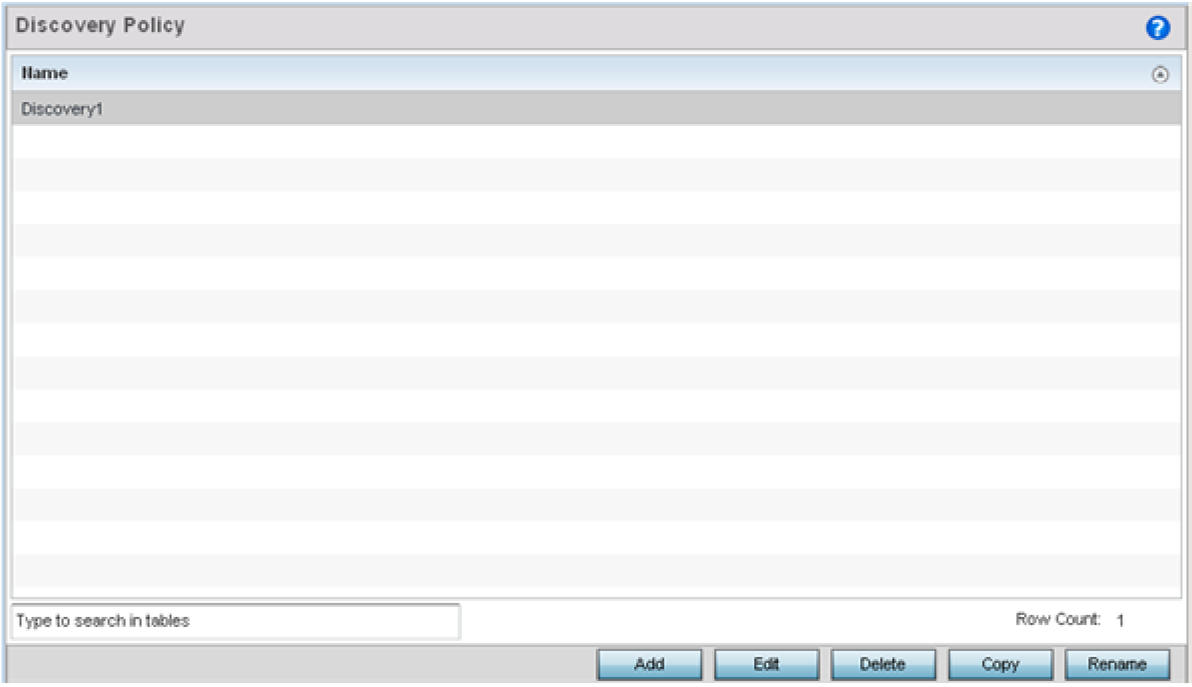


Figure 365: Bonjour Gateway - Discovery Policy Screen

5 Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration..

Optionally, **Rename** a policy or **Copy** a policy to a different location.

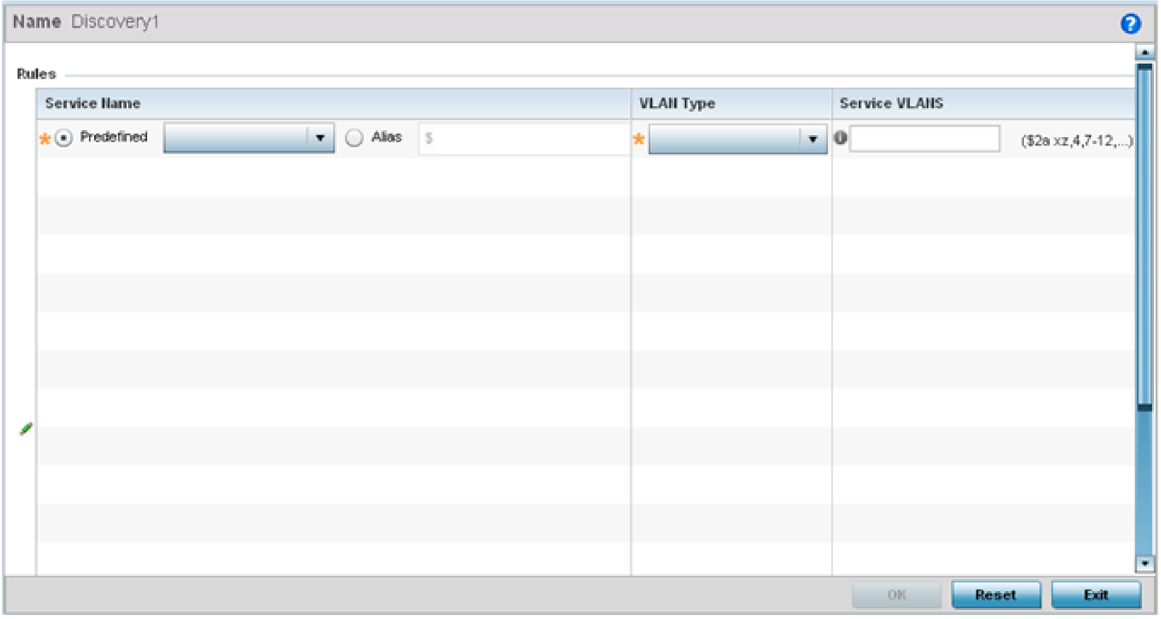


Figure 366: Bonjour - Discovery Policy - Add/Edit Policy Screen

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. • Predefined – Use the drop-down menu to select from a list of predefined Apple services (Scanner, Printer, HomeSharing etc.). • 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. • `local` – The VLAN(s) defined in the **Service VLAN** field use a local bridging mode. • `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.
Instance Name	Optionally, specify the selected Bonjour service's instance name. When specified, the Bonjour service discovery queries contain the instance name. of the service to be discovered. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, $BONJOURSTRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring a string alias, see Network Basic Alias Configuration on page 499. This option is useful especially in large distributed, enterprise networks. Use it to create different instances of a Bonjour service for the different organizations or departments (VLANS) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).

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.

To display Bonjour forwarding policy information:

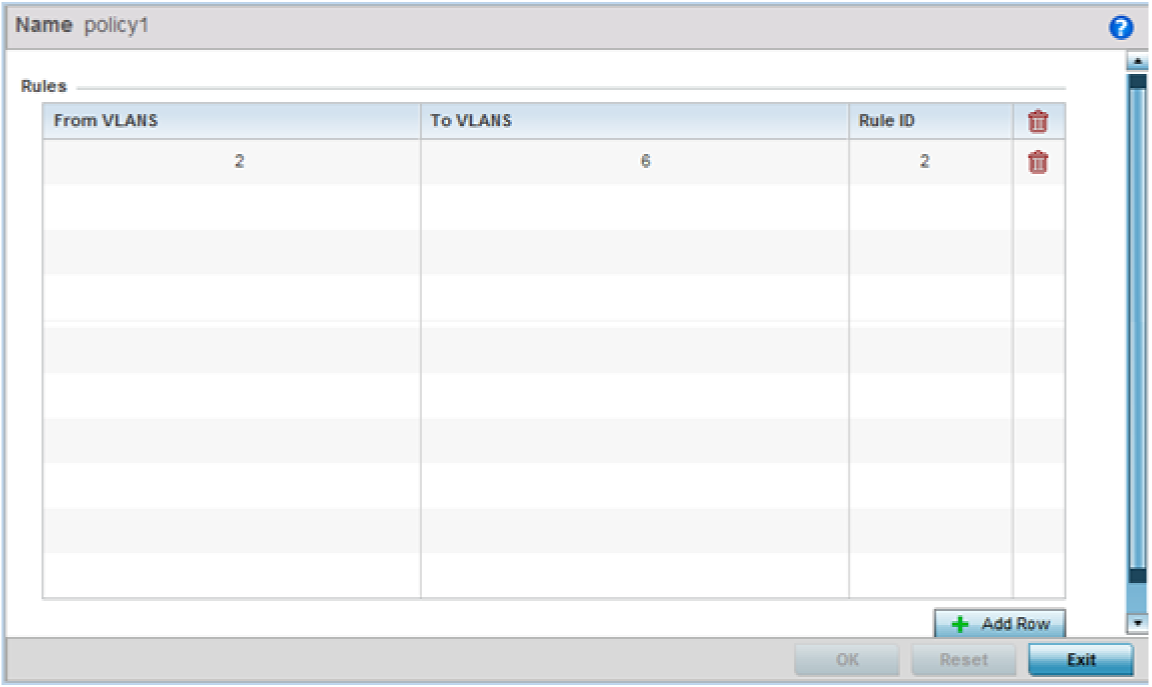
1 Select **Configuration**.

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.



Name policy1

Rules

From VLANS	To VLANS	Rule ID
2	6	2

Figure 367: 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..

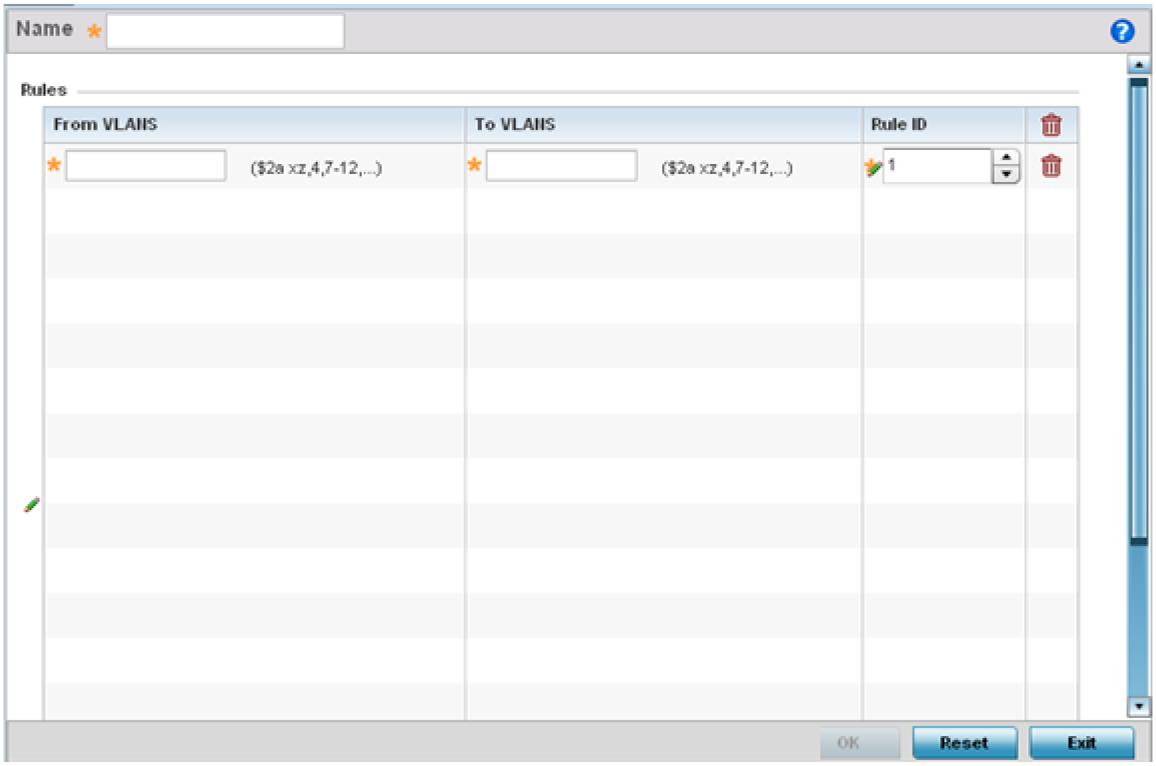


Figure 368: Bonjour Gateway - Forwarding Policy - Add Screen

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.

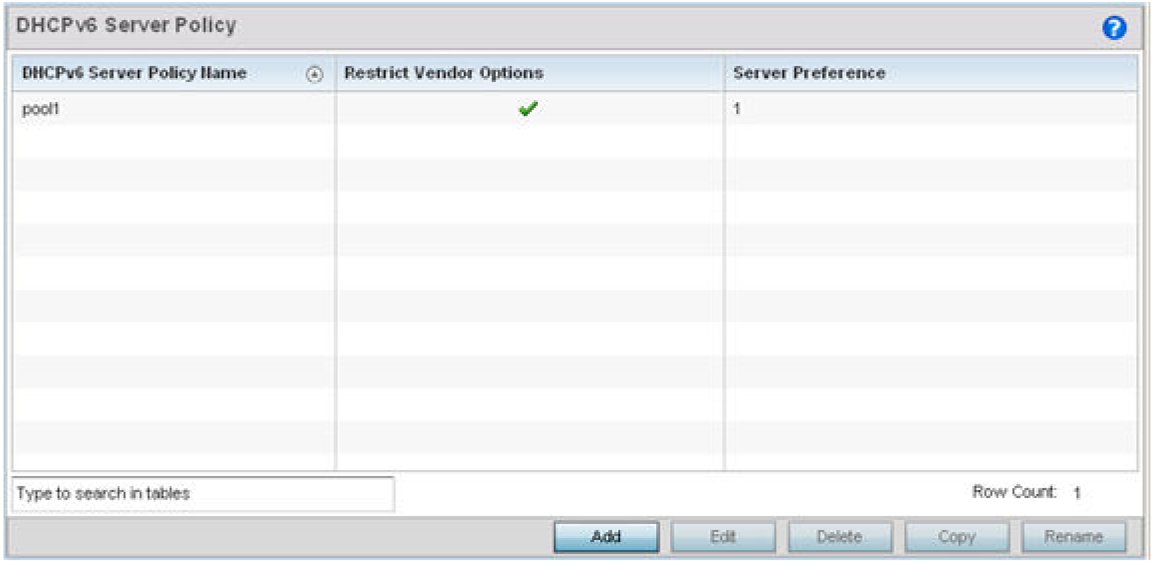
Refer to the following for more information on configuring the DHCPv6 Server Policy parameters:

- Defining DHCPv6 Options on page 880
- DHCPv6 Pool Configuration on page 882

To access and review the local DHCPv6 server configuration:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**.

The DHCPv6 Server Policy screen displays.



DHCPv6 Server Policy Name	Restrict Vendor Options	Server Preference
pool1	✓	1

Row Count: 1

Figure 369: 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.

   Optionally **Rename** or **Copy** a policy to a different location.

Defining DHCPv6 Options

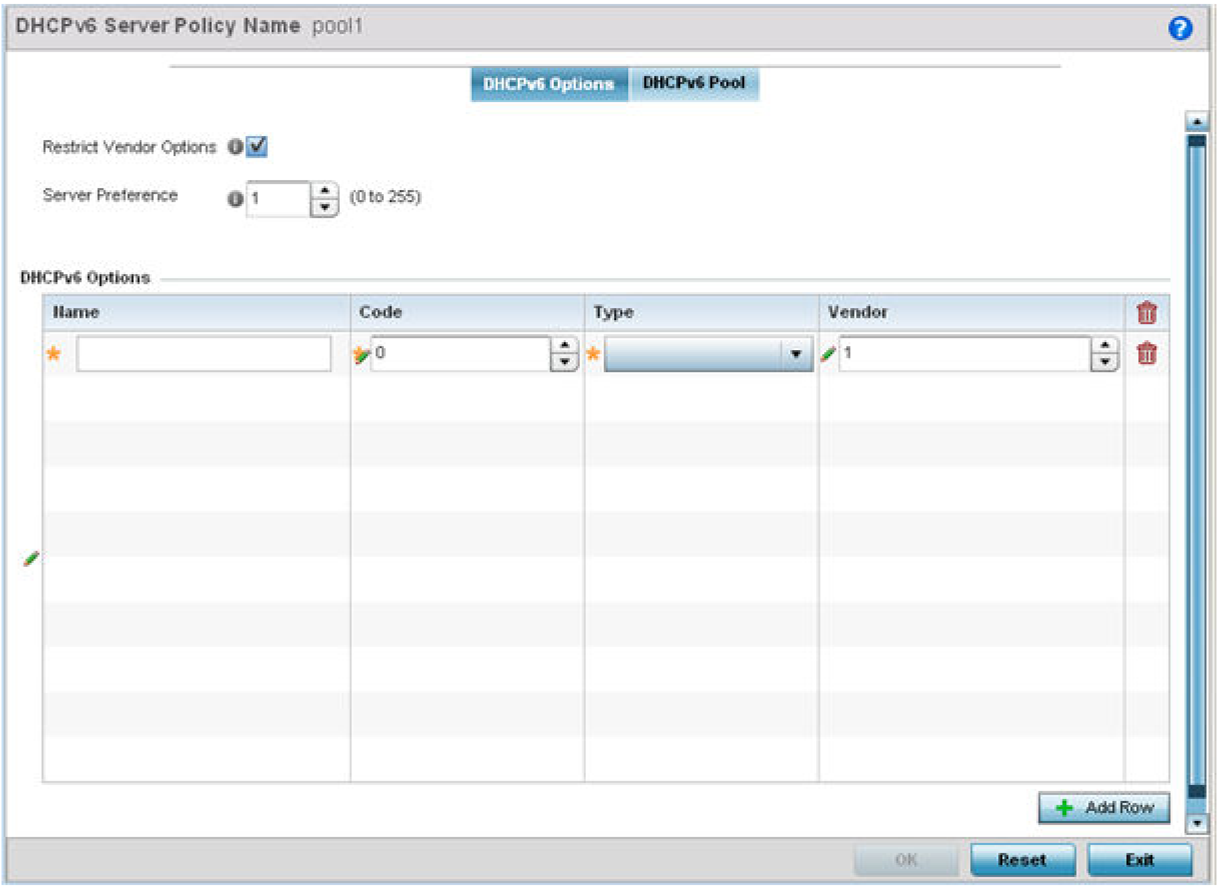
DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided 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.



DHCPv6 Server Policy Name pool1

Restrict Vendor Options ☑

Server Preference 1 (0 to 255)

Code 0

Vendor 1

Figure 370: 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.

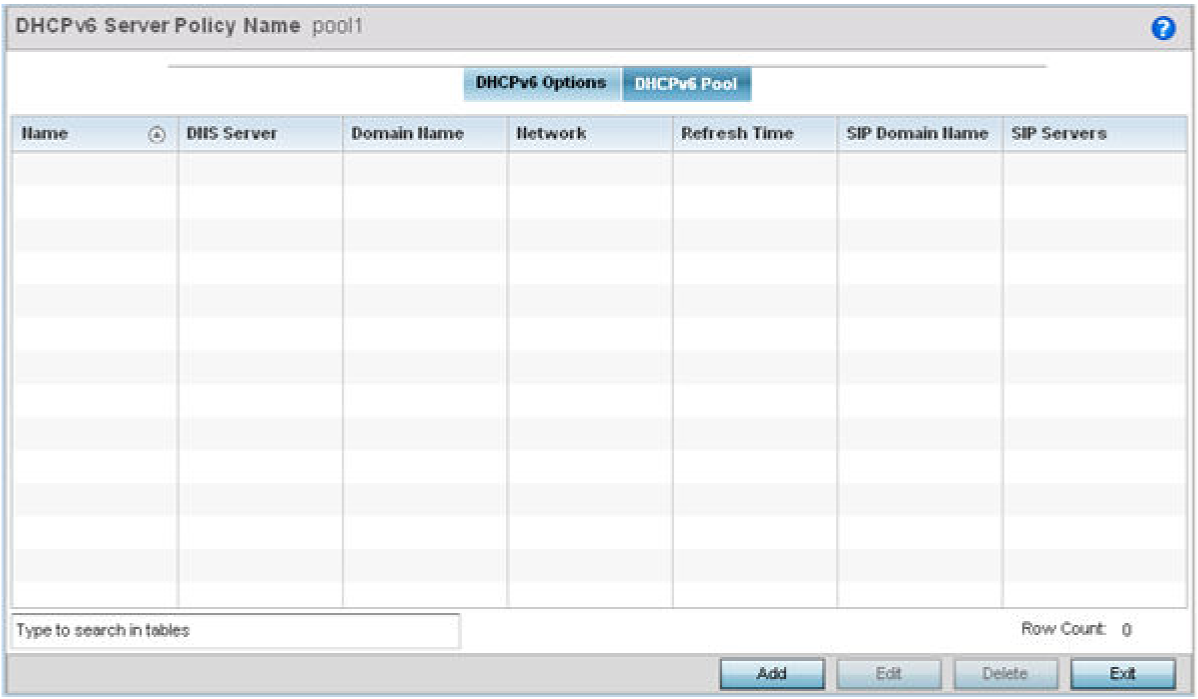
Click **Reset** to revert the screen to its last saved configuration.

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.


DHCPv6 Server Policy Name pool1

Name	DNS Server	Domain Name	Network	Refresh Time	SIP Domain Name	SIP Servers

Row Count 0

Figure 371: 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.

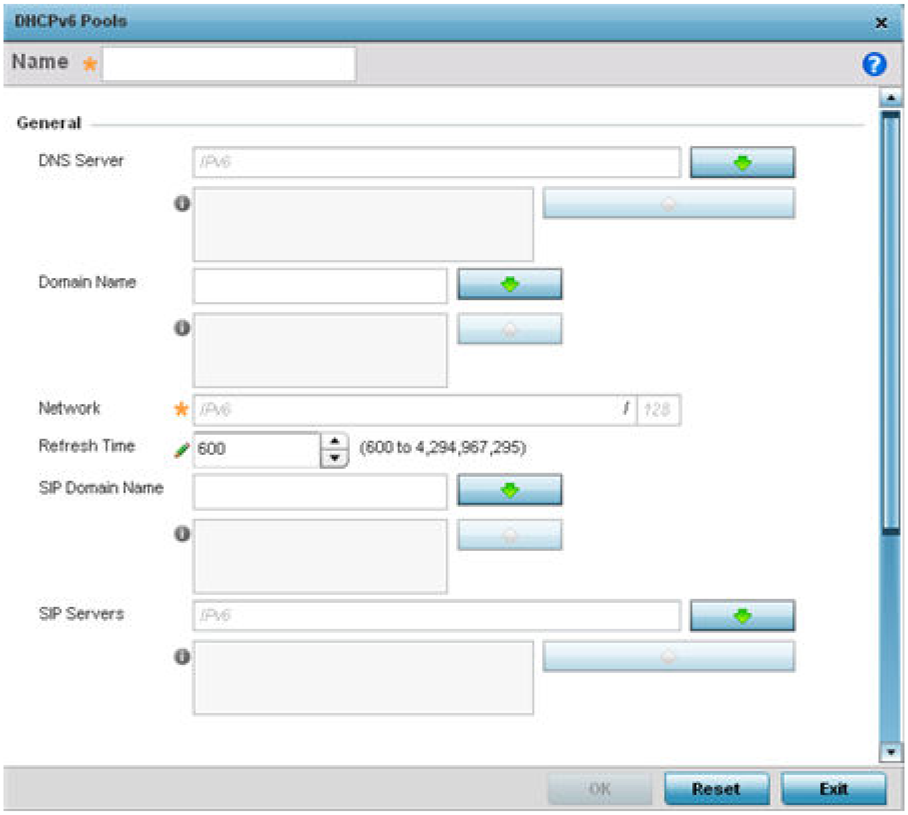


Figure 372: DHCP Server Policy - DHCPv6 Pool - Add/Edit Screen

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 access point’s 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.

Controllers and service platforms have full internal RADIUS resource capability. Additionally, all access points maintain a local RADIUS resource.

The local enforcement of user-based policies is configurable. User policies include dynamic VLAN assignment and access restrictions based on time of day. 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 885
- Defining User Pools on page 888
- RADIUS Server Policies on page 892
- RADIUS Deployment Considerations on page 898

Creating RADIUS Groups

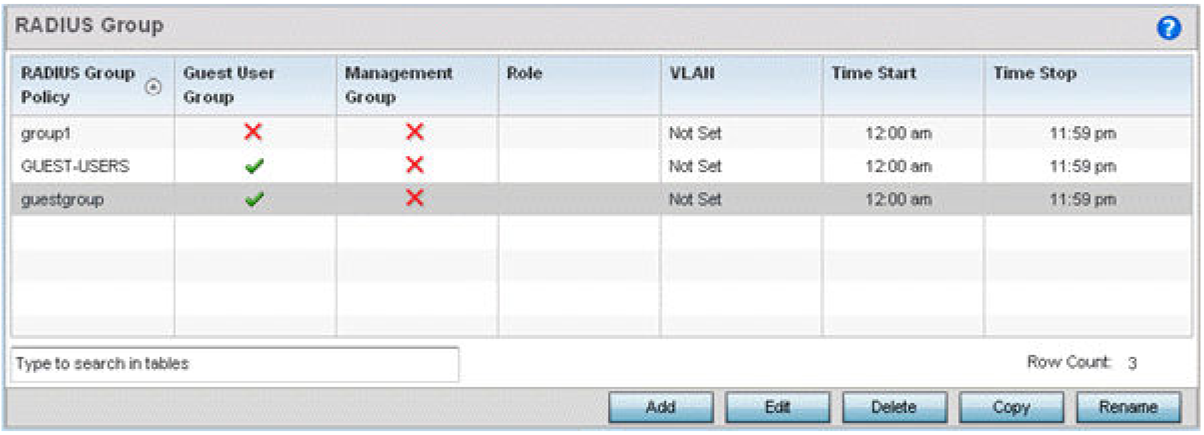
The RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in a local database. The user ID in the received access request is mapped to the specified group for authentication. RADIUS groups allows the enforcement of the following 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.



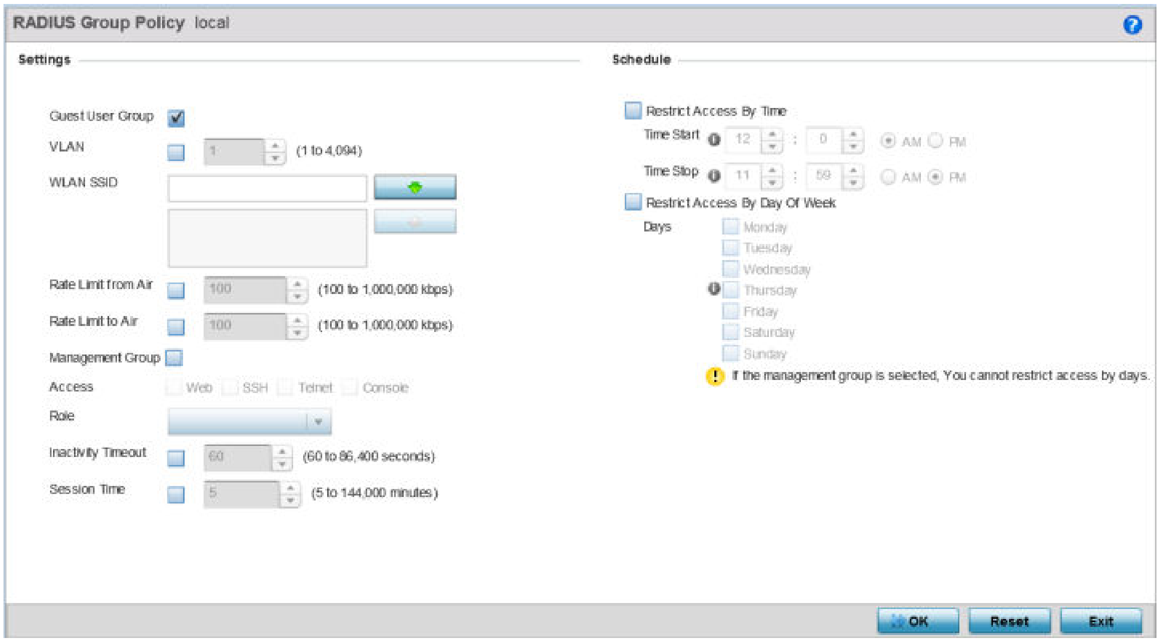
RADIUS Group Policy	Guest User Group	Management Group	Role	VLAN	Time Start	Time Stop
group1	✗	✗		Not Set	12:00 am	11:59 pm
GUEST-USERS	✓	✗		Not Set	12:00 am	11:59 pm
guestgroup	✓	✗		Not Set	12:00 am	11:59 pm

Figure 373: 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: • **`monitor`** - Read-only access • **`helpdesk`** - Helpdesk/support access • **`network-admin`** - Wired and wireless access • **`security-admin`** - Full read/write access • **`system-admin`** - System administrator access
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.



Guest User Group ☑
VLAN ☐ 1 (1 to 4,094)
WLAN SSID
Rate Limit from Air ☐ 100 (100 to 1,000,000 kbps)
Rate Limit to Air ☐ 100 (100 to 1,000,000 kbps)
Management Group ☐
Access ☐ Web ☐ SSH ☐ Telnet ☐ Console
Role
Inactivity Timeout ☐ 60 (60 to 86,400 seconds)
Session Time ☐ 5 (5 to 144,000 minutes)

☐ Restrict Access By Time
Time Start 12 : 0 ● AM ○ PM
Time Stop 11 : 59 ○ AM ● PM
☐ Restrict Access By Day Of Week
Days ☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday
☐ Sunday
If the management group is selected, You cannot restrict access by days.

Figure 374: 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.
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: • **`Web`** - Web access through browser is permitted. • **`SSH`** - SSH access through command line is permitted. • **`Telnet`** - Telnet access through command line is permitted. • **`Console`** - Console access to the device is permitted. The conditions defined within the policy are applied to authentication requests on these interfaces only.
Role	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: • **`monitor`** - Read-only access • **`helpdesk`** - Helpdesk/support access • **`network-admin`** - Wired and wireless access • **`security-admin`** - Full read/write access • **`system-admin`** - System administrator access
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.
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

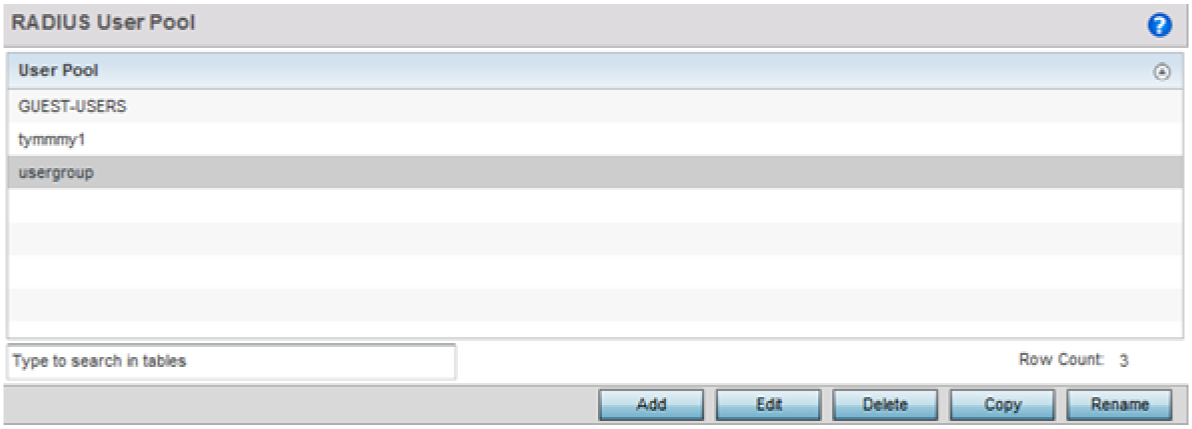
A user pool defines policies for individual user access to local (controller, service platform or Access Point managed) RADIUS resources. User pools are a convenient means of providing RADIUS resources based on the pool's unique permissions (temporary or permanent). A pool can contain a single user or 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.



RADIUS User Pool

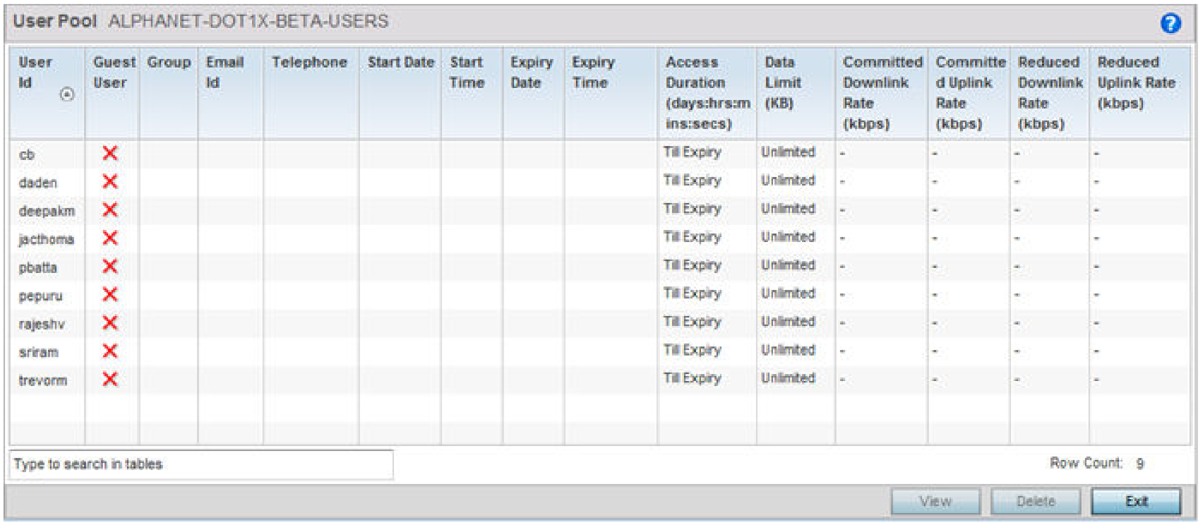
User Pool
GUEST-USERS
tymmmy1
usergroup

Figure 375: 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.



User Pool ALPHANET-DOT1X-BETA-USERS

User Id	Guest User	Group	Email Id	Telephone	Start Date	Start Time	Expiry Date	Expiry Time	Access Duration (days:hrs:mins:secs)	Data Limit (KB)	Committed Downlink Rate (kbps)	Committed Uplink Rate (kbps)	Reduced Downlink Rate (kbps)	Reduced Uplink Rate (kbps)
cb	✗								Till Expiry	Unlimited	-	-	-	-
daden	✗								Till Expiry	Unlimited	-	-	-	-
deepakm	✗								Till Expiry	Unlimited	-	-	-	-
jacthoma	✗								Till Expiry	Unlimited	-	-	-	-
pbatta	✗								Till Expiry	Unlimited	-	-	-	-
pepuru	✗								Till Expiry	Unlimited	-	-	-	-
rajeshv	✗								Till Expiry	Unlimited	-	-	-	-
sriram	✗								Till Expiry	Unlimited	-	-	-	-
trevorm	✗								Till Expiry	Unlimited	-	-	-	-

Figure 376: RADIUS User Pool - User Pools - Details Screen

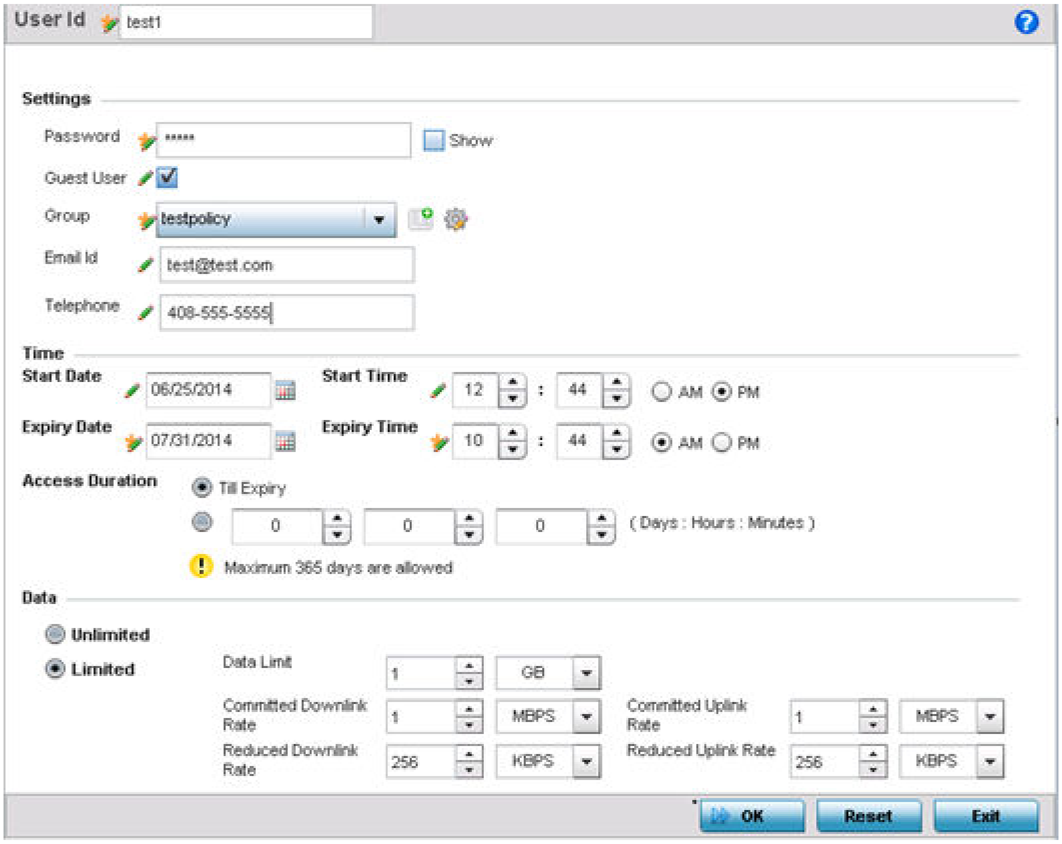
5 Refer to the following **User Pool** configurations.

They define when specific user IDs have access to 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 Email address (in 64 characters or less) of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.
Telephone	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.
Start Date	The month, day and year the listed user ID can access local RADIUS server resources.
Start Time	The time the listed user ID can access local RADIUS server resources. 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 local RADIUS server resources.
Expiry Time	The time the listed user loses access to 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.



User Id: test1

Settings
Password: ***** ☐ Show
Guest User: ☑
Group: testpolicy
Email Id: test@test.com
Telephone: 408-555-5555

Time
Start Date: 06/25/2014 Start Time: 12 : 44 ○ AM ● PM
Expiry Date: 07/31/2014 Expiry Time: 10 : 44 ● AM ○ PM
Access Duration: ● Till Expiry
○ 0 0 0 (Days : Hours : Minutes)
Maximum 365 days are allowed

Data
○ Unlimited
● Limited
Data Limit: 1 GB
Committed Downlink Rate: 1 MBPS Committed Uplink Rate: 1 MBPS
Reduced Downlink Rate: 256 KBPS Reduced Uplink Rate: 256 KBPS

Figure 377: 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.
Email ID	Enter the email address (in 64 characters or less) of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.
Telephone	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.

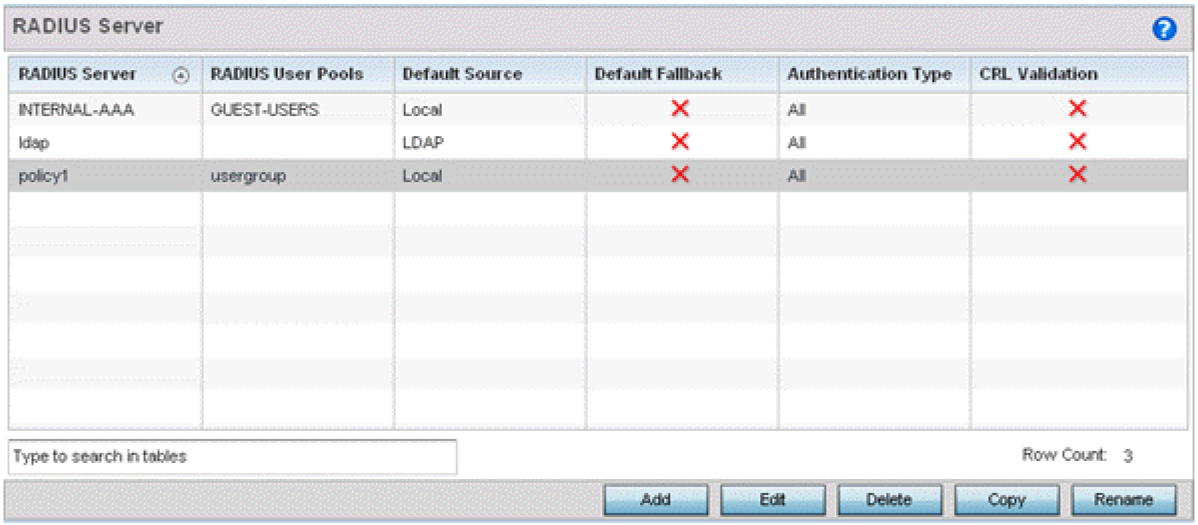
RADIUS Server Policies

A RADIUS server policy is a unique authentication and authorization configuration for client connection requests, authenticating users and returning the configuration information necessary to deliver service to the requesting client and user. The client is the entity with authentication information requiring validation. The controller, service platform or Access Point's local RADIUS server has a database of authentication information used to validate the client's authentication request.

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.

1 Select **RADIUS** → **Server Policy**.

The Server Policy Browser displays. This screen lists existing server policies by group or randomly. A policy can be selected and modified from the browser.



RADIUS Server

RADIUS Server	RADIUS User Pools	Default Source	Default Fallback	Authentication Type	CRL Validation
INTERNAL-AAA	GUEST-USERS	Local	✗	All	✗
ldap		LDAP	✗	All	✗
policy1	usergroup	Local	✗	All	✗

Type to search in tables

Row Count: 3

Figure 378: RADIUS Server Policy Screen

2 Refer to the RADIUS Server screen to review high-level server policy configuration data:

RADIUS Server Policy	Lists the administrator assigned policy name defined upon creation of the server policy.
RADIUS User Pools	Lists the user pools assigned to this server policy. These are the client users who an administrator has assigned to each listed group and who must adhere to its network access requirements before granted access to controller or service platform resources.
Default Source	Displays the RADIUS resource designated for user authentication requests. Options include Local (resident controller or service platform RADIUS server resources) or LDAP (designated remote LDAP resource).
Default Fallback	States whether a fallback is enabled providing a revert back to local RADIUS resources if the designated external LDAP resource were to fail or become unavailable. A green checkmark indicates Default Fallback is enabled. A red “X” indicates it’s disabled. Default Fallback is disabled by default.
Authentication Type	Lists the local EAP authentication scheme used with this policy. The following EAP authentication types are supported by the local RADIUS and remote LDAP servers: • All – Enables both TTLS and PEAP • TLS - Uses TLS as the EAP type • TTLS and MD5 - The EAP type is TTLS with default authentication using MD5 • TTLS and PAP - The EAP type is TTLS with default authentication using PAP • TTLS and MSCHAPv2 - The EAP type is TTLS with default authentication using MSCHAPv2 • PEAP and GTC - The EAP type is PEAP with default authentication using GTC • PEAP and MSCHAPv2 - The EAP type is PEAP with default authentication using MSCHAPv2
CRL Validation	Specifies whether a *Certificate Revocation List* (CRL) check is made. A green checkmark indicates CRL validation is enabled. A red “X” indicates it’s disabled.

3 Select a server policy from the Server Policy Browser to edit or delete.

4 Click **Copy** to copy the settings of a selected (existing) RADIUS server configuration to a new or existing policy.

When selected, a small dialogue displays prompting the administrator to enter the name of policy to copy the existing policy settings to. Enter the name of the RADIUS server policy receiving the existing server policy settings within the **Copy To** field and click **Copy** to initiate the configuration copy operation. This feature streamlines the creation of RADIUS server policies using the attributes of existing server policies.

5 An existing RADIUS server policy can be renamed at any time by selecting it from among the listed policies and clicking **Rename**.

This allows an administrator to simply rename a server policy without having to create (or edit) a new policy with all the same settings.

Configuring RADIUS Clients

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or access point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm to create a 16 octet value which is XORed 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 to be incorrect, and the user is not authenticated.

To define a RADIUS client configuration:

1 Select the Client tab from the RADIUS Server Policy screen.

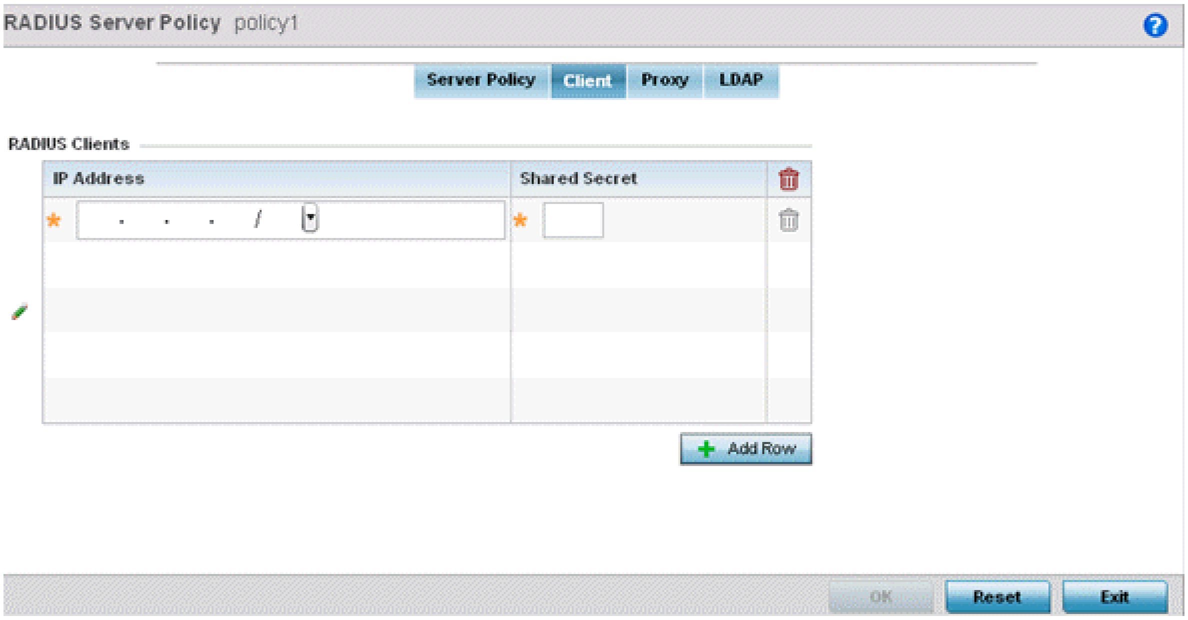


Figure 379: RADIUS Server Policy Screen - Add/Edit - Client Tab

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 a RADIUS Proxy

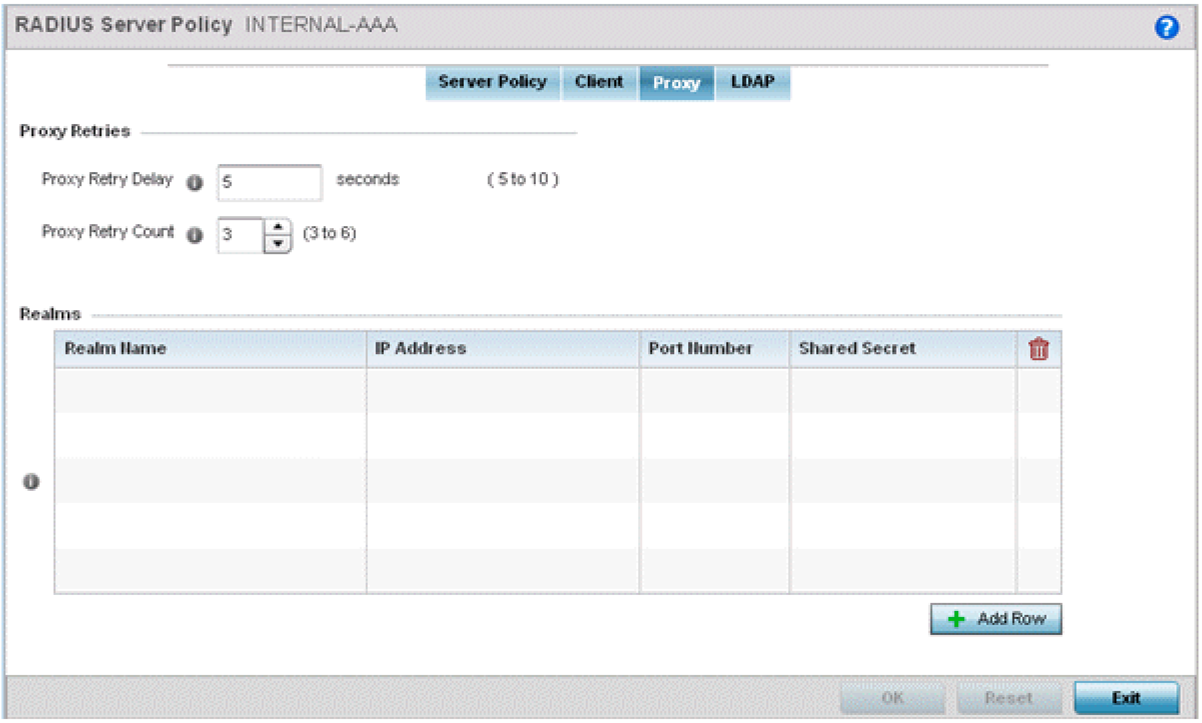
A user's access request is sent to a proxy server if it cannot be authenticated by a controller, service platform or access point's local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, 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 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.

To define a proxy configuration:

1 Select the **Proxy** tab from the RADIUS Server Policy screen.



Proxy Retry Delay: 5

Proxy Retry Count: 3

Figure 380: RADIUS Server Policy Screen - Add/Edit - Proxy Tab

2 Enter the Proxy server retry delay time in the **Proxy Retry Delay** field. Enter 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 server retry count value in the **Proxy Retry Count** field. Set the number of retries (from 3 - 6) sent to 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 entry.

5 Enter the realm name in the **Realm Name** field. The realm name cannot exceed 50 characters. When the RADIUS server receives a request for a user name with a realm, 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 and either accepting or rejecting the request on behalf of the local RADIUS server.

7 In the **Port Number** field, 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 and 65535. The default port is 1812.

8 Enter the RADIUS client shared secret password in the **Shared Secret** field. This password is for authenticating the RADIUS proxy.

Select the **Show** checkbox to expose the shared secret's actual character string, leaving the option unselected displays the shared secret as a string of asterisks (*).

9 Click **OK** to save the changes. Click **Reset** to revert to the last saved configuration.

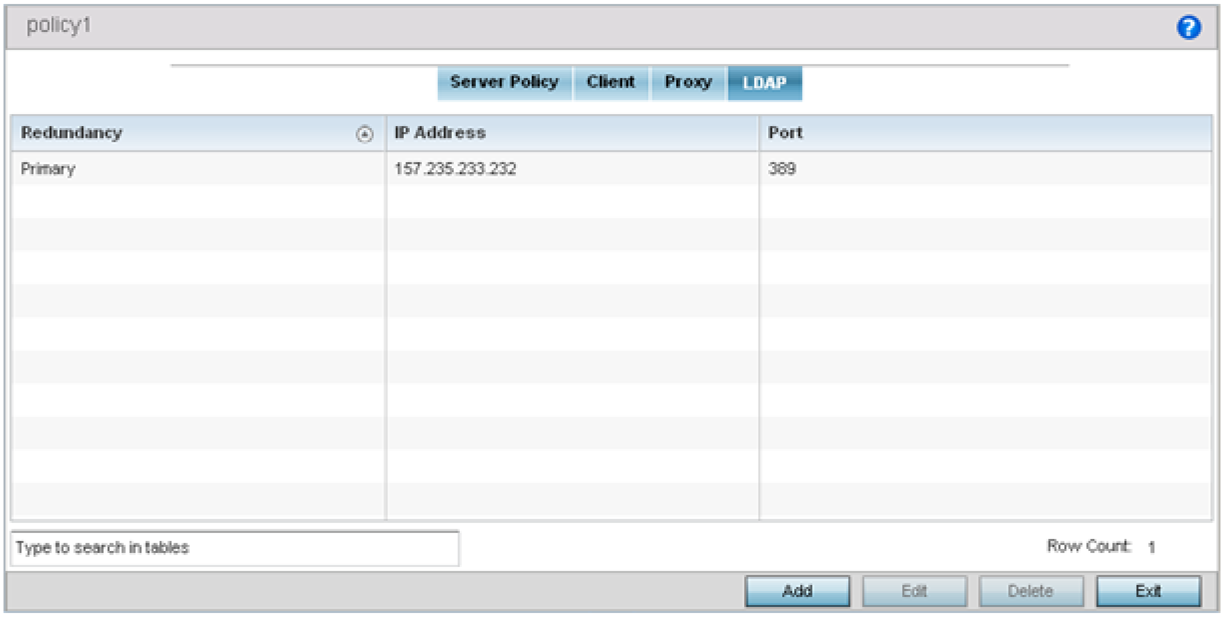
Configuring an LDAP Server Configuration

Administrators have the option of using RADIUS server resources to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative overhead, making the RADIUS authorization process more secure and efficient.

RADIUS is not just a database. It's a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just 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. Local controller, service platform or access point RADIUS resources provide the tools to perform user authentication and authorize users based on complex checks and logic. There's no way to perform such complex authorization checks from a LDAP user database alone.

To configure an LDAP server configuration for use with the RADIUS server:

1 Select the LDAP tab from the RADIUS Server screen.



Redundancy	IP Address	Port
Primary	157.235.233.232	389

Figure 381: RADIUS Server Policy Screen - LDAP Tab

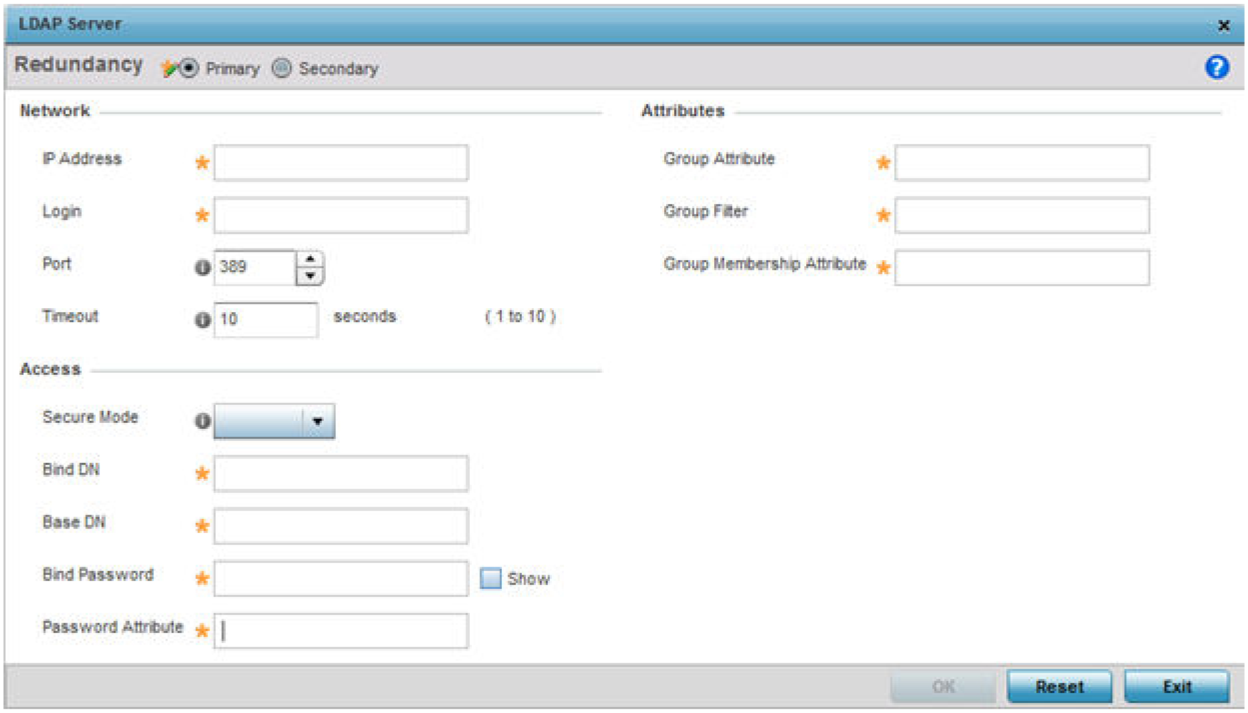
Note

If you are using LDAP for external authentication, PEAP-MSCHAPv2 can be used only if the LDAP server returns the password as plain text. PEAP-MSCHAPv2 is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory Server.

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	Displays 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 were to become unavailable.
IP Address	Displays the IP address of the external LDAP server acting as the data source for the RADIUS server.
Port	Lists the physical port number used by the RADIUS server to secure a connection with the remote LDAP server resource.
Timeout	Lists 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.



Redundancy ● Primary ○ Secondary

Port 389

Timeout 10 seconds (1 to 10)

Bind Password ☐ Show

Figure 382: LDAP Server Add Screen

4 Set the following **Network** address information required for the connection to an external LDAP server resource:

Redundancy	Define 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 were to become unavailable.
IP Address	Set the 128-character maximum IP address or FQDN of the external LDAP server acting as the data source for the RADIUS server.
Login	Define 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.
Timeout	Set an interval from 1 - 10 seconds the local RADIUS server uses as a wait period for a response from the primary or secondary LDAP server. 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	Specify 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. The default port value for start-tls is 389. The default port value for stls-mode is 636.
Bind DN	Specify 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	Specify 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). It identifies an entry distinctly from any other entries that have the same parent.
Bind Password	Enter a valid password for the LDAP server. Select the Show checkbox to expose the password's actual character string, leaving the option unselected displays the password as a string of asterisks (*). The password cannot exceed 32 characters.
Password Attribute	Enter 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	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	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.

RADIUS Deployment Considerations

Before defining the RADIUS server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Each RADIUS client should 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 the 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.

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.

   The upper left-hand side of the user interface displays a Services menu pane where Captive Portal, DHCP Server Policy, RADIUS and Smart Caching configuration options can be selected.
3. Select **URL Lists**.

   The URL Lists screen displays existing policies. New policies can be created. Existing policies can be modified, deleted or copied.

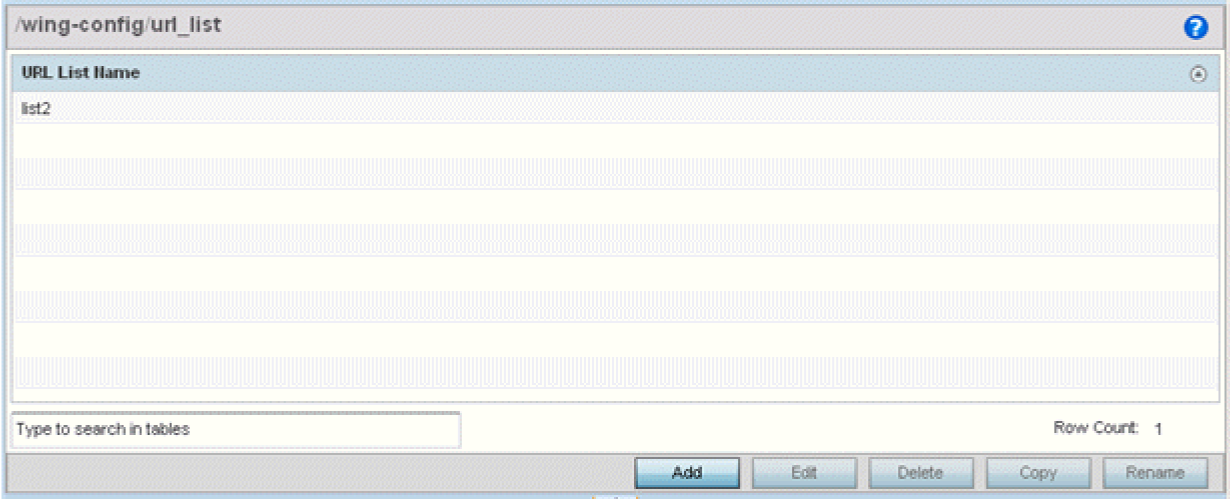


Figure 383: Smart Caching - URL List Name Screen

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.

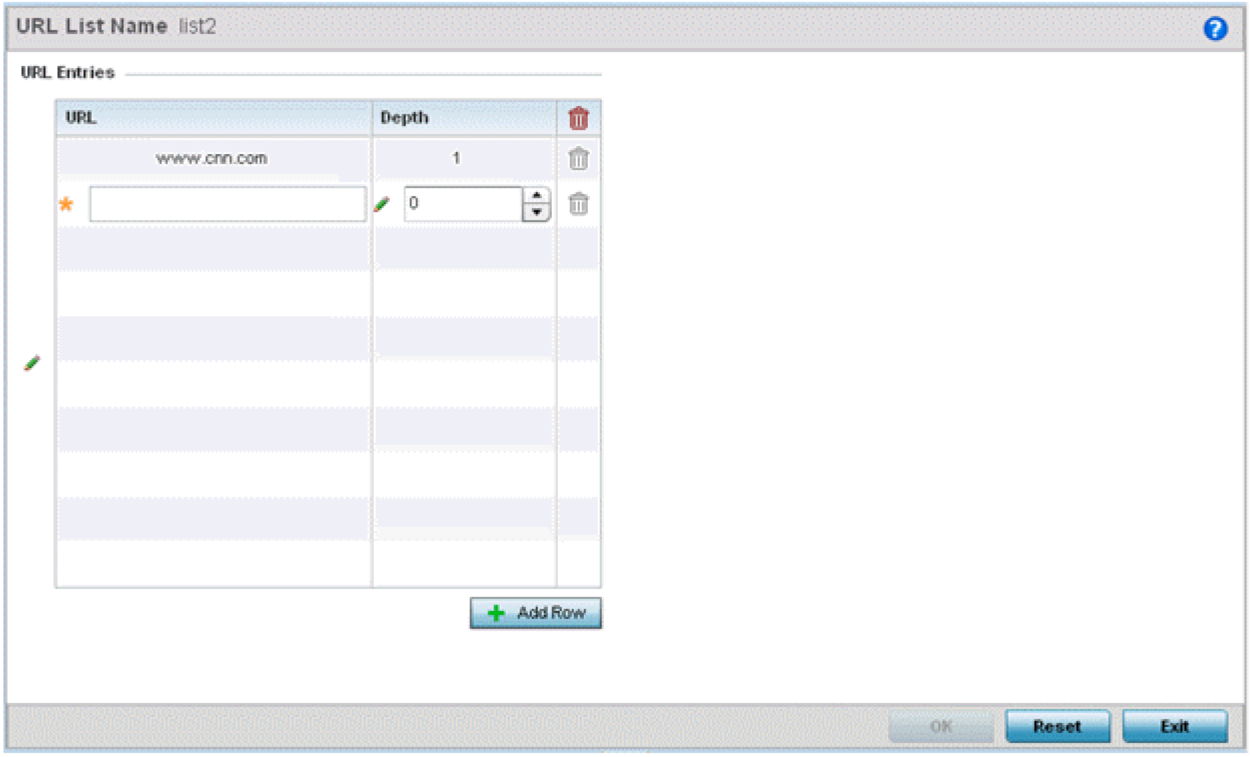


Figure 384: URL List Name - Add/Edit Screen

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.

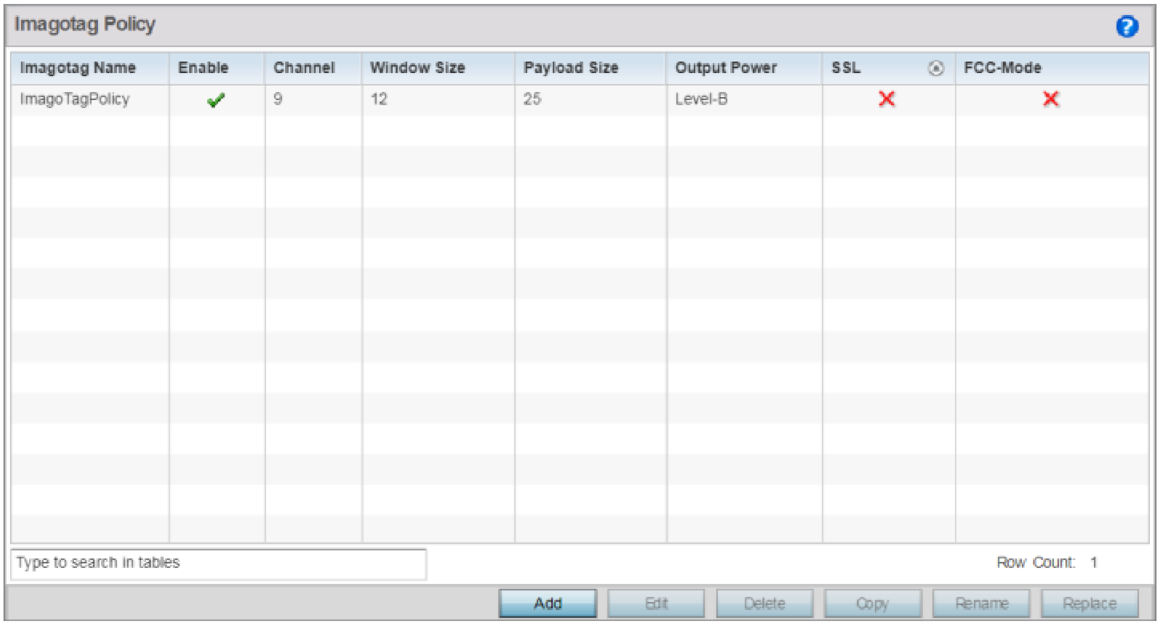
To navigate to the Imagotag Policy screen:

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.



Imagotag Name	Enable	Channel	Window Size	Payload Size	Output Power	SSL	FCC-Mode
ImagoTagPolicy	✓	9	12	25	Level-B	✗	✗

Row Count: 1

Figure 385: 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.

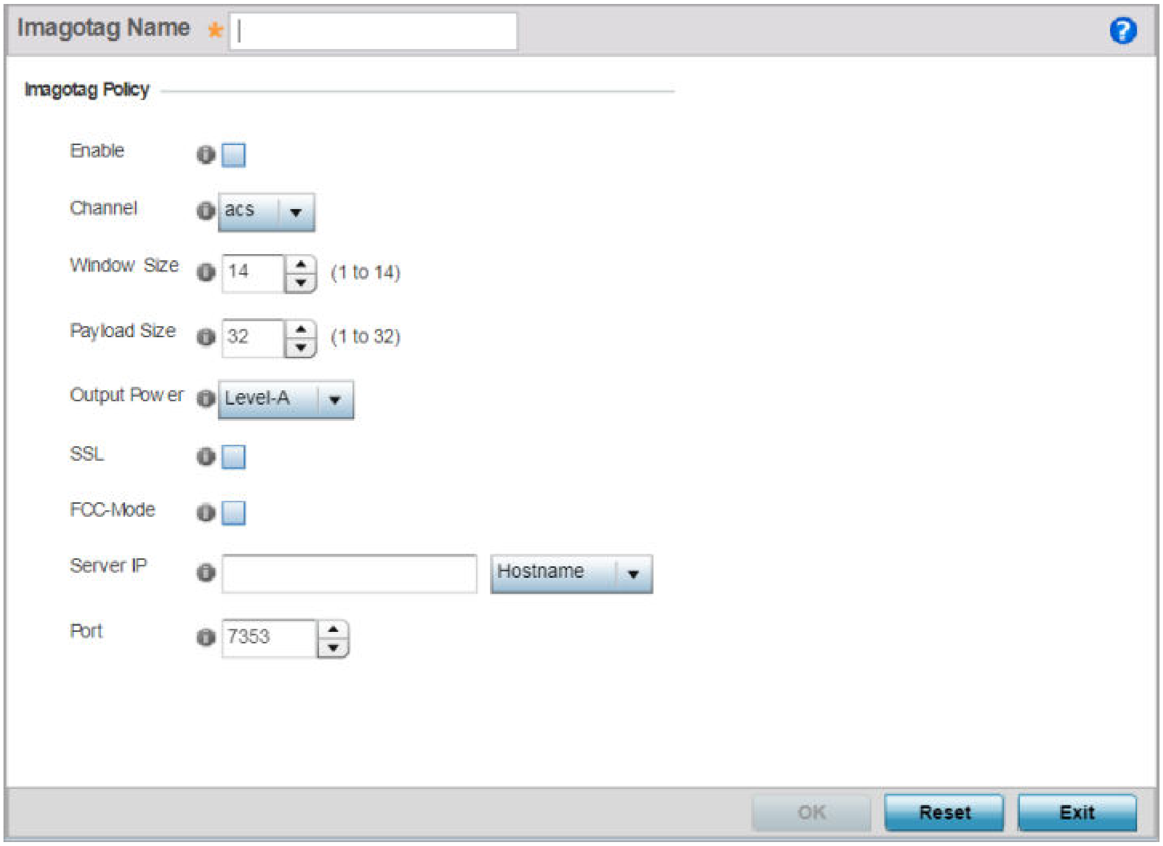

Imagotag Name
Imagotag Policy
Enable ☐
Channel acs
Window Size 14 (1 to 14)
Payload Size 32 (1 to 32)
Output Power Level-A
SSL ☐
FCC-Mode ☐
Server IP Hostname
Port 7353

Figure 386: 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: • ACS *(Auto-Channel Selection)* - Enables auto channel selection mode. This is the default setting. • 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. • 1-14 - Set a value between 1-14 bytes. The default value is 14 bytes. 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. • 1-32 - Specify the value from 1 - 32 bytes. The default setting is 32 bytes. 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: • Level-A – 1 dBm. This is the default setting. • Level-B - -4 dBm • Level-C - -6 dBm • Level-D - -12 dBm • Level-E - 0 dBm • Level-F - -2 dBm • Level-G - -8 dBm • Level-H - -10 dBm 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. 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.

12 Management Access

Viewing Management Access Policies
Adding or Editing a Management Access Policy
EX3500 Management Policies
Configuring a Hierarchical Tree
Management Access Deployment Considerations

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.

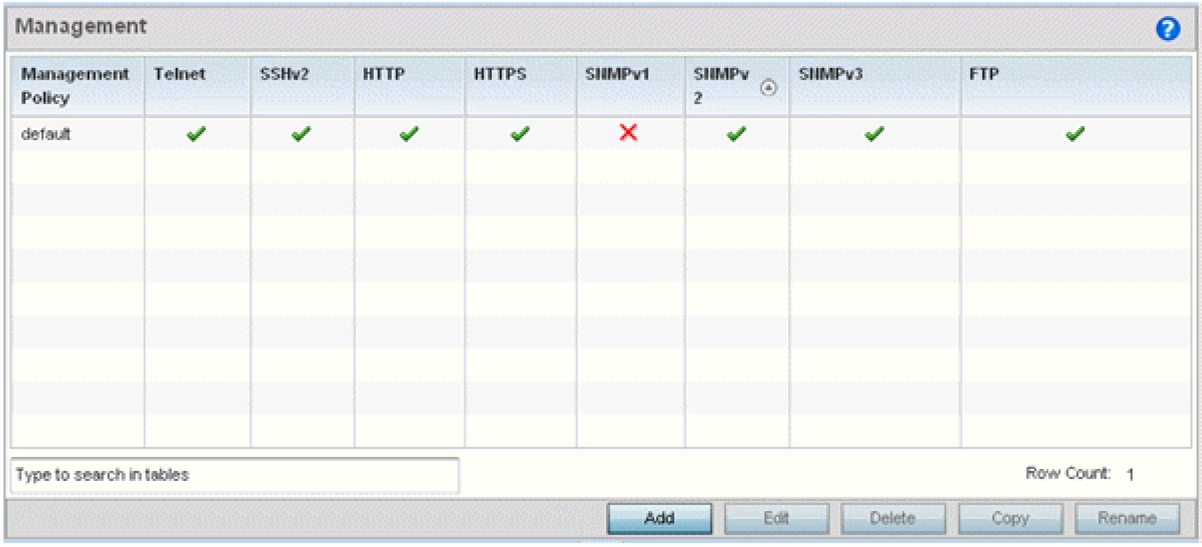
Viewing Management Access Policies

Management Access policies display in the left-hand side of the controller, service platform or access point UI. Existing policies can be updated as management permissions change, or new policies can be added as needed.

To view and modify existing Management Access policies:

1 Go to **Configuration** → **Management** → **Management Policy**.

The Management screen displays by default. This screen lists management policies created thus far and their unique protocol support configurations.



Management Policy	Telnet	SSHv2	HTTP	HTTPS	SNMPv1	SNMPv2	SNMPv3	FTP
default	✓	✓	✓	✓	✗	✓	✓	✓

Row Count: 1

2 Refer to the following Management access policy configurations to determine whether these existing policies can be used as is, require modification or a new policy requires creation:

A green check mark indicates controller, service platform or access point access is allowed using the listed protocol. A red X indicates device access is denied using the listed protocol.

Management Policy	Displays the name of the Management Access policy assigned when initially created. The name cannot be updated when modifying a policy.
Telnet	Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication.
SSHv2	SSH (Secure Shell) version 2, like Telnet, provides a command line interface to a remote host. However, all SSH transmissions are encrypted, increasing their security.
HTTP	HTTP (Hypertext Transfer Protocol) provides access to the device's UI using a Web browser. This protocol is not very secure.
HTTPS	HTTPS (Hypertext Transfer Protocol Secure) provides fairly secure access to the device's GUI using a Web browser. Unlike HTTP, HTTPS uses encryption for transmission, and is therefore more secure.
SNMPv1	SNMP (Simple Network Management Protocol) exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified. SNMP is generally used to monitor a system's performance and other parameters. SNMP v1 is easy to set up, and only requires a plain text. It does not support 64 bit counters, only 32 bit counters, and that provides little security.
SNMPv2	SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk.

SNMPv3	SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
FTP	FTP (File Transfer Protocol) is a standard protocol for files transfers over a TCP/IP network.

3 If it's determined a Management Access policy requires creation or modification, refer to Adding or Editing a Management Access Policy. If necessary, select an existing Management Access policy and select **Delete** to permanently remove it from the list of those available.

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 an Allowed Location Configuration	Use the Allowed Locations tab as means to control a user's access to locations (RF Domains/sites/tree-node paths) within your managed network. Use this option to configure an allowed-locations tag and associate one or more locations with the tag.
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.
Setting T5 PowerBroadband SNMP	Use the T5 PowerBroadband tab set a unique SNMP configuration for T5 controller models.

For deployment considerations and recommendations impacting a controller or service platform’s Management Access policy configuration, refer to Management Access Deployment Considerations on page 942.

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.

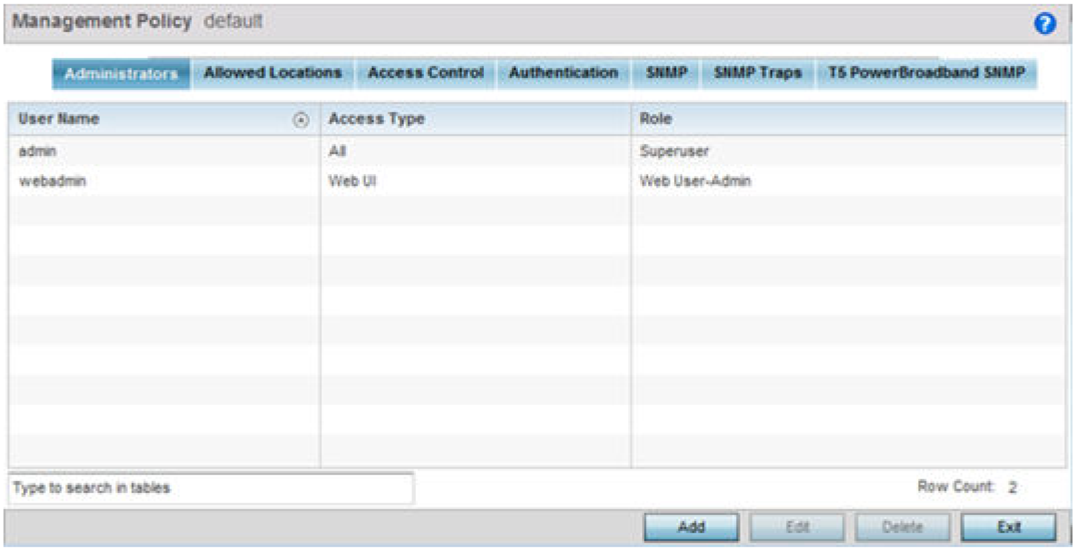
The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller 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.



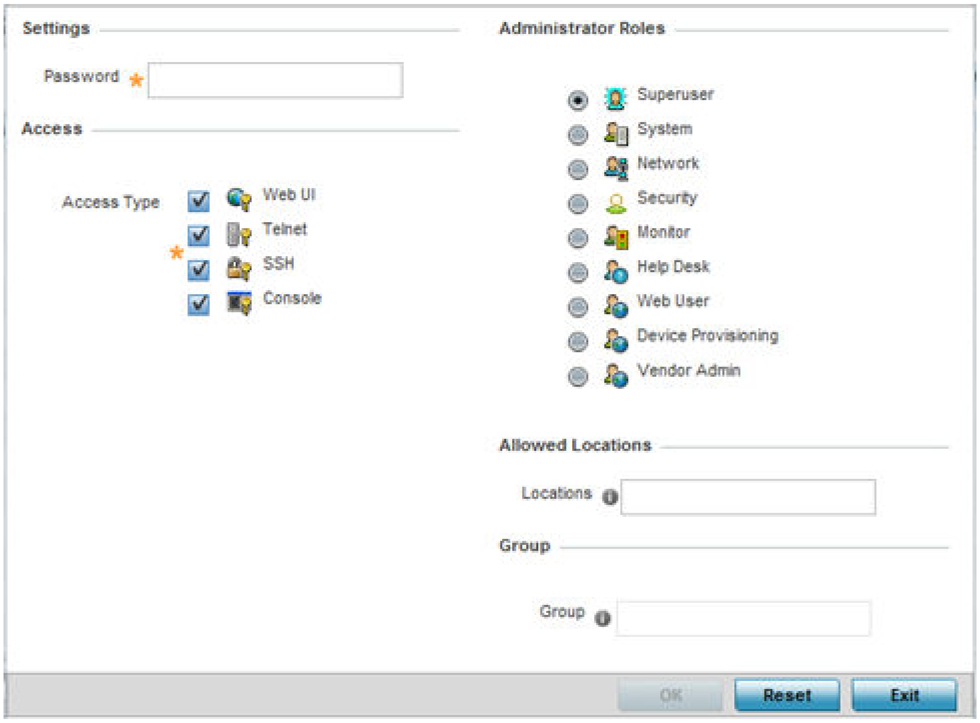
User Name	Access Type	Role
admin	All	Superuser
webadmin	Web UI	Web User-Admin

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.



Access Type ☑ Web UI ☑ Telnet ☑ SSH ☑ Console

Administrator Roles ● Superuser

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. **Note:** 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. **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. **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.

Note

Ensure that the allowed-locations tag is existing and configured. Use the **Allowed Locations** tab to create a tag and map it to locations (RF Domains, sites, tree-node paths, etc.) within your managed network. For more information, see Setting an Allowed Location Configuration on page 911.

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 an Allowed Location Configuration

The **Allowed Locations** option is a means to control a user's access to locations (RF Domains/sites/tree-node paths) within your managed network. Use this option to configure an allowed-locations tag and associate one or more locations with the tag. After you have created an allowed-locations tag, use the **Administrators** screen to apply these tags to users.

Note
The allowed-locations tag is ONLY applicable to the WiNG 'Device Provisioning' user. By applying the allowed-locations tag, the device provisioning user will only be able to provision devices that fall within his/her purview of responsibility.

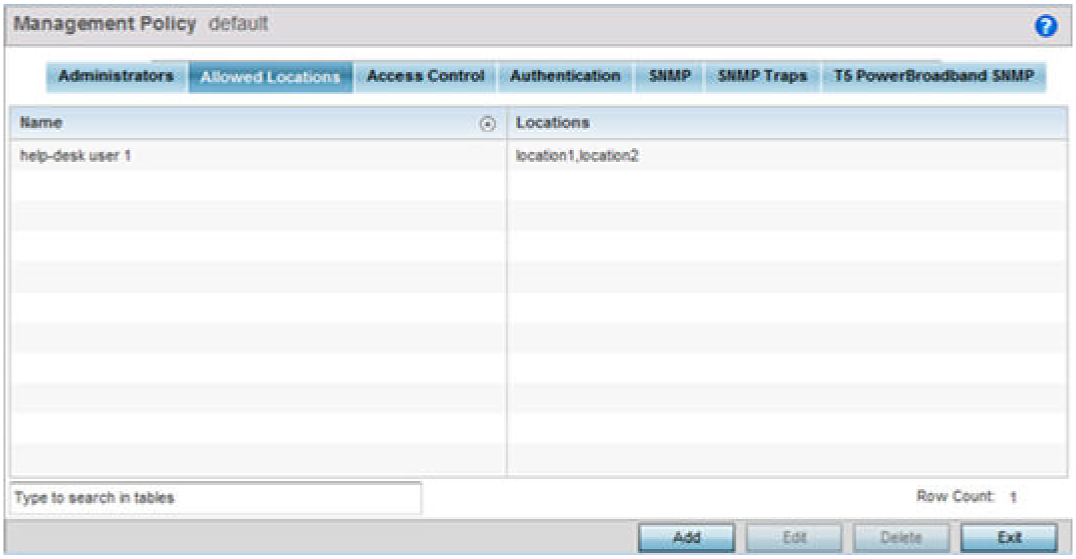
Note
However, if you are an NSight admin and you are using WiNG 5.9.2 and earlier version, you can apply the Allowed Locations tag for all NSight user roles.

Note
For information on user roles and how to configure them, see Creating an Administrator Configuration on page 907.

To set an allowed location configuration:

1 Select the **Allowed Locations** tab.

The **Allowed Location** screen lists existing users and their permitted locations.



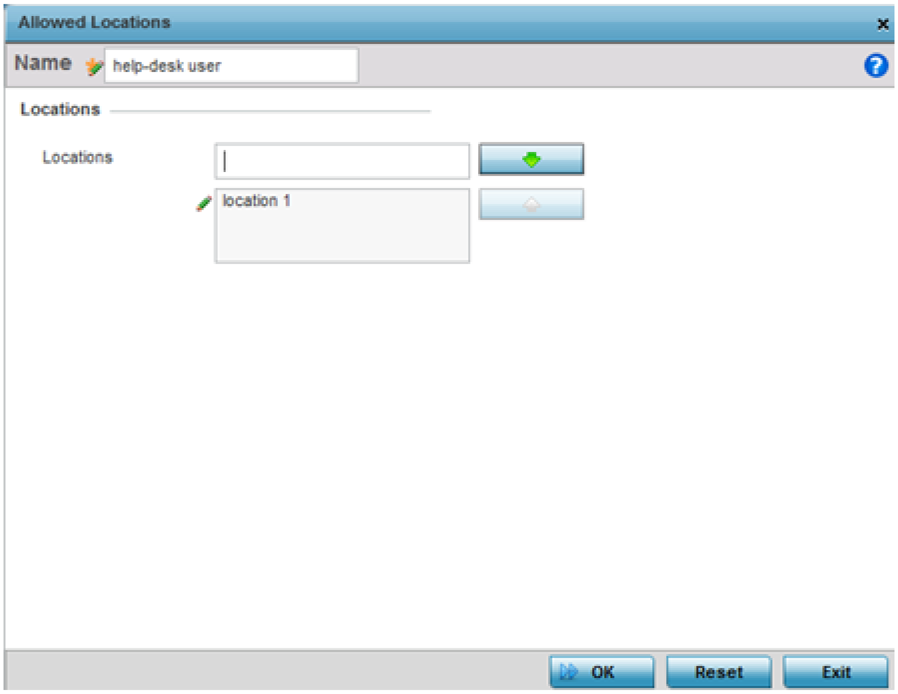
Name	Locations
help-desk user 1	location1,location2

Row Count: 1

2 Review existing allowed location configurations.

3 Select **Add** to create a new allowed location configuration. To modify or delete an existing configuration, select it from the available list and click **Edit** or **Delete**respectively.

The Allowed Locations window displays.



4 Set or modify the following allowed location parameters:

Name	If adding a new Allowed Locations configuration, provide a 32 character maximum name. Provide a name that identifies the associated locations (RF Domain).
Locations	Specify the RF Domain name in the Locations field and use the green, downward navigation arrow to move it below to the list of enabled locations. You can associate a single RF Domain or multiple RF Domains with an Allowed Locations tag. The location can also be specified as a Tree-node Path or multiple Tree-node Paths. Save and exit the screen to enable the locations tags. To remove an enabled location, select it from the enabled list and click the red, upward navigation arrow.

5 Click **OK** to update the allowed location configuration.

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

Setting the Access Control Configuration

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

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.

- *Source hosts* - Management access can be restricted to one or more hosts by specifying their IP addresses
- *Source subnets* - Management access can be restricted to one or more subnets
- *IP ACL* - Management access can be based on the policies defined in an IP based ACL

In the following example, a controller has two IP interfaces defined with VLAN10 hosting management and network services and VLAN70 providing guest services. For security the guest network is separated from all trusted VLANs by a firewall.

Interface	Description	IP Address	Management
VLAN10	Services	Yes	Yes
VLAN70	Guest	Yes	No

By default, management services are accessible on both VLAN10 and VLAN70, and that's not desirable to an administrator. By restricting access to VLAN10, the controller only accepts management sessions on VLAN10. Management access on VLAN70 is longer available.

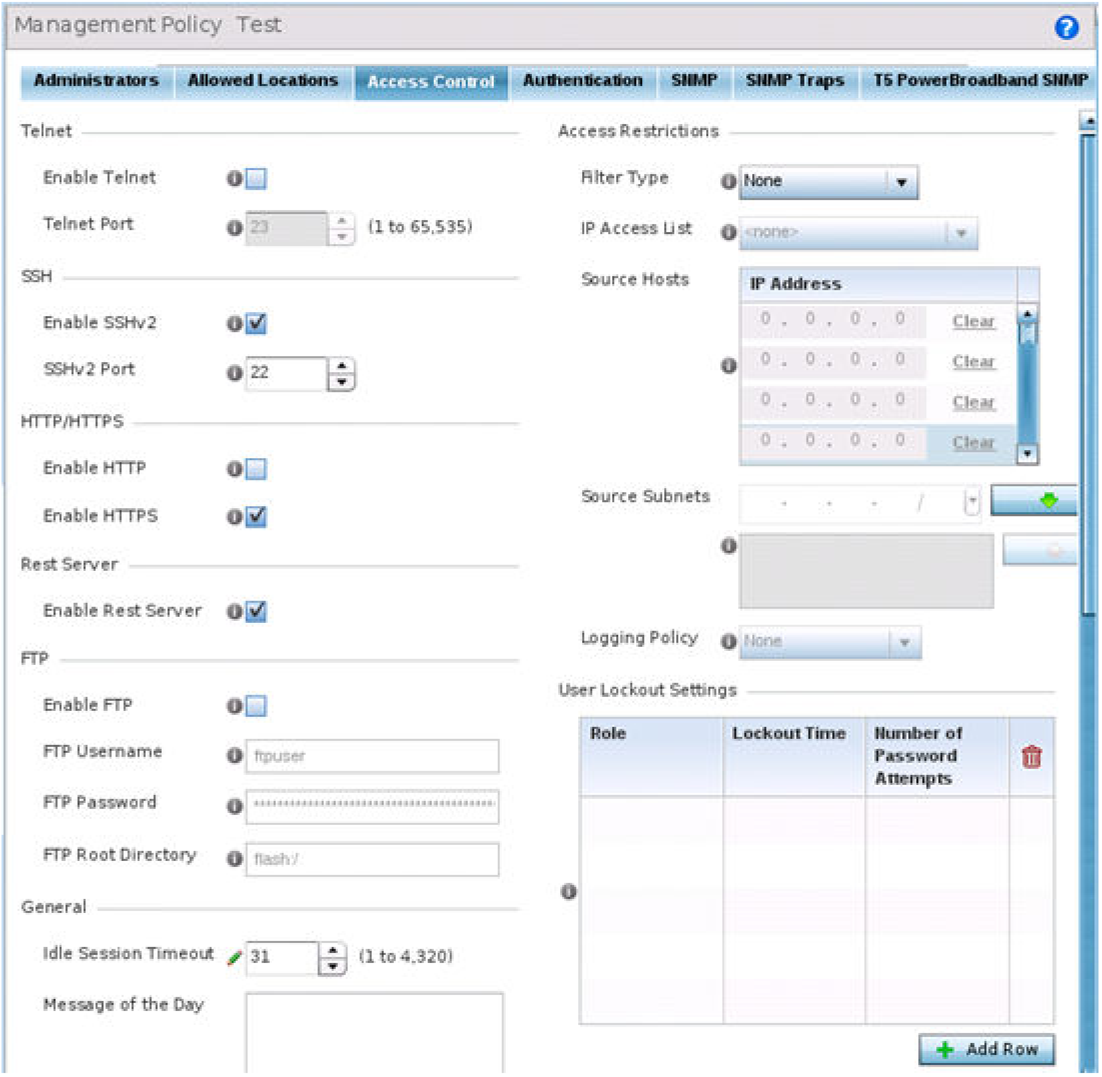
Administrators can secure access to a controller or service platform by disabling less secure interfaces. By default, the CLI, SNMP and FTP disable interfaces that do not support encryption or authentication. However, Web management using HTTP is enabled. Insecure management interfaces such as Telnet, 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.



Telnet

Enable Telnet ☐

Telnet Port 23 (1 to 65,535)

SSH

Enable SSHv2 ☑

SSHv2 Port 22

HTTP/HTTPS

Enable HTTP ☐

Enable HTTPS ☑

Rest Server

Enable Rest Server ☑

FTP

Enable FTP ☐

FTP Username ftpuser

FTP Password ••

FTP Root Directory flash:/

General

Idle Session Timeout 31 (1 to 4,320)

Message of the Day

Access Restrictions

Filter Type None

IP Access List <none>

Source Hosts 0 . 0 . 0 . 0

Source Subnets

Logging Policy None

User Lockout Settings

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 Select the **Enable Rest Server** option, within the Rest Server field, to facilitate device on-boarding. When selected, the REST server allows vendor-specific users access to the online device registration portal. All requests and responses to and from the on-boarding portal are handled by the REST server through restful Application Programming Interface (API) transactions. The REST server serves the Web pages used to associate a device's MAC address with a specific vendor group. This option is enabled by default.

6 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:/

7 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.

8 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.

9 Set the **User Lockout** Settings. Click **Add Row** to configure the following role-based user-account lockout and unlock criteria:

Role	Specify the user-role for which account lockout is to be enabled. The options are: • device-provisioning-admin • helpdesk • monitor • network-admin • security-admin • system-admin • vendor-admin • web-user-admin Note: You can enable account lockout for multiple roles. After specifying the role/roles, set the Lockout Time and Number of Password Attempts. User-account lockout is individually applied to each account within the specified role/roles. For example, consider the 'monitor' role having two users: 'user1' and 'user2'. The Number of Password Attempts and Lockout Time is set at '5' attempts and '10' minutes respectively. In this scenario, user2 makes 5 consecutive, failed login attempts, and the user2 account is locked out for 10 minutes. However, during this lockout time the user1 account remains active.
Lockout Time	Specify the maximum time for which an account remains locked. Specify a value from 0 to 600 minutes. The value '0' indicates that the account is permanently locked.
Number of Password Attempts	Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 to 100.

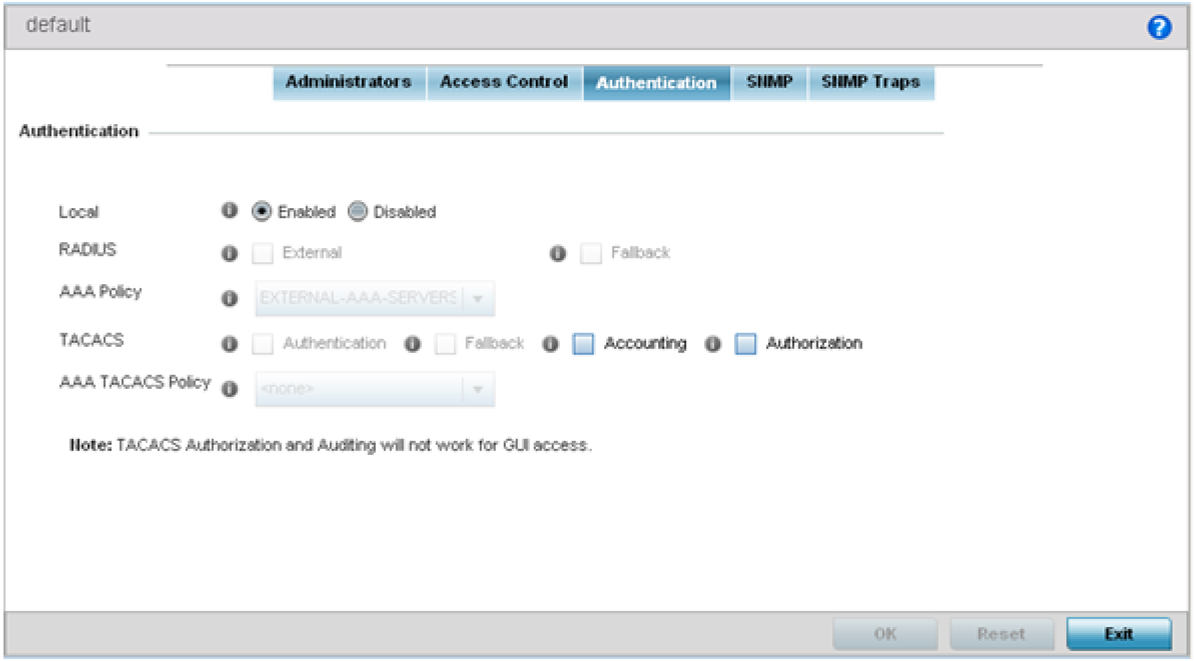
10 Click **OK** to save the Access Control configuration or click **Reset** to revert to the last saved configuration.

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.



Authentication

Local ● Enabled ○ Disabled

RADIUS ☐ External ☐ Fallback

AAA Policy EXTERNAL-AAA-SERVERS

TACACS ☐ Authentication ☐ Fallback ☐ Accounting ☐ Authorization

AAA TACACS Policy <none>

Note: TACACS Authorization and Auditing will not work for GUI access.

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.
AAA Policy	Define the AAA policy used to authenticate user validation requests to the controller or service platform managed network. Select the **`Create`** icon as needed to define a new AAA policy or select the **`Edit`** icon to modify the configuration of an existing policy.
TACACS	If local authentication is disabled, optionally select **`Authentication`** or **`Fallback`** (only one authentication or fallback option can be selected) or **`Accounting`** and **`Authorization`**. TACACS policies control user access to devices and network resources while providing separate accounting, authentication, and authorization services.
AAA TACACS Policy	Select an existing AAA TACACS policy (if available), or select **`Create`** to define a new policy or **`Edit`** to modify an existing one.

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.

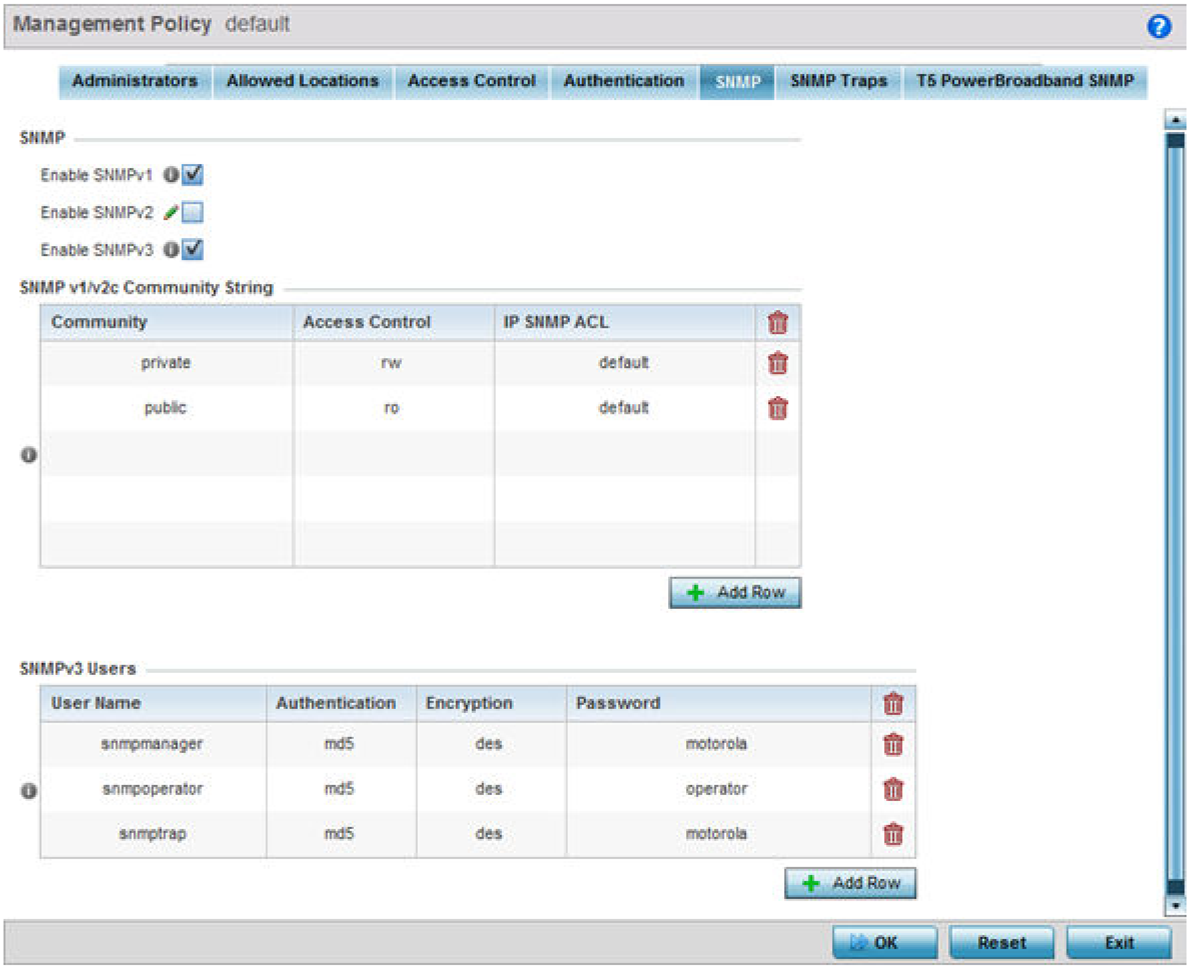
Setting the SNMP Configuration

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.



Management Policy default

SNMP

Enable SNMPv1 ☑

Enable SNMPv2 ☐

Enable SNMPv3 ☑

SNMP v1/v2c Community String

Community	Access Control	IP SNMP ACL
private	rw	default
public	ro	default

SNMPv3 Users

User Name	Authentication	Encryption	Password
snmpmanager	md5	des	motorola
snmpoperator	md5	des	operator
snmptrap	md5	des	motorola

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: • Read Only - Allows a remote device to retrieve information. • 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

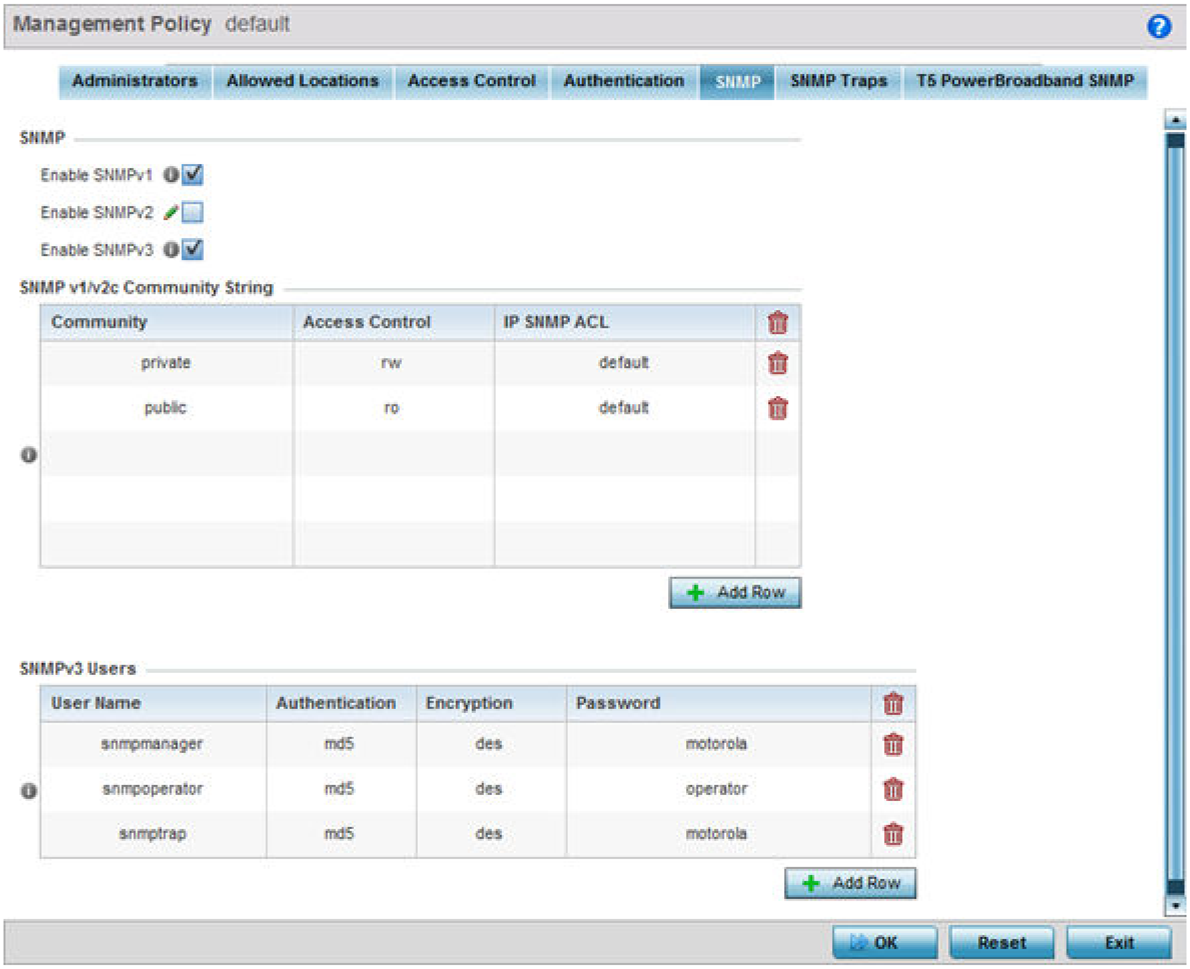
Controller, service platform and access point managed networks use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions), and are an important fault management tool.

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.



Management Policy default

SNMP

Enable SNMPv1 ☑

Enable SNMPv2 ☐

Enable SNMPv3 ☑

SNMP v1/v2c Community String

Community	Access Control	IP SNMP ACL
private	rw	default
public	ro	default

SNMPv3 Users

User Name	Authentication	Encryption	Password
snmpmanager	md5	des	motorola
snmpoperator	md5	des	operator
snmptrap	md5	des	motorola

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`**.

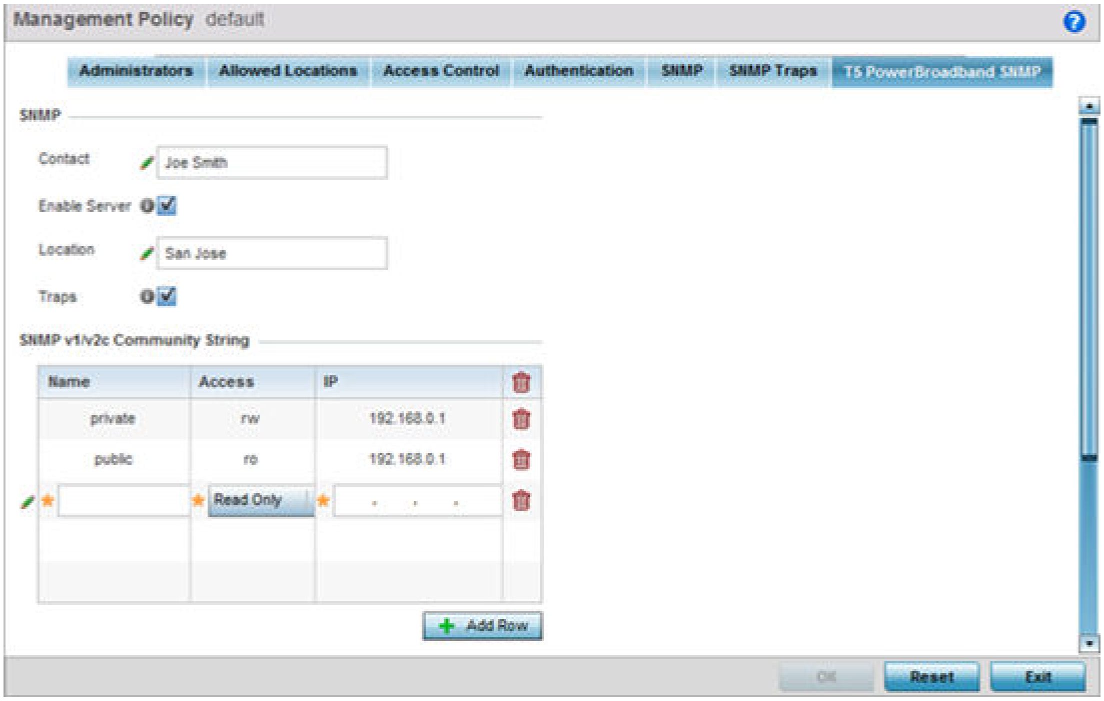
4 Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

Setting T5 PowerBroadband SNMP Configuration

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

To define a T5 controller power broadband SNMP configuration:

1 Select the T5 Power Broadband tab.



SNMP

Contact: Joe Smith

Enable Server ☑

Location: San Jose

Traps ☑

SNMP v1/v2c Community String

Name	Access	IP
private	rw	192.168.0.1
public	ro	192.168.0.1
	Read Only	. . .

2 Set the following SNMP settings:

Contact	Set a 64 character maximum contact name for the administration of T5 controller SNMP events.
Enable Server	Select this option to enable SNMP event management for the T5 controller. This setting is disabled by default.
Location	Set a 64 character maximum location for the SNMP resource dedicated to T5 controller support.
Traps	Select this option for SNMP trap support for the T5 controller. 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.

3 Set the SNMP v1/v2c Community String configuration for T5 controller usage. 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	Set a 32 character maximum SNMP community string.
Access	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: Read Only - Allows a remote device to retrieve information. Read-Write - Allows a remote device to modify settings.
IP	Set the IP address of the SNMP manager.

4 Use the **Host** table to define up to 4 SNMP receiver resource IP addresses.

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

EX3500 Management Policies

The EX3500 series switch is a Gigabit Ethernet Layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four Small Form Factor Pluggable (SFP) transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. Each EX3500 series switch includes an SNMP-based management agent, which provides both in-band and out-of-band access for management. An EX3500 series switch utilizes an embedded HTTP Web agent and command line interface (CLI) somewhat different from the WiNG operating system, while still enabling the EX3500 series switch to provide WiNG controllers PoE and port management resources.

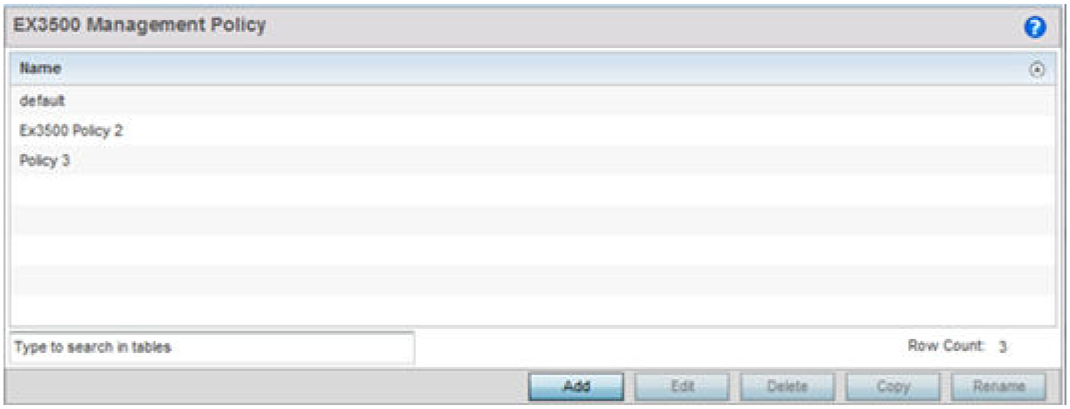
Going forward NX9600, NX9500, NX7500, NX5500 WiNG managed services platforms and WiNG VMs can discover, adopt and partially manage EX3500 series Ethernet switches, as DHCP option 193 has been added to support external device adoption. DHCP option 193 is a simplified form of DHCP options 191 and 192 used by WiNG devices currently. DHCP option 193 supports pool1, hello-interval and adjacency-hold-time parameters.

Note
WiNG can partially manage an EX3500 without using DHCP option 193. In this case the EX3500 must be directly configured to specify the IPv4 addresses of potential WiNG adopters, using the EX3500 controller host ip address CLI command.

WiNG service platforms leave the proprietary operating system running the EX3500 switches unmodified, and partially manage them utilizing standardized WiNG interfaces. WiNG service platforms use a translation layer to communicate with EX3500 series switches.

To set EX3500 management settings for user EX3500 user group creation, authentication, password management and SNMP:

Go to **Configuration** > **Management** > **EX3500 Management Policy**.



The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify the attributes of a policy or **Delete** to remove an obsolete list from those available. Existing lists can be copied or renamed as needed.

For more information, refer to the following:

- EX3500 User Groups on page 925
- EX3500 Authentication on page 927
- EX3500 Exec Password Management on page 928
- EX3500 System Settings on page 930
- EX3500 SNMP Management on page 931

EX3500 User Groups

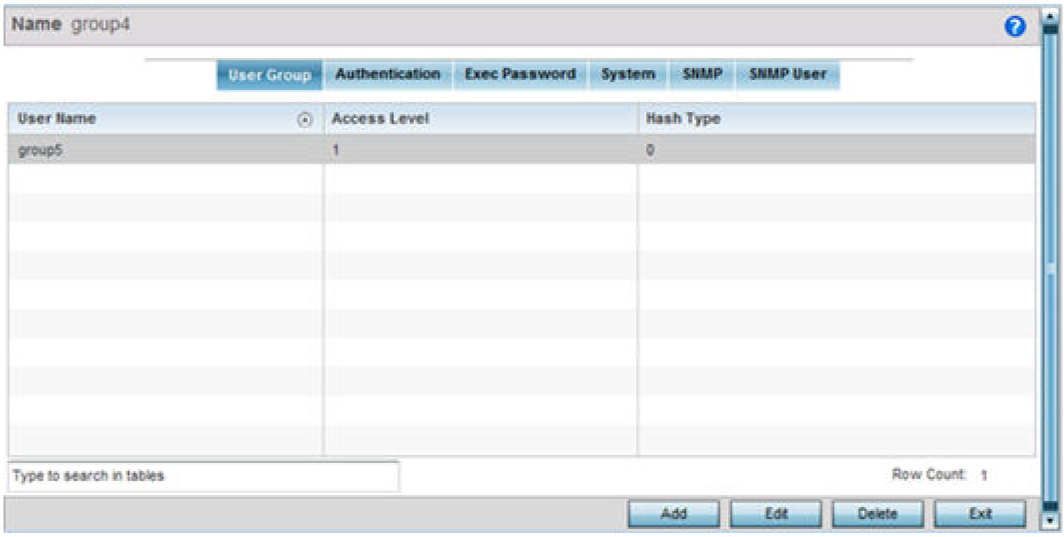
EX3500 switch user groups are stored in a local database on the WiNG service platform. Each user group can be assigned unique access levels and passswords to provide administrative priority.

To set an EX3500 user group configuration:

1. Go to **Configuration** > **Management** > **EX3500 Management Policy**.

   The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

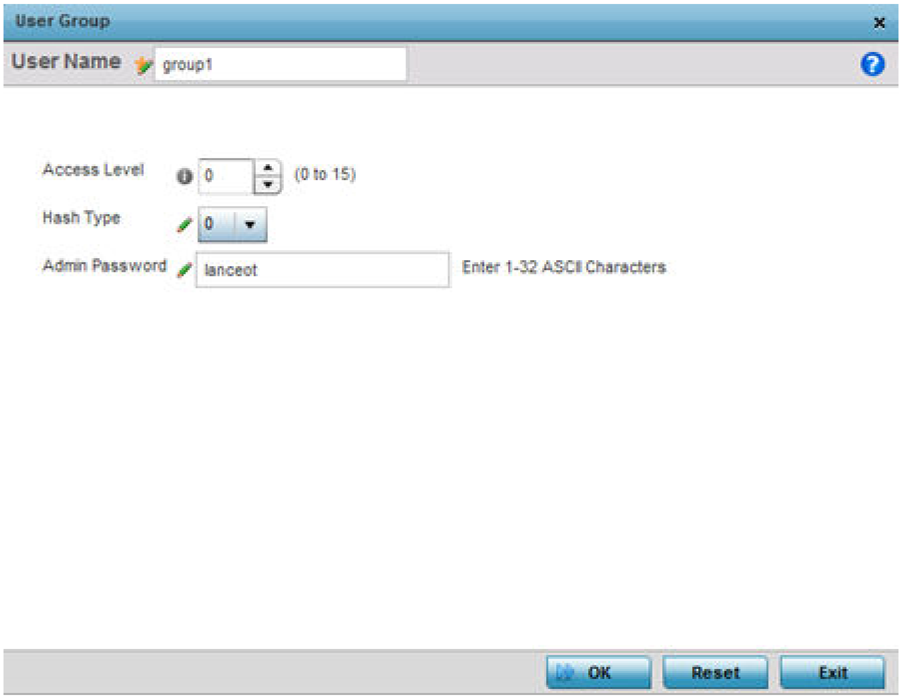
2 If creating a new EX35000 user group, assign it a **Name** up to 32 characters. Select **Continue**.



Name group4

User Name	Access Level	Hash Type
group5	1	0

3 Select **Add** to create a new EX3500 user group, **Edit** to modify an existing group or **Delete** to remove an obsolete group. Set the following User Group attributes:



User Name group1

Access Level 0 (0 to 15)

Hash Type 0

Admin Password lanceot Enter 1-32 ASCII Characters

Access Level	Use the spinner control to set an access level from 0 - 15 serving as the access priority of each user group requesting access and interoperability with an EX3500 switch. Access level 0 corresponds to a guest user with minimal access to commands while access level 15 corresponds to an administrator user with full access to all commands.
Hash Type	Select either 0 or 7 to define the hash in plain text (0) or encrypted characters (7).
Admin Password	Create a 32 character maximum password for the EX3500 user group.

4 Select **OK** when completed to update the EX3500 user group configuration. Select **Reset** to revert the screen back to its last saved configuration.

EX3500 Authentication

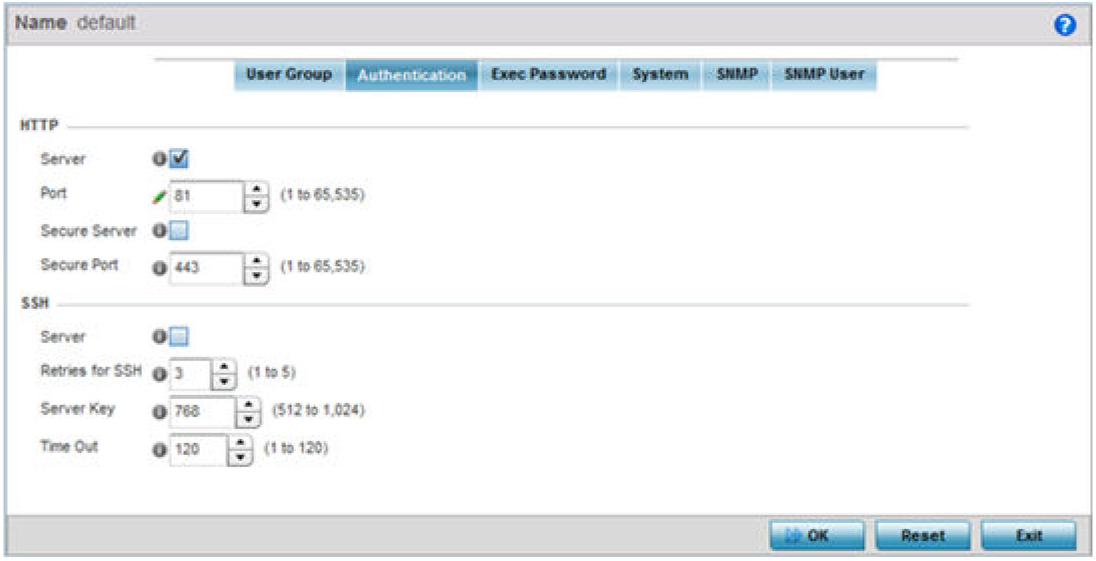
Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

To authenticate an EX3500 management policy:

1 Go to **Configuration** > **Management** > **EX3500 Management Policy**.

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

2 Select the Authentication tab.



Name default

HTTP

Server ☑

Port 81 (1 to 65,535)

Secure Server ☐

Secure Port 443 (1 to 65,535)

SSH

Server ☐

Retries for SSH 3 (1 to 5)

Server Key 768 (512 to 1,024)

Time Out 120 (1 to 120)

3 Select the following HTTP server settings to authenticating a HTTP connection to an EX3500:

Server	When selected, access the EX3500 using HTTP from any Windows PC, Linux PC or other device that uses HTTP. This setting is enabled by default.
Port	Set the HTTP port number from 1 - 65,535. The default port is 80.
Secure Server	Select this option to secure HTTP over a designated secure port.
Secure Port	Use the spinner control to select a secure port from 1 - 65, 535.

4 Select the following **SSH** server settings to authenticate a SSH connection to an EX3500:

Server	When selected, access the EX3500 using SSH from any Windows PC, Linux PC or other device that uses SSH. This setting is enabled by default.
Retries for SSH	Set the maximum number of retries, from 1 - 5, for connection to the SSH server resource. The default setting is 3.
Server Key	Set the SSH server key length from 512 - 1,024. The default length is 768.
Time Out	Set the inactivity timeout for the SSH server resource from 1 - 120 seconds. When this setting is exceeded, the SSH server resource becomes unreachable and must be reauthenticated. The default value is 120 seconds.

5 Select **OK** when completed to update the EX3500 authentication configuration. Select **Reset** to revert the screen back to its last saved configuration.

EX3500 Exec Password Management

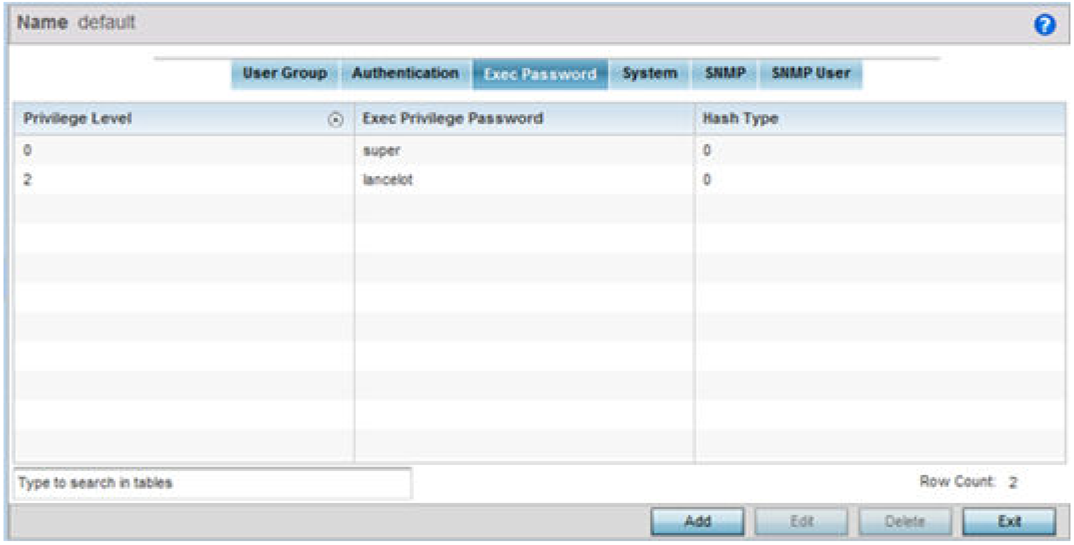
Each EX3500 management policy can have a unique exec password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

To administrate EX3500 management passwords and their privileges:

1 Go to **Configuration** > **Management** > **EX3500 Management Policy**.

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

2 Select the Exec Password tab.

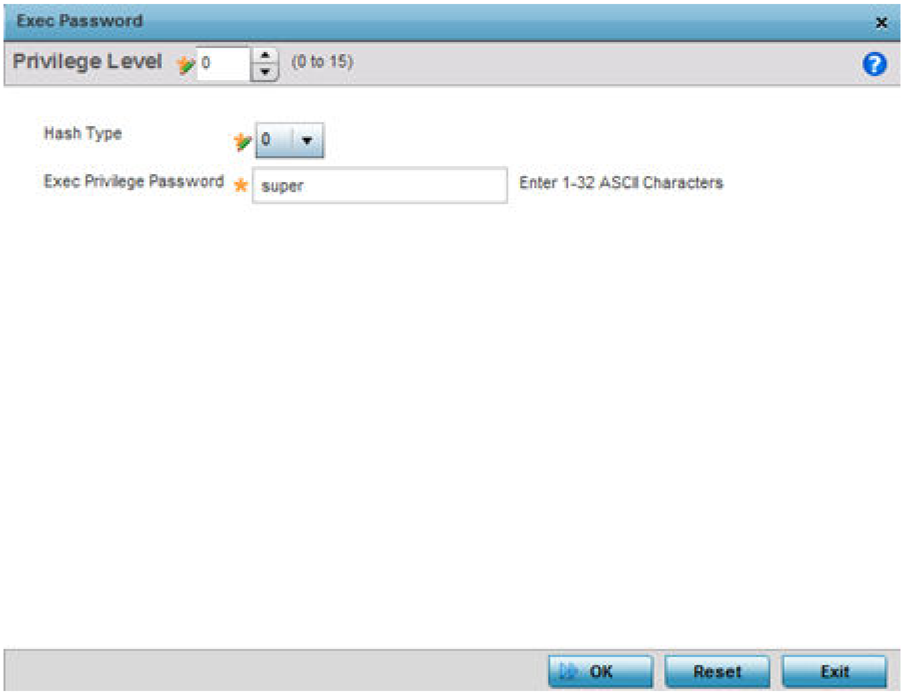


Name default

Privilege Level	Exec Privilege Password	Hash Type
0	super	0
2	lancelot	0

Row Count: 2

3 Select **Add** to create a new EX3500 exec password, **Edit** to modify an existing password configuration or **Delete** to remove an obsolete password.



Privilege Level 0 (0 to 15)

Hash Type 0

Exec Privilege Password super Enter 1-32 ASCII Characters

4 Assign a privilege level from 0 - 15. 0 provides the least access, while level 15 provides the most access. The commands available at each level vary.

5 Select the following Exec Password settings:

Hash Type	Select either 0 or 7 to define the hash in plain text (0) or encrypted characters (7).
Exec Privilege Password	Create a 32 character maximum password for the EX3500 exec password.

6 Select **OK** when completed to update the EX3500 exec password. Select **Reset** to revert the screen back to its last saved configuration.

EX3500 System Settings

An EX3500 management policy can be customized to include high and low alarm thresholds for EX3500 memory and CPU utilization.

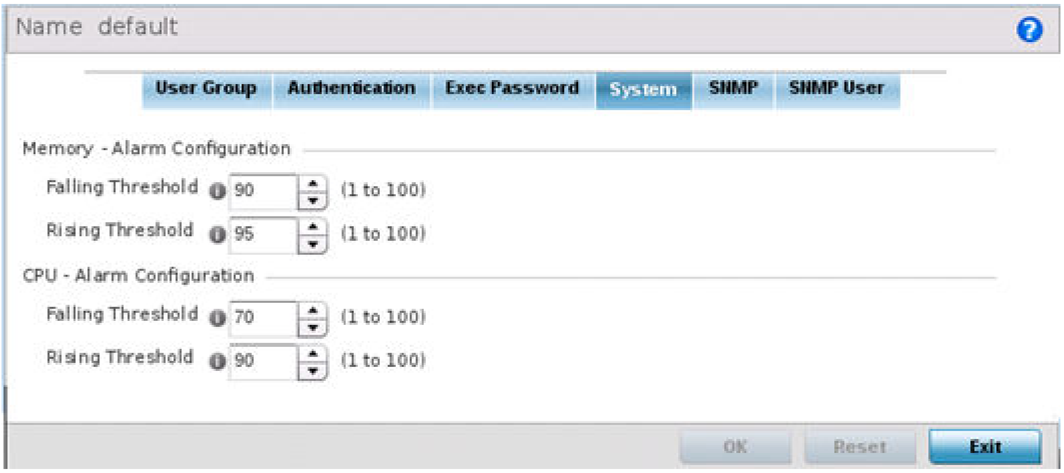
The Memory and CPU rising and falling thresholds control when the EX3500 generates SNMP traps if these thresholds are exceeded. A trap is generated when the utilization exceeds the rising threshold, and another trap is generated after the utilization drops below the falling threshold. These thresholds do not protect the resource, they provide notification of an excessive use of the resource.

To administrate EX3500 management policy memory and CPU threshold settings:

1 Go to **Configuration** > **Management** > **EX3500 Management Policy**.

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

2 Select the System tab.



Memory - Alarm Configuration

Falling Threshold 90 (1 to 100)

Rising Threshold 95 (1 to 100)

CPU - Alarm Configuration

Falling Threshold 70 (1 to 100)

Rising Threshold 90 (1 to 100)

3 Set the following Memory - Alarm Configuration threshold settings:

Falling Threshold	Set the threshold for clearing the EX3500 memory utilization alarm. Once the rising threshold is exceeded, the memory utilization must drop below this threshold for the alarm to clear. The threshold is set as a percentage from 1 - 100, with a default of 90.
Rising Threshold	Set the threshold for EX3500 memory utilization as too high. The threshold is set as a percentage from 1 - 100, with a default of 95.

4 Set the following CPU - Alarm Configuration threshold settings:

Falling Threshold	Set the threshold for clearing the EX3500 CPU (processor) utilization alarm. Once the rising threshold is exceeded, the CPU (processor) utilization must drop below this threshold for the alarm to clear. The threshold is set as a percentage from 1 - 100, with a default of 70.
Rising Threshold	Set the notification threshold for EX3500 CPU (processor) utilization as too high. The threshold is set as a percentage from 1 - 100, with a default of 90.

5 Select **OK** when completed to update the EX3500 system threshold settings. Select **Reset** to revert the screen back to its last saved configuration.

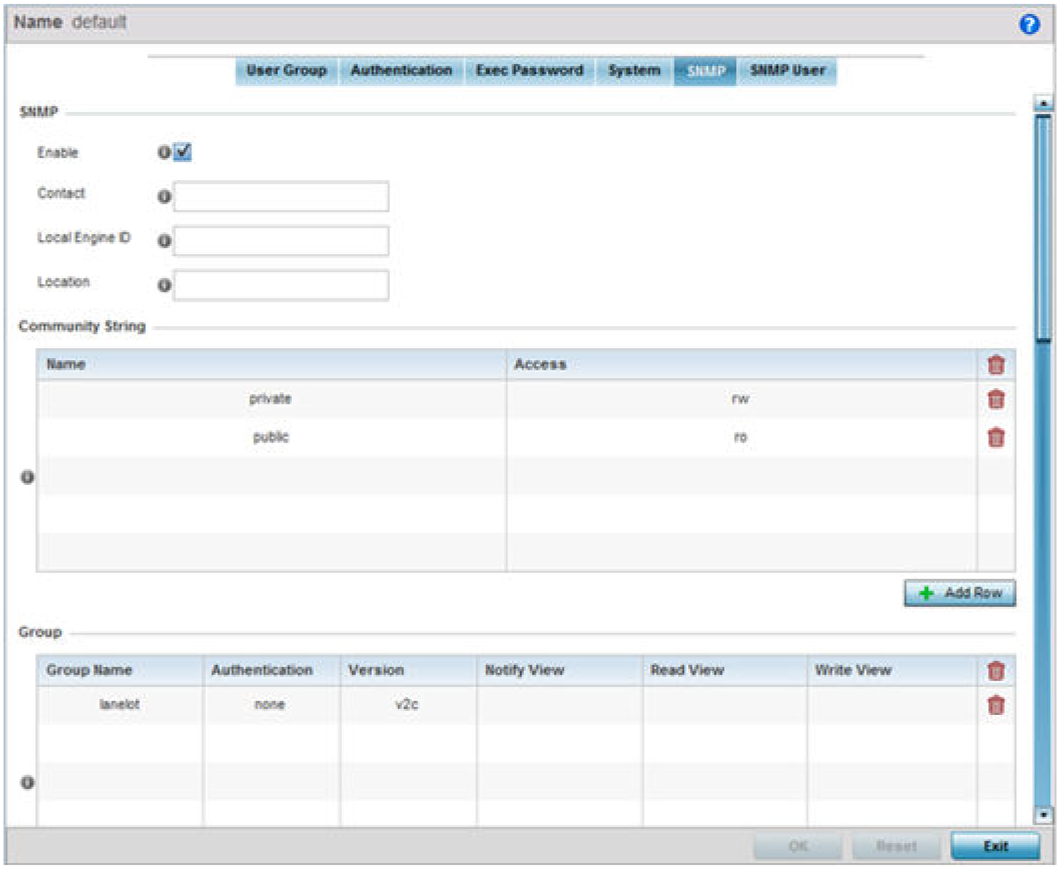
EX3500 SNMP Management

Optionally use the Simple Network Management Protocol (SNMP) with the EX3500 management policy for statistics gathering, or to fully manage the EX3500. SNMP is an application layer protocol that facilitates the exchange of management information between the controller or service platform and a managed device. SNMP enabled devices listen on port 161 (by default) for SNMP packets from the controller or service platform's 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.

1 Go to **Configuration** > **Management** > **EX3500 Management Policy**.

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

2 Select the **SNMP** tab.



Name default

SNMP

Enable ☑

Contact

Local Engine ID

Location

Community String

Name	Access
private	rw
public	ro

Group

Group Name	Authentication	Version	Notify View	Read View	Write View
lanelot	none	v2c			

3 Set the following **SNMP** settings:

Enable	Select the checkbox to enable SNMPv1, SNMPv2 or SNMPv3 support. The SNMP version utilized is selected and mapped to a user group within the Group table.
Contact	Define a 255 character maximum SNMP contact name for responsible for the WiNG administration of the EX3500 switch.
Local Engine ID	Set a 64 character maximum local engine ID. The local engine ID is the administratively unique identifier of an SNMPv3 engine used for identification, not addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411.
Location	Assign a 255 character maximum EX3500 switch location reflecting the switch's physical deployment location.

4 Select **+ Add Row** and set the following **Community Strings**:

Name	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	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: Read Only - Allows a remote device to retrieve information. Read-Write - Allows a remote device to modify settings.

5 Select + Add Row and set the following **Group** settings for SNMP management of the EX3500:

Group Name	Define a 32 character maximum name for this SNMP group. A maximum of 17 groups can be set for EX3500 model switches.
Authentication	If utilizing SNMPv3 as the version for this group, select whether auth, noauth or priv is applied to this group as a credential exchange and validation mechanism. This setting is not enabled if utilizing either SNMPv1 or SNMPv2.
Version	Apply either SNMPv1, SNMPv2 or SNMPv3 to this EX3500 SNMP group. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
Notify View	Set a 32 character maximum notify string to restrict and filter the objects in the notification.
Read View	Set an optional 32 character maximum string indicating that users who belong to this group have read access to the EX3500 switch.
Write View	Set an optional 32 character maximum string indicating that users who belong to this group have write access to the EX3500 switch.

6 Set the following SNMP Traps for SNMP event management of the EX3500:

Authentication	Select the checkbox to enable trap generation for user authentication events when accessing a EX3500 switch from a WiNG managed controller. This feature is disabled by default.
Enable SNMP Trap	Select the checkbox to enable EX3500 MAC generation traps. When enabled a trap is generated when a dynamic MAC address is added or removed to/from the switch's address table. This feature is disabled by default.
Link Up Down	Select this option to generate a trap a when either a link is established or broken between the EX3500 switch and a connected device (WiNG managed or not).

7 Refer to the SNMP View table and select **+ Add Row** to include or exclude up to 31 SNMP views.

View Name	Enter a 32 alphanumeric character maximum name to identify the EX3500 SNMP MIB view. A view is a set of MIB view subtrees, or a family of subtrees, where each is a subtree within the managed object naming tree. Create MIB views to control the OID range that SNMPv3 users can access.
OID Tree	Provide an OID string to include or exclude from the view. The OID string is 128 characters in length.
View Access	Designate whether view access is included or excluded for the subtree or family of subtrees from the MIB view. If creating an excluded view subtree, consider creating a corresponding included entry with the same view name to allow subtrees outside of the excluded subtree to be included.

8 Refer to the Notify Filter table and select **+ Add Row** to set up to 5 remote resources for archive and retrieval.

Name	Enter a 26 character maximum name for the filter. Notifications indicate erroneous user authentication requests, restarts, connection closures, connection loss to a neighbor router or other events.
Remote Host	Provide a destination IP address for a remote server resource for trap filters.

9 Refer to the Remote Engine table and select **+ Add Row** to set up to 5 remote IDs and addresses.

Remote Engine IP	Enter a remote engine IP address for the remote SNMP agent of the device where the user resides.
Remote Engine Id	Provide an Id 9 - 64 characters in length. If configuring the EX3500 management for SNMP V3, is it necessary to configure an engine ID, as passwords are localized using the SNMP ID of the SNMP engine. The remote agent's SNMP engine ID is needed when computing authentication from a password.

10 Refer to the Host table and select **+ Add Row** to set the trap receiver host configuration.

Authentication	If using SNMPv3, define the authentication scheme for user credential validation as either auth, noauth or priv.
Community String	Provide the 1 - 32 character text community strings for accessing EX3500 switch configuration files. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices.
Inform	Enable this option to enable an EX3500 switch to send inform requests to SNMP managers.Traps are not as reliable than informs since an acknowledgment is not sent from the receiving end when a trap is received. A SNMP manager that receives an inform acknowledges the message with an SNMP response.
IP	Define the trap receiver's IP address.
Retry	Set the number of server connection retries (from 1 - 255). When no response is received after the last retry attempt, the connection session is terminated with the trap receiver IP address.
Timeout	Configures the duration (in seconds) the host connection process is shutdown temporarily before a reset of the process is attempted for the set number of retries.
UDP Port	Set the port of the server resource dedicated to receiving EX3500 switch SNMP traps. The default port is port 162.
Version	Set whether SNMP version 1, 2 or 3 is used with this dedicated host. Versions 1 and 2 provide no data security. 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.

EX3500 SNMP Users

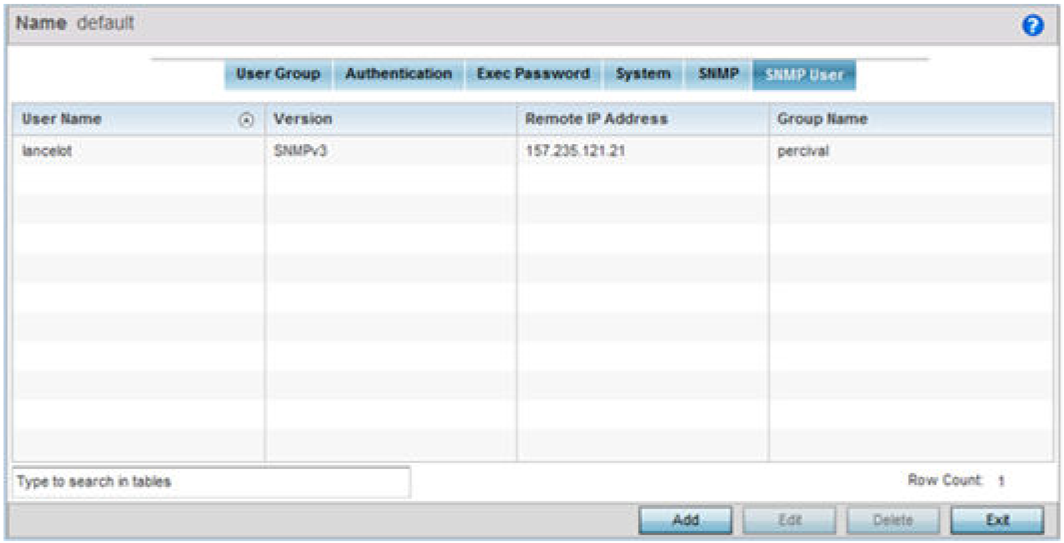
An EX3500 SNMP management session utilizes unique SNMP users with specific authentication and privacy parameters.

To administrate EX3500 SNMP users and their permissions:

1 Go to **Configuration** > **Management** > **EX3500 Management Policy**.

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

2 Select the **SNMP User** tab.

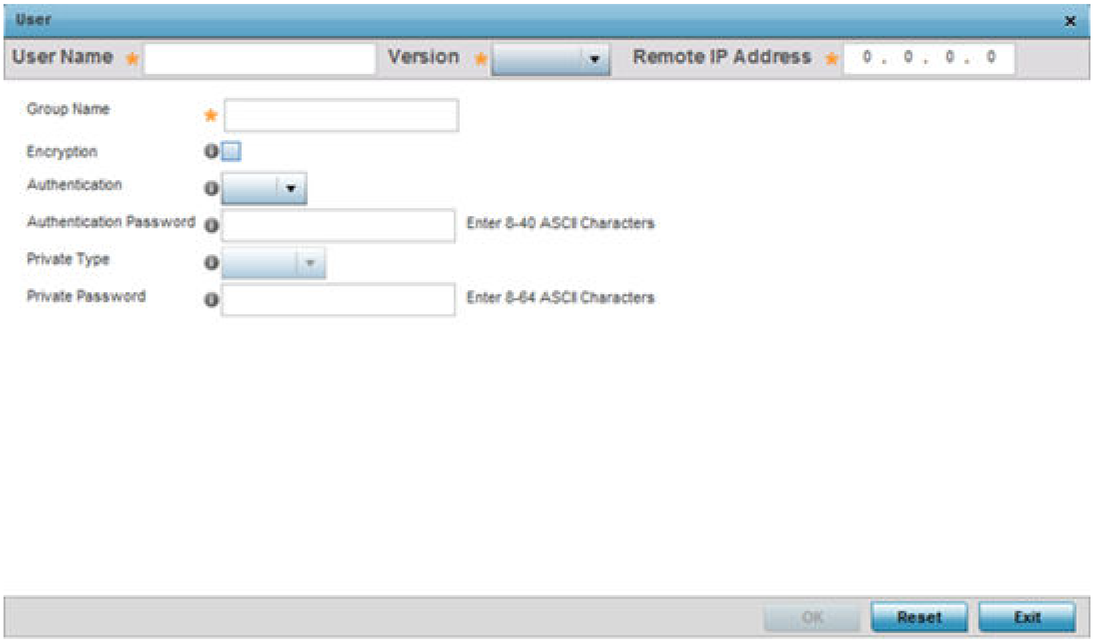


User Name	Version	Remote IP Address	Group Name
lancelot	SNMPv3	157.235.121.21	percival

3 Review the following EX3500 SNMP user credentials to determine whether a new user requires creation on an existing user configuration needs modification:

User Name	Displays the 32 character maximum SNMP user name assigned the specific SNMP version and remote SNMP server resource listed. More than one user can be assigned to the same EX3500 SNMP user group.
Version	Lists whether SNMPv1, SNMPv2 or SNMPv3 is applied to this EX3500 SNMP user. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
Remote IP Address	Lists the remote server resource designated for receiving SNMP trap and inform event messages for the listed SNMP user.
Group Name	Lists the 32 character maximum name assigned to this SNMP group, as SNMP access rights are organized by groups. The trap group name can be any string and is embedded in the community name field of a trap. A maximum of 17 groups can be set for EX3500 model switches.

4 Select **Add** to create a new user configuration or **Edit** to modify the attributes of an existing EX3500 SNMP user configuration.



5 Set the following SNMP user credentials for the EX3500 SNMP user:

User Name	Enter a 32 character maximum SNMP user name for EX3500 SNMP session management.
Version	Use the drop-down menu to define whether SNMPv1, SNMPv2 or SNMPv3 is applied to this EX3500 SNMP user configuration. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
Remote IP Address	Set the remote server resource IP address designated for receiving SNMP trap and inform event messages for this SNMP user.
Group Name	Enter a 32 character maximum for a SNMP group. The group name can be any string and is embedded in the community name field of a SNMP trap.
Encryption	When using SNMPv3, the Encryption option becomes available to scramble packet contents and prevent them from exposure to unauthorized sources.

Authentication	When using SNMPv3, the Authentication option becomes available to ensure messaging is from a valid source. SNMPv3 uses the user-based security model (USM) for message security and the view-based access control model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.
Authentication Password	Enter a 8 - 40 character ASCII authentication password. The selected authentication password ensures only trusted and authorized users can access an EX3500 SNMP management session.
Private Type	Use the drop-down menu to specify the privacy type. The Advanced Encryption Standard (AES) is utilized as one of the privacy protocol options for SNMPv3 messages in either an aes128, aes192 or aes256 format and are recommended. 3DES and des56 are also options, but are considered somewhat insecure and vulnerable to brute-force-attacks.
Private Password	Enter a 8 - 64 character ASCII password to secure the privacy type selected.

6. Select **OK** when completed to update the EX3500 SNMP user settings. Select **Reset** to revert the screen back to its last saved configuration.

Configuring a Hierarchical Tree

Tree Setup is unique because it is not a policy (which is reused in other objects), but rather a global configuration that represents the tree displayed for Dashboard, Operations, and Statistics. However since it is set as a configuration, it follows the standard configuration methods, and requires a **Commit** before it taking effect and a **Save** to become persistent across reboots.

ADSP can run as a virtual machine on NX9500 and NX9510 model service platforms. WiNG communicates with ADSP using a single sign-on (SSO) authentication mechanism. Once the user is logged in, WiNG gains access to ADSP without being prompted to login again at ADSP. There is no synchronization between the WiNG and ADSP databases. ADSP has its own user database stored locally within its virtual machine. This local database is accessed if a user logs directly into ADSP.

WiNG and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, WiNG has added support for an ADSPlike hierarchal tree. The tree resides within WiNG, and ADSP reads it from WiNG and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from WiNG.

Note
The hierarchical tree is available on both controllers and service platforms, but not access points.

WiNG uses the following containers within the tree to be consistent with ADSP's hierarchy conventions:

- Country
- Region

- City
- Campus

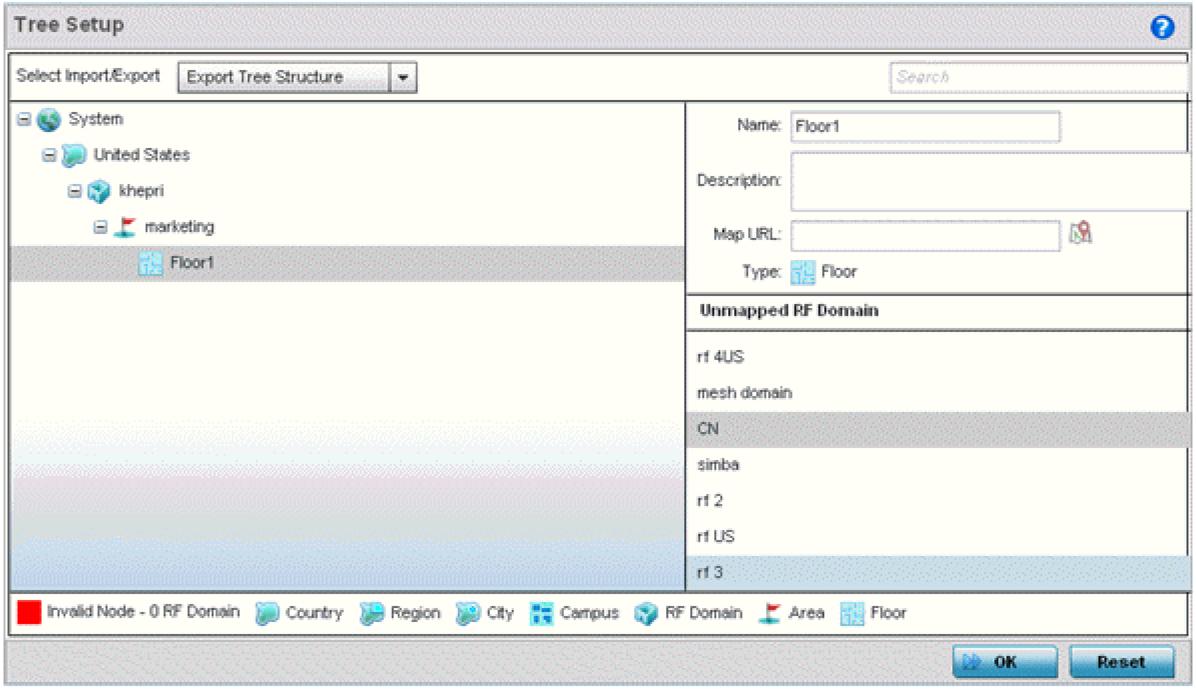
Hierarchy rules are enforced in the containers. For example, a city can be created under a country or region, but not vice versa. An RF Domain can be placed in any container. However, there cannot be any additional containers under the RF Domain. WiNG's RF Domain's already use areas and floors, and these will continue to work as they currently do. Floors are also numbered to be consistent with ADSP's usage.

To configure a hierarchical tree to use with ADSP:

1 Select **Configuration** > **Management**.

2 Click **Tree Setup** on the top left-hand corner of the UI.

The Tree Setup screen displays with a System node that requires population with the containers to represent the deployment shared between WiNG and ADSP. The Country, Region, City and Campus containers can be defined in any order, but at least one of these containers is required within the hierarchy before the RF Domain can be added and the hierarchy defined as valid.



Select Import/Export: Export Tree Structure

- System
  - United States
    - khepri
      - marketing
        - Floor1

Name: Floor1

Description:

Map URL:

Type: Floor

Unmapped RF Domain

rf 4US
mesh domain
CN
simba
rf 2
rf US
rf 3

3 To add a Country, Region, City or Campus to the tree, select System from the upper, left-hand, portion of the Tree Setup screen.

> Note
>
> If a complete tree configuration has been saved and exported for archive to remote location, it can be imported back into the Tree Setup screen and utilized without having to re-configure the containers and RF Domain of that tree. Select Import to utilize and existing tree configuration.

> Note
>
> If a tree container (country, region, city or campus) has a red box around it, it either has invalid attributes or a RF Domain requires addition.

An Add Child link displays on the right-hand side of the display.

4 If adding a country, go to **Type** > **Name** to scroll to the country of deployment where the RF Domain resides.

Adding a country first is a good idea since regions, city and campus can all be added as child items in the tree structure. However, the selected country is an invalid tree node until a RF Domain is applied.

5 If adding a region, select Region from the Type drop-down menu and use the Name parameter to enter its name. Select Add to display the region.

A city and campus can be added as child items in the tree structure under a region. An RF Domain can be mapped anywhere down the hierarchy for a region and not just directly under a Country. For example, a region can have city and campus and one RF Domain mapped.

6 If adding a city, select City from the Type drop-down menu and use the Name parameter to enter its name. Select Add to display the city.

Only a campus can be added as a child item under a city. The city is an invalid tree node until a RF Domain is applied somewhere within the directory tree.

7 If adding a campus, select Campus from the Type drop-down menu and use the Name parameter to enter its name. Select Add to display the campus.

A Campus is the last node in the hierarchy before A RF Domain, and it cannot be valid unless it has a RF Domain mapped to it.

8 Select the **add RF Domain** link at the right-hand side of any container to display an Unmapped RF Domain screen.

9 Provide the default RF Domain name whose deployment area and floor is mapped graphically, and whose events are shared between WiNG and ADSP. Select **Add** to display the RF Domain within its respective place in the tree hierarchy. A default RF Domain can also be dragged into the tree from the right-hand side of the screen.

10 Once the RF Domain is in the tree, select the **add child** link at the right-hand side of the RF Domain to display a screen where the RF Domain deployment **Area** and **Floor** are defined. Once defined, select **Add** to populate the tree with the Area and Floor.

11 Provide the **Map URL** to upload the floor plan created under an Area. Each area can have multiple floors

> Note
>
> While the MAP URL graphic file represents the RF Domain's physical device deployment area, devices cannot be dragged into topology or manipulated. To define a network topology that allows an administrator to add devices and manipulate locations, refer to Network View

12 Edit a tree node at any time by selecting it from amongst the Tree Setup screen, and referring to the right-hand side of the screen where a field displays to modify the container.

13 Optionally, select Tree Import Export Template to upload a template.csv file if one is needed for container configuration.

A sample of the tree template is provided here for reference:

Row Description

record type (folder),server,Name,Description,Type,Floor Number,Path(slash delimited),Command(add|delete)

Actual Row is CSV file

```
folder,localhost,US,Country Description,Country,,
folder,localhost,Southeast,Region Description,Region,,US
folder,localhost,Alpharetta,City Description,City,,US/Southeast
folder,localhost,Sanctuary Park,Campus Description,Campus,,US/Southeast/Alpharetta
folder,localhost,The Falls 1125,Domain Description,RFDomain,,US/Southeast/Alpharetta/
Sanctuary Park
folder,localhost,Queens,,Area,,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125
folder,localhost,FloorQLab,,Floor,1,US/Southeast/Alpharetta/Sanctuary Park/The Falls
1125/Queens
folder,localhost,FloorSLab,,Floor,2,US/Southeast/Alpharetta/Sanctuary Park/The Falls
1125/Queens
folder,localhost,FloorTLab,,Floor,3,US/Southeast/Alpharetta/Sanctuary Park/The Falls
1125/Queens
```

In the CSV file, configure specifc tree node properties:

Index 1: Record Type. This value is always 'folder'. Import/export allows the configuration of folder nodes only. Leaf nodes cannot be configured like devices.

Index 2: Server Name. This value is always 'localhost' as we are supporting the import/export from localhost only.

Index 3: Name. This configures the name/label of the tree node. This is the value which is visible to the user in Tree node.

Index 4: Description. This configures the additional information in form, which user wants to store with the Tree node.

Index 5: Type. This configures the type of the Tree node. Type can take one of the value "country, region, city, campus, rfdomain, area, floor".

Index 6: Floor Number. This is configures the floor number. This is applicable only for the floor node.

Index 7: Path. This is /'(slash delimited) from the 'root'.

Index 8: add|delete. Allows manipulation of the node. If no value is specified, the default is 'add' . If value is 'delete' then reference node is removed.

14 Select **Import Tree Structure** to optionally import a .csv file with pre-defined the containers and RF Domain. Importing an existing tree saves an administrator from creating a new one from the beginning.

15 Once the tree topology is defined to your satisfaction, select **Export Tree Structure** to archive the tree topology (in .csv file format) to a defined location.

The exported tree topology can be re-imported and automatically displayed within the **Tree Setup** screen at any time.

16 Select **OK** to update the tree setup configuration. Select **Reset** to revert to the last saved configuration.

Note
Since the tree is set as a configuration, it follows standard configuration methods, and requires a Commit before it taking effect and A Save to become persistent across reboots.

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.

13 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.

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

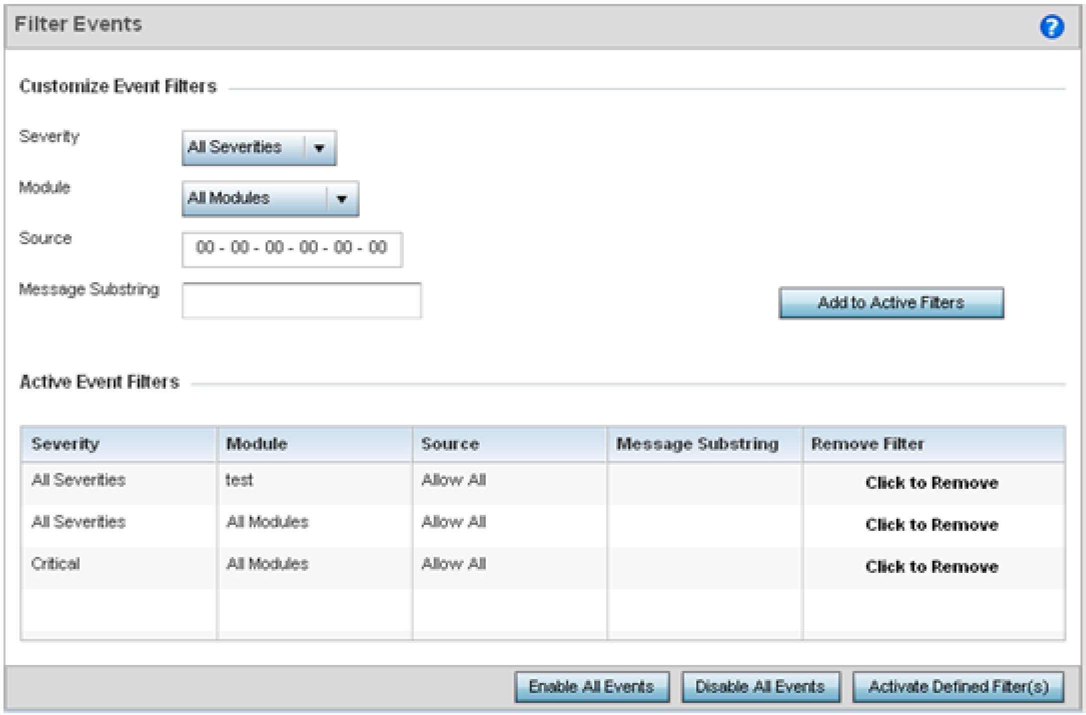
Fault management enables user's administering multiple sites to assess how individual devices are performing and review issues impacting the network. Use the Fault Management screens to administrate errors generated by a controller, service platform, access point or wireless client.

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.



Customize Event Filters

Severity: All Severities
Module: All Modules
Source: 00 - 00 - 00 - 00 - 00 - 00
Message Substring:

Active Event Filters

Severity	Module	Source	Message Substring	Remove Filter
All Severities	test	Allow All		Click to Remove
All Severities	All Modules	Allow All		Click to Remove
Critical	All Modules	Allow All		Click to Remove

Figure 387: 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: *All Severities* – All events are displayed, irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *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

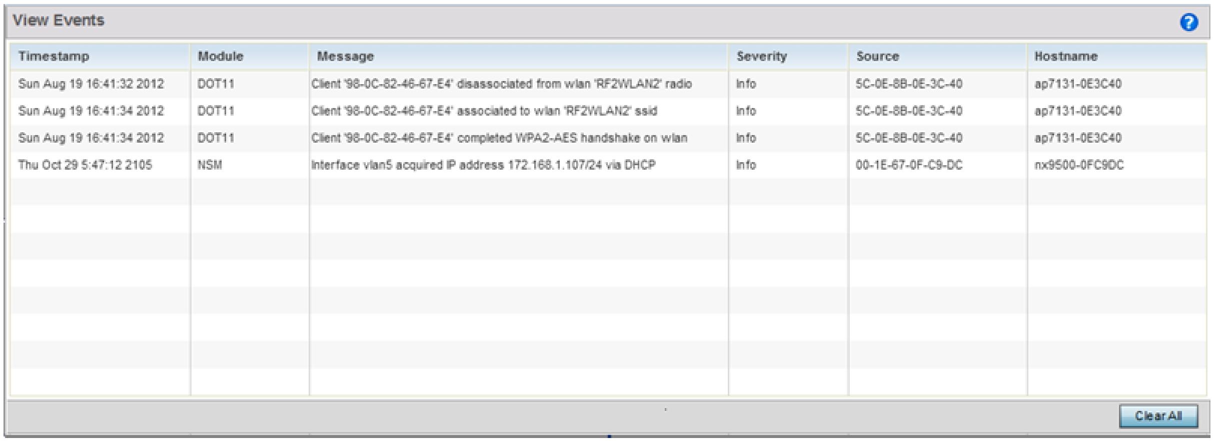
Filters cannot be persisted across sessions. They must be created every time a new session is established.

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**.



View Events

Timestamp	Module	Message	Severity	Source	Hostname
Sun Aug 19 16:41:32 2012	DOT11	Client '98-0C-82-46-67-E4' disassociated from wlan 'RF2WLAN2' radio	Info	5C-0E-8B-0E-3C-40	ap7131-0E3C40
Sun Aug 19 16:41:34 2012	DOT11	Client '98-0C-82-46-67-E4' associated to wlan 'RF2WLAN2' ssid	Info	5C-0E-8B-0E-3C-40	ap7131-0E3C40
Sun Aug 19 16:41:34 2012	DOT11	Client '98-0C-82-46-67-E4' completed WPA2-AES handshake on wlan	Info	5C-0E-8B-0E-3C-40	ap7131-0E3C40
Thu Oct 29 5:47:12 2105	NSM	Interface vlan5 acquired IP address 172.168.1.107/24 via DHCP	Info	00-1E-67-0F-C9-DC	nx9500-0FC9DC

Figure 388: 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: *All Severities* – All events are displayed irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *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**

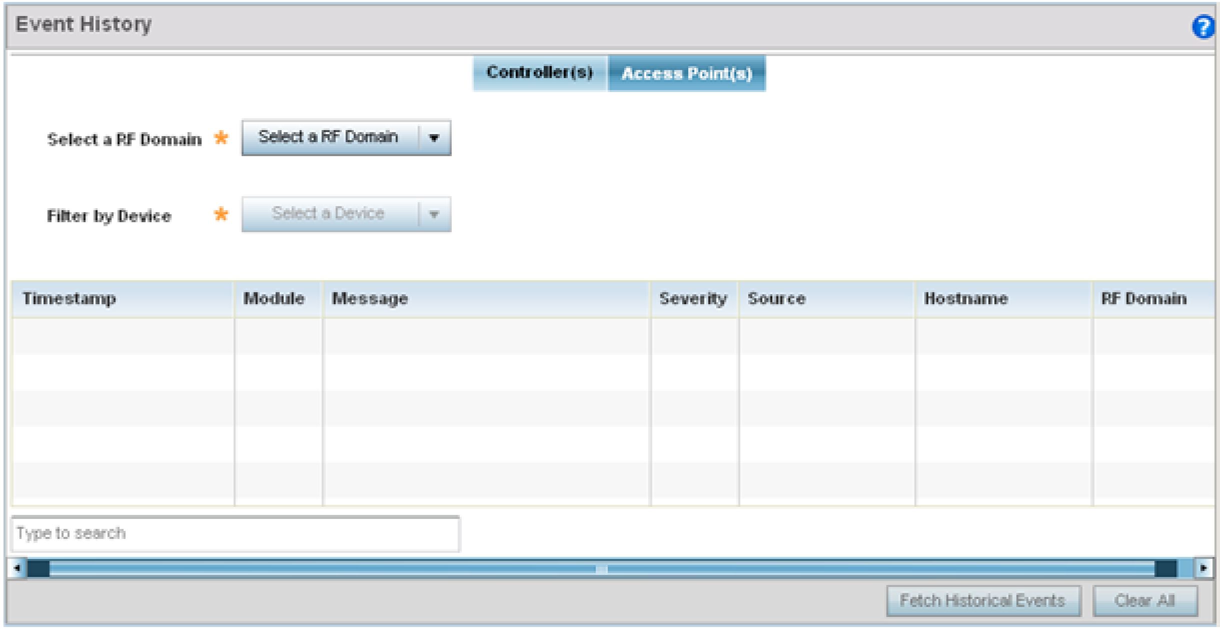


Figure 389: Fault Management - Event History screen

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: *All Severities* – All events are displayed irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *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.

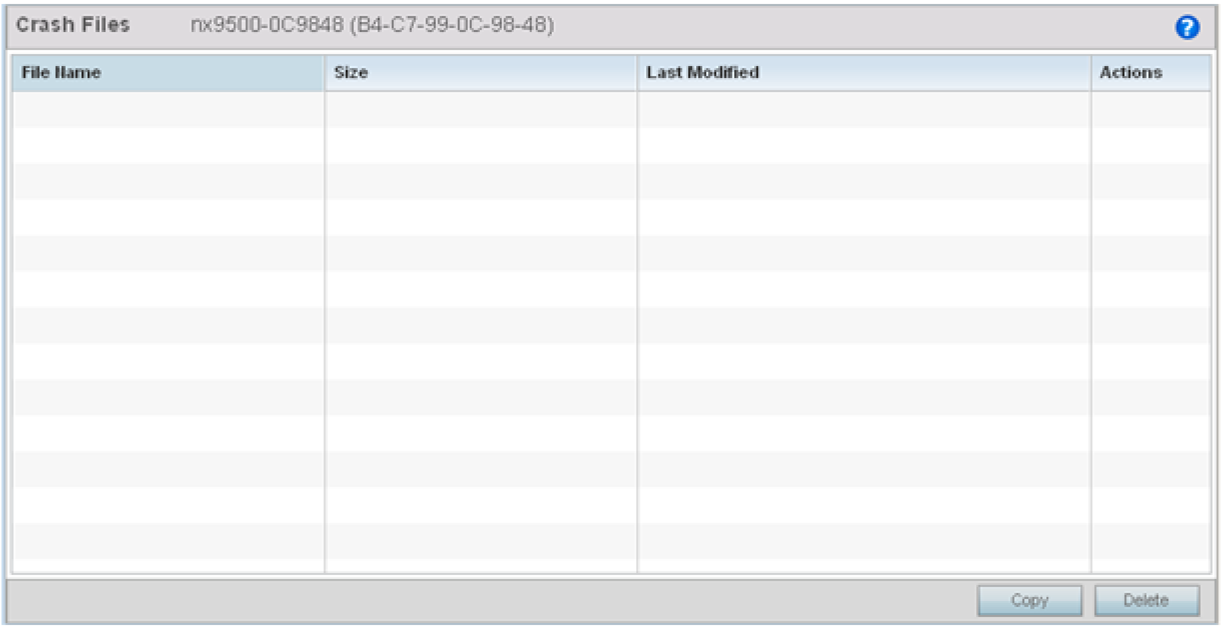


Figure 390: Crash Files screen

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 948
- Viewing UI Logs on page 949
- View Sessions on page 951

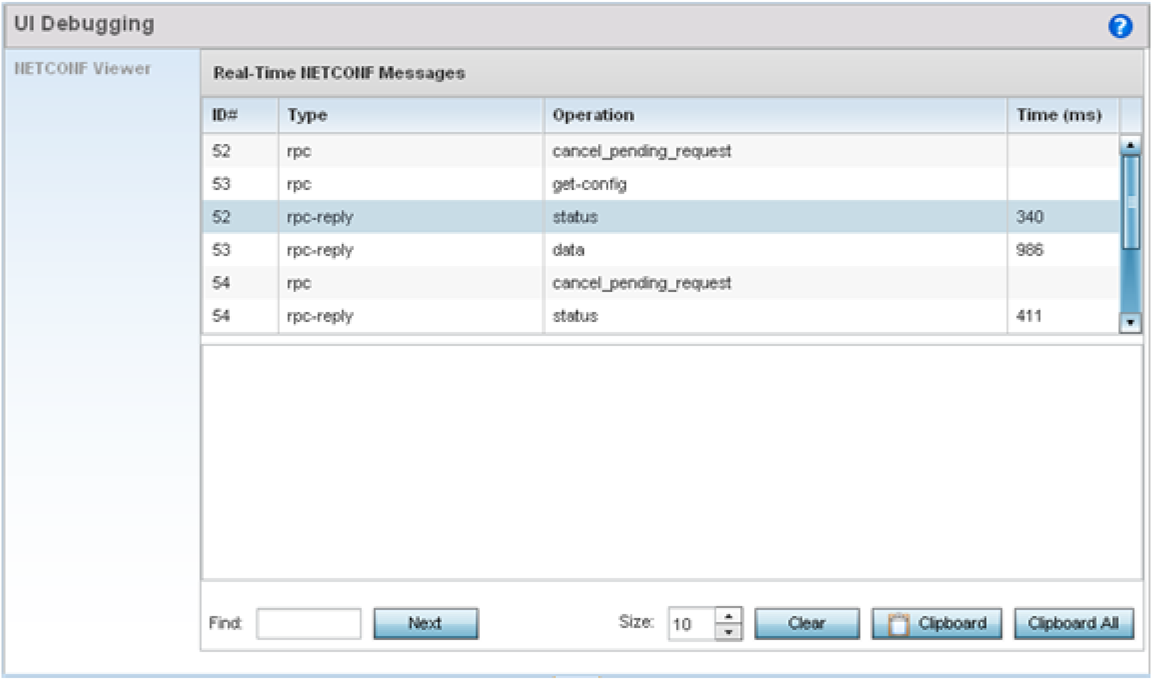
UI Debugging

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.



ID#	Type	Operation	Time (ms)
52	rpc	cancel_pending_request	
53	rpc	get-config	
52	rpc-reply	status	340
53	rpc-reply	data	986
54	rpc	cancel_pending_request	
54	rpc-reply	status	411

Size: 10

Figure 391: 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.

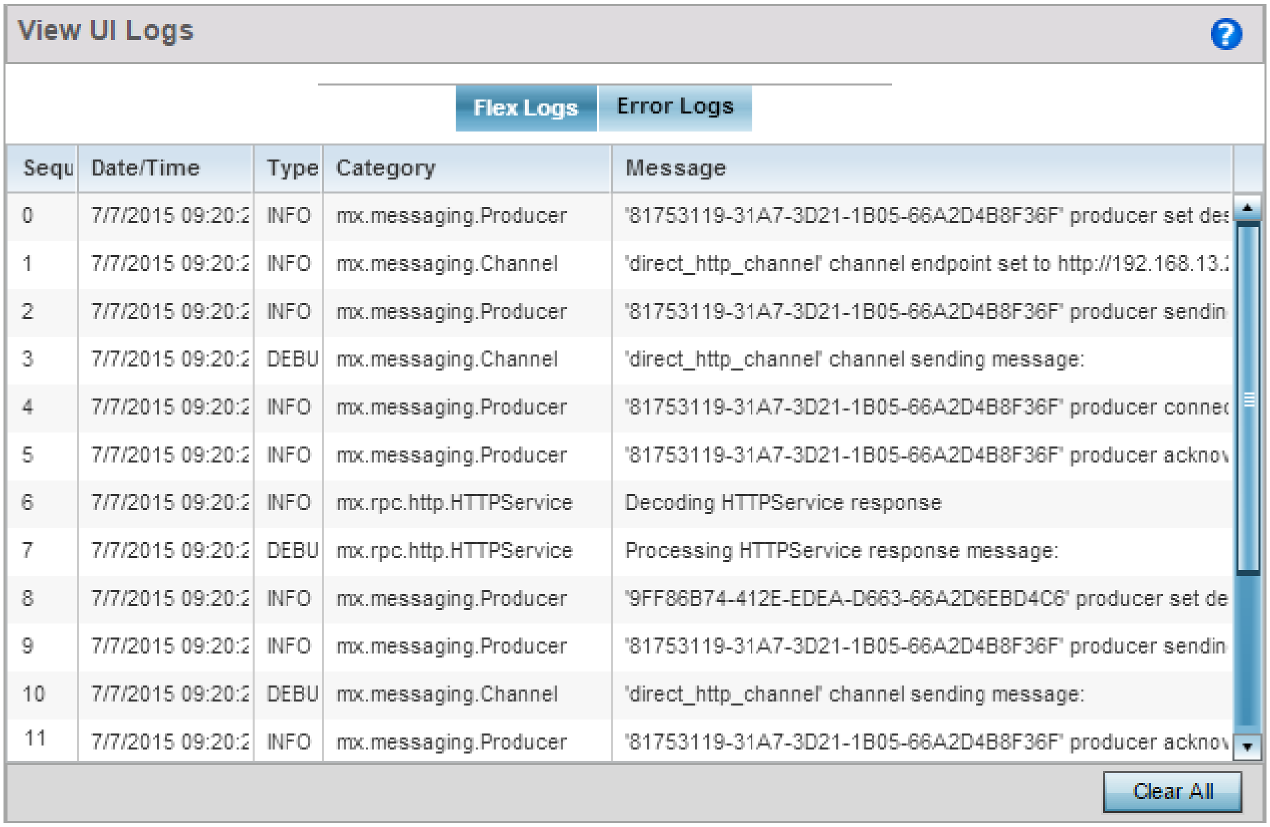
Viewing UI Logs

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.



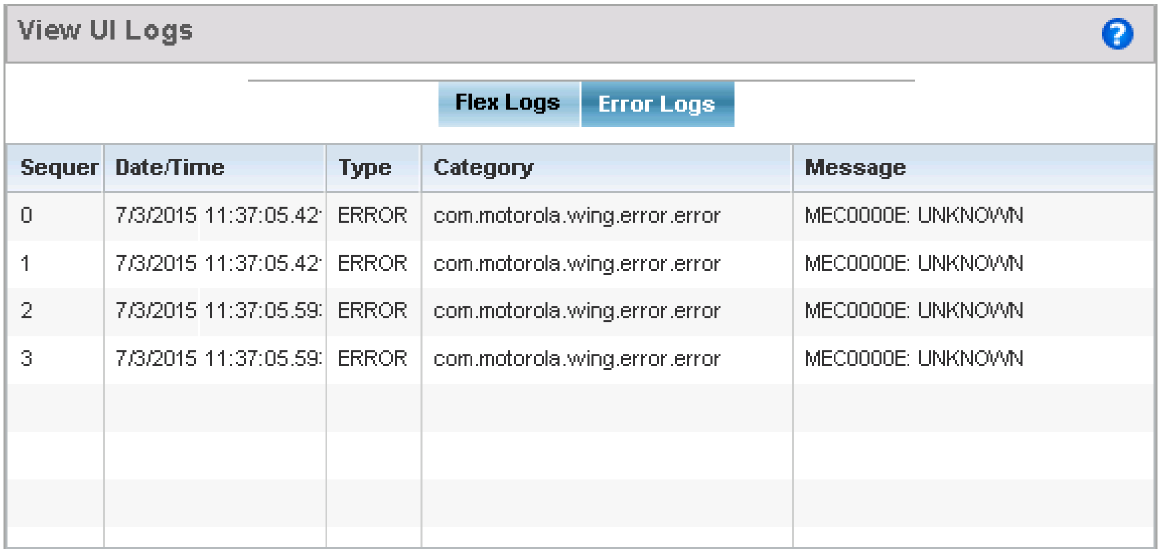
Sequ	Date/Time	Type	Category	Message
0	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer set des
1	7/7/2015 09:20:2	INFO	mx.messaging.Channel	'direct_http_channel' channel endpoint set to http://192.168.13.2
2	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer sendin
3	7/7/2015 09:20:2	DEBU	mx.messaging.Channel	'direct_http_channel' channel sending message:
4	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer connec
5	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer acknov
6	7/7/2015 09:20:2	INFO	mx.rpc.http.HTTPService	Decoding HTTPService response
7	7/7/2015 09:20:2	DEBU	mx.rpc.http.HTTPService	Processing HTTPService response message:
8	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'9FF86B74-412E-EDEA-D663-66A2D6EBD4C6' producer set de
9	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer sendin
10	7/7/2015 09:20:2	DEBU	mx.messaging.Channel	'direct_http_channel' channel sending message:
11	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer acknov

Figure 392: 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.



Sequer	Date/Time	Type	Category	Message
0	7/3/2015 11:37:05.42	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
1	7/3/2015 11:37:05.42	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
2	7/3/2015 11:37:05.59	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
3	7/3/2015 11:37:05.59	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN

Figure 393: View UI Logs - Error Logs tab

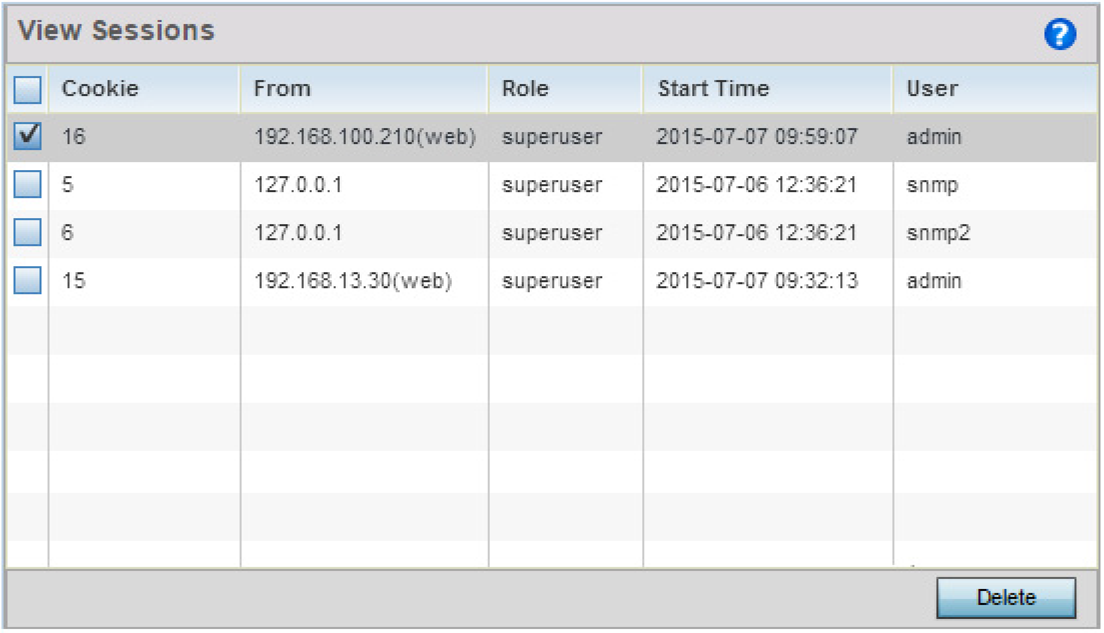
The Sequence (order of occurrence), Date/Time, Type, Category and Message items display for each log option selected.

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



☐	Cookie	From	Role	Start Time	User
☑	16	192.168.100.210(web)	superuser	2015-07-07 09:59:07	admin
☐	5	127.0.0.1	superuser	2015-07-06 12:36:21	snmp
☐	6	127.0.0.1	superuser	2015-07-06 12:36:21	snmp2
☐	15	192.168.13.30(web)	superuser	2015-07-07 09:32:13	admin

Figure 394: 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**.

14 Operations

Device Operations
Certificates
Smart RF

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.

On controllers and service platforms, Smart RF policies can be applied to specific RF Domains, to add site specific deployment configurations and self recovery values to groups of devices within pre-defined physical RF coverage areas.

For more information, refer to the following:

- Device Operations
- Certificates
- Smart RF

Device Operations

Updated device firmware and configuration files are periodically released to the Support Web site. If an access point's (or its associated device's) firmware is older than the version on the Web site, update to the latest firmware version for full feature functionality and optimal controller or service platform 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.

For more information, refer to the following:

- Operations Summary on page 953
- Adopted Device Upgrades on page 955
- Using the File Management Browser on page 963
- Restarting Adopted Devices on page 965
- Captive Portal Configuration on page 967
- Crypto CMP Certificate on page 970

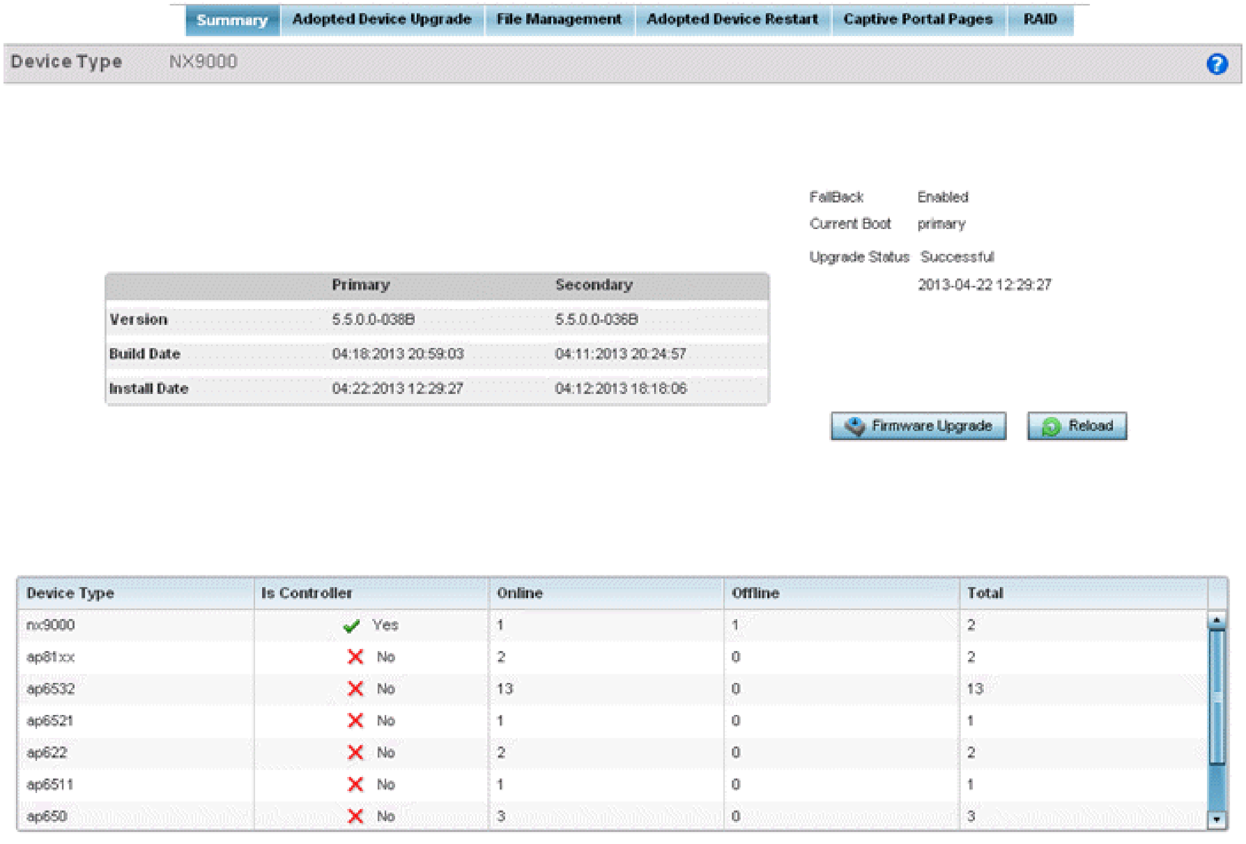
- RAID on page 970
- Re-elect Controller on page 972

Operations Summary

The Summary screen displays firmware information for a controller, service platform or access point selected from either the RF Domain or Network tabs on the left-hand side of the screen.

1 Got to **Operations** → **Devices** → **System**.

2 Expand one of the **RF Domains** listed within the System node, and select a target device. The selected device's Summary page displays by default.



Device Type NX9000

FallBack Enabled
Current Boot primary
Upgrade Status Successful
2013-04-22 12:29:27

	Primary	Secondary
Version	5.5.0.0-038B	5.5.0.0-036B
Build Date	04:18:2013 20:59:03	04:11:2013 20:24:57
Install Date	04:22:2013 12:29:27	04:12:2013 18:18:06

Device Type	Is Controller	Online	Offline	Total
nx9000	✓ Yes	1	1	2
ap81xx	✗ No	2	0	2
ap6532	✗ No	13	0	13
ap6521	✗ No	1	0	1
ap622	✗ No	2	0	2
ap6511	✗ No	1	0	1
ap650	✗ No	3	0	3

3 Refer to the following to determine whether a firmware image needs to be updated for the selected device, or a device requires a restart or revert to previous settings.

Version	Displays the primary and secondary firmware image version defined for the selected device. Keep in mind, secondary images with an older build version have a reduced feature and may limit the device.
Build Date	Displays the date the primary and secondary firmware image was built for the selected device.
Install Date	Displays the date the firmware was installed for the selected device.
Fallback	Lists whether fallback is currently enabled for the selected device. When enabled, the device reverts back to the last successfully installed firmware image if something were to happen in its next firmware upgrade that would render the device inoperable.

Current Boot	Lists firmware image for the device on the current boot.
Upgrade Status	Displays the status of the last firmware upgrade performed for each listed device managed by this controller, service platform or Virtual Controller mode access point.
Firmware Upgrade	Select this option to display the firmware upgrade window for the selected device. Select the *Apply* button to perform the function.
Reload	Select this option to restart the selected device. Selecting this option restarts the target device using the specified options in the settings window. Restarting a device resets all data collection values to zero. Select the *Reload* button to perform the function.

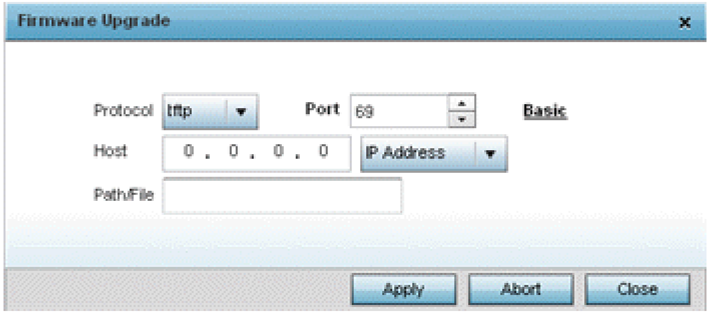
4 Refer to the device table for basic information for known device types. The device table displays the Device Type, Is Controller status, Online, Offline and Total device counts.

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.



Protocol: tftp
Port: 69
Host: 0 . 0 . 0 . 0
IP Address
Path/File:

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: *tftp* *ftp* *sftp* *http* *cf* *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.

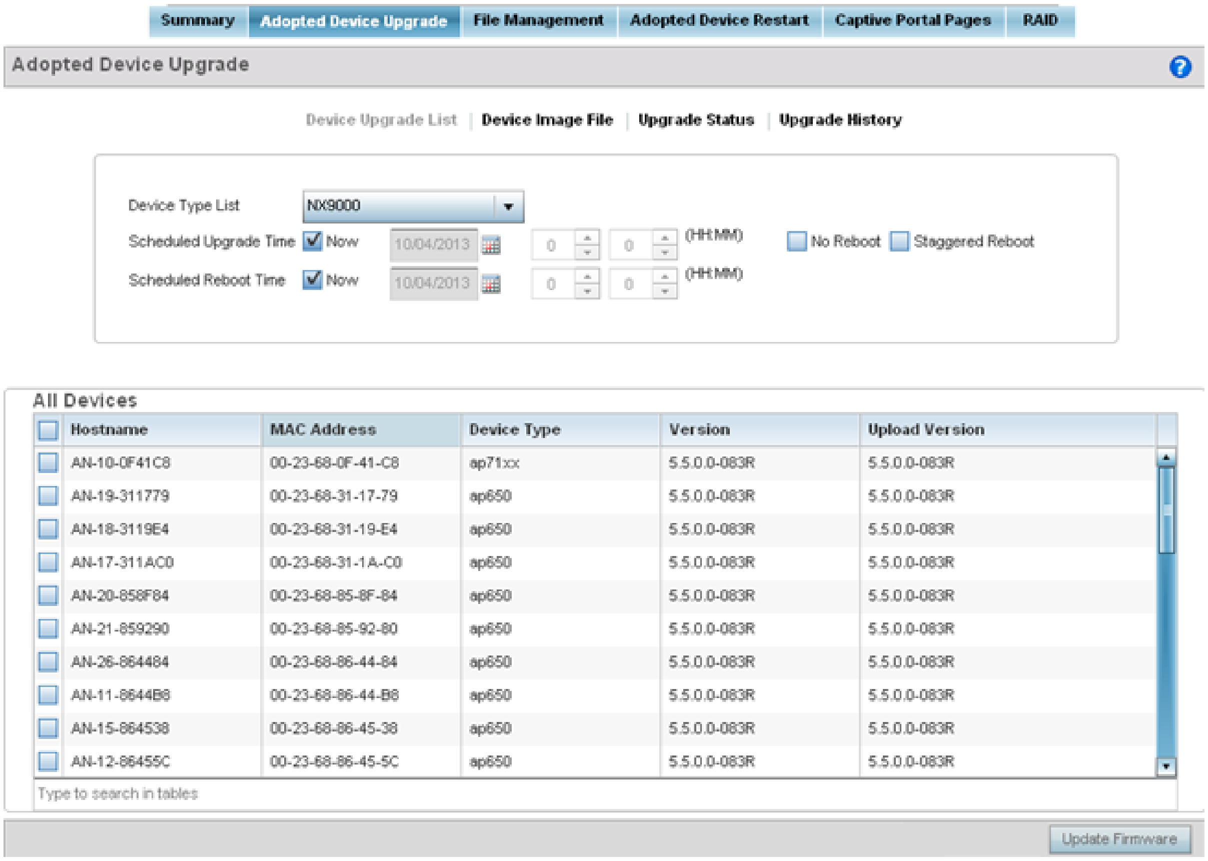
7. Select **Apply** to start the firmware update. Select **Abort** to terminate an in process firmware update. Select **Close** to close the upgrade pop up screen. The upgrade continues in the background.

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.



Device Type List: NX9000

Scheduled Upgrade Time: ☑ Now 10/04/2013 0 0 (HH:MM) ☐ No Reboot ☐ Staggered Reboot

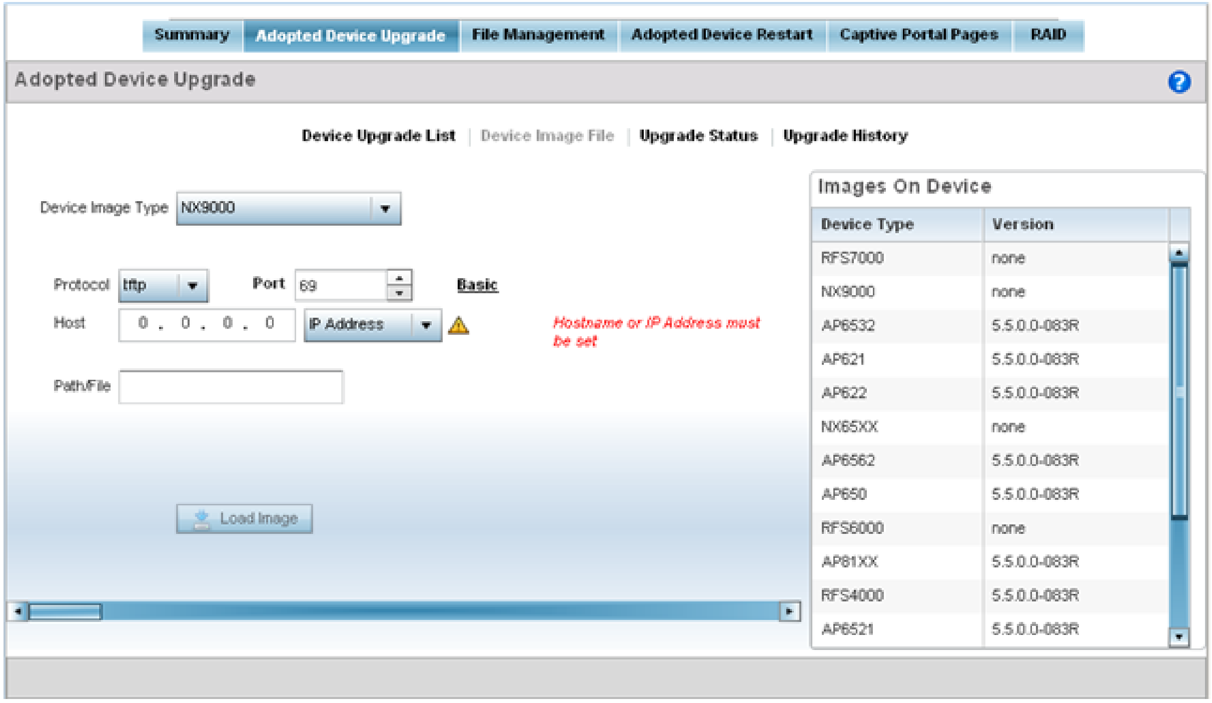
Scheduled Reboot Time: ☑ Now 10/04/2013 0 0 (HH:MM)

All Devices

☐	Hostname	MAC Address	Device Type	Version	Upload Version
☐	AN-10-0F41C8	00-23-68-0F-41-C8	ap71xx	5.5.0.0-083R	5.5.0.0-083R
☐	AN-19-311779	00-23-68-31-17-79	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-18-3119E4	00-23-68-31-19-E4	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-17-311AC0	00-23-68-31-1A-C0	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-20-858F84	00-23-68-85-8F-84	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-21-859290	00-23-68-85-92-80	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-26-864484	00-23-68-86-44-84	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-11-8644B8	00-23-68-86-44-B8	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-15-864538	00-23-68-86-45-38	ap650	5.5.0.0-083R	5.5.0.0-083R
☐	AN-12-86455C	00-23-68-86-45-5C	ap650	5.5.0.0-083R	5.5.0.0-083R

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.



Device Image Type: NX9000

Protocol: tftp

Port: 69

Host: 0 . 0 . 0 . 0 IP Address

Path/File:

Hostname or IP Address must be set

Images On Device

Device Type	Version
RFS7000	none
NX9000	none
AP6532	5.5.0.0-083R
AP621	5.5.0.0-083R
AP622	5.5.0.0-083R
NX65XX	none
AP6562	5.5.0.0-083R
AP650	5.5.0.0-083R
RFS6000	none
AP81XX	5.5.0.0-083R
RFS4000	5.5.0.0-083R
AP6521	5.5.0.0-083R

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: *tftp* *ftp* *sftp* *http* *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

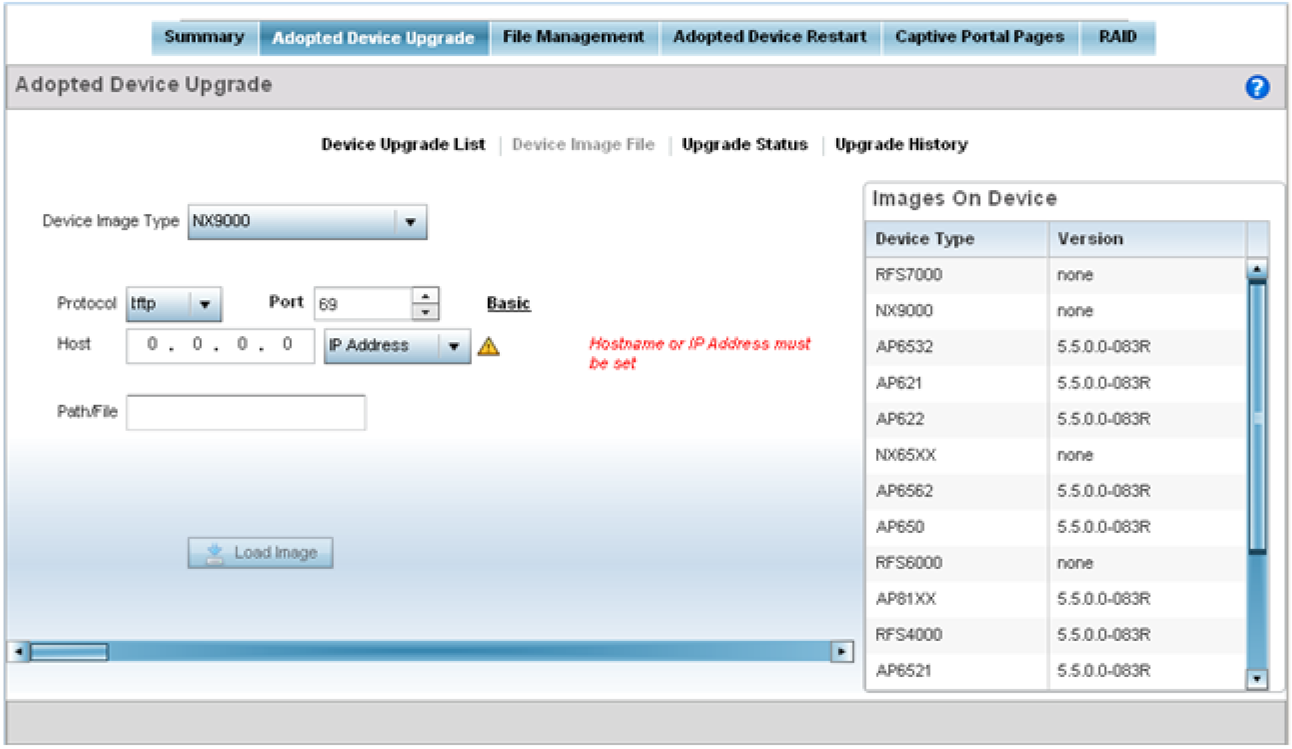
Use the **Device Image File** screen to select device image types for firmware updates and set the transfer protocol used for staging the firmware to the device itself prior to its update.

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**.



Device Image Type NX9000

Protocol tftp Port 69

Host 0 . 0 . 0 . 0 IP Address

Hostname or IP Address must be set

Path/File

Images On Device

Device Type	Version
RFS7000	none
NX9000	none
AP6532	5.5.0.0-083R
AP621	5.5.0.0-083R
AP622	5.5.0.0-083R
NX65XX	none
AP6562	5.5.0.0-083R
AP650	5.5.0.0-083R
RFS6000	none
AP81XX	5.5.0.0-083R
RFS4000	5.5.0.0-083R
AP6521	5.5.0.0-083R

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: *tftp* *ftp* *sftp* *http* *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.

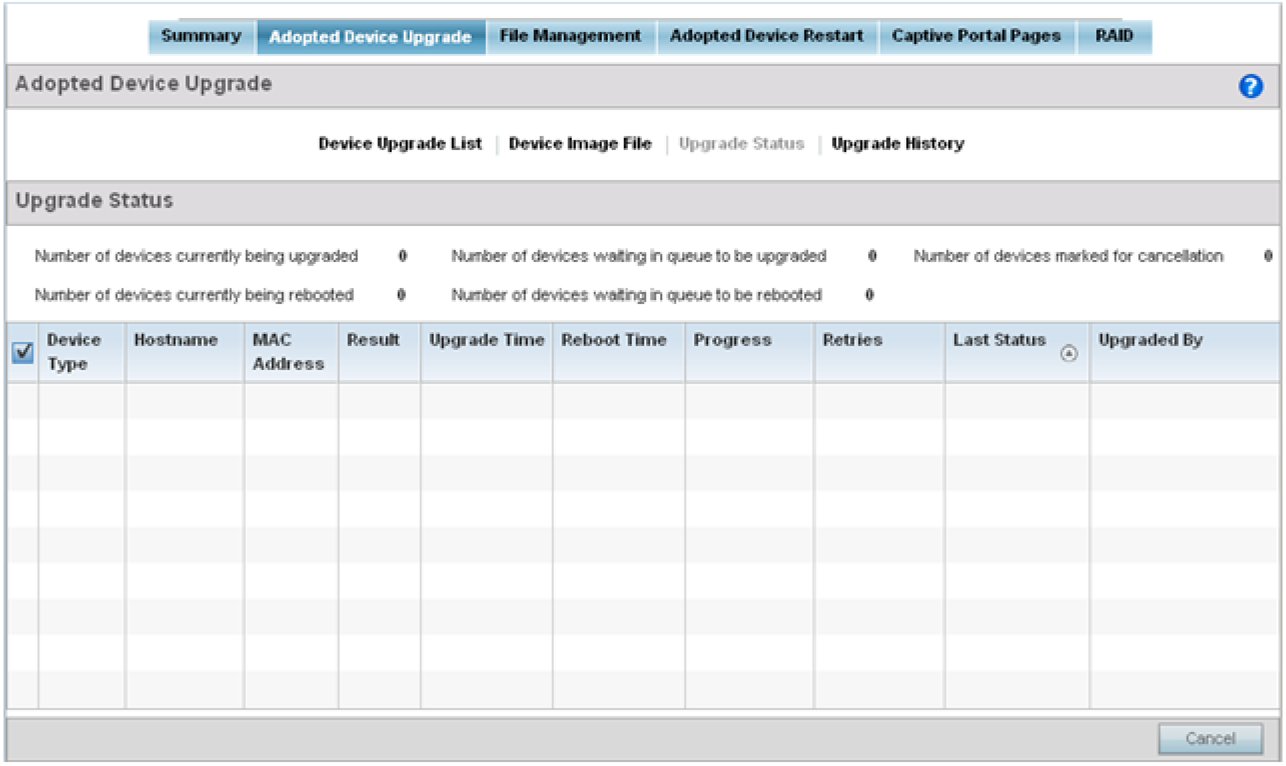
The firmware image is loaded to the flash/upgrade directory (not the flash/cache directory). If the NOC pushes the image, then it is loaded to flash/cache/upgrade.

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**.



Number of devices currently being upgraded 0
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

☑	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By

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.

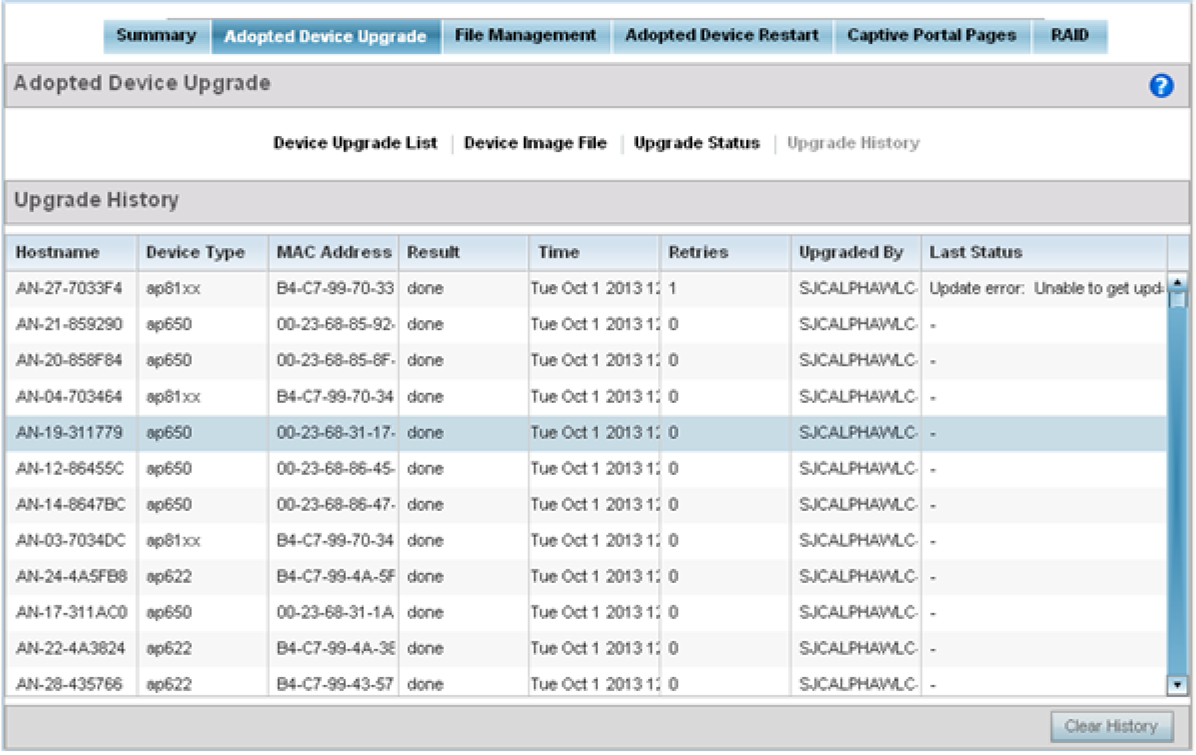
7 Refer to the following status reported for each current or scheduled upgrade operation:

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.



Hostname	Device Type	MAC Address	Result	Time	Retries	Upgraded By	Last Status
AN-27-7033F4	ap81xx	B4-C7-99-70-33	done	Tue Oct 1 2013 1	1	SJCALPHAWLC-	Update error: Unable to get upd-
AN-21-859290	ap650	00-23-68-85-92-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-20-858F84	ap650	00-23-68-85-8F-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-04-703464	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-19-311779	ap650	00-23-68-31-17-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-12-86455C	ap650	00-23-68-86-45-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-14-8647BC	ap650	00-23-68-86-47-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-03-7034DC	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-24-4A5FB8	ap622	B4-C7-99-4A-5F	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-17-311AC0	ap650	00-23-68-31-1A	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-22-4A3824	ap622	B4-C7-99-4A-3	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-
AN-28-435766	ap622	B4-C7-99-43-57	done	Tue Oct 1 2013 1	0	SJCALPHAWLC-	-

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:

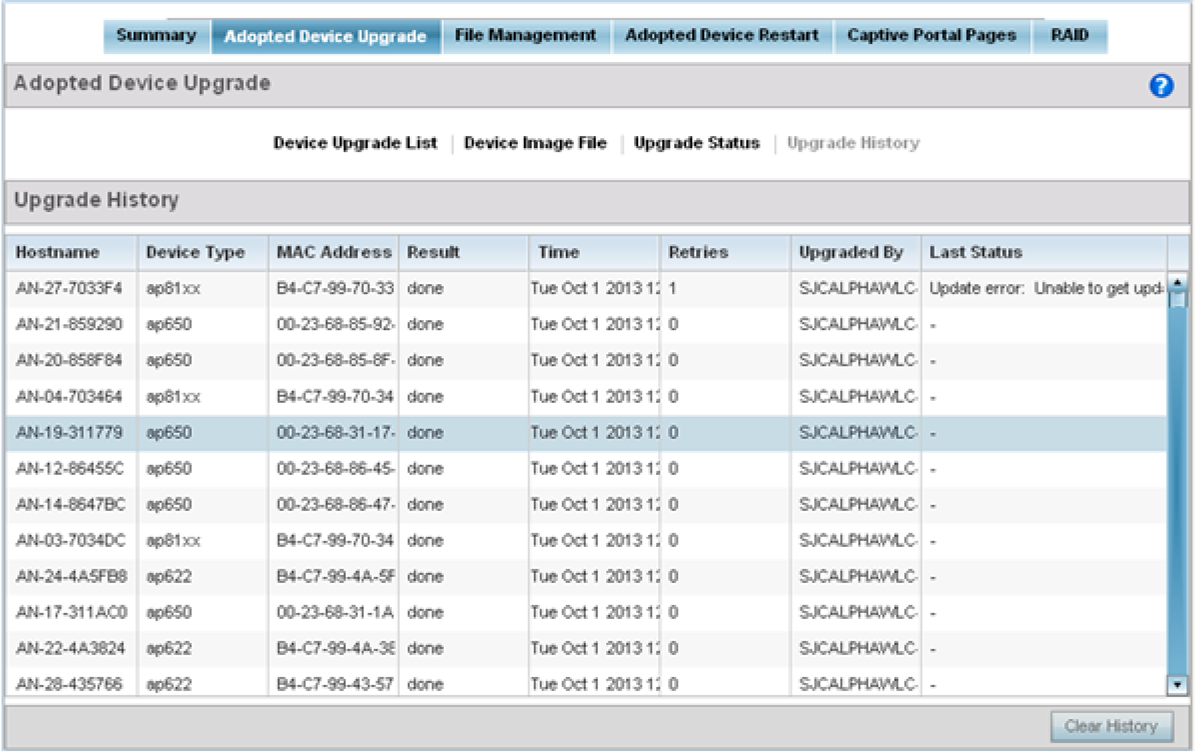
1 Select **Operations**.

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**.



Hostname	Device Type	MAC Address	Result	Time	Retries	Upgraded By	Last Status
AN-27-7033F4	ap81xx	B4-C7-99-70-33	done	Tue Oct 1 2013 1	1	SJCALPHAWLC	Update error: Unable to get upd
AN-21-859290	ap650	00-23-68-85-92-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-20-858F84	ap650	00-23-68-85-8F-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-04-703464	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-19-311779	ap650	00-23-68-31-17-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-12-86455C	ap650	00-23-68-86-45-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-14-8647BC	ap650	00-23-68-86-47-	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-03-7034DC	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-24-4A5FB8	ap622	B4-C7-99-4A-5F	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-17-311AC0	ap650	00-23-68-31-1A	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-22-4A3824	ap622	B4-C7-99-4A-3	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-
AN-28-435766	ap622	B4-C7-99-43-57	done	Tue Oct 1 2013 1	0	SJCALPHAWLC	-

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

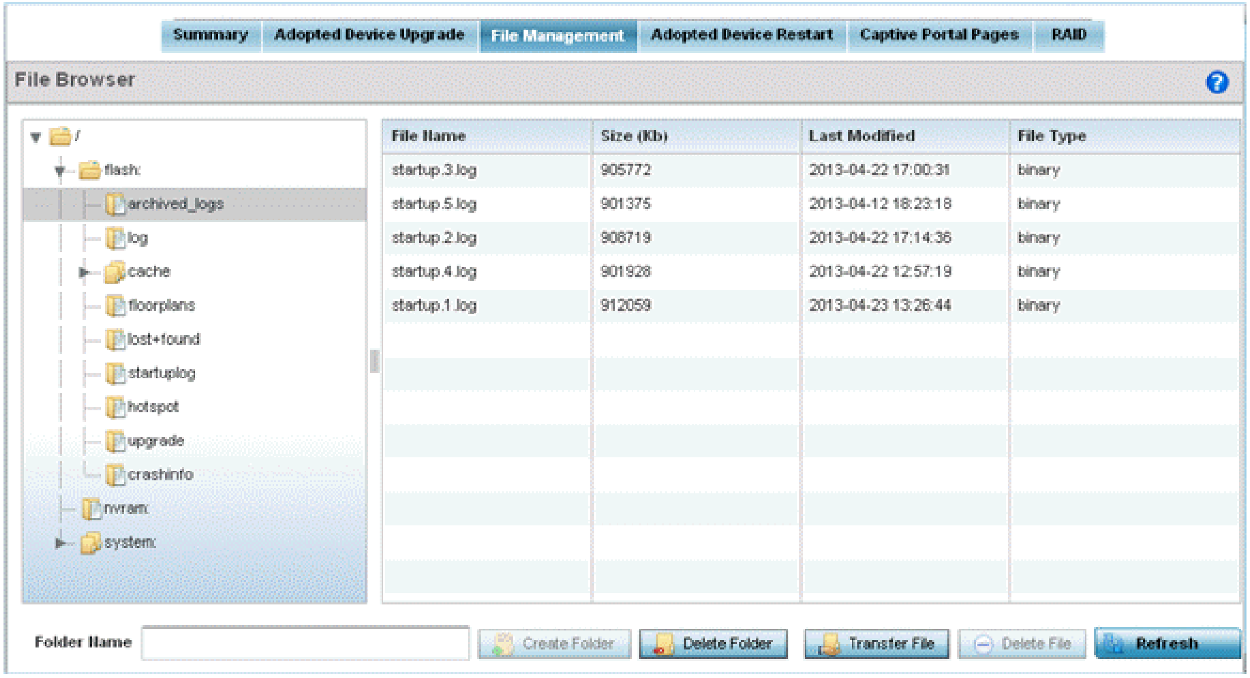
Controllers, service platforms and access points can utilize a File Browser allowing an administrator to review the files residing on a internal or external memory resource. Directories can be created and maintained for each File Browser location and folders and files can be moved and deleted as needed.

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.**



File Name	Size (Kb)	Last Modified	File Type
startup.3.log	905772	2013-04-22 17:00:31	binary
startup.5.log	901375	2013-04-12 18:23:18	binary
startup.2.log	908719	2013-04-22 17:14:36	binary
startup.4.log	901928	2013-04-22 12:57:19	binary
startup.1.log	912059	2013-04-23 13:26:44	binary

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.

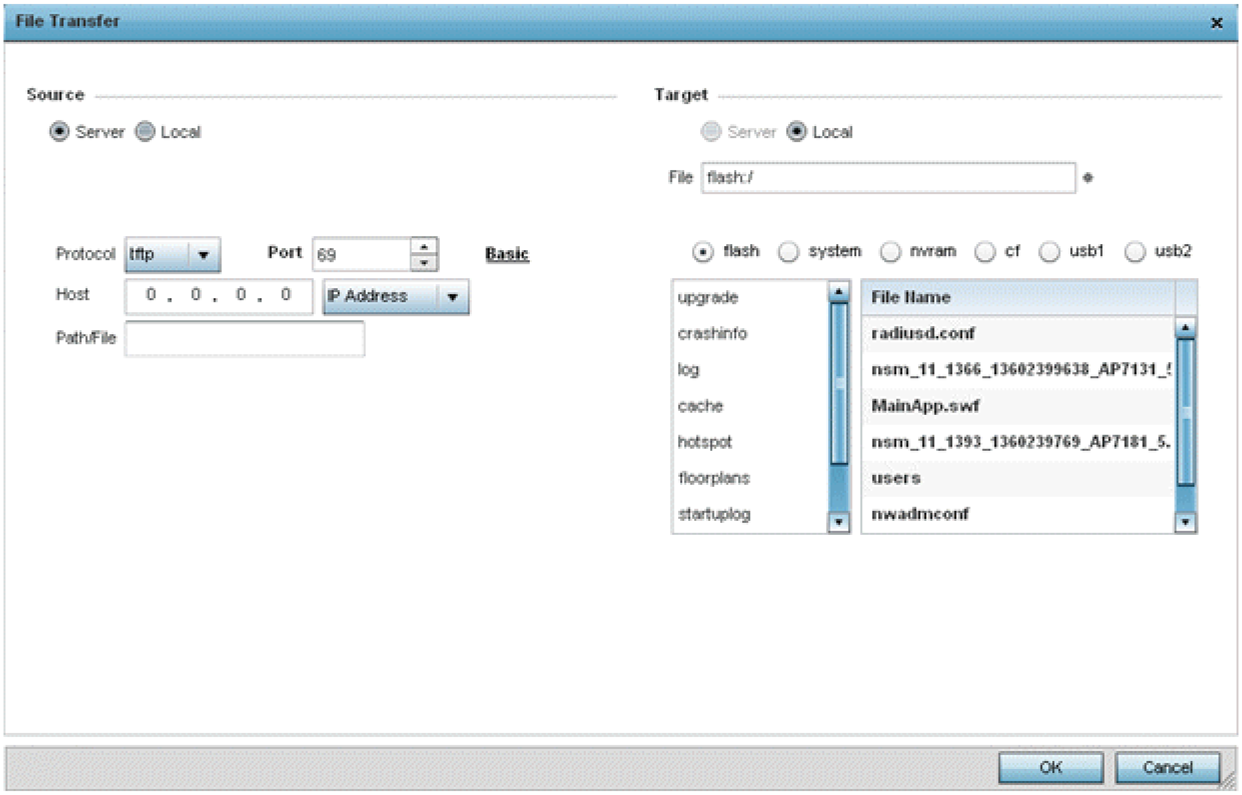
Managing File Transfers

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.



File Transfer

Source: ● Server ○ Local

Protocol: tftp

Port: 69

Host: 0 . 0 . 0 . 0 (IP Address)

Path/File:

Target: ○ Server ● Local

File: flash:/

● flash ○ system ○ nvram ○ cf ○ usb1 ○ usb2

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. Select *Server* to indicate the source of the file is a remote server external to the controller or access point. 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: •*tftp* •*ftp* •*sftp* •*http* •*cf* •*usb1-4* 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. 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. 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. 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. 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. This parameter is required only when *Server* is selected as the Source.
Target	Select the target destination to transfer the file. •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. •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.

Restarting Adopted Devices

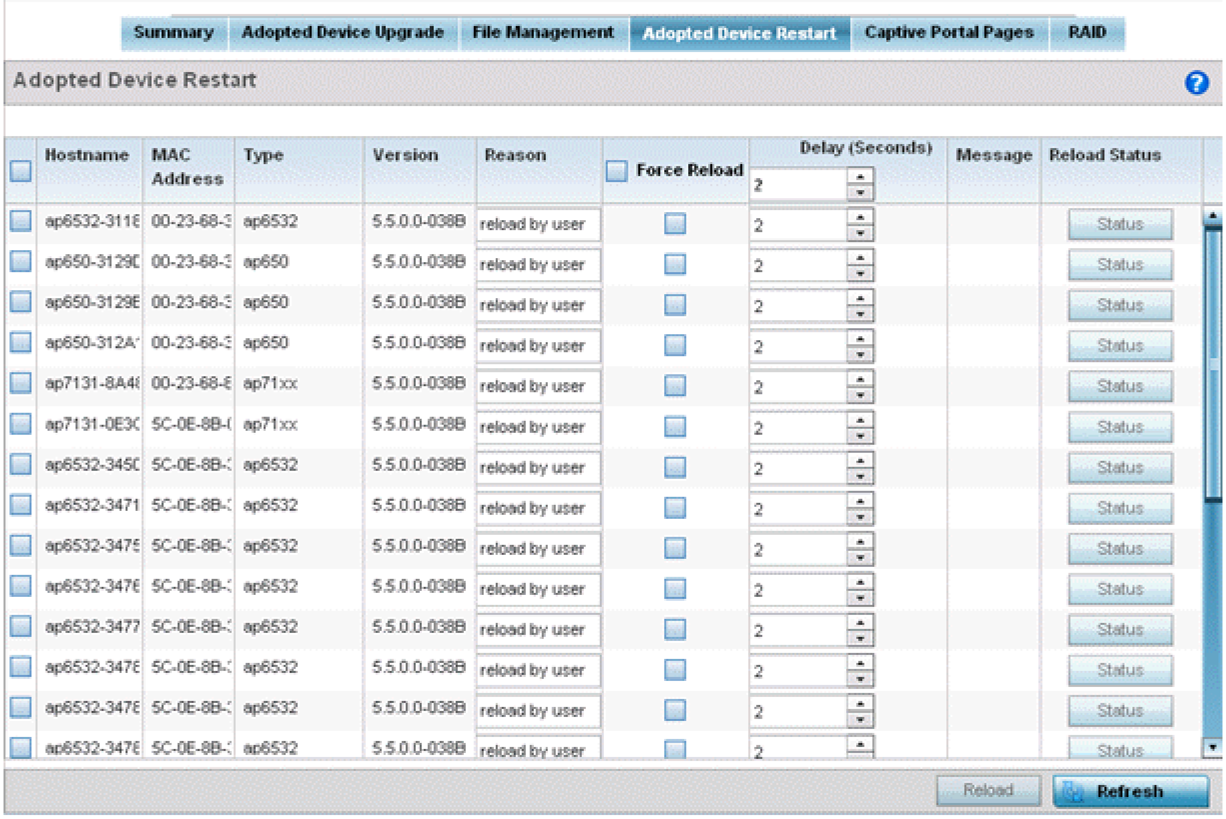
Controllers and service platforms can restart their adopted access points as needed for firmware upgrades or other administrative activities. access points set in Controller AP mode also have the ability to restart adopted peer model access points.

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.**



☐	Hostname	MAC Address	Type	Version	Reason	☐ Force Reload	Delay (Seconds)	Message	Reload Status
							2		
☐	ap6532-311	00-23-68-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap650-3129	00-23-68-	ap650	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap650-3129	00-23-68-	ap650	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap650-312A	00-23-68-	ap650	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap7131-8A4	00-23-68-	ap71xx	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap7131-0E3	5C-0E-8B-	ap71xx	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-345	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-3471	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-347	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-347	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-3477	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-347	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-347	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status
☐	ap6532-347	5C-0E-8B-	ap6532	5.5.0.0-038B	reload by user	☐	2		Status

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:

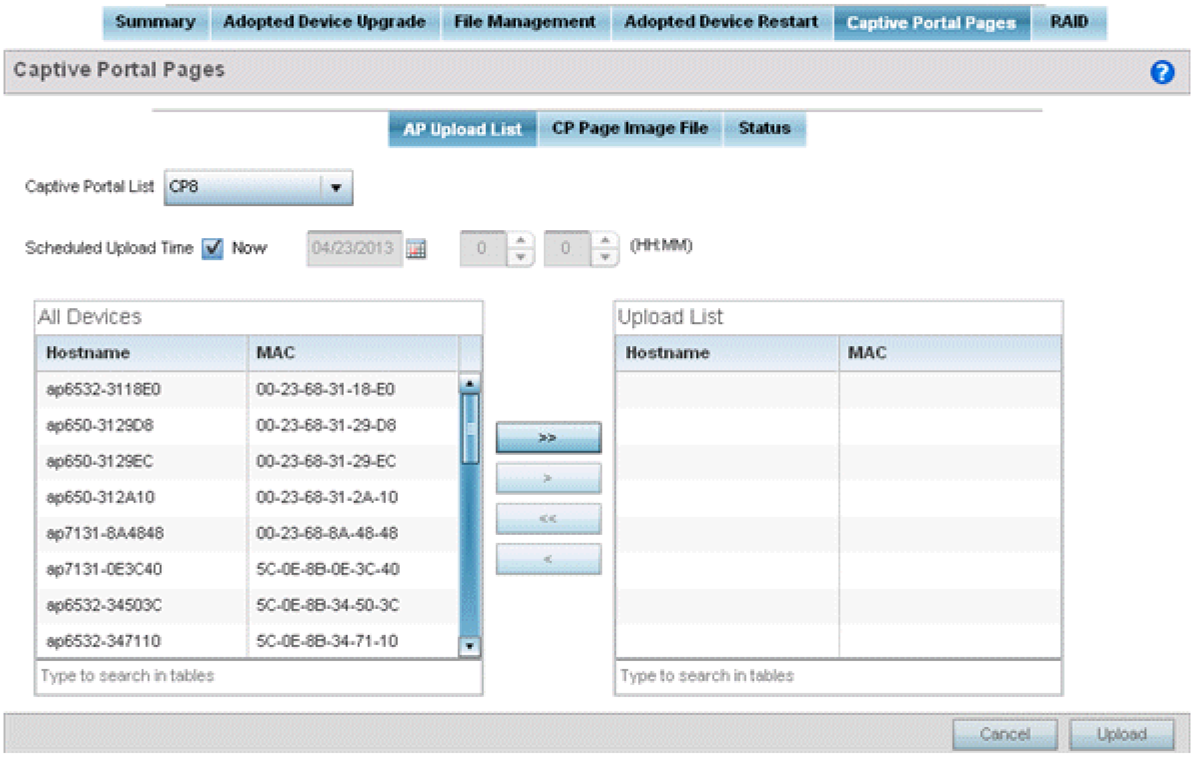
- AP Upload
- CP Page Image File
- Status

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.



Captive Portal List: CP8

Scheduled Upload Time ☑ Now 04/23/2013 0 0 (HH:MM)

All Devices

Hostname	MAC
ap6532-3118E0	00-23-68-31-18-E0
ap650-3129D8	00-23-68-31-29-D8
ap650-3129EC	00-23-68-31-29-EC
ap650-312A10	00-23-68-31-2A-10
ap7131-8A4848	00-23-68-8A-48-48
ap7131-0E3C40	5C-0E-8B-0E-3C-40
ap6532-34503C	5C-0E-8B-34-50-3C
ap6532-347110	5C-0E-8B-34-71-10

Type to search in tables

Upload List

Hostname	MAC

Type to search in tables

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

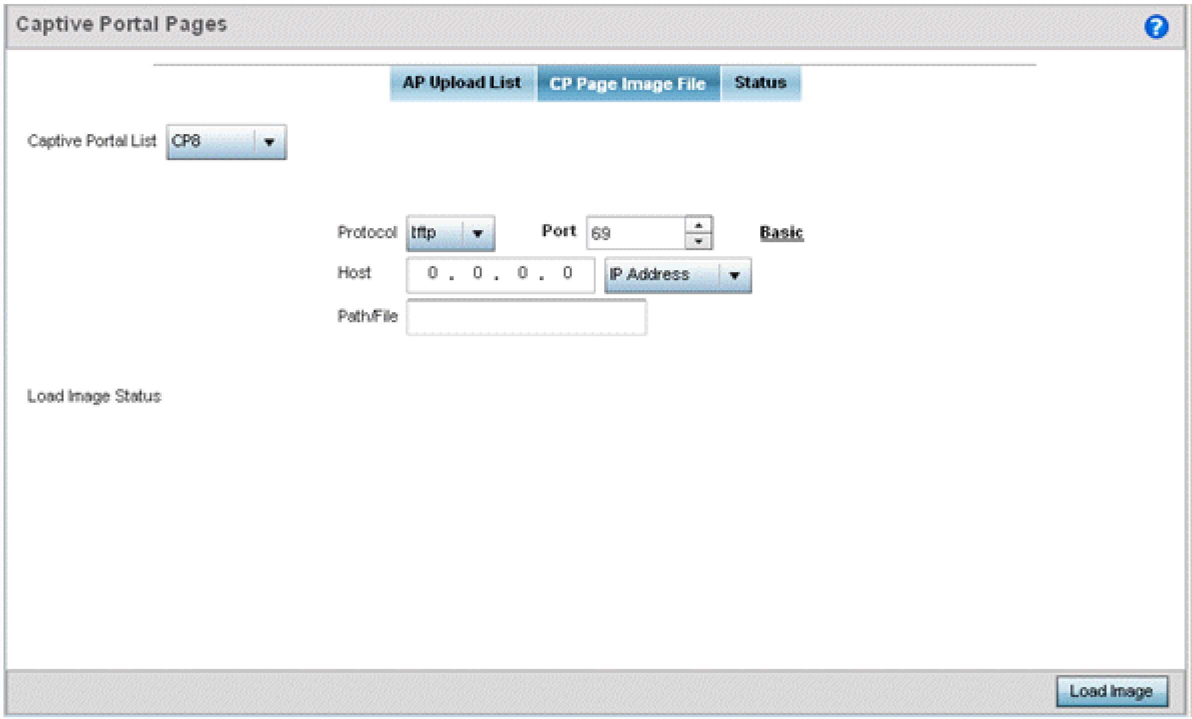
Use the **CP Pages Image File** screen to set the way managed access points receive captive portal images files required to provision captive portal access to requesting clients. Captive portal image files are the login, welcome and conditions pages specifically.

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.



Captive Portal List: CP8

Protocol: tftp

Port: 69

Host: 0 . 0 . 0 . 0

IP Address

Path/File

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.

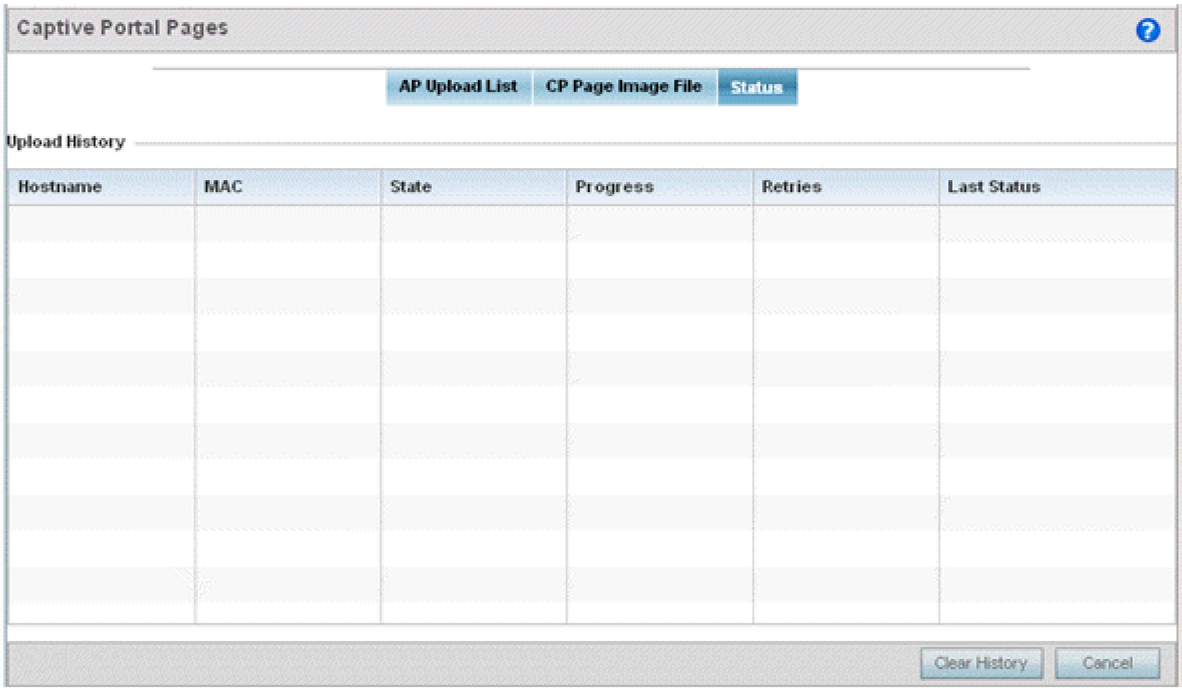
5 Select Load Image to upload the image file. Optionally, refer to the Load Image Status field to review the status of the current upload.

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.

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.

RAID

An administrator can configure a NX 95XX series RAID controller in respect to both its collective drive array as well as individual drive behavior and diagnostics. The service platform's array alarm can silenced, drive LEDs can be illuminated and stopped, drive consistency (integrity) checks can be made and the array can be prepared for drive replacements.

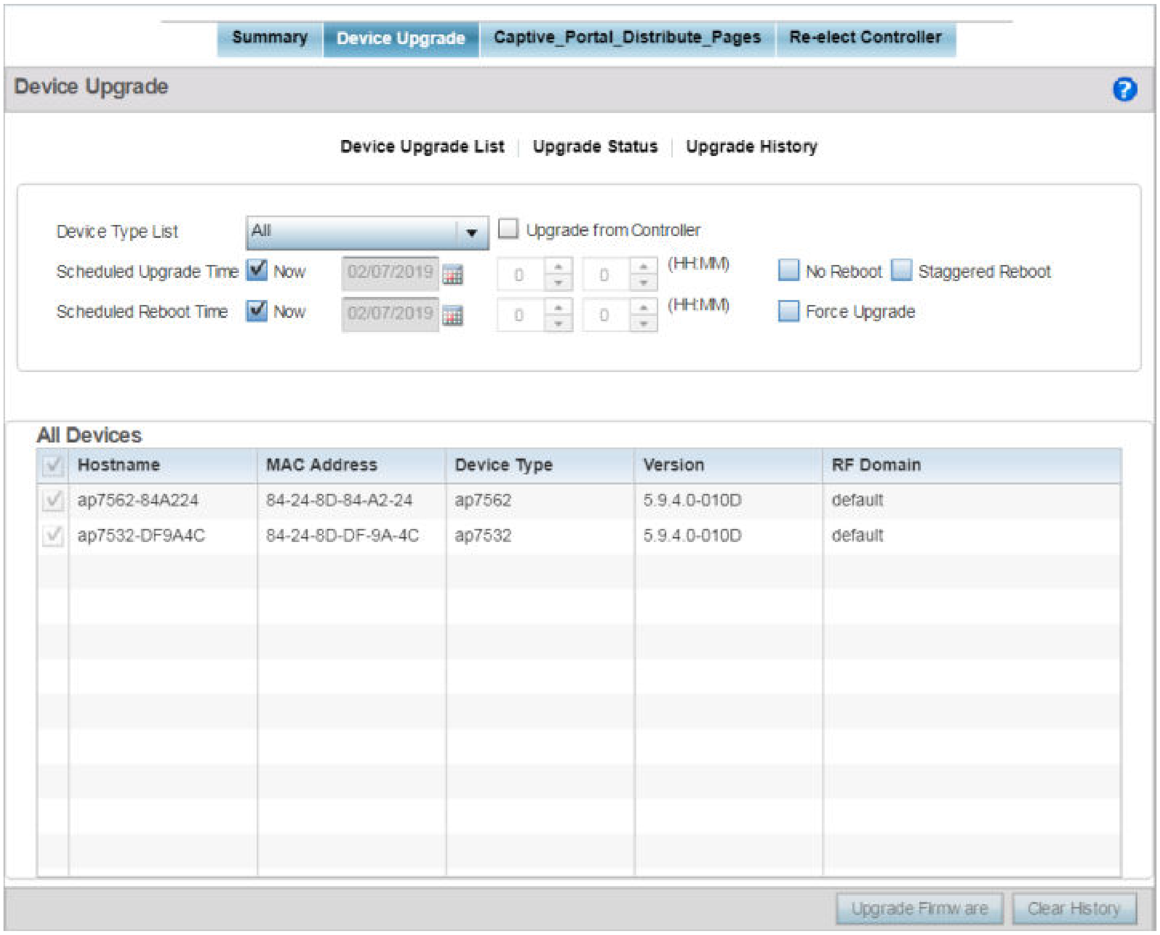
RAID controller drive arrays are available within the NX 95XX models only. However, they can be administrated on behalf of a NX 95XX profile by a different model service platform or controller.

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 954.

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.



Device Type List: All
☐ Upgrade from Controller
Scheduled Upgrade Time: ☑ Now 02/07/2019 0 0 (HH:MM) ☐ No Reboot ☐ Staggered Reboot
Scheduled Reboot Time: ☑ Now 02/07/2019 0 0 (HH:MM) ☐ Force Upgrade

All Devices

☑	Hostname	MAC Address	Device Type	Version	RF Domain
☑	ap7562-84A224	84-24-8D-84-A2-24	ap7562	5.9.4.0-010D	default
☑	ap7532-DF9A4C	84-24-8D-DF-9A-4C	ap7532	5.9.4.0-010D	default

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.

Re-elect Controller

Use the Tunnel Controller Re-election screen to identity available access point resources within a selected RF Domain and optionally make some, or all, of the Access Points available to initiate tunnel connections

---

Note

Take care when selecting access points for controller re-election, as client connections may be broken on upon re-election. Ensure an elected access point's client load can be compensated by another access point in the same RF Domain.

To re-elect controller adoption resources for tunnel establishment:

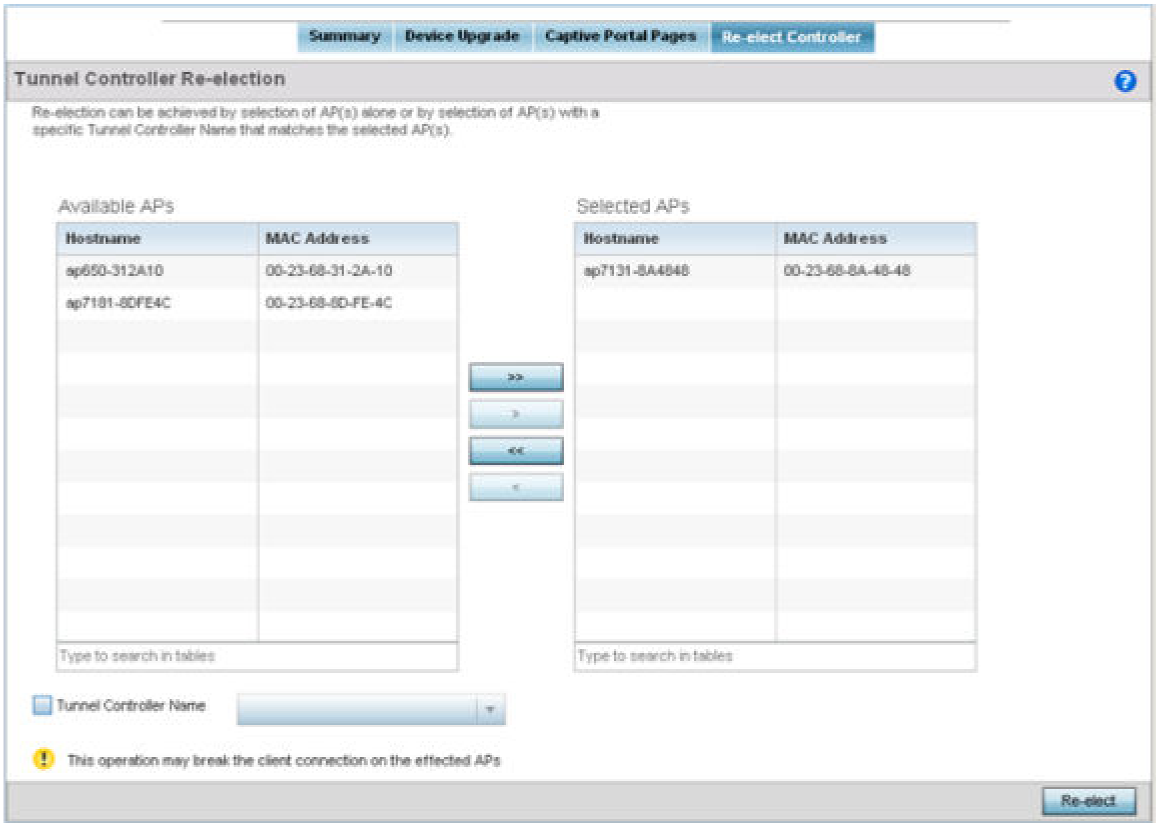
1. Select **Operations**.
2. Ensure a RF Domain is selected from the Operations menu on the top, left-hand, side of the screen. Otherwise, the Re-elect Controller screen cannot be located, as it does not display at either the system or device levels of the hierarchal tree.

3 Select the **Re-elect Controller** tab.

Note

The Re-elect Controller tab is only available at the RF Domain level of the UI’s hierarchal tree and is not available for individual controllers, service platforms and Access Points.

The Tunnel Controller Re-election screen diplays.



Re-election can be achieved by selection of AP(s) alone or by selection of AP(s) with a specific Tunnel Controller Name that matches the selected AP(s).

Available APs

Hostname	MAC Address
ap650-312A10	00-23-68-31-2A-10
ap7181-8DFE4C	00-23-68-8D-FE-4C

Selected APs

Hostname	MAC Address
ap7131-8A4848	00-23-68-8A-48-48

☐ Tunnel Controller Name

This operation may break the client connection on the effected APs

4 Refer to the Available APs column, and use the **>** button to move the selected access point into the list of Selected APs available for RF Domain Manager candidacy. Use the **>>** button to move all listed access points into the Selected APs table.

The re-election process can be achieved through the selection of an individual access point, or through the selection of several access points with a specific Tunnel Controller Name matching the selected access points.

5 Select **Re-elect** to designate the Selected AP(s) as resources capable of tunnel establishment.

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:

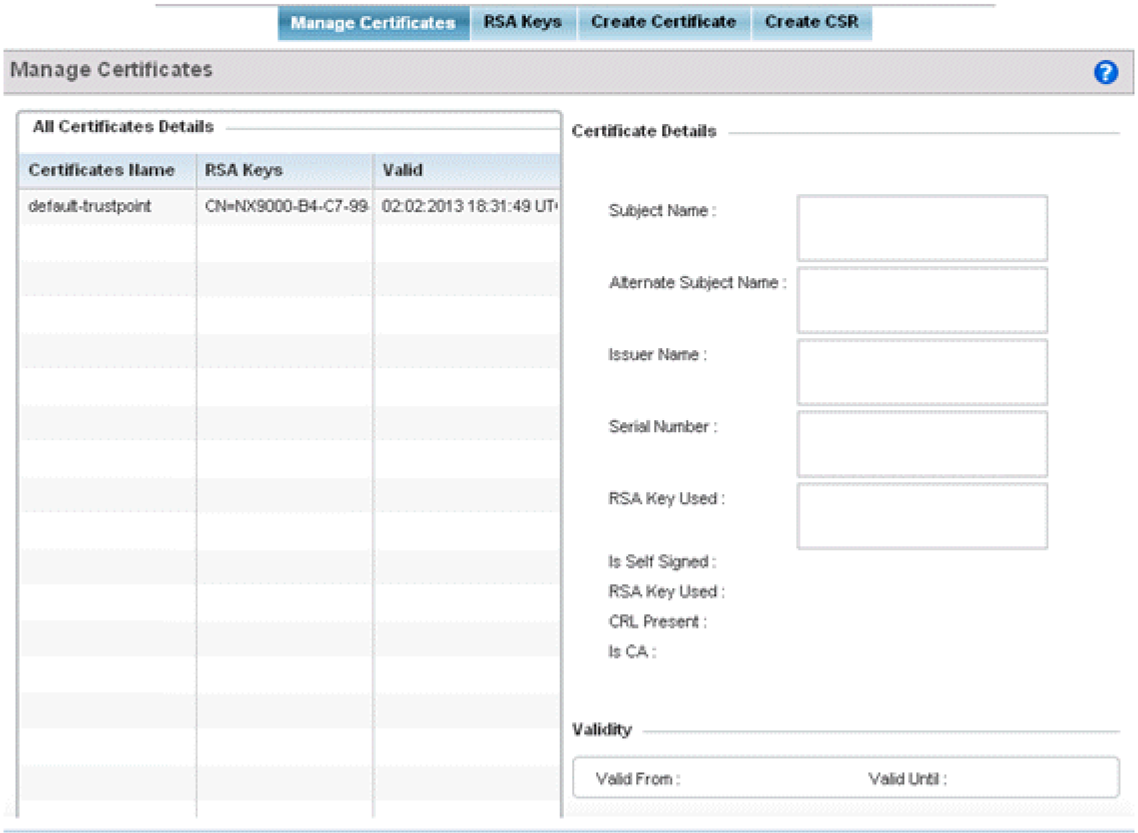
- Certificate Management on page 974
- RSA Key Management on page 983
- Certificate Creation on page 73
- Generating a Certificate Signing Request on page 74

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.



All Certificates Details

Certificates Name	RSA Keys	Valid
default-trustpoint	CN=NX9000-B4-C7-99	02:02:2013 18:31:49 UT

Certificate Details

Subject Name :
Alternate Subject Name :
Issuer Name :
Serial Number :
RSA Key Used :
Is Self Signed :
RSA Key Used :
CRL Present :
Is CA :

Validity

Valid From :
Valid Until :

The **Manage Certificates** screen displays for the selected MAC address.

3 Select a device from amongst those displayed to review its certificate.

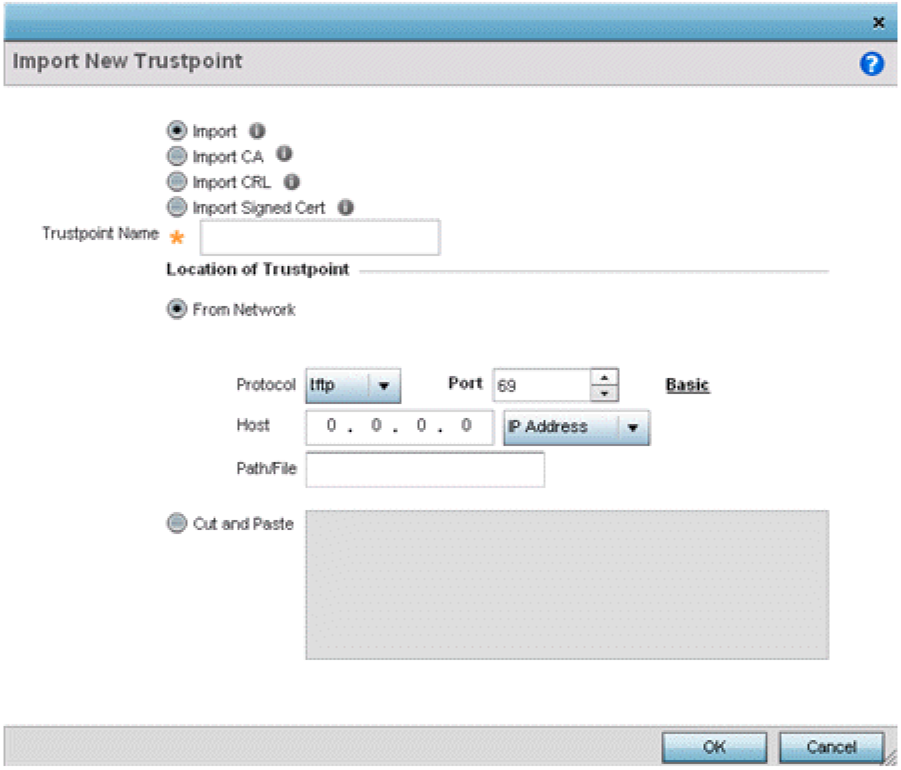
4 Refer to the **All Certificate Details** to review the certificate's properties, self-signed credentials, validity period and CA information.

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.



● Import

● From Network

Protocol: tftp

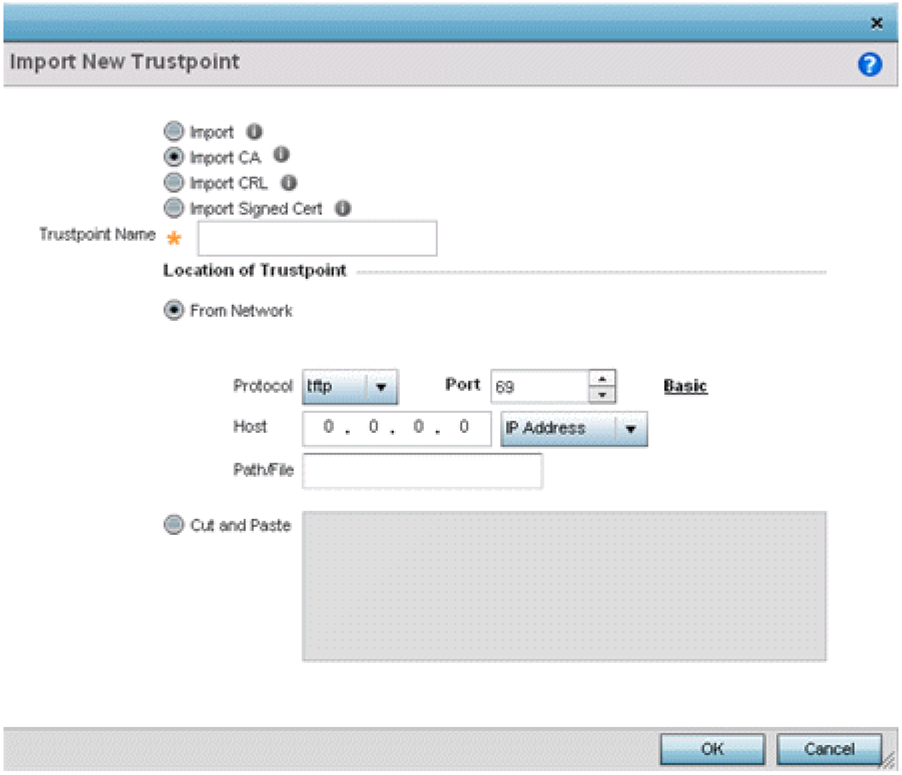
Port: 69

Host: 0 . 0 . 0 . 0 — IP Address

Figure 395: 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.



○ Import
● Import CA
○ Import CRL
○ Import Signed Cert

Trustpoint Name *

● From Network

Protocol: tftp
Port: 69
Host: 0 . 0 . 0 . 0 IP Address
Path/File:

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: • tftp • ftp • sftp • http • cf • usb1-4
Port	Set the port. This option is not valid for **`cf`** and **`usb1-4`**.

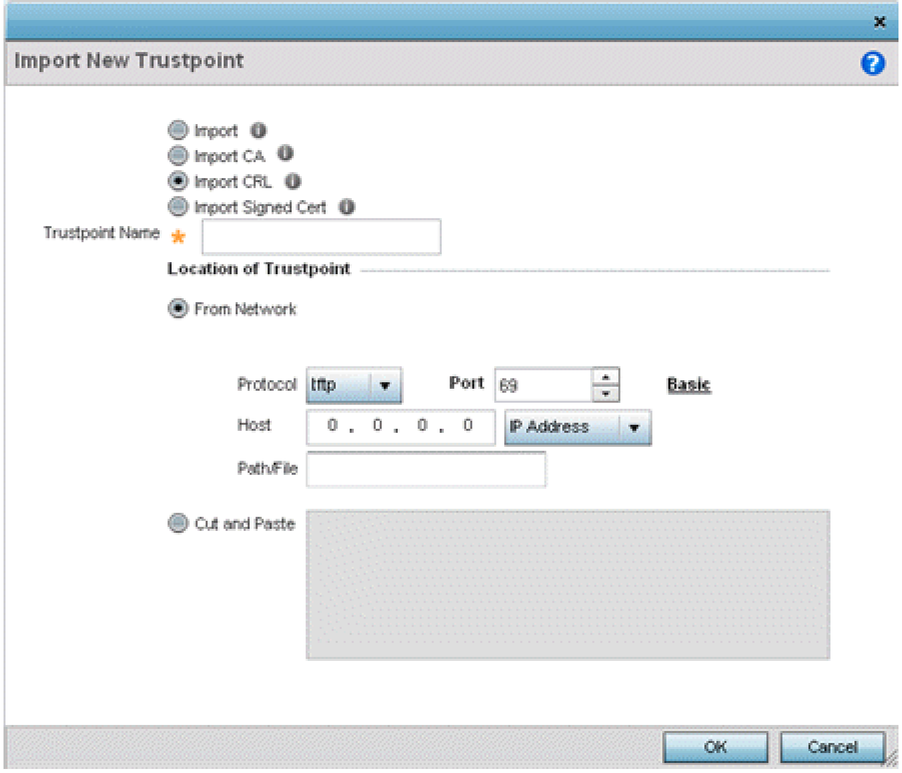
Host	Provide the hostname string or numeric IP address of the server used to import the trustpoint. Hostnames cannot include an underscore character. This option is not valid for `cf` and `usb1-4`. Select **IPv4 Address** to use an IPv4 formatted address as the host. Select **IPv6 Address** to use an 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.

For information on creating a CRL to use with a trustpoint, refer to Setting the Certificate Revocation List (CRL) Configuration on page 678 .



Import New Trustpoint

○ Import
○ Import CA
● Import CRL
○ Import Signed Cert

Trustpoint Name *

Location of Trustpoint

● From Network

Protocol: tftp
Port: 69
Host: 0 . 0 . 0 . 0 — IP Address
Path/File

○ Cut and Paste

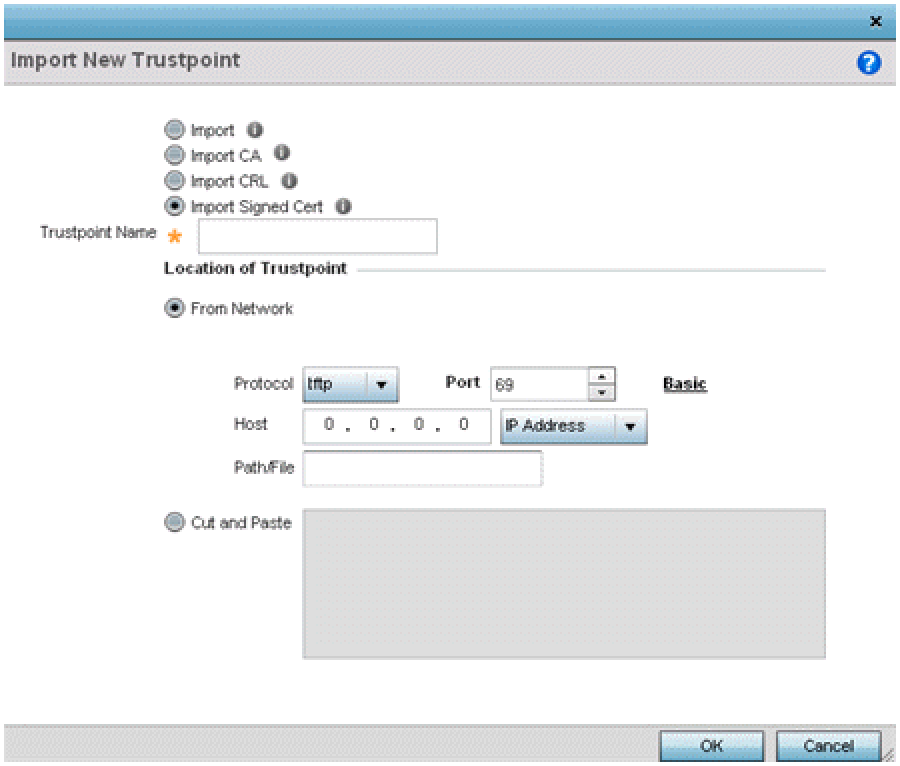
5 Define the following configuration parameters required to import a CRL:

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: • tftp • ftp • sftp • http • cf • 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`**. 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.



● Import Signed Cert

Trustpoint Name

● From Network

Protocol tftp

Port 69

Host 0 . 0 . 0 . 0 IP Address

Path/File

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: • tftp • ftp • sftp • http • cf • 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`. 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

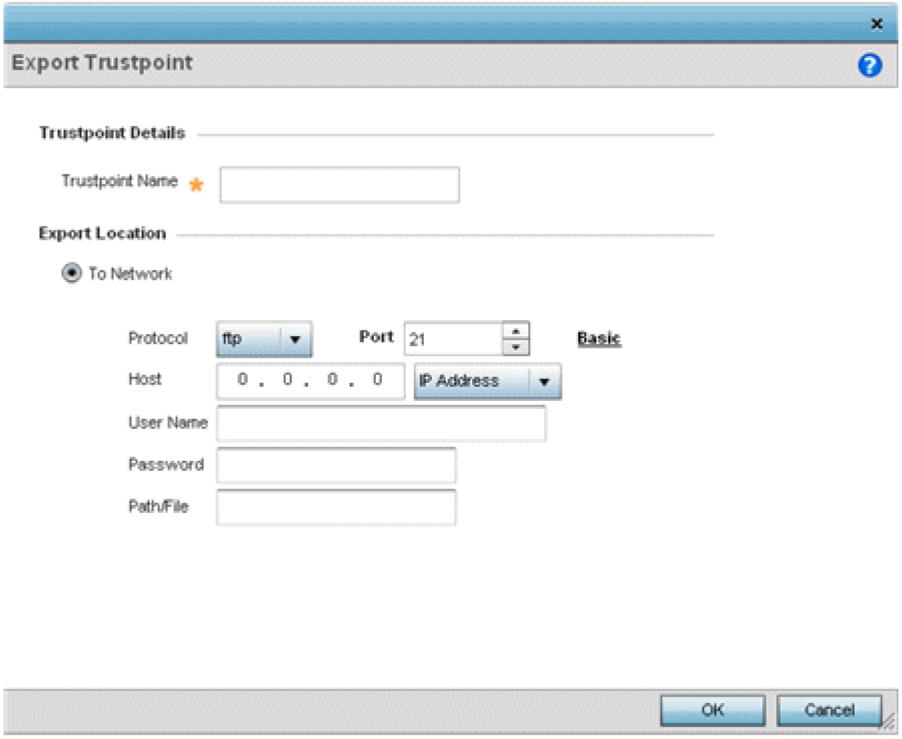
Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled 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.



Export Trustpoint

Trustpoint Details

Trustpoint Name *

Export Location

● To Network

Protocol: ftp

Port: 21

Host: 0 . 0 . 0 . 0 IP Address

User Name

Password

Path/File

Figure 396: 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: • tftp • ftp • sftp • http • cf • 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`. 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.

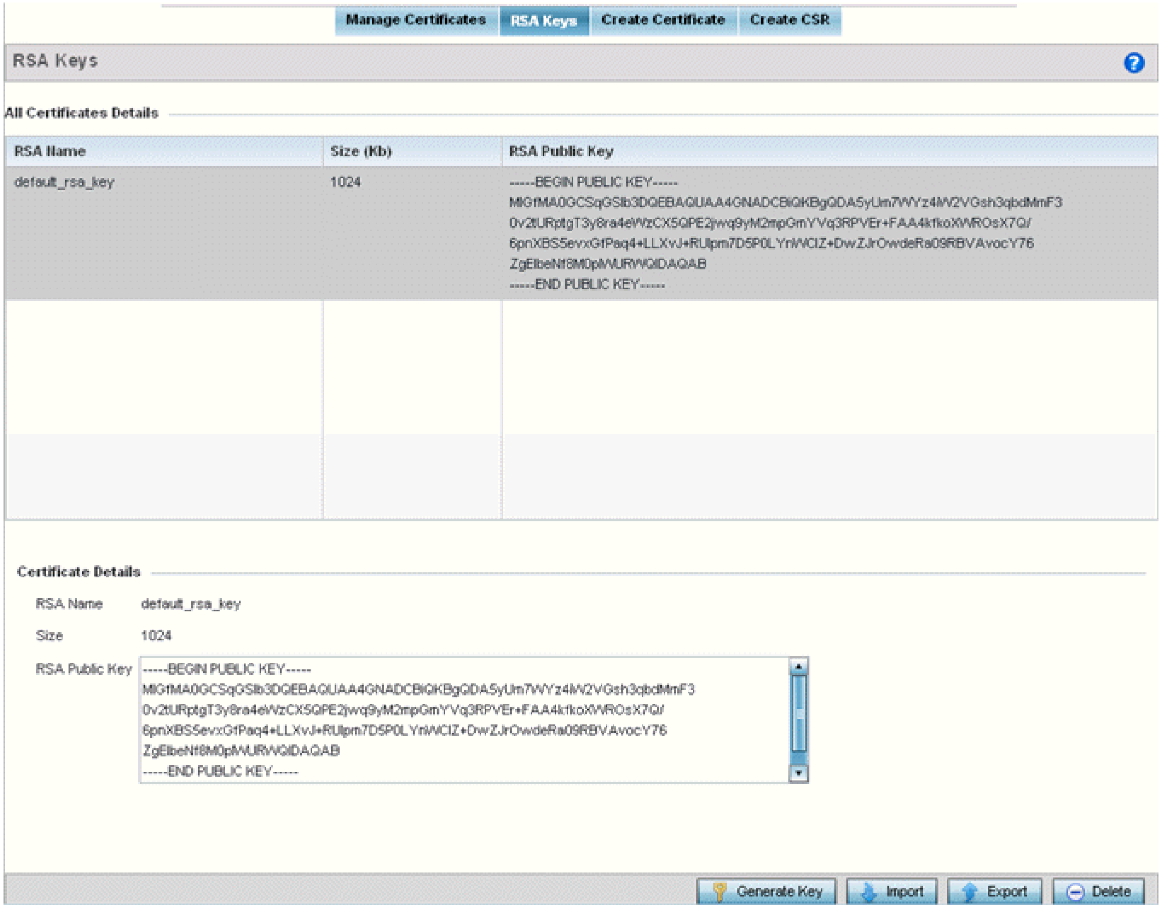
RSA Key Management

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.



RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5yUm7WYz4lW2VGsh3qbdMmF3 0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4kfkoXWROsX7Q/ 6pnXBS5evxGfPaq4+LLXvJ+RUlpm7D5P0LYnWCIZ+DwZJrOwdeRa09RBVAvocY76 ZgElbeNf8M0pWURWQIDAQAB -----END PUBLIC KEY-----

RSA Name default_rsa_key

Size 1024

RSA Public Key

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5yUm7WYz4lW2VGsh3qbdMmF3
0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4kfkoXWROsX7Q/
6pnXBS5evxGfPaq4+LLXvJ+RUlpm7D5P0LYnWCIZ+DwZJrOwdeRa09RBVAvocY76
ZgElbeNf8M0pWURWQIDAQAB
-----END PUBLIC KEY-----
```

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.

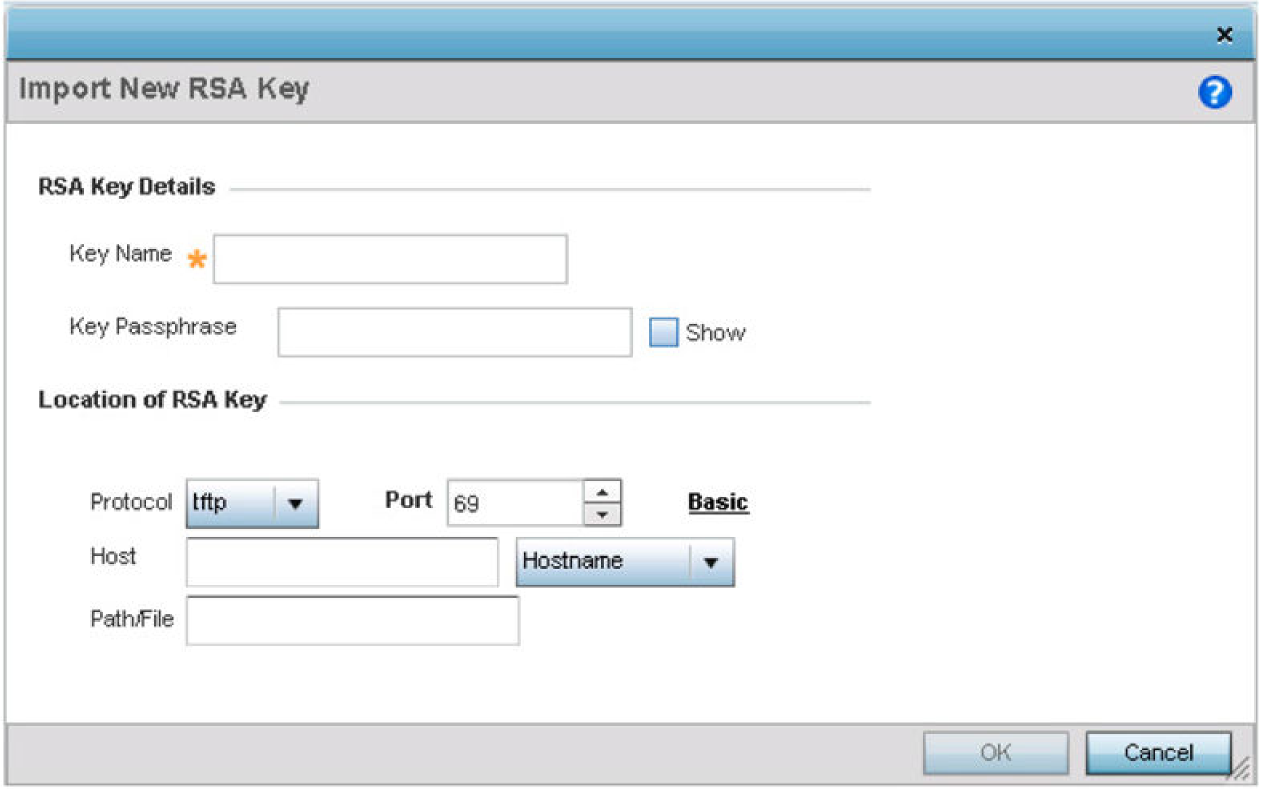


Figure 397: Certificate Management - Import New RSA Key Screen

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: • tftp • ftp • sftp • http • cf • 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`. 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

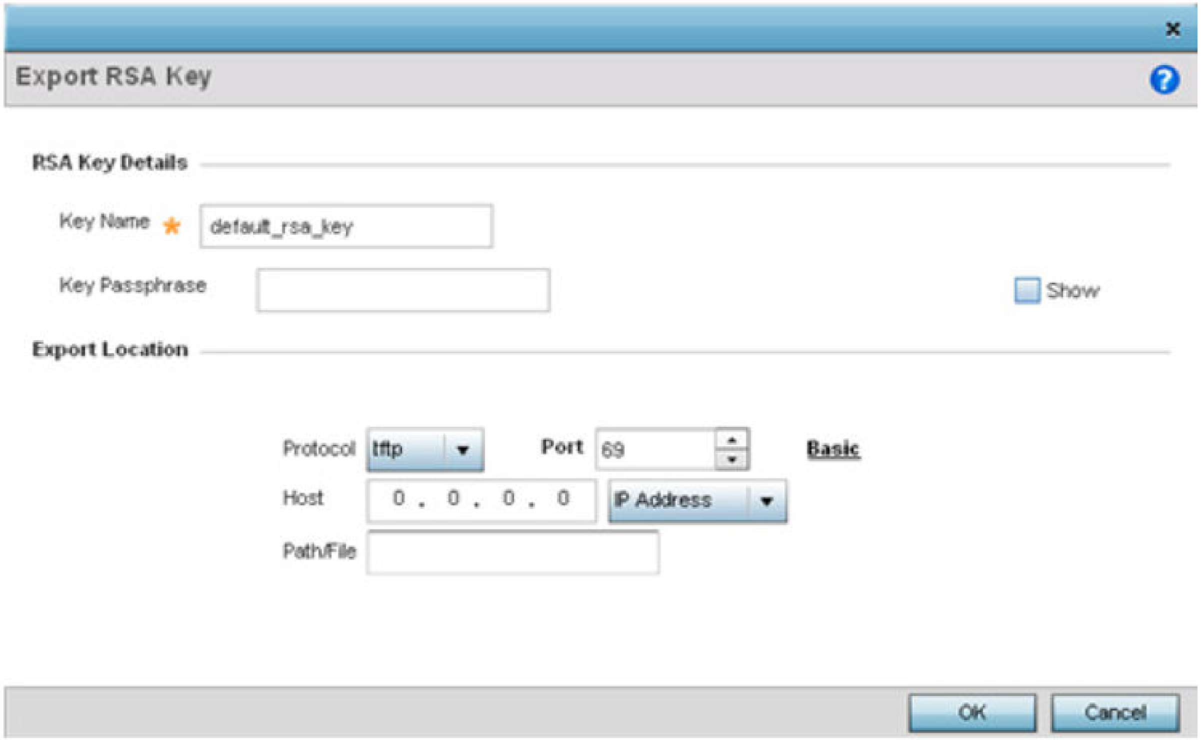
The keys utilized by a controller, service platform or access point can be exported to an external resource for archive and future use.

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.



Key Name * default_rsa_key

Key Passphrase

☐ Show

Protocol tftp

Port 69

Host 0 . 0 . 0 . 0 IP Address

Path/File

Figure 398: 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: • tftp • ftp • sftp • http • cf • 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`. 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:

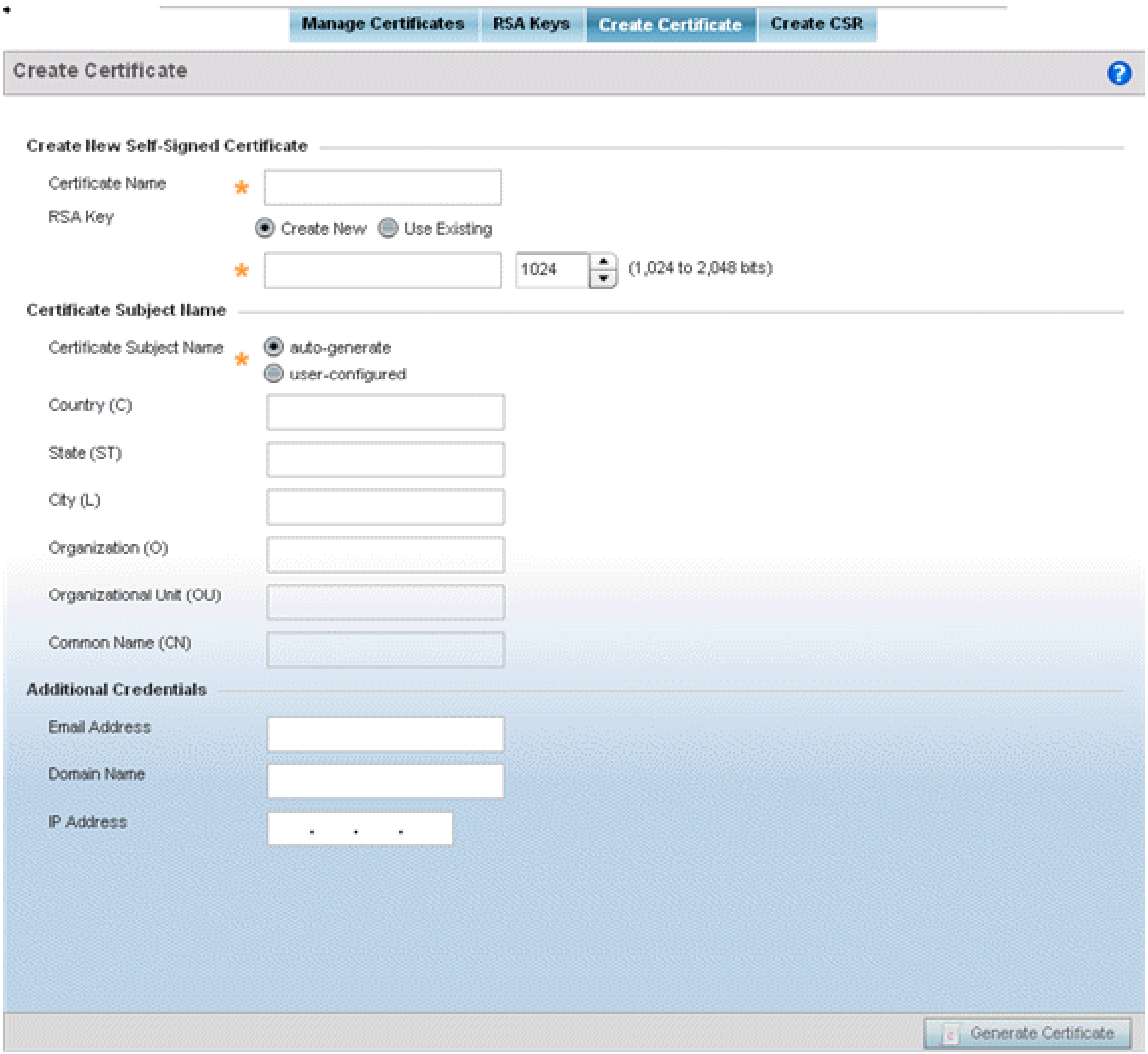
1. Select **RSA Keys** tab from the Certificate Management screen.
2. Select the **Delete** button from within the RSA Keys tab.
3. Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate.
4. Select **OK** to proceed with the deletion, or **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.



RSA Key ● Create New ○ Use Existing

1024 (1,024 to 2,048 bits)

Certificate Subject Name ● auto-generate ○ user-configured

Figure 399: 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.

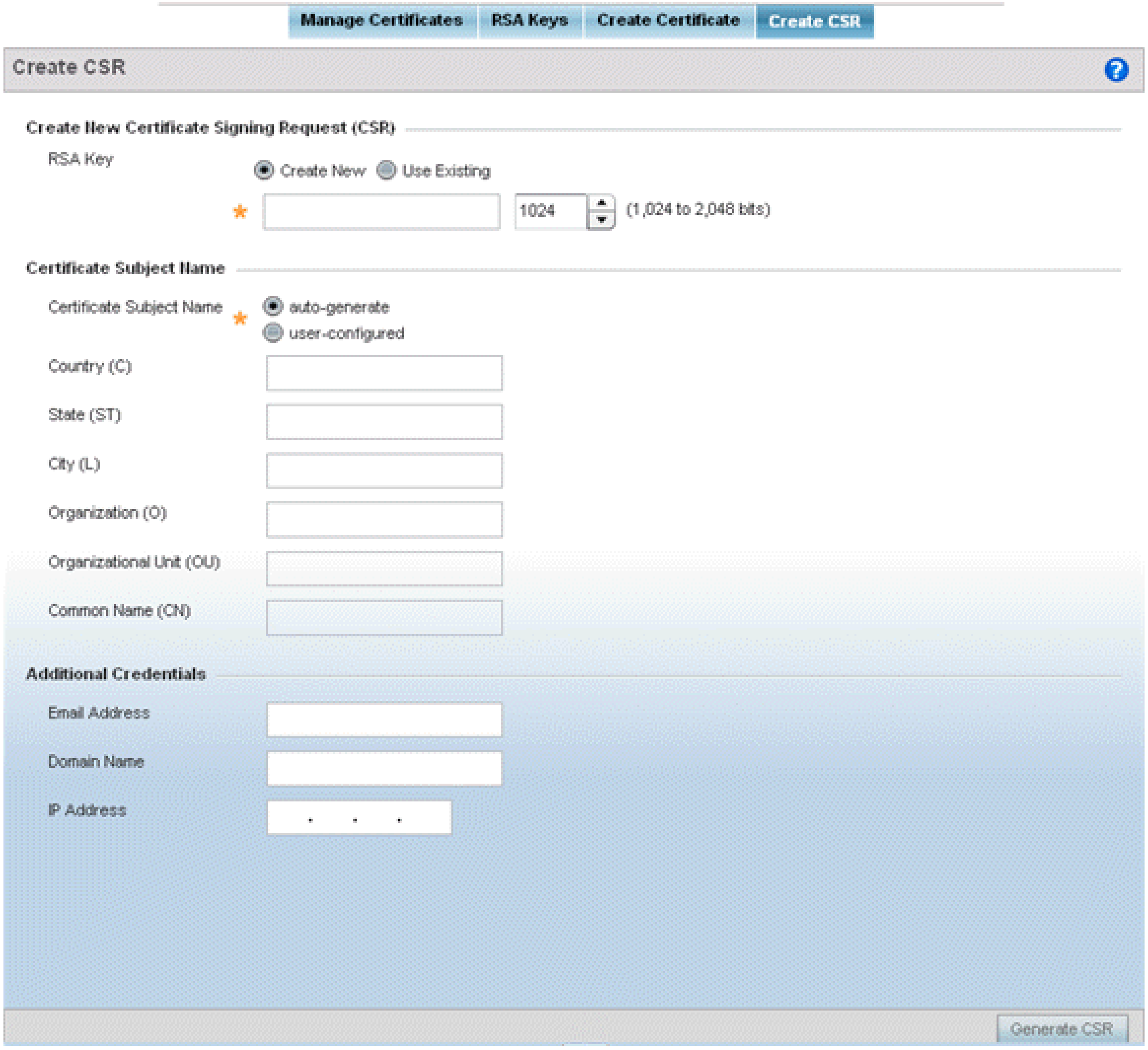


Figure 400: Certificate Management - Create CSR Screen

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.

Smart RF is supported in standalone and clustered environments. In standalone environments, an individual controller, service platform or access point manages the calibration and monitoring phases. In clustered environments, a Smart Scan master is elected, and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart Scan master coordinates calibration and configuration and during the monitoring phase receives information from the Smart RF clients. Smart RF calibration can be triggered manually or continues at run-time, all the time.

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

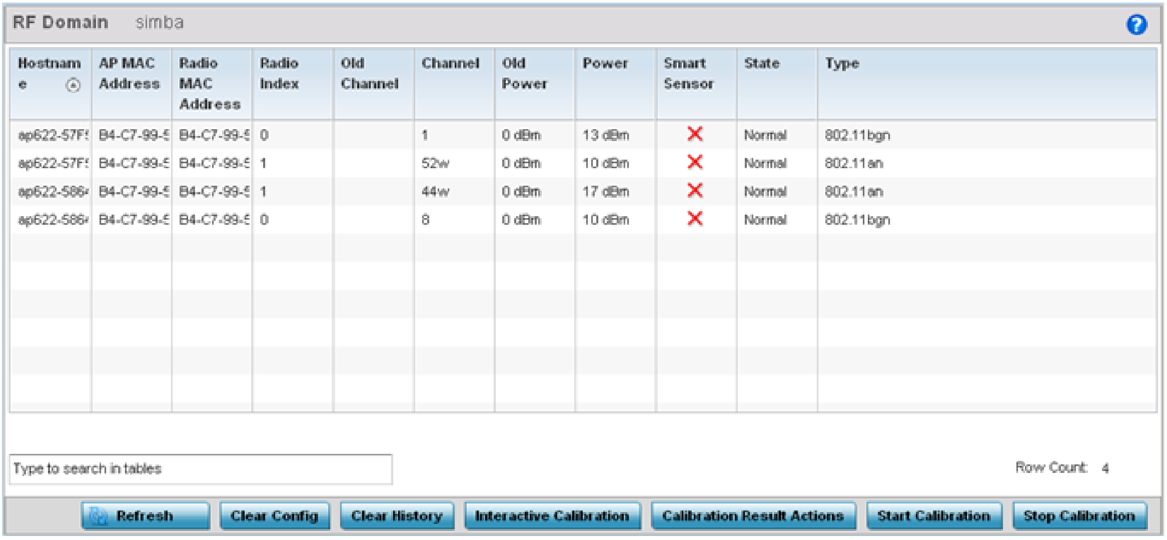
When calibration is initiated, Smart RF instructs adopted radios (within a selected RF Domain) to beacon on a specific legal channel, using a specific transmit power setting. Smart RF measures the signal strength of each beacon received from both managed and unmanaged neighboring APs to define a RF map 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. Expand the System mode in the upper, left-hand, side of the user interface to display the RF Domains available for Smart RF calibration.
4. Select a RF Domain from amongst those displayed.

   The Smart RF screen displays information specific to the devices within the selected RF Domain using data from the last interactive calibration.



RF Domain simba

Hostname	AP MAC Address	Radio MAC Address	Radio Index	Old Channel	Channel	Old Power	Power	Smart Sensor	State	Type
ap622-57F	B4-C7-99-	B4-C7-99-	0		1	0 dBm	13 dBm	✗	Normal	802.11bgn
ap622-57F	B4-C7-99-	B4-C7-99-	1		52w	0 dBm	10 dBm	✗	Normal	802.11an
ap622-586	B4-C7-99-	B4-C7-99-	1		44w	0 dBm	17 dBm	✗	Normal	802.11an
ap622-586	B4-C7-99-	B4-C7-99-	0		8	0 dBm	10 dBm	✗	Normal	802.11bgn

Row Count: 4

5. 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.

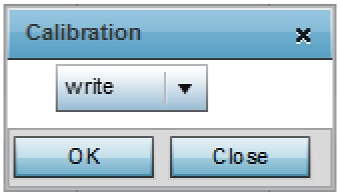
Radio Index	Displays a numerical index assigned to each listed access point radio when it was added to the network. This index helps distinguish this radio from others within this RF Domain with similar configurations. This value is not subject to change as a result of a calibration activity, but each 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.

6 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.

7 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.

8 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.

9 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.

10 The calibration process can be stopped by selecting the **Stop Calibration** button.

15 Statistics

System Statistics
RF Domain Statistics
Controller Statistics
EX3500 Interface Extended IF
Access Point Statistics
Wireless Client Statistics
Guest Access Statistics

This chapter describes statistics displayed by the GUI *(graphical user interface)*. Statistics are available for controllers or service platforms 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.

RFS controller and NX series service platform statistics (both available under Wireless Controller 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.

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 996
- RF Domain Statistics on page 1009
- Controller Statistics on page 1060
- Wireless Client Statistics on page 1334
- Guest Access Statistics on page 1346

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
- Licenses
- WIPS Summary

The following devices can report system data:

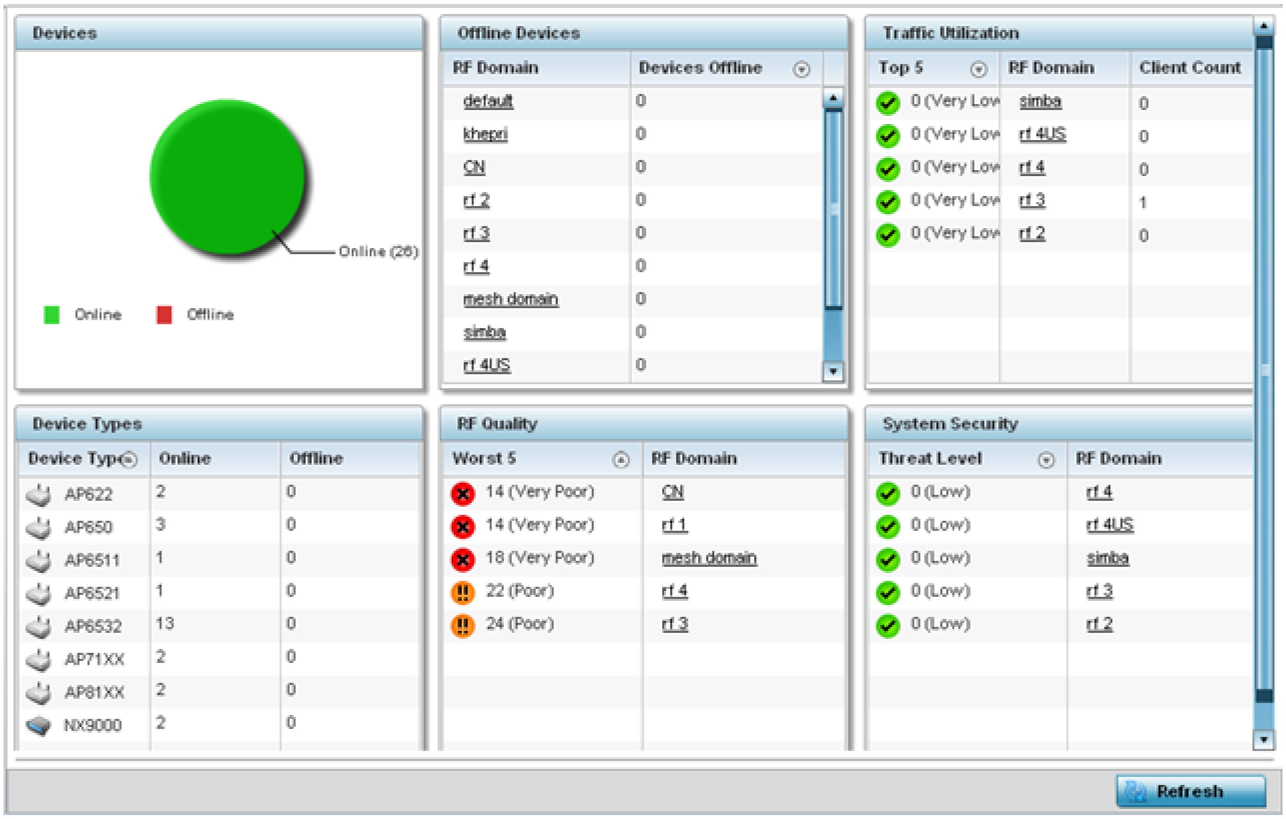
- Access Points - AP 6522, AP 6562, AP 7161, AP 7502, AP-7522, AP 7532, AP 7562, AP 7602, AP-7612, AP 7622, AP7632, AP7662, AP-8163, AP-8432, AP-8533
- Wireless Controllers - RFS 4000
- Service Platforms - NX 5500, NX 7510, NX 95XX, NX 96XX, VX

Health

The **Health** screen displays the overall performance of the controller or service platform 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.



Offline Devices

RF Domain	Devices Offline
default	0
khepri	0
CN	0
rf 2	0
rf 3	0
rf 4	0
mesh domain	0
simba	0
rf 4US	0

Traffic Utilization

Top 5	RF Domain	Client Count
✓ 0 (Very Low	simba	0
✓ 0 (Very Low	rf 4US	0
✓ 0 (Very Low	rf 4	0
✓ 0 (Very Low	rf 3	1
✓ 0 (Very Low	rf 2	0

Device Types

Device Type	Online	Offline
AP622	2	0
AP650	3	0
AP6511	1	0
AP6521	1	0
AP6532	13	0
AP71XX	2	0
AP81XX	2	0
NX9000	2	0

RF Quality

Worst 5	RF Domain
✗ 14 (Very Poor)	CN
✗ 14 (Very Poor)	rf 1
✗ 18 (Very Poor)	mesh domain
‼ 22 (Poor)	rf 4
‼ 24 (Poor)	rf 3

System Security

Threat Level	RF Domain
✓ 0 (Low)	rf 4
✓ 0 (Low)	rf 4US
✓ 0 (Low)	simba
✓ 0 (Low)	rf 3
✓ 0 (Low)	rf 2

Figure 401: Statistics - System - Health Screen

3 The Devices table displays the total number of devices in the controller or service platform managed managed 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 Traffic Utilization table displays the top 5 RF Domains with the most effective resource utilization. Utilization is dependent on the number of devices connected to the RF Domain.

Top 5	Displays the top 5 RF Domains in terms of usage index. Utilization index is a measure of how efficiently the domain is utilized. This value is defined as a percentage of current throughput relative to the maximum possible throughput. The values are: • 0-20 – Very low utilization • 20-40 – Low utilization • 40-60 – Moderate utilization • 60 and above – High utilization
RF Domain	Displays the name of the RF Domain. Each listed RF Domain can be selected to display device membership and performance data in greater detail.
Client Count	Displays the number of wireless clients associated with the RF Domain.

6 The **Device Types** table displays the kinds of devices detected within the system. Each device type displays the number currently online and offline.

7 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: • 0-50 – Poor Quality • 50-75 – Medium Quality • 75-100 – Good Quality
RF Domain	Displays the name of the RF Domain wherein system statistics are polled for the poorly performing device.

8 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 wireless controller or service platform.

Threat Level	Displays the threat perception value. This value can be interpreted as: • 0-2 – Low threat level • 3-4 – Moderate threat level • 5 – High threat level
RF Domain	Displays the name of the target RF Domain for which the threat level is displayed.

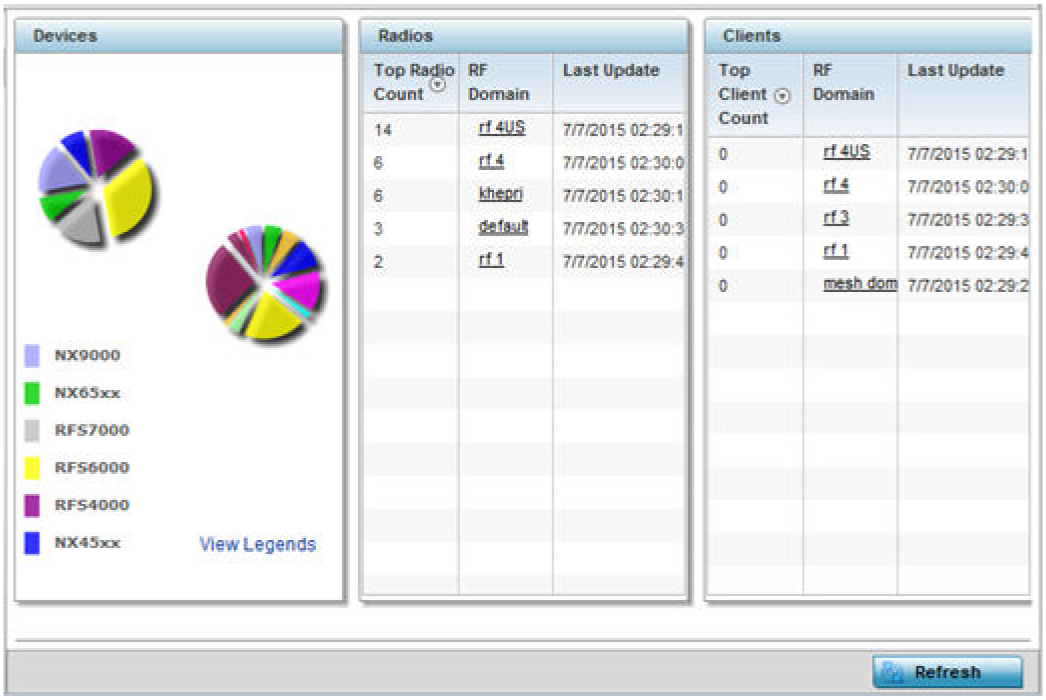
9 Select **Refresh** at any time to update the statistics counters to their latest values.

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.



Top Radio Count	RF Domain	Last Update
14	rf 4US	7/7/2015 02:29:1
6	rf 4	7/7/2015 02:30:0
6	khepri	7/7/2015 02:30:1
3	default	7/7/2015 02:30:3
2	rf 1	7/7/2015 02:29:4

Top Client Count	RF Domain	Last Update
0	rf 4US	7/7/2015 02:29:1
0	rf 4	7/7/2015 02:30:0
0	rf 3	7/7/2015 02:29:3
0	rf 1	7/7/2015 02:29:4
0	mesh dom	7/7/2015 02:29:2

2 The **Devices** table displays an exploded pie chart depicting the controller, service platform and access point device type distribution by model. The device on the left displays managing controller models. Select View Legends to assess connected access points. 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 wireless controller or service platform 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 wireless controller or service platform. 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

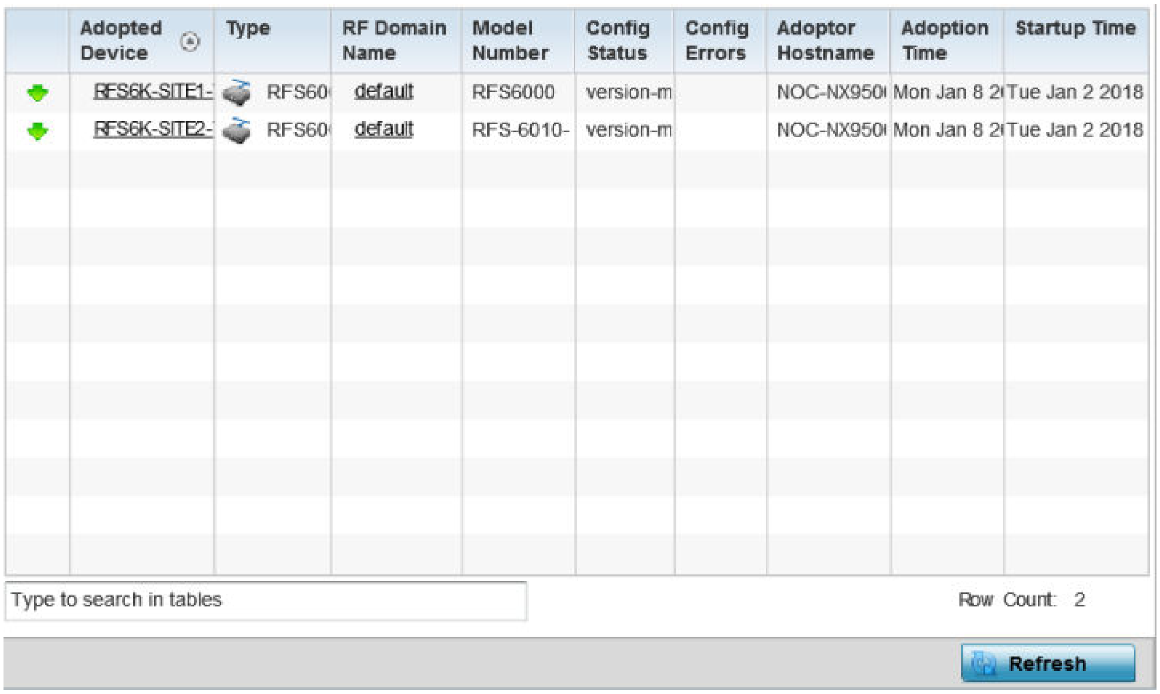
The **Adopted Devices** screen displays a list of devices adopted to the wireless controller or service platform managed network. Use this screen to view a list of devices and their current status.

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.



	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Config Errors	Adoptor Hostname	Adoption Time	Startup Time
↓	RFS6K-SITE1-	RFS60	default	RFS6000	version-m		NOC-NX950	Mon Jan 8 2	Tue Jan 2 2018
↓	RFS6K-SITE2-	RFS60	default	RFS-6010-	version-m		NOC-NX950	Mon Jan 8 2	Tue Jan 2 2018

Row Count: 2

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

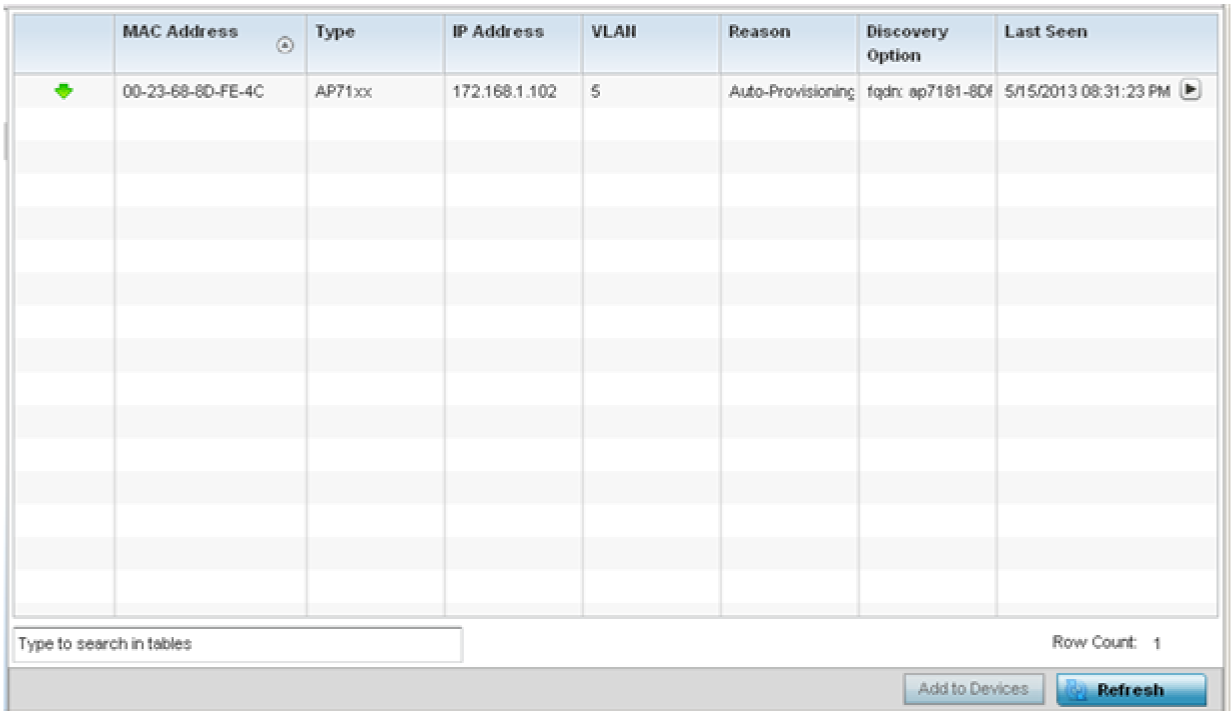
4 Click **Refresh** to update the statistics counters to their latest values.

Pending Adoptions

The Pending Devices screen displays those devices detected within a controller or service platform 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.



	MAC Address	Type	IP Address	VLAN	Reason	Discovery Option	Last Seen
▼	00-23-68-8D-FE-4C	AP71xx	172.168.1.102	5	Auto-Provisioning	fqdn: ap7181-8D	5/15/2013 08:31:23 PM ▶

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.

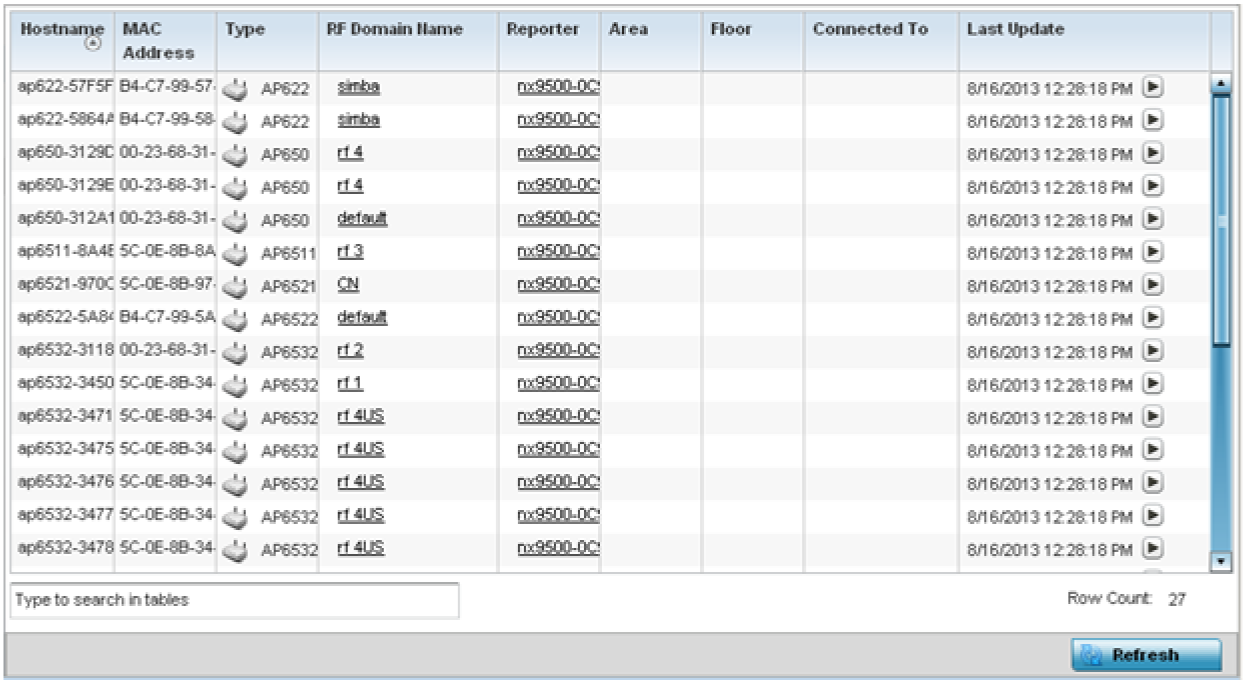
4. Click **Refresh** to update the statistics counters to their latest values.

Offline Devices

The **Offline Devices** screen displays a list of devices within the wireless controller or service platform 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.



Hostname	MAC Address	Type	RF Domain Name	Reporter	Area	Floor	Connected To	Last Update
ap622-57F5F	B4-C7-99-57-	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM
ap622-5864	B4-C7-99-58-	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM
ap650-3129	00-23-68-31-	AP650	rf 4	nx9500-0C				8/16/2013 12:28:18 PM
ap650-3129E	00-23-68-31-	AP650	rf 4	nx9500-0C				8/16/2013 12:28:18 PM
ap650-312A1	00-23-68-31-	AP650	default	nx9500-0C				8/16/2013 12:28:18 PM
ap6511-8A4	5C-0E-8B-8A	AP6511	rf 3	nx9500-0C				8/16/2013 12:28:18 PM
ap6521-970	5C-0E-8B-97-	AP6521	CN	nx9500-0C				8/16/2013 12:28:18 PM
ap6522-5A8	B4-C7-99-5A	AP6522	default	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3118	00-23-68-31-	AP6532	rf 2	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3450	5C-0E-8B-34-	AP6532	rf 1	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3471	5C-0E-8B-34-	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3475	5C-0E-8B-34-	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3476	5C-0E-8B-34-	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3477	5C-0E-8B-34-	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3478	5C-0E-8B-34-	AP6532	rf 4US	nx9500-0C				8/16/2013 12:28:18 PM

The **Offline Devices** screen lists the following information:

Hostname	Lists the administrator assigned hostname provided when the device was detected within the controller, service platform or access point managed 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 the date and time stamp of the last time the device was detected within the controller or service platform managed network. Select the arrow next to the date and time to toggle between standard time and UTC.

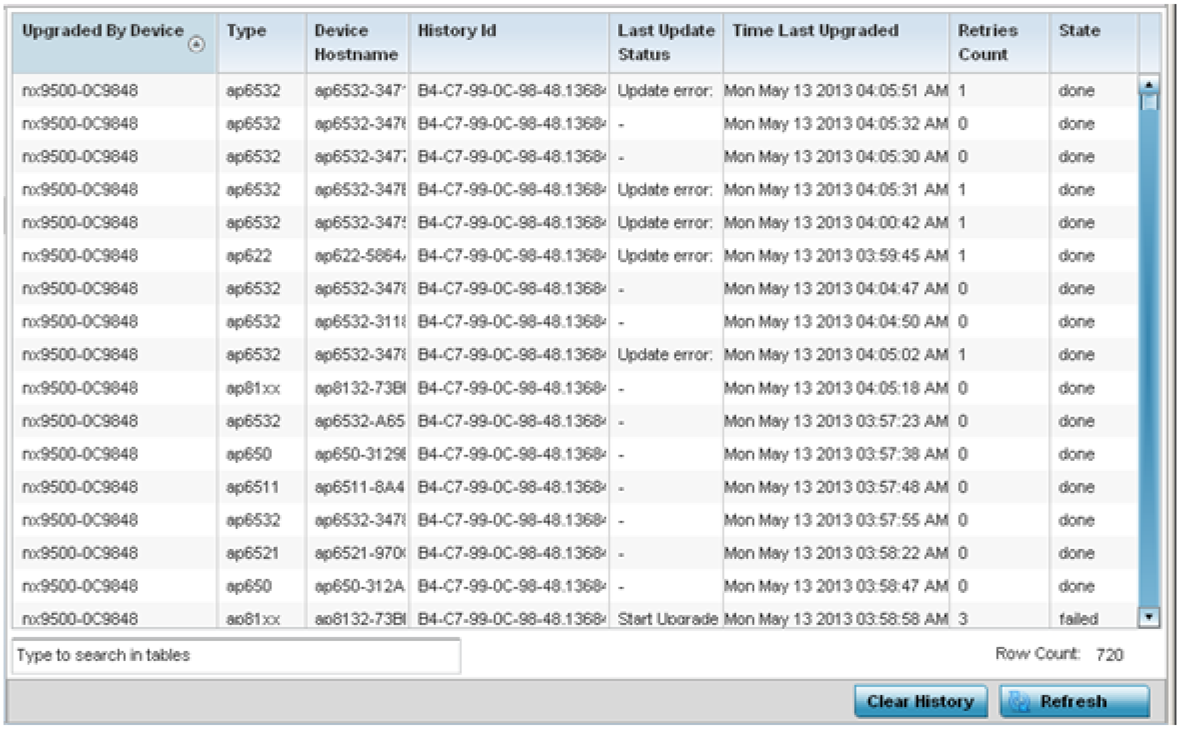
4 Click **Refresh** to update the statistics counters to their latest values.

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.



Upgraded By Device	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:51 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:32 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:30 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:31 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:00:42 AM	1	done
nx9500-0C9848	ap622	ap622-5864	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 03:59:45 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:47 AM	0	done
nx9500-0C9848	ap6532	ap6532-311	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:50 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:02 AM	1	done
nx9500-0C9848	ap81xx	ap8132-73B	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:18 AM	0	done
nx9500-0C9848	ap6532	ap6532-A65	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:23 AM	0	done
nx9500-0C9848	ap650	ap650-3129	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:38 AM	0	done
nx9500-0C9848	ap6511	ap6511-8A4	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:48 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:55 AM	0	done
nx9500-0C9848	ap6521	ap6521-970	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:22 AM	0	done
nx9500-0C9848	ap650	ap650-312A	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:47 AM	0	done
nx9500-0C9848	ap81xx	ap8132-73B	B4-C7-99-0C-98-48.1368	Start Upgrade	Mon May 13 2013 03:58:58 AM	3	failed

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.

Licenses

The Licenses statistics screen displays available licenses for devices within a cluster. It displays the total number of AP licenses. Native (local) and Guest license utilization can now be separately tracked as well.

To view a licenses statistics within the controller or service platform managed network:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** node from the left navigation pane.
3. Select **Licenses** from the left-hand side of the UI.

   The Native Summary tab displays by default.

   > Note
   > For more information on the Native License Summary screen, click here.

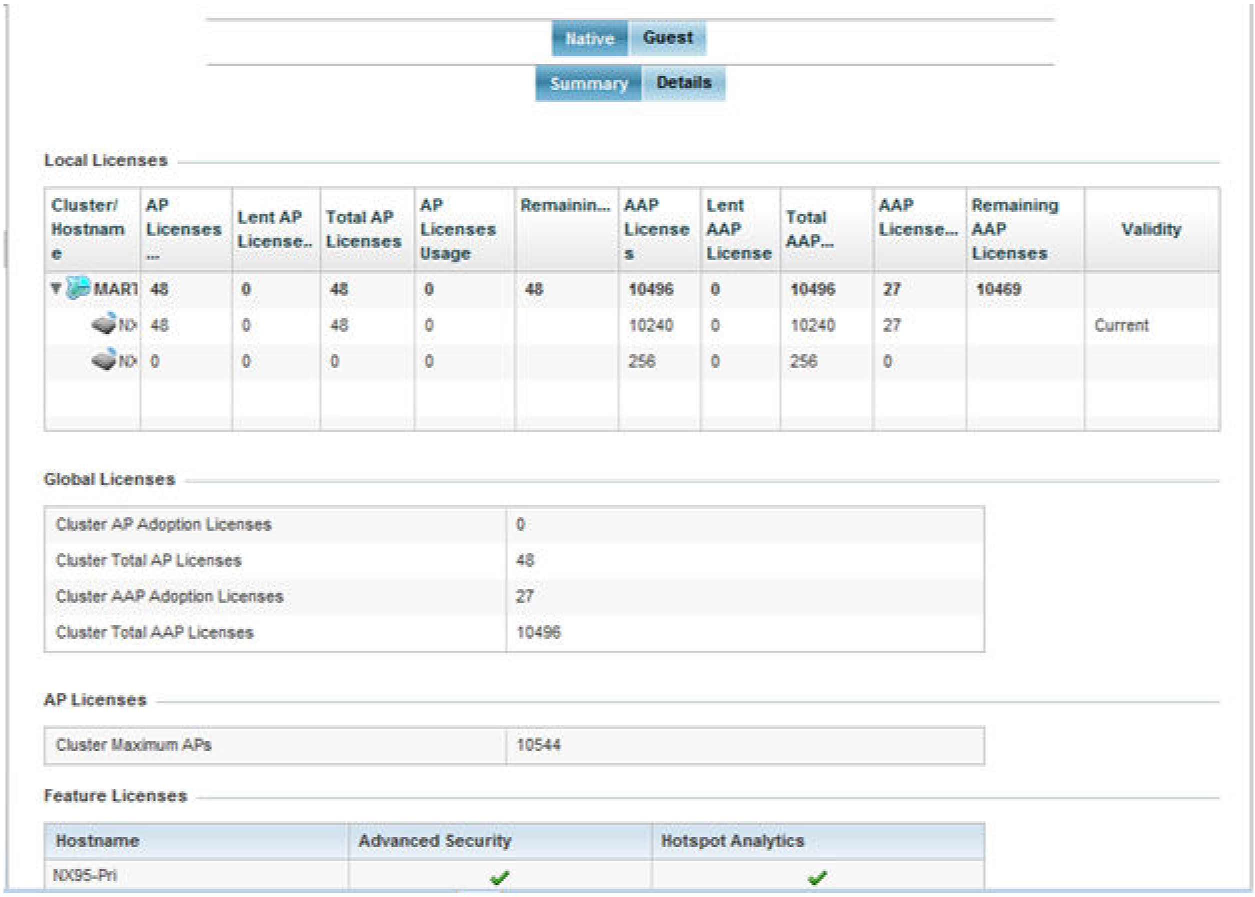
4. Select Native Details to view detailed license information.

   > Note
   > For more information on the **Native > License > Details** screen, click here.

Native/Guest Summary Screen

The Native/Guest Summary tab displays available licenses for cluster member devices. It displays the total number of AP *(Access Point)* and AAP *(Adaptive Access Point)* licenses that can be utilized amongst members.

> Note
> The Summary page for the Native and Guest tabs display same set of information for local and guest devices respectively. Therefore, the following information applies to both.



Local Licenses

Cluster/ Hostname	AP Licenses ...	Lent AP License..	Total AP Licenses	AP Licenses Usage	Remainin...	AAP Licenses	Lent AAP License	Total AAP...	AAP License...	Remaining AAP Licenses	Validity
MART	48	0	48	0	48	10496	0	10496	27	10469	
NX	48	0	48	0		10240	0	10240	27		Current
NX	0	0	0	0		256	0	256	0		

Global Licenses

Cluster AP Adoption Licenses	0
Cluster Total AP Licenses	48
Cluster AAP Adoption Licenses	27
Cluster Total AAP Licenses	10496

AP Licenses

Cluster Maximum APs	10544

Feature Licenses

Hostname	Advanced Security	Hotspot Analytics
NX95-Pri	✓	✓

Figure 402: Statistics - Licenses Screen

The Local Licenses table provides the following information:

Cluster/Hostname	Lists the administrator-assigned cluster hostname whose license count and utilization is tallied in this Local Licenses table.
AP Licenses Installed	Lists the number of AP connections available to this controller or service platform under the terms of the current license.
Lent AP Licenses	Displays the number of AP licenses lent (from this controller or service platform) to a cluster member to compensate for an AP's license deficiency.
Total AP Licenses	Displays the total number of AP connection licenses currently available to this controller or service platform.
AP License Usage	Lists the number of AP connections currently utilized by this controller or service platform out of the total available under the terms of the current license.
Remaining AP Licenses	Lists the remaining number of access point licenses available from the pooled license capabilities of all the members of the cluster.
AAP Licenses Installed	Lists the number of AAP connections available to this controller or service platform under the terms of the current license.
Lent AAP Licenses	Displays the number of AAP licenses lent (from this controller or service platform) to a cluster member to compensate for an AP licenses deficiency.
Total AAP Licenses	Displays the total number of AAP connection licenses currently available to this controller or service platform.

AAP Licenses Usage	Lists the number of AAP connections currently utilized by this controller or service platform out of the total available under the terms of the current license.
Remaining AAP Licenses	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
Validity	Displays validity information for the license's legal usage with the controller or service platform.

The **Global Licenses** area provides the following information:

Cluster AP Adoption Licenses	Displays the current number of AP adoption licenses utilized by controller or service platform connected APs within a cluster.
Cluster Total AP Licenses	Displays the total number of AP adoption licenses available to controller or service platform connected APs within a cluster.
Cluster AAP Adoption Licenses	Displays the current number of AAP adoption licenses utilized by controller or service platform connected APs within a cluster.
Cluster Total AAP Licenses	Displays the total number of AAP adoption licenses available to controller or service platform connected APs within a cluster.

The **AP Licenses** table provides the following information:

Cluster Maximum APs	Lists the maximum number of APs permitted in a cluster under the terms of the current license.

The **Featured Licenses** area provides the following information:

Hostname	Displays the administrator assigned hostname of the controller, service platform or AP whose potentially implemented a advanced security, WIPS or Analytics feature licenses.
Advanced Security	Displays whether the separately licensed Advanced Security application is installed for each hostname.
Advanced WIPS	Displays whether a separately licensed Advanced WIPS application is installed (separately licensed) for each listed hostname.
Hotspot Analytics	Displays whether a separately licensed Analytics application is installed for supported NX 95XX service platforms.

Native/Guest Details Screen

Refer to the **Native/Guest Details** screen to further assess the total number of cluster member licenses available, cluster memberships, current utilization versus total licenses available, borrowed licenses, remaining licenses and license validity.

Note

The **Details** page for the **Native** and **Guest** tabs display same set of information for local and guest devices respectively. Therefore, the following information applies to both.

Refer the following table for license utilization data:

Cluster/Hostname	Lists the administrator assigned cluster hostname whose license count and utilization is listed and tallied for member controllers, service platforms or AP.
AP Licenses Installed	Lists the number of AP connections available to this controller or service or peer AP under the terms of the current license.
Borrowed AP Licenses	Displays the number of AP licenses temporarily borrowed from a cluster member to compensate for an AP license deficiency.
Total AP Licenses	Displays the total number of AP connection licenses currently available to clustered devices.
AP License Usage	Lists the number of AP connections currently utilized out of the total available under the terms of current licenses.
Remaining AP Licenses	Lists the remaining number of AP licenses available from the pooled license capabilities of cluster members.
AAP Licenses Installed	Lists the number of *Adaptive Access Point* (AAP) connections available under the terms of current licenses.
Borrowed AAP Licenses	Displays the number of AAP licenses temporarily borrowed from a cluster member to compensate for an AAP license deficiency.
Total AAP Licenses	Displays the total number of AAP connection licenses currently available to clustered devices.
AAP Licenses Usage	Lists the number of AAP connections currently utilized out of the total available under the terms of the current licenses.
Remaining AAP Licenses	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
Validity	Displays validity information for the license's legal usage by cluster member devices.

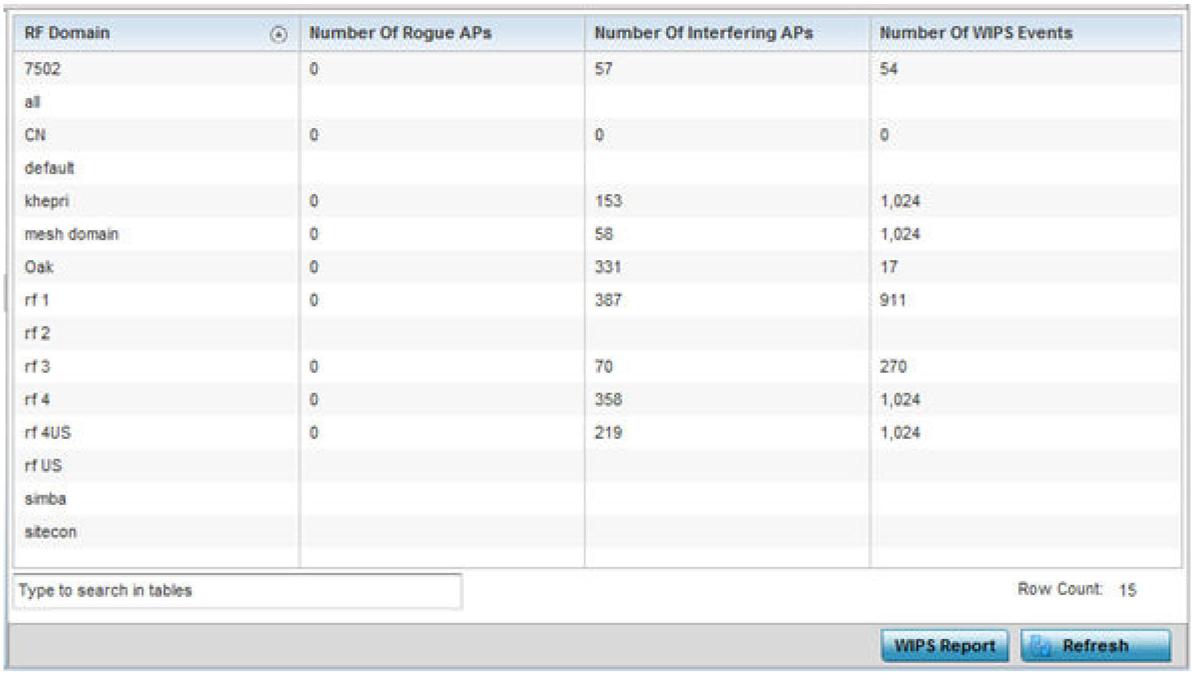
WIPS Summary

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.



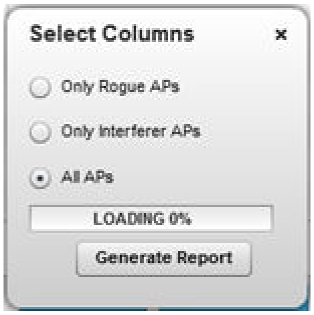
RF Domain	Number Of Rogue APs	Number Of Interfering APs	Number Of WIPS Events
7502	0	57	54
all			
CN	0	0	0
default			
khepri	0	153	1,024
mesh domain	0	58	1,024
Oak	0	331	17
rf 1	0	387	911
rf 2			
rf 3	0	70	270
rf 4	0	358	1,024
rf 4US	0	219	1,024
rf US			
simba			
sitecon			

Row Count: 15

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.



Select Columns ×

○ Only Rogue APs

○ Only Interferer APs

● All APs

LOADING 0%

Generate Report

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
- Application Visibility
- Coverage Hole Detection

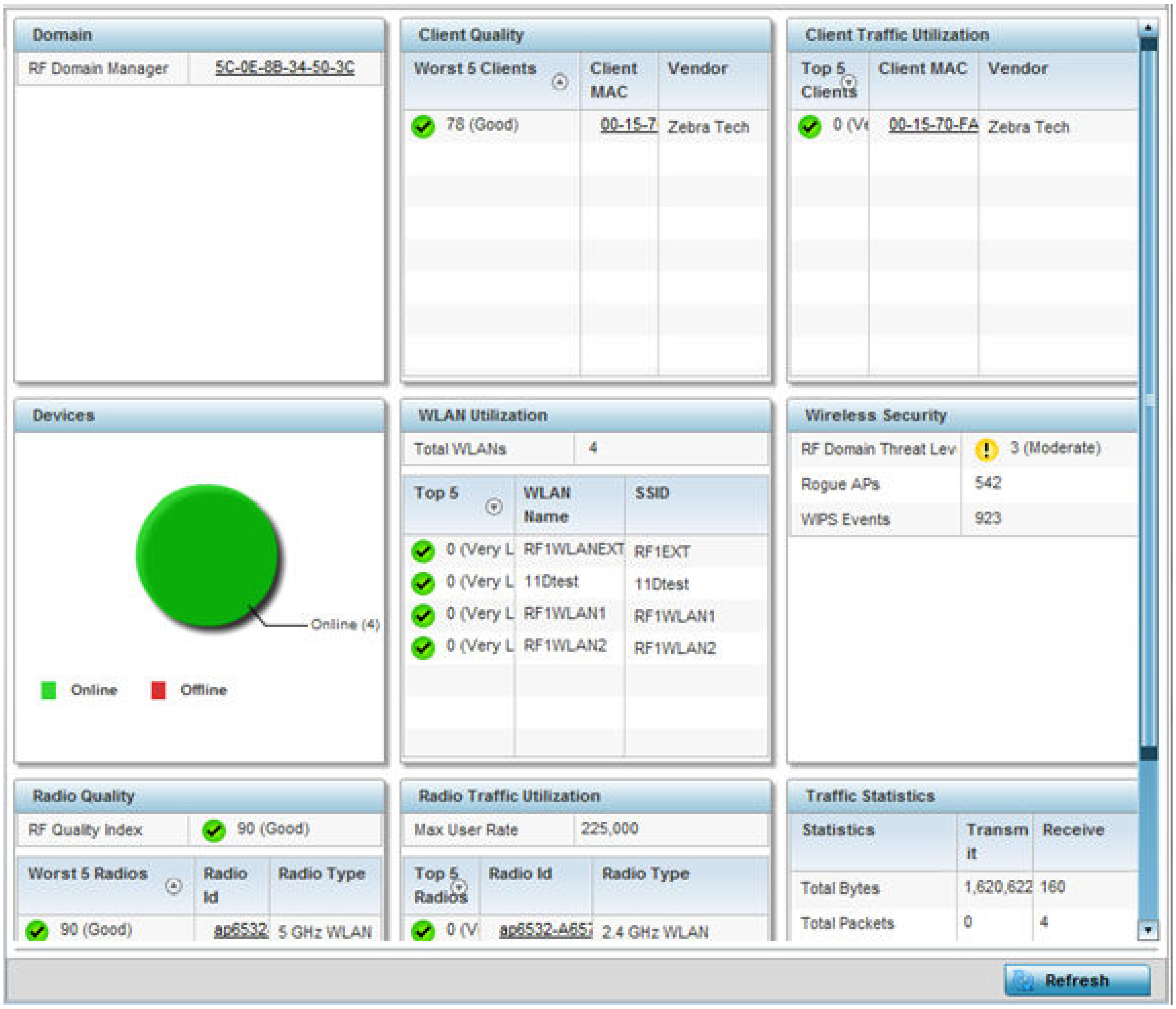
Health

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.



Domain

RF Domain Manager	5C-0E-8B-34-50-3C

Client Quality

Worst 5 Clients	Client MAC	Vendor
✓ 78 (Good)	00-15-7	Zebra Tech

Client Traffic Utilization

Top 5 Clients	Client MAC	Vendor
✓ 0 (Ve	00-15-70-FA	Zebra Tech

Devices

WLAN Utilization

Total WLANs	4

Top 5	WLAN Name	SSID
✓ 0 (Very L	RF1WLANEXT	RF1EXT
✓ 0 (Very L	11Dtest	11Dtest
✓ 0 (Very L	RF1WLAN1	RF1WLAN1
✓ 0 (Very L	RF1WLAN2	RF1WLAN2

Wireless Security

RF Domain Threat Lev	! 3 (Moderate)
Rogue APs	542
WIPS Events	923

Radio Quality

RF Quality Index	✓ 90 (Good)

Worst 5 Radios	Radio Id	Radio Type
✓ 90 (Good)	ap6532	5 GHz WLAN

Radio Traffic Utilization

Max User Rate	225,000

Top 5 Radios	Radio Id	Radio Type
✓ 0 (V	ap6532-A65	2.4 GHz WLAN

Traffic Statistics

Statistics	Transmit	Receive
Total Bytes	1,620,622	160
Total Packets	0	4

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:

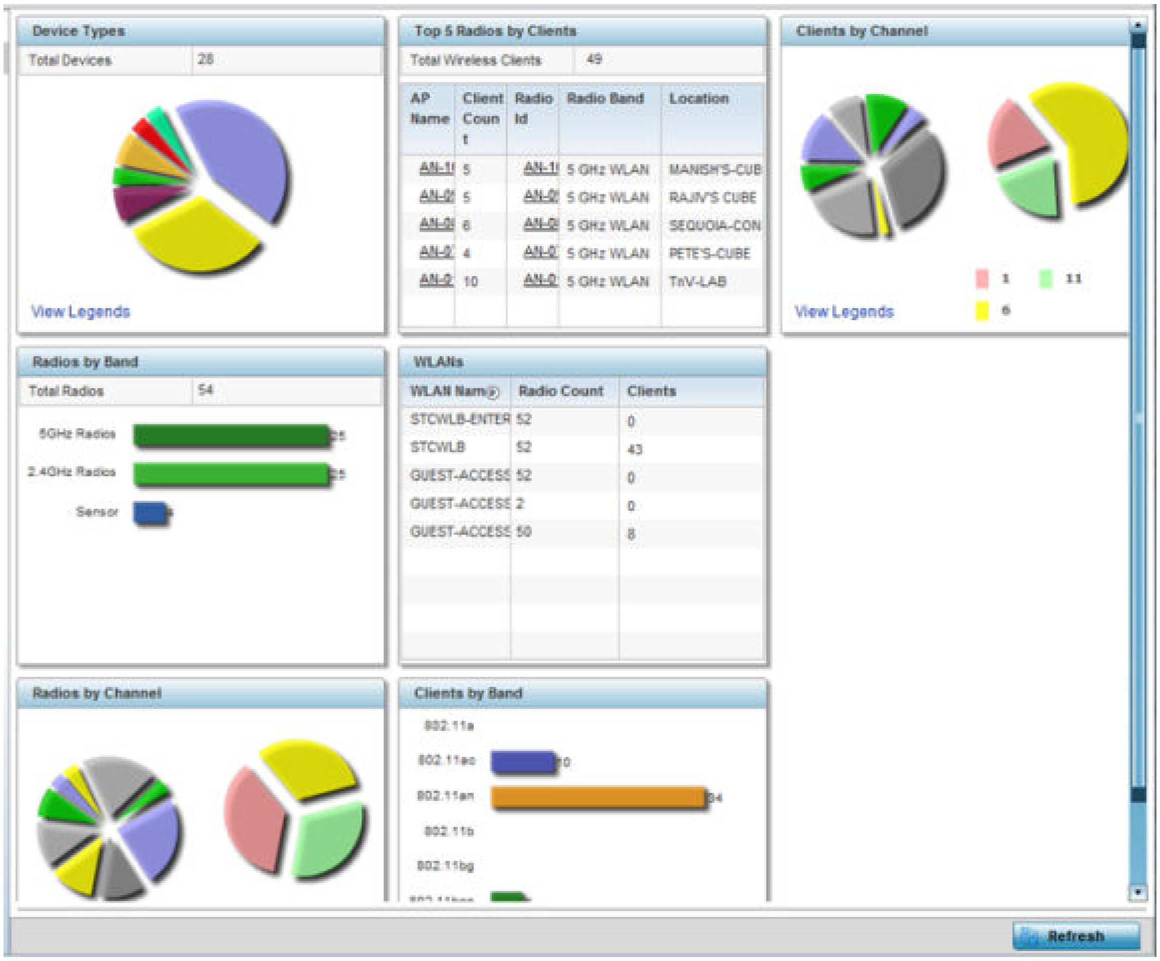
1 Select the **Statistics** → **System** menu from the Web UI.

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.



Total Devices	28

Top 5 Radios by Clients

Total Wireless Clients	49

AP Name	Client Count	Radio Id	Radio Band	Location
AN-1	5	AN-1	5 GHz WLAN	MANISH'S-CUB
AN-0	5	AN-0	5 GHz WLAN	RAJIV'S CUBE
AN-0	6	AN-0	5 GHz WLAN	SEQUOIA-CON
AN-0	4	AN-0	5 GHz WLAN	PETE'S-CUBE
AN-0	10	AN-0	5 GHz WLAN	TnV-LAB

Total Radios	54

WLANs

WLAN Name	Radio Count	Clients
STCWLB-ENTER	52	0
STCWLB	52	43
GUEST-ACCESS	52	0
GUEST-ACCESS	2	0
GUEST-ACCESS	50	8

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.

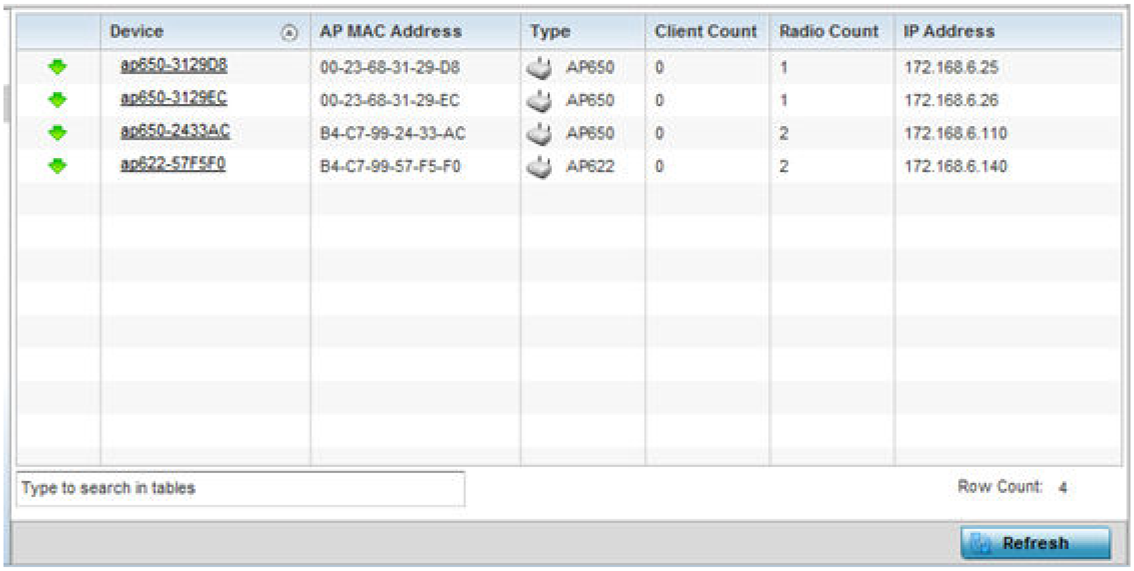
Devices

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 and select and RF Domain.

   The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
3. Select **Devices** from the RF Domain menu.



	Device	AP MAC Address	Type	Client Count	Radio Count	IP Address
🟩	ap650-3129D8	00-23-68-31-29-D8	AP650	0	1	172.168.6.25
🟩	ap650-3129EC	00-23-68-31-29-EC	AP650	0	1	172.168.6.26
🟩	ap650-2433AC	B4-C7-99-24-33-AC	AP650	0	2	172.168.6.110
🟩	ap622-57F5F0	B4-C7-99-57-F5-F0	AP622	0	2	172.168.6.140

4 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.

5 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:

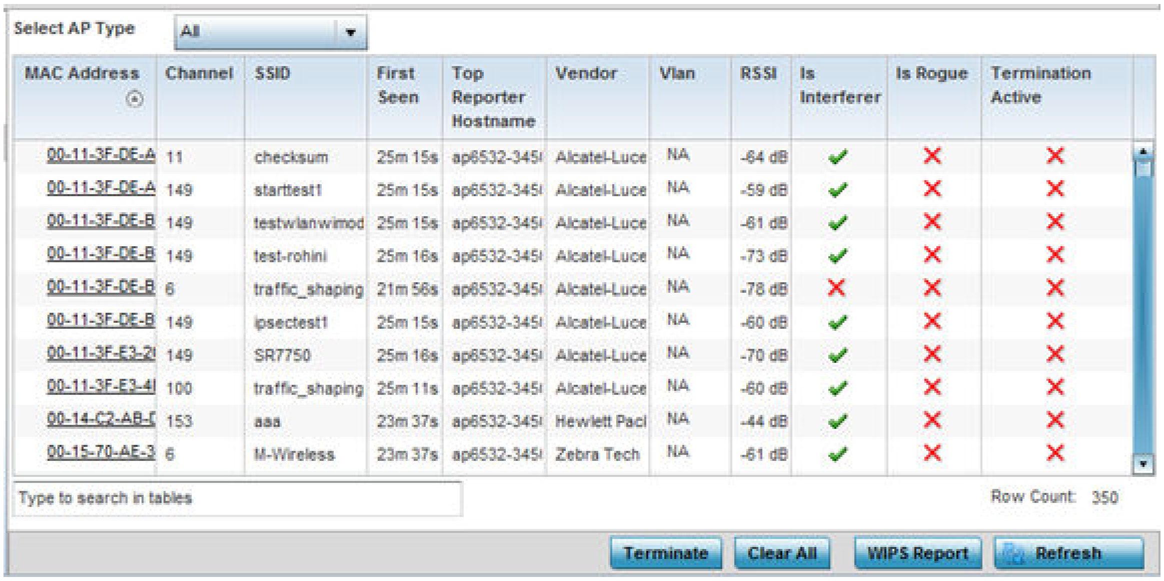
1 Go to **Statistics** → **System**.

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.



Select AP Type: All

MAC Address	Channel	SSID	First Seen	Top Reporter Hostname	Vendor	Vlan	RSSI	Is Interferer	Is Rogue	Termination Active
00-11-3F-DE-A	11	checksum	25m 15s	ap6532-345	Alcatel-Luce	NA	-64 dB	✓	✗	✗
00-11-3F-DE-A	149	starttest1	25m 15s	ap6532-345	Alcatel-Luce	NA	-59 dB	✓	✗	✗
00-11-3F-DE-B	149	testwlanwimod	25m 15s	ap6532-345	Alcatel-Luce	NA	-61 dB	✓	✗	✗
00-11-3F-DE-B	149	test-rohini	25m 16s	ap6532-345	Alcatel-Luce	NA	-73 dB	✓	✗	✗
00-11-3F-DE-B	6	traffic_shaping	21m 56s	ap6532-345	Alcatel-Luce	NA	-78 dB	✗	✗	✗
00-11-3F-DE-B	149	ipsectest1	25m 15s	ap6532-345	Alcatel-Luce	NA	-60 dB	✓	✗	✗
00-11-3F-E3-2	149	SR7750	25m 16s	ap6532-345	Alcatel-Luce	NA	-70 dB	✓	✗	✗
00-11-3F-E3-4	100	traffic_shaping	25m 11s	ap6532-345	Alcatel-Luce	NA	-60 dB	✓	✗	✗
00-14-C2-AB-C	153	aaa	23m 37s	ap6532-345	Hewlett Pacl	NA	-44 dB	✓	✗	✗
00-15-70-AE-3	6	M-Wireless	23m 37s	ap6532-345	Zebra Tech	NA	-61 dB	✓	✗	✗

Type to search in tables

Row Count: 350

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.

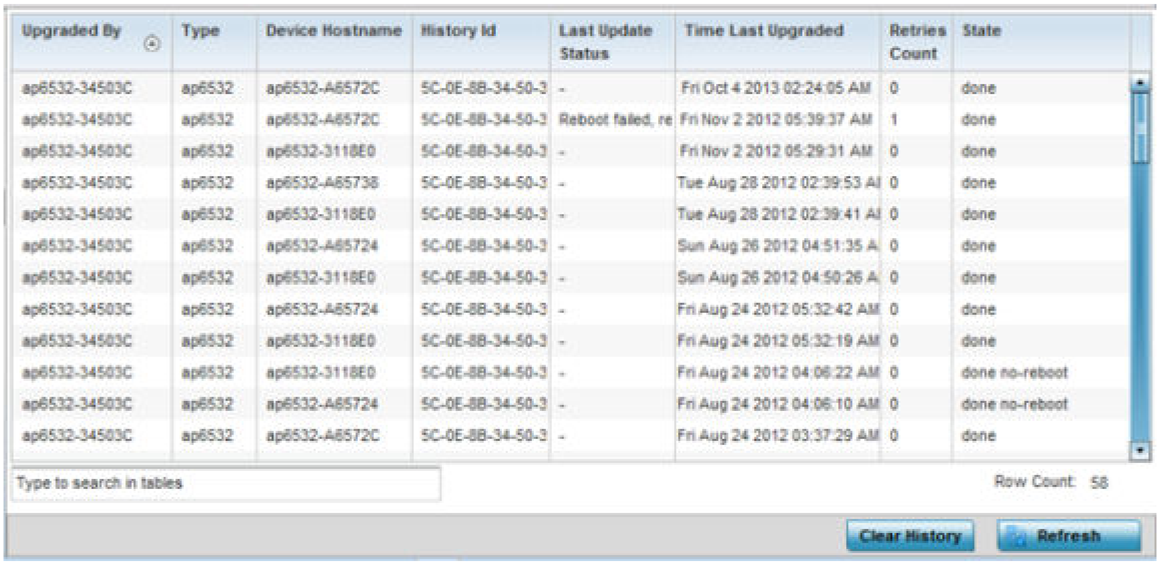
The **System** node expands to display the RF Domains created within the managed network.

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.



Upgraded By	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	-	Fri Oct 4 2013 02:24:05 AM	0	done
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	Reboot failed, re	Fri Nov 2 2012 05:39:37 AM	1	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Nov 2 2012 05:29:31 AM	0	done
ap6532-34503C	ap6532	ap6532-A65738	5C-0E-8B-34-50-3	-	Tue Aug 28 2012 02:39:53 AI	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Tue Aug 28 2012 02:39:41 AI	0	done
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Sun Aug 26 2012 04:51:35 A	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Sun Aug 26 2012 04:50:26 A	0	done
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 05:32:42 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 05:32:19 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 04:06:22 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 04:06:10 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 03:37:29 AM	0	done

Row Count: 58

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.

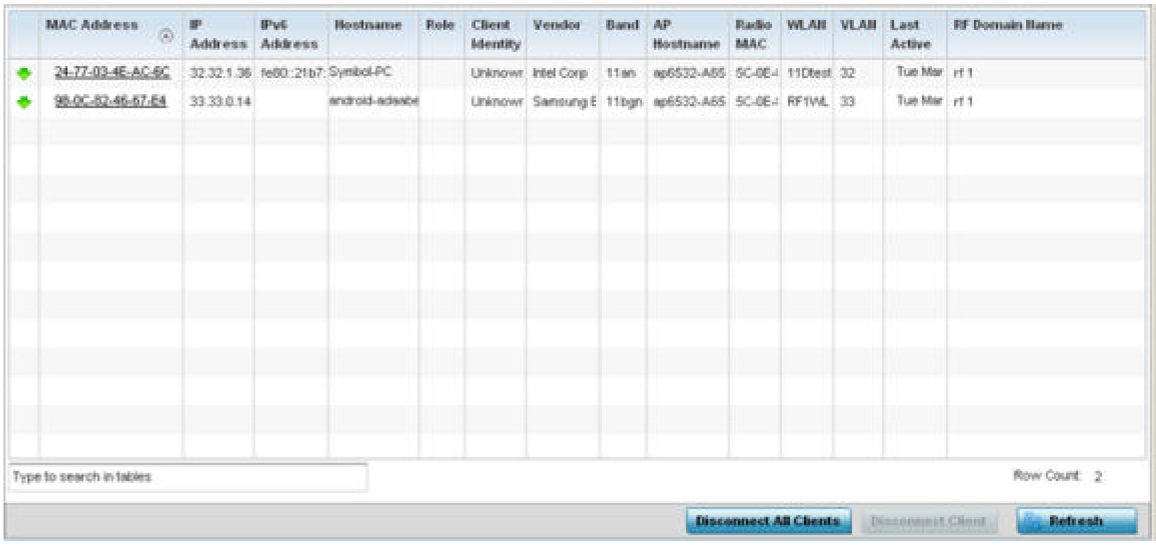
To review a RF Domain's connected wireless clients:

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.



MAC Address	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active	RF Domain Name
24-77-03-4E-AC-6C	32.32.1.36	fe80::21b7:	Symbol-PC		Unknowr	Intel Corp	11an	ap6532-A65	5C-0E-	11Dtest	32	Tue Mar	rf 1
98-0C-82-46-67-E4	33.33.0.14		android-adsabe		Unknowr	Samsung E	11bgn	ap6532-A65	5C-0E-	RF1WL	33	Tue Mar	rf 1

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, controller or service platform 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.

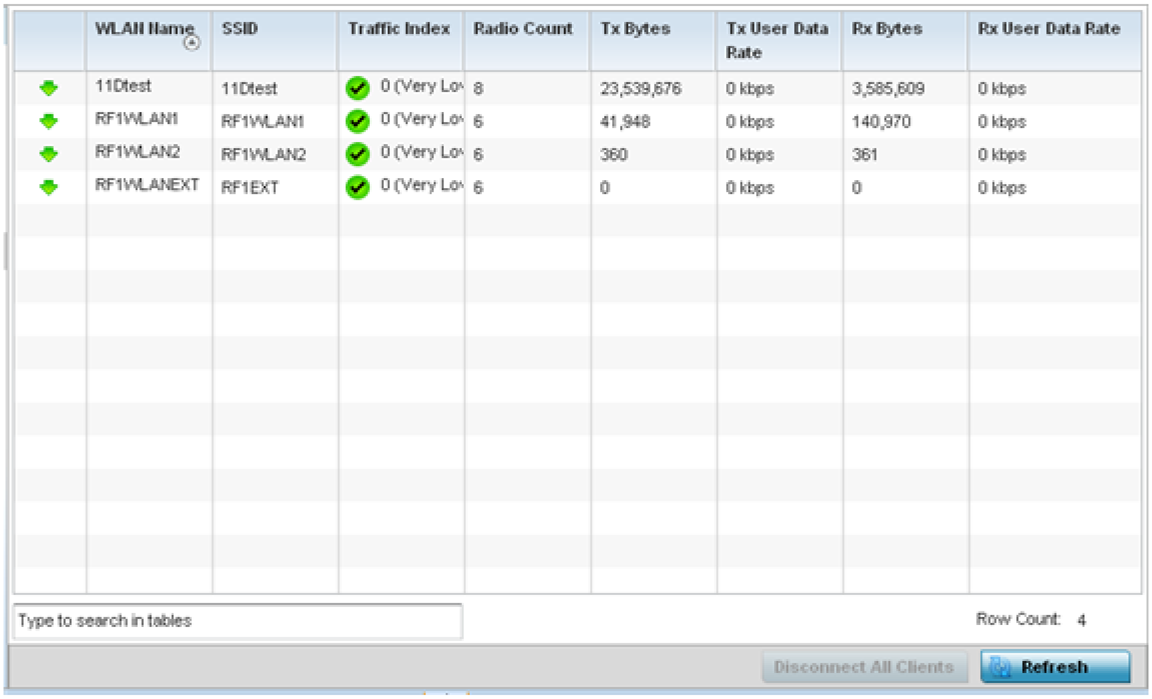
The **System** node expands to display the RF Domains created within the managed network.

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.



	WLAN Name	SSID	Traffic Index	Radio Count	Tx Bytes	Tx User Data Rate	Rx Bytes	Rx User Data Rate
⬇	11Dtest	11Dtest	✓ 0 (Very Lo	8	23,539,676	0 kbps	3,585,609	0 kbps
⬇	RF1WLAN1	RF1WLAN1	✓ 0 (Very Lo	6	41,948	0 kbps	140,970	0 kbps
⬇	RF1WLAN2	RF1WLAN2	✓ 0 (Very Lo	6	360	0 kbps	361	0 kbps
⬇	RF1WLANEXT	RF1EXT	✓ 0 (Very Lo	6	0	0 kbps	0	0 kbps

Row Count: 4

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: • **`0 – 20`** - (very low utilization) • **`20 – 40`** - (low utilization) • **`40 – 60`** - (moderate utilization) • **`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:

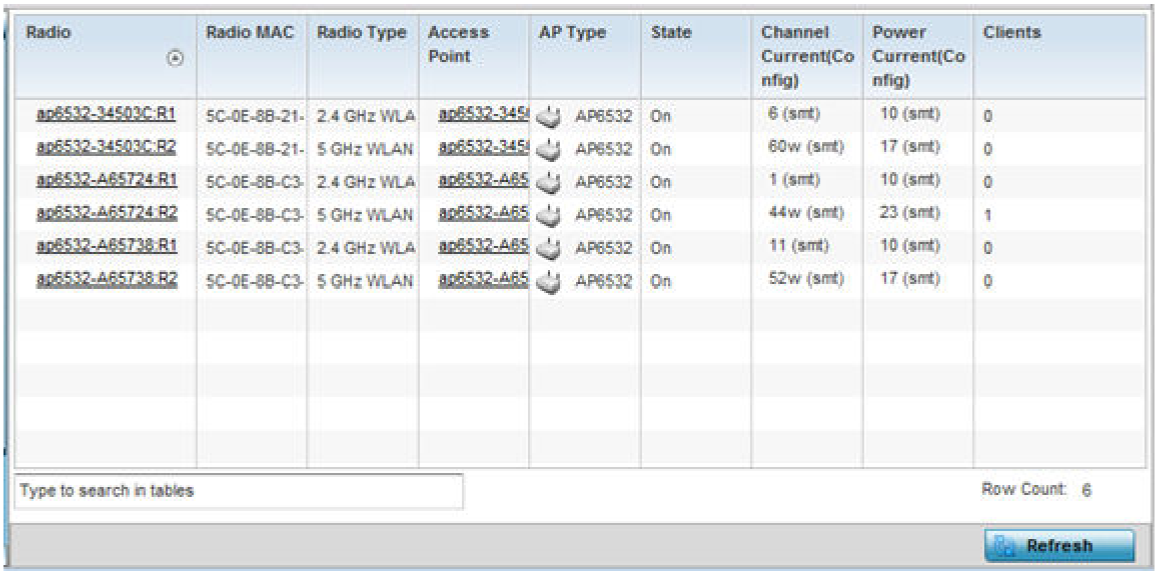
1 Go to **Statistics** → **System** menu from the Web UI.

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.



Radio	Radio MAC	Radio Type	Access Point	AP Type	State	Channel Current(Config)	Power Current(Config)	Clients
ap6532-34503C:R1	5C-0E-8B-21-	2.4 GHz WLA	ap6532-345	AP6532	On	6 (smt)	10 (smt)	0
ap6532-34503C:R2	5C-0E-8B-21-	5 GHz WLAN	ap6532-345	AP6532	On	60w (smt)	17 (smt)	0
ap6532-A65724:R1	5C-0E-8B-C3-	2.4 GHz WLA	ap6532-A65	AP6532	On	1 (smt)	10 (smt)	0
ap6532-A65724:R2	5C-0E-8B-C3-	5 GHz WLAN	ap6532-A65	AP6532	On	44w (smt)	23 (smt)	1
ap6532-A65738:R1	5C-0E-8B-C3-	2.4 GHz WLA	ap6532-A65	AP6532	On	11 (smt)	10 (smt)	0
ap6532-A65738:R2	5C-0E-8B-C3-	5 GHz WLAN	ap6532-A65	AP6532	On	52w (smt)	17 (smt)	0

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:

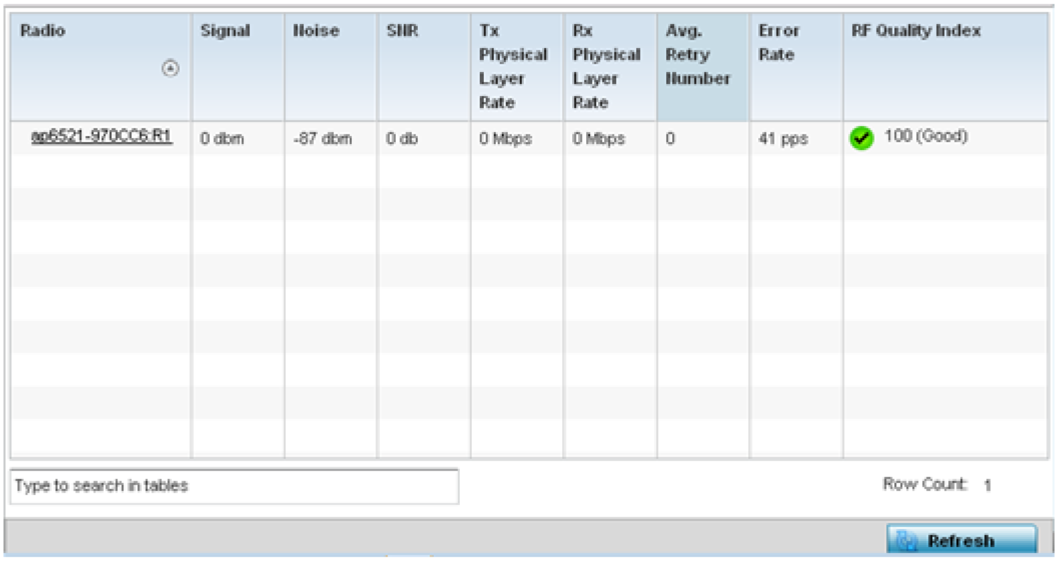
1 Select the **Statistics** → **System** menu from the Web UI.

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.



Radio	Signal	Noise	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Avg. Retry Number	Error Rate	RF Quality Index
ap6521-970CC6:R1	0 dbm	-87 dbm	0 db	0 Mbps	0 Mbps	0	41 pps	✓ 100 (Good)

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: • **`0 – 50`** - (Poor) • **`50 – 75`** - (Medium) • **`75 – 100`** - (Good)

5 Periodically click **Refresh** to update the contents of the screen to their latest values

Radio Traffic Statistics

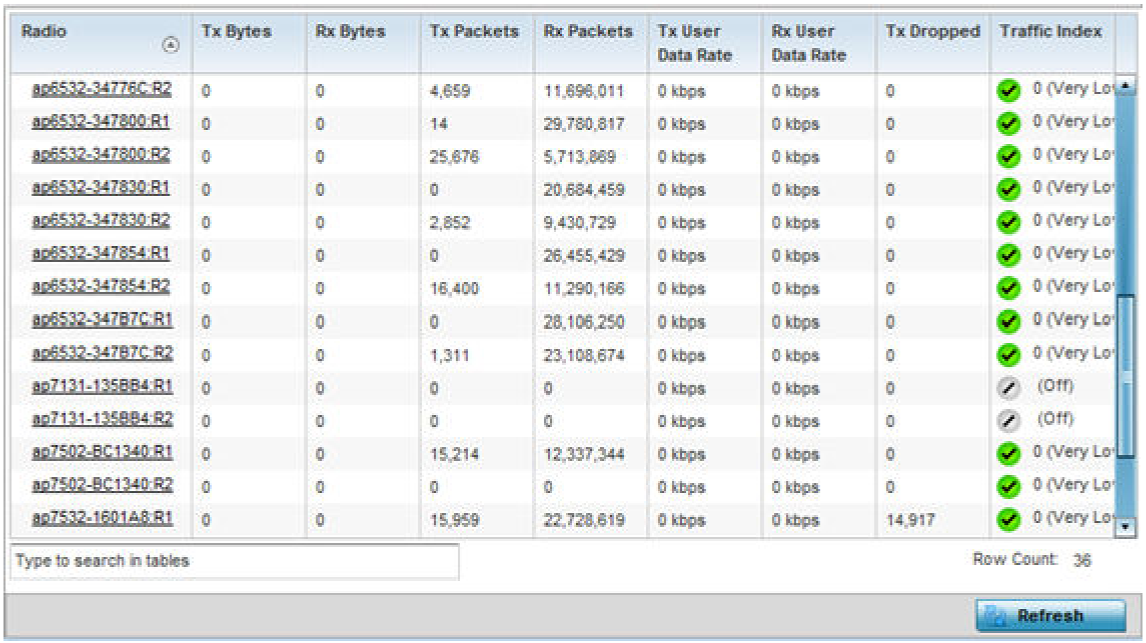
The Traffic Statistics screen displays transmit and receive data as well as data rate and packet drop and error information for RF Domain member radios. Individual RF Domain member radios can be selected and to information specific to that radio as troubleshoot requirements dictate.

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.



Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Traffic Index
ap6532-34776C:R2	0	0	4,659	11,696,011	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347800:R1	0	0	14	29,780,817	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347800:R2	0	0	25,676	5,713,869	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347830:R1	0	0	0	20,684,459	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347830:R2	0	0	2,852	9,430,729	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347854:R1	0	0	0	26,455,429	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347854:R2	0	0	16,400	11,290,166	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-3478 7C:R1	0	0	0	28,106,250	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap6532-347B7C:R2	0	0	1,311	23,108,674	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap7131-135BB4:R1	0	0	0	0	0 kbps	0 kbps	0	(Off)
ap7131-135BB4:R2	0	0	0	0	0 kbps	0 kbps	0	(Off)
ap7502-BC1340:R1	0	0	15,214	12,337,344	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap7502-BC1340:R2	0	0	0	0	0 kbps	0 kbps	0	✓ 0 (Very Lo
ap7532-1601A8:R1	0	0	15,959	22,728,619	0 kbps	0 kbps	14,917	✓ 0 (Very Lo

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

AP-8432 and AP-8533 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-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 raises an alarm.

AP-8432 and AP-8533 model access points emit either iBeacon or Eddystone-URL beacons. The AP's Bluetooth radio periodically sends non-connectable, undirected LE *(low-energy)* advertisement packets. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are still customizable.

1 Select the **Statistics** menu from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

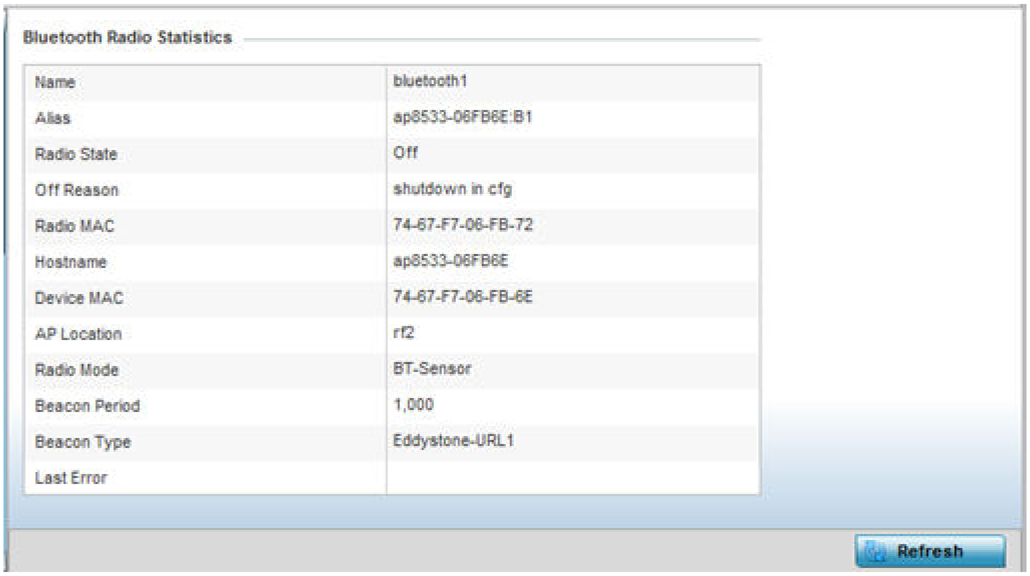
The **System** node expands to display the RF Domains created within the managed network.

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.



Bluetooth Radio Statistics

Name	bluetooth1
Alias	ap8533-06FB6E:B1
Radio State	Off
Off Reason	shutdown in cfg
Radio MAC	74-67-F7-06-FB-72
Hostname	ap8533-06FB6E
Device MAC	74-67-F7-06-FB-6E
AP Location	rf2
Radio Mode	BT-Sensor
Beacon Period	1,000
Beacon Type	Eddystone-URL1
Last Error	

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.

5. 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.

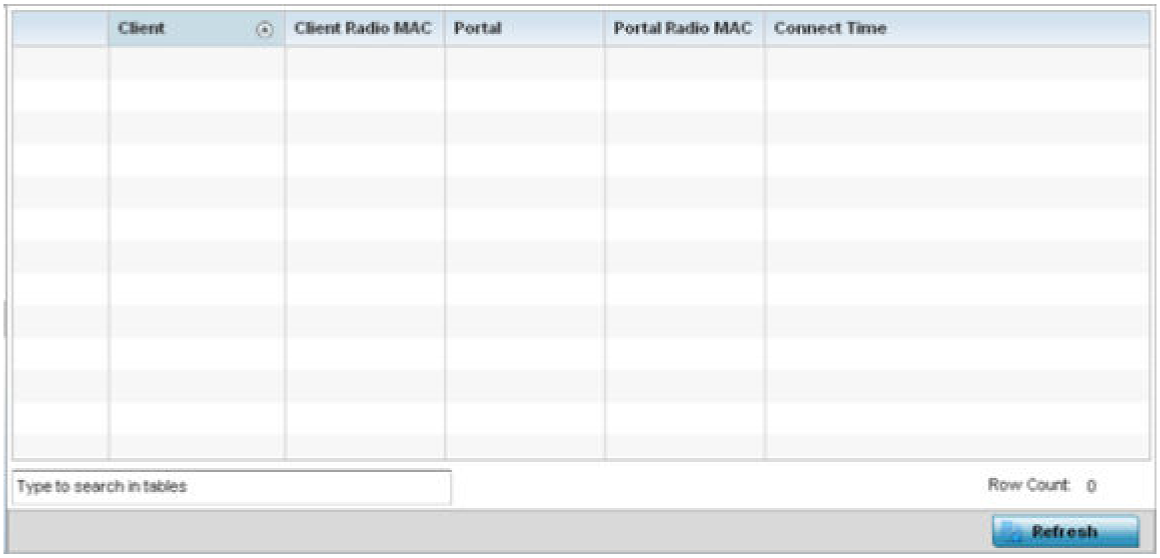
To view Mesh statistics for RF Domain member mesh node connected clients:

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.

The **RF Domain > Mesh Point** option has the following sub-menus:

- MCX Geographical View on page 1029.
- MCX Logical View on page 1030.
- Device Type on page 1031.
- Device Brief Info on page 1036.
- Device Data Transmit on page 1042.

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.

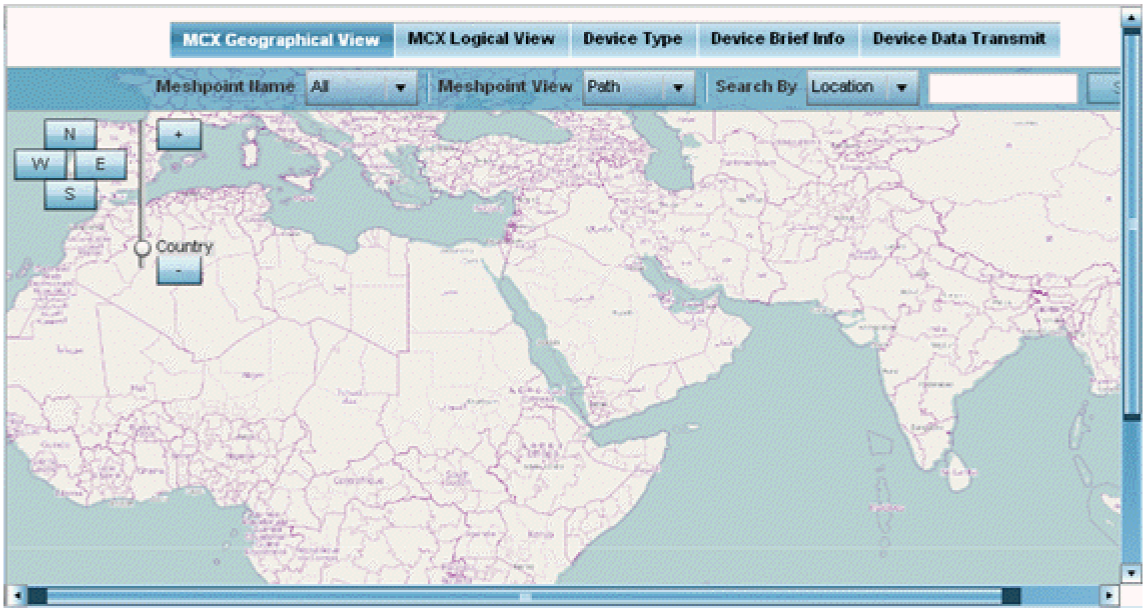
The **System** node expands to display the RF Domains created within the managed network.

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.

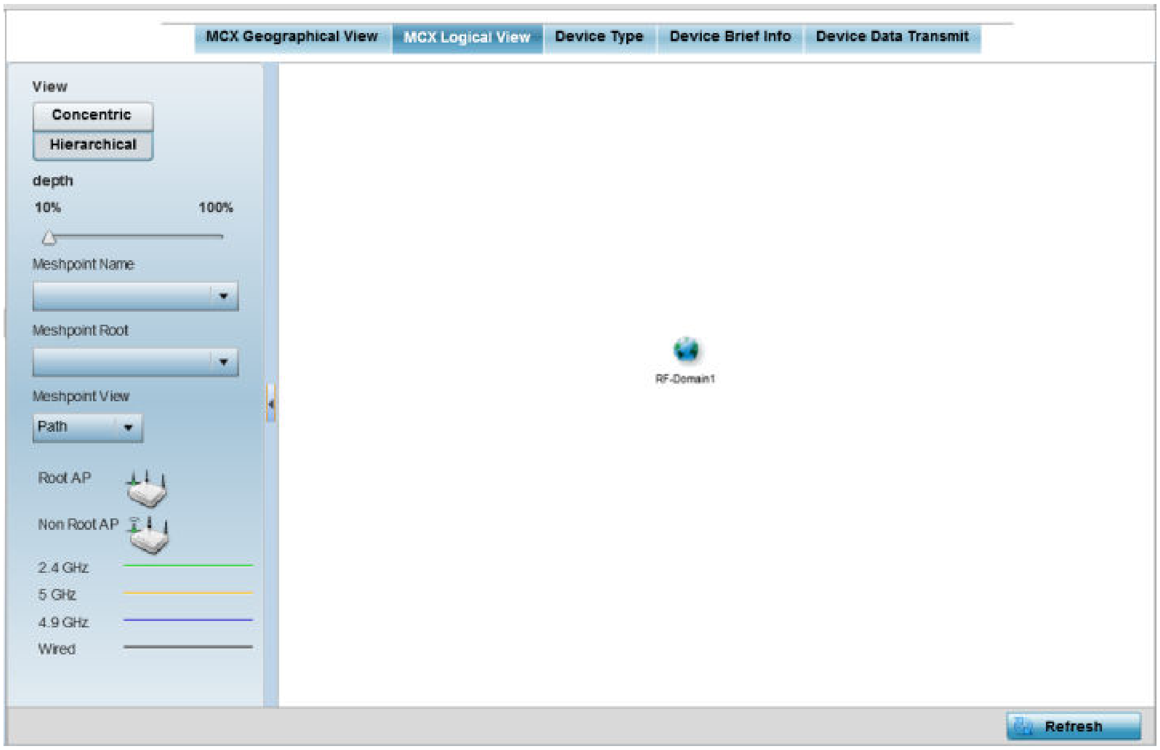
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

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:

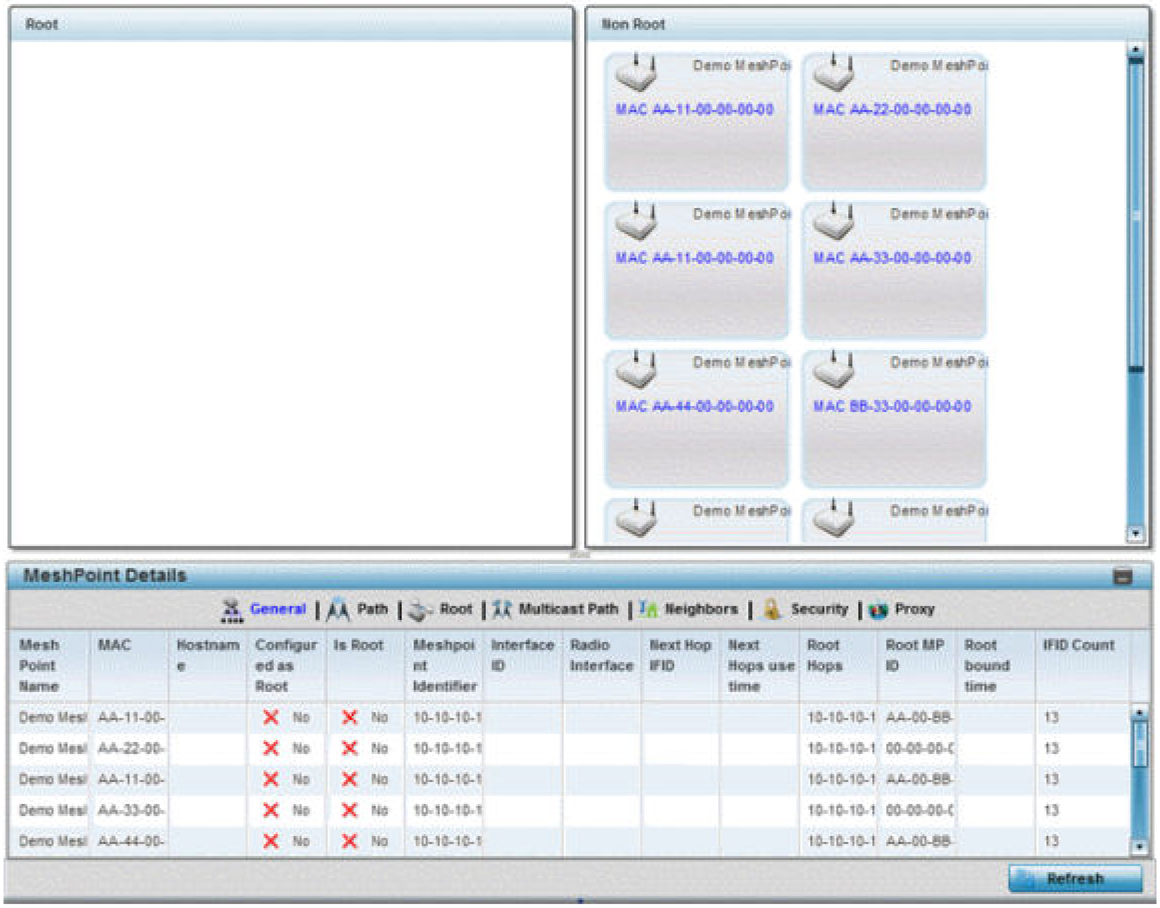
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node on the top, left-hand side of the screen.

   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.



Mesh Point Name	MAC	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Interface ID	Radio Interface	Next Hop IFID	Next Hops use time	Root Hops	Root MP ID	Root bound time	IFID Count
Demo Mesl	AA-11-00-		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-		13
Demo Mesl	AA-22-00-		✗ No	✗ No	10-10-10-1					10-10-10-1	00-00-00-(		13
Demo Mesl	AA-11-00-		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-		13
Demo Mesl	AA-33-00-		✗ No	✗ No	10-10-10-1					10-10-10-1	00-00-00-(		13
Demo Mesl	AA-44-00-		✗ No	✗ No	10-10-10-1					10-10-10-1	AA-00-BB-		13

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. • **`8`** – The current next hop to the recommended root. • **`7`** – Any secondary next hop to the recommended root to has a good potential route metric. • **`6`** – A next hop to an alternate root node. • **`5`** – A downstream node currently hopping through to get to the root. • **`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). • **`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. • **`2`** – Reserved for active peer to peer routes and is not currently used. • **`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. • **`0`** – A neighbor bound to a different root node. • **`-1`** – Not a member of the mesh as it has a different mesh ID. 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: • `Init` - indicates the link has not been established or has expired. • `Enabled -` indicates the link is available for communication. • `Failed` - indicates the attempt to establish the link failed and cannot be retried yet. • `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.

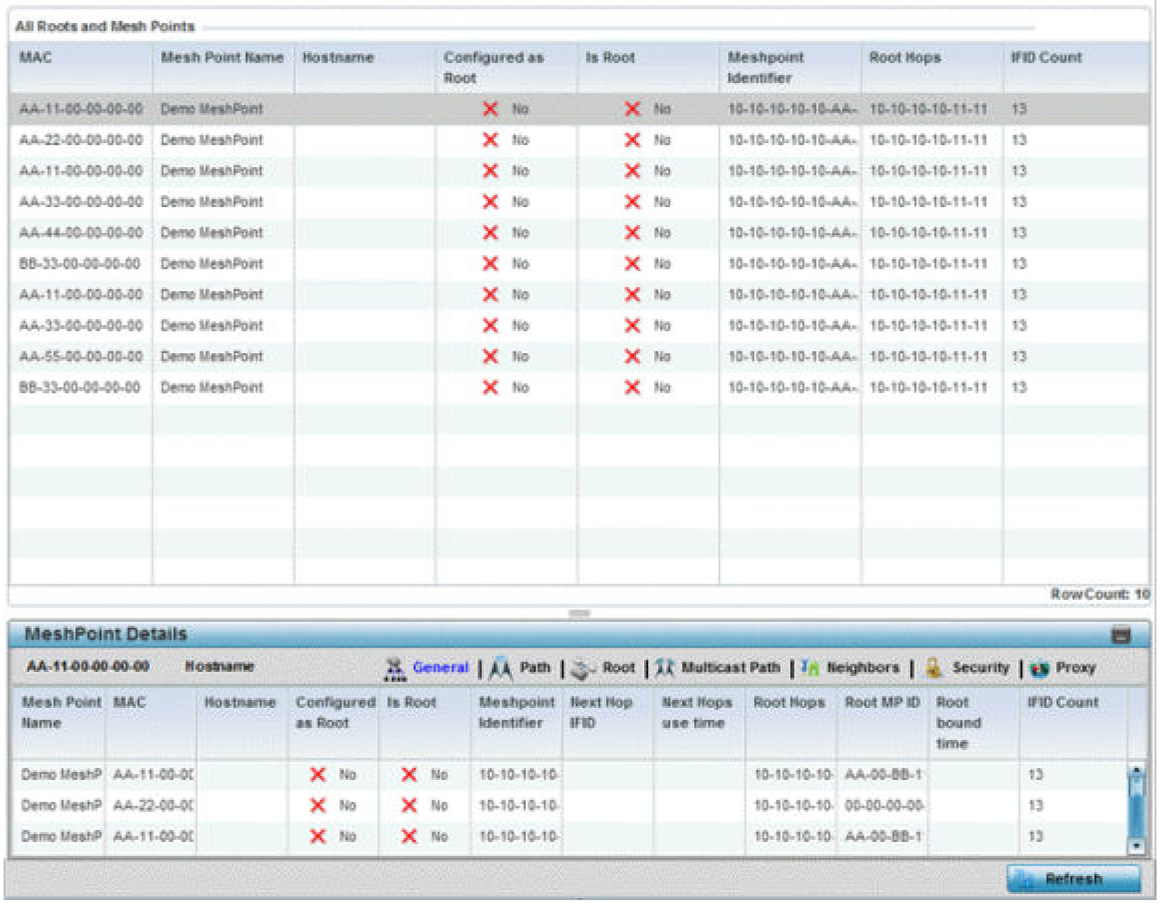
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

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.



All Roots and Mesh Points

MAC	Mesh Point Name	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Root Hops	IFID Count
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-22-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-44-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
AA-55-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-10-AA-	10-10-10-10-11-11	13

RowCount: 10

MeshPoint Details

AA-11-00-00-00-00 Hostname

Mesh Point Name	MAC	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Next Hop IFID	Next Hops use time	Root Hops	Root MP ID	Root bound time	IFID Count
Demo MeshP	AA-11-00-0(		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13
Demo MeshP	AA-22-00-0(		✗ No	✗ No	10-10-10-10-			10-10-10-10-	00-00-00-00-		13
Demo MeshP	AA-11-00-0(		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13

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. • **8** – The current next hop to the recommended root. • **7** – Any secondary next hop to the recommended root to has a good potential route metric. • **6** – A next hop to an alternate root node. • **5** – A downstream node currently hopping through to get to the root. • **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). • **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. • **2** – Reserved for active peer to peer routes and is not currently used. • **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. • **0** – A neighbor bound to a different root node. • **-1** – Not a member of the mesh as it has a different mesh ID. 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: • **Init** - indicates the link has not been established or has expired. • **Enabled -** indicates the link is available for communication. • **Failed** - indicates the attempt to establish the link failed and cannot be retried yet. • **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.

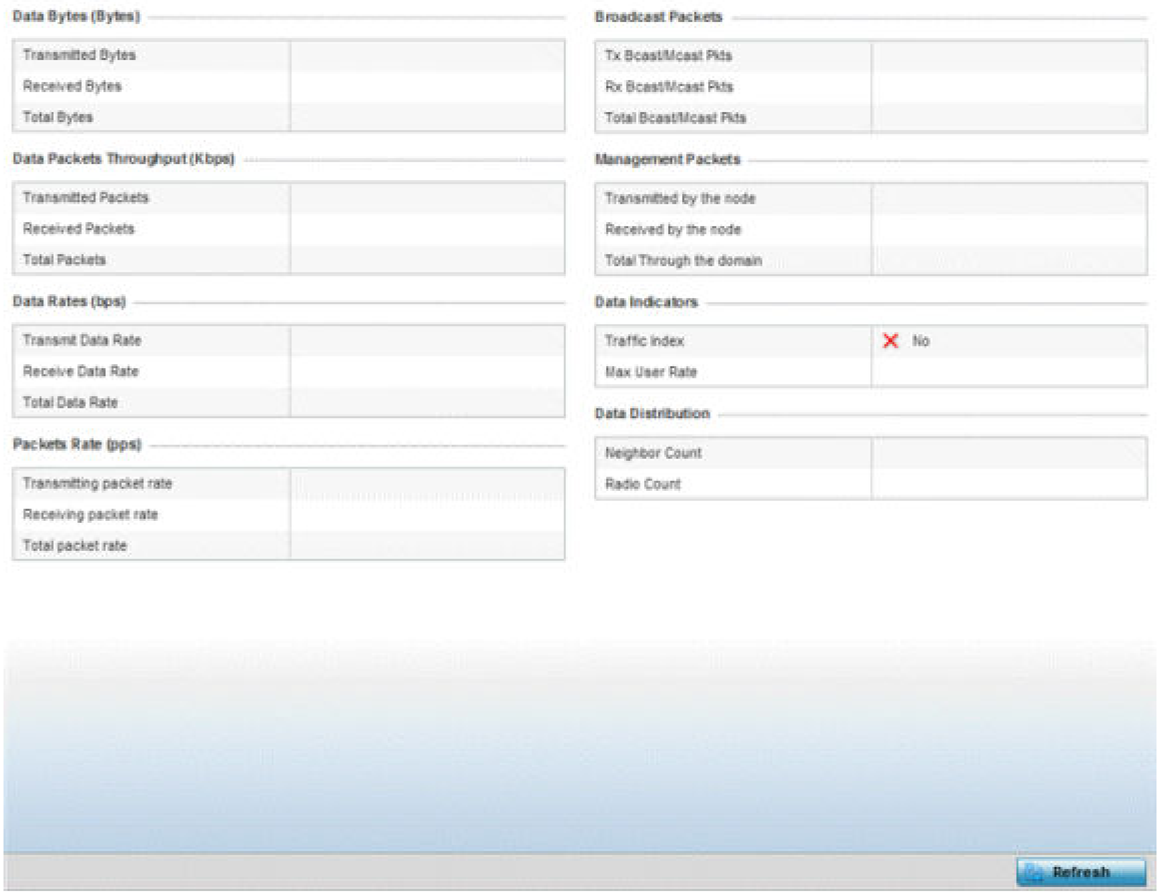
The RF Domain statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

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 1044.
- SMART RF - Details - Details on page 1047.
- SMART RF - Details - Energy Graph on page 1048.
- SMART RF - History on page 1049.

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.

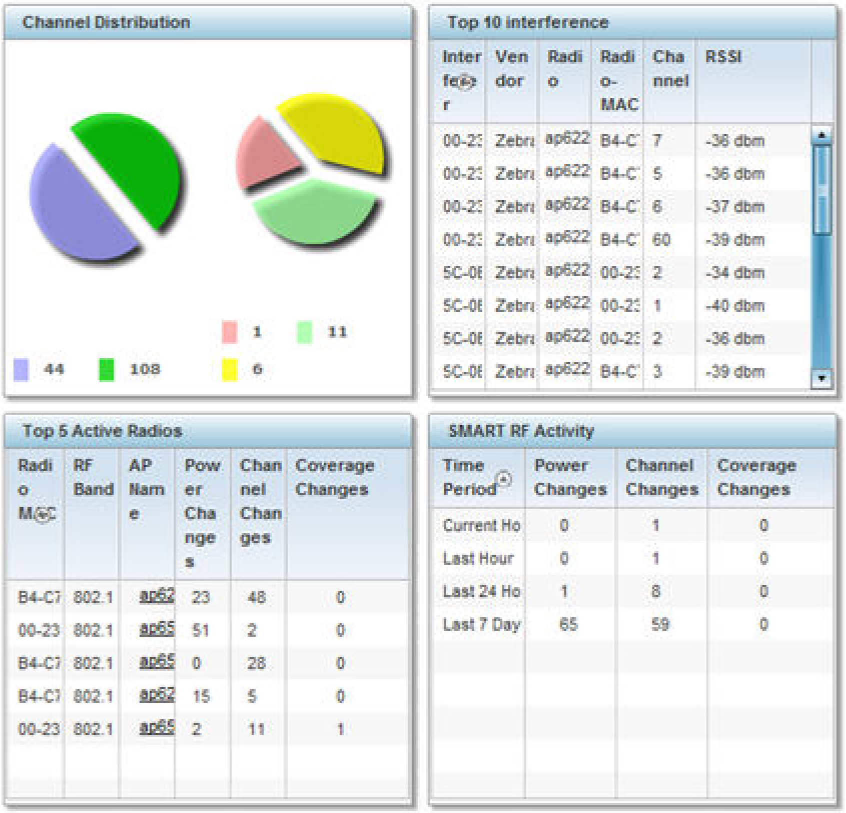
The **System** node expands to display the RF Domains created within the managed network.

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.



Channel Distribution

Top 10 interference

Interferer	Vendor	Radio	Radio-MAC	Channel	RSSI
00-2	Zebr	ap622	B4-C	7	-36 dbm
00-2	Zebr	ap622	B4-C	5	-36 dbm
00-2	Zebr	ap622	B4-C	6	-37 dbm
00-2	Zebr	ap622	B4-C	60	-39 dbm
5C-0	Zebr	ap622	00-2	2	-34 dbm
5C-0	Zebr	ap622	00-2	1	-40 dbm
5C-0	Zebr	ap622	00-2	2	-36 dbm
5C-0	Zebr	ap622	B4-C	3	-39 dbm

Top 5 Active Radios

Radio MAC	RF Band	AP Name	Power Changes	Channel Changes	Coverage Changes
B4-C	802.1	ap62	23	48	0
00-23	802.1	ap65	51	2	0
B4-C	802.1	ap65	0	28	0
B4-C	802.1	ap62	15	5	0
00-23	802.1	ap65	2	11	1

SMART RF Activity

Time Period	Power Changes	Channel Changes	Coverage Changes
Current Ho	0	1	0
Last Hour	0	1	0
Last 24 Ho	1	8	0
Last 7 Day	65	59	0

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.

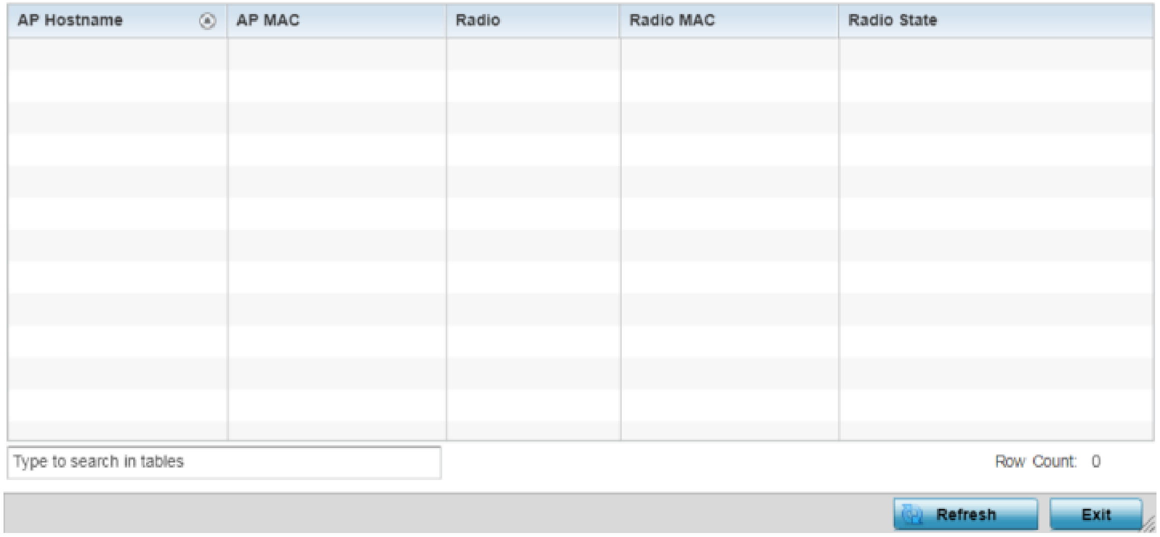
SMART RF - Select Shutdown

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:



AP Hostname	AP MAC	Radio	Radio MAC	Radio State

Figure 403: 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. The Smart RF select-shutdown option, auto-shutdowns selected 2.4 GHz radios, in dual-band networks, to maintain CCI levels within specified limits. Note: For information on enabling select shutdown, see Configuring Smart RF Select Shutdown Settings on page 419.
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.

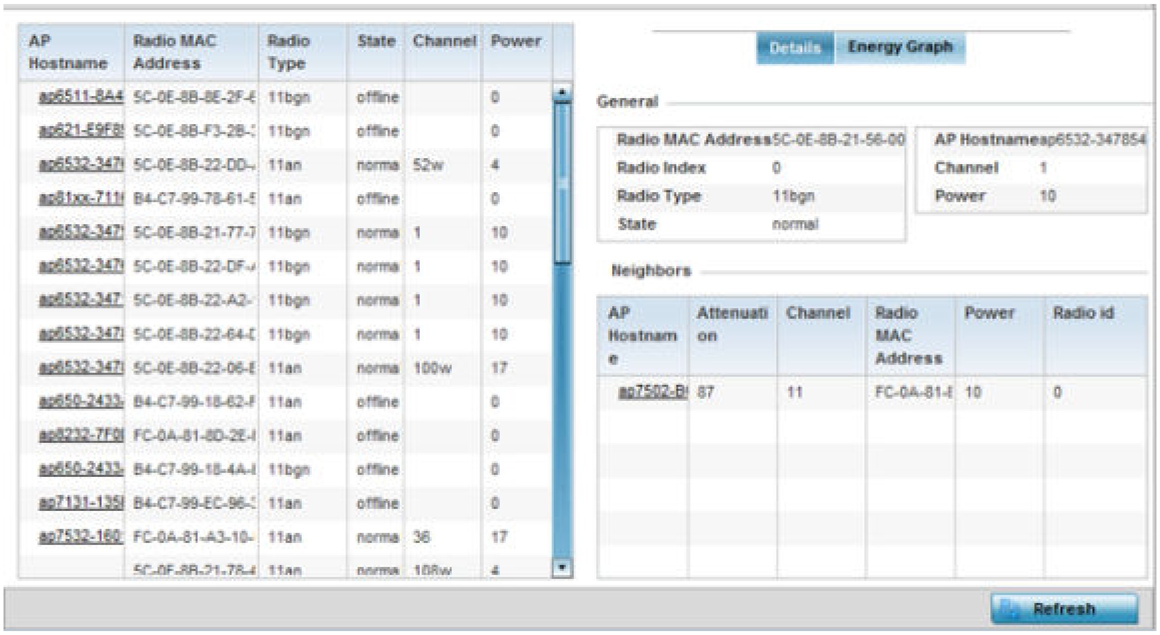
3 Select an RF Domain from the list.

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.



AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power
ap6511-8A4	5C-0E-8B-8E-2F-	11bgn	offline		0
ap621-E9F8	5C-0E-8B-F3-2B-	11bgn	offline		0
ap6532-347	5C-0E-8B-22-DD-	11an	norma	52w	4
ap81xx-711	B4-C7-99-78-61-	11an	offline		0
ap6532-347	5C-0E-8B-21-77-	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-DF-	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-A2-	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-64-	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-06-	11an	norma	100w	17
ap650-2433	B4-C7-99-18-62-	11an	offline		0
ap8232-7F0	FC-0A-81-8D-2E-	11an	offline		0
ap650-2433	B4-C7-99-18-4A-	11bgn	offline		0
ap7131-135	B4-C7-99-EC-96-	11an	offline		0
ap7532-160	FC-0A-81-A3-10-	11an	norma	36	17
	5C-0E-8B-21-78-	11an	norma	108w	4

General

Radio MAC Address	5C-0E-8B-21-56-00
Radio Index	0
Radio Type	11bgn
State	normal

AP Hostname	ap6532-347854
Channel	1
Power	10

Neighbors

AP Hostname	Attenuation	Channel	Radio MAC Address	Power	Radio id
ap7502-B	87	11	FC-0A-81-	10	0

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

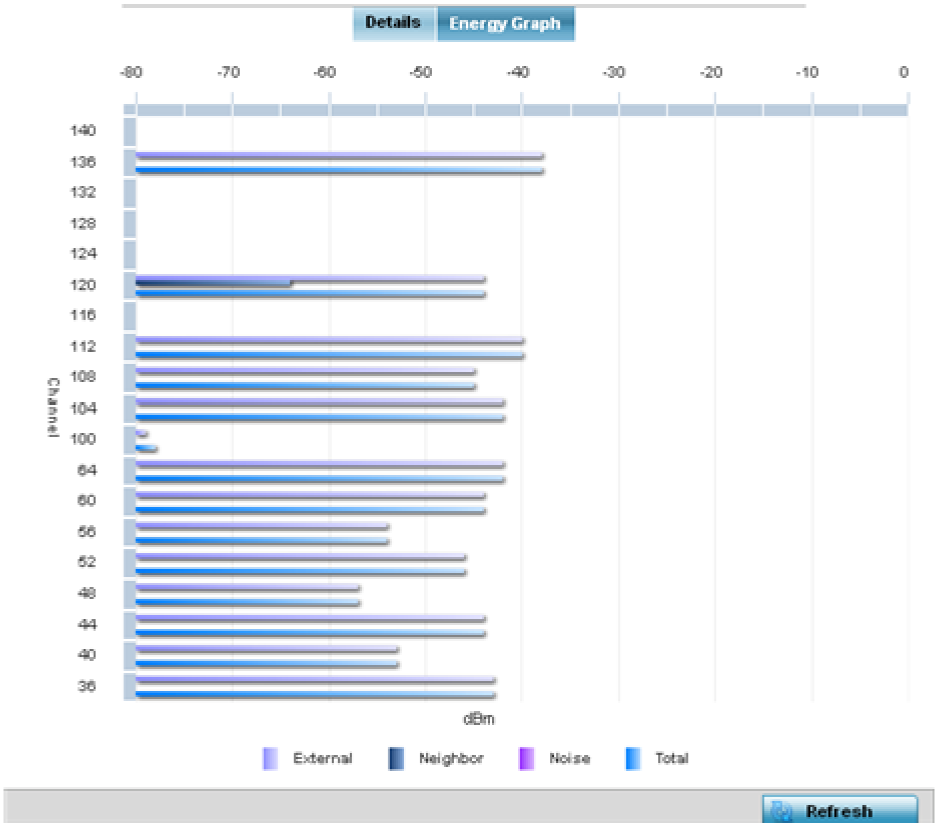
The SMART RF Energy Graph screen displays the RF Domain member AP's radio's operating channel, noise level and neighbor count. Use this information to assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

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.

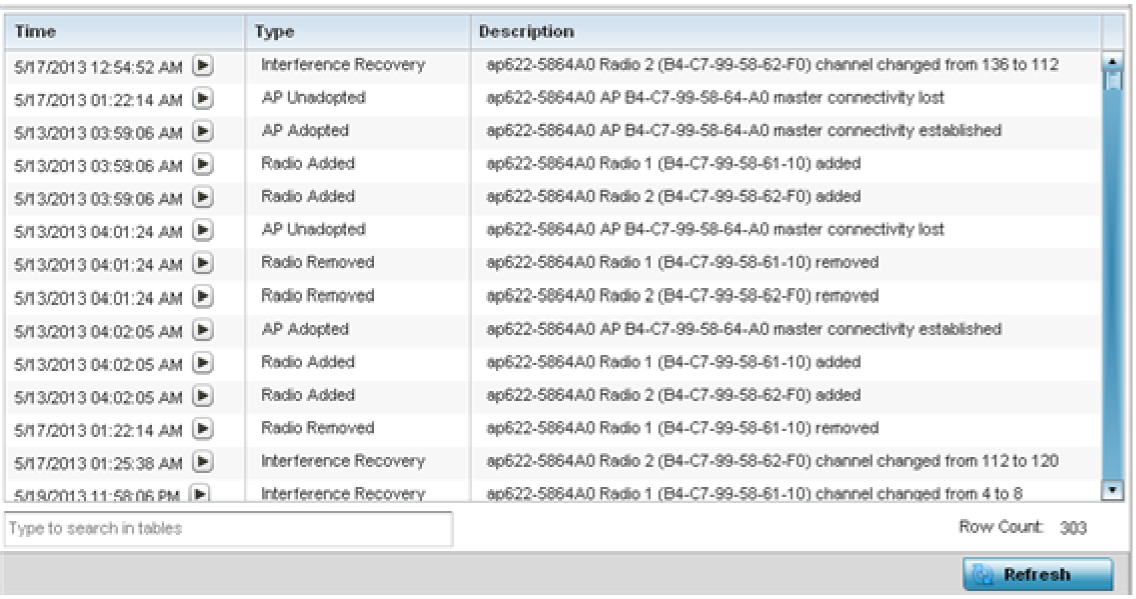
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node on the top, left-hand side of the screen.

   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.



Time	Type	Description
5/17/2013 12:54:52 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 136 to 112
5/17/2013 01:22:14 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 03:59:06 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/13/2013 04:01:24 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) removed
5/13/2013 04:02:05 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/17/2013 01:22:14 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/17/2013 01:25:38 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 112 to 120
5/19/2013 11:58:06 PM	Interference Recovery	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) channel changed from 4 to 8

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.

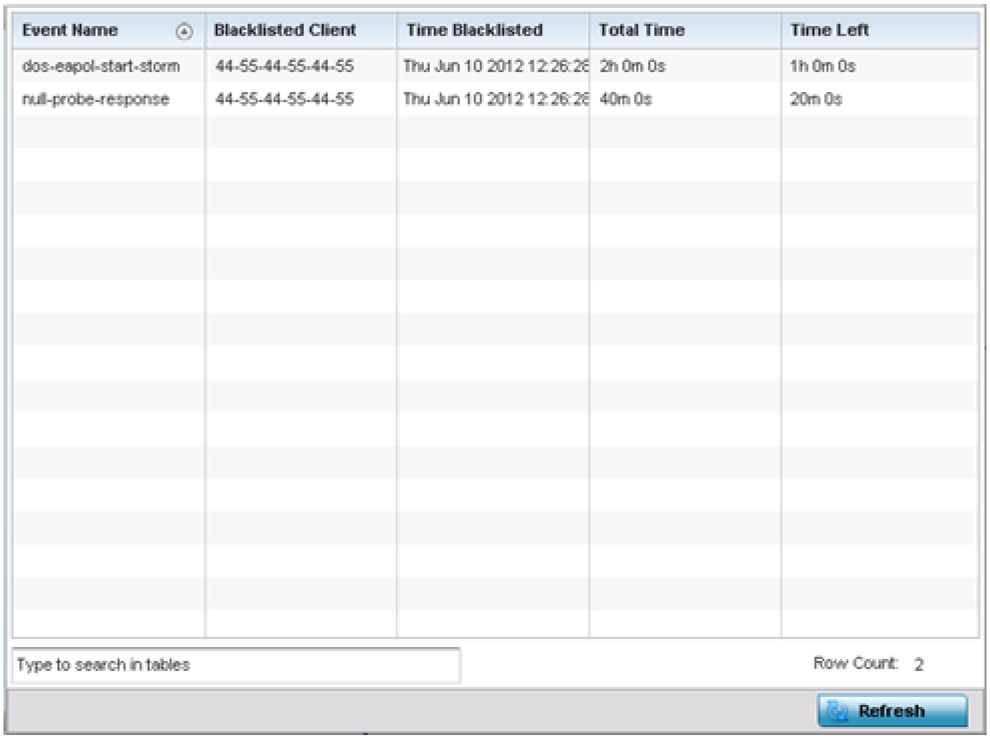
The **System** node expands to display the RF Domains created within the managed network.

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.



Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-eapol-start-storm	44-55-44-55-44-55	Thu Jun 10 2012 12:26:2	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2012 12:26:2	40m 0s	20m 0s

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.

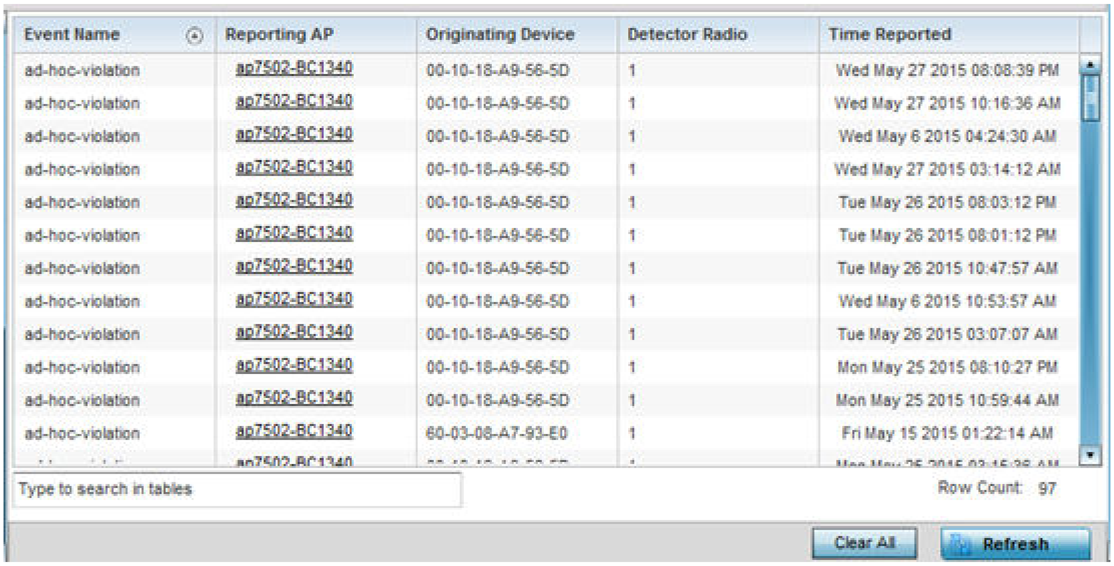
To view the rogue access point statistics:

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.



Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	ap7502-BC1340	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

Row Count: 97

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.

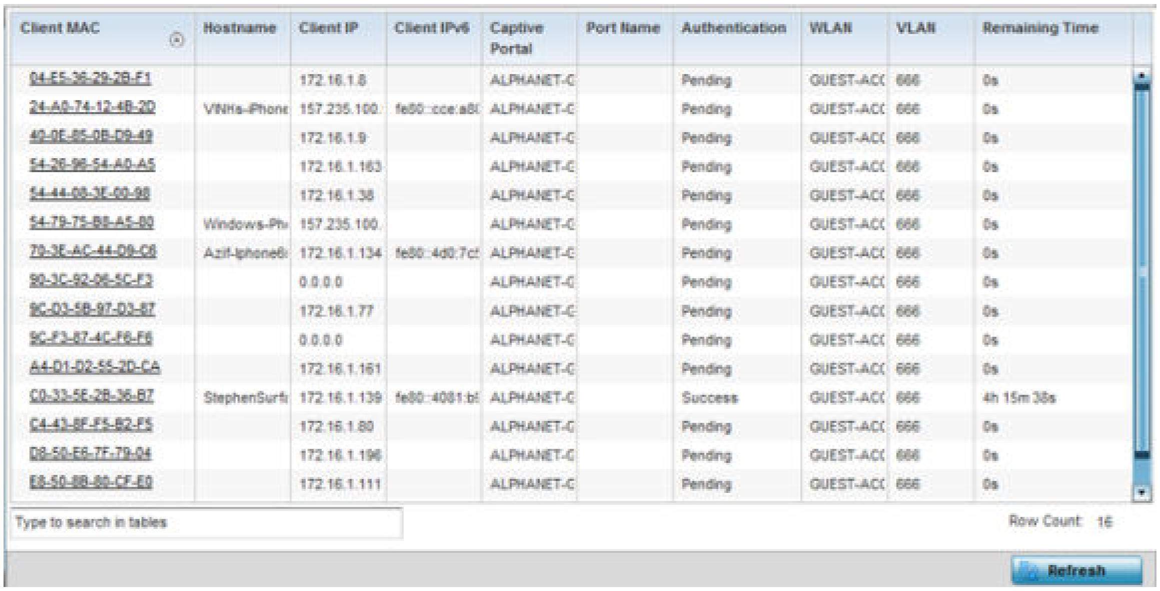
The **System** node expands to display the RF Domains created within the managed network.

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.



Client MAC	Hostname	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
04-E5-36-29-2B-F1		172.16.1.8		ALPHANET-C		Pending	GUEST-ACC	666	0s
24-A0-74-12-4B-2D	VINHs-iPhone	157.235.100.	fe80::cce:a8	ALPHANET-C		Pending	GUEST-ACC	666	0s
40-0E-85-0B-D9-49		172.16.1.9		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-26-96-54-A0-A5		172.16.1.163		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-44-08-3E-00-98		172.16.1.38		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-79-75-B8-A5-80	Windows-Ph	157.235.100.		ALPHANET-C		Pending	GUEST-ACC	666	0s
70-3E-AC-44-D9-C8	Azif-iphone6	172.16.1.134	fe80::4d0:7c	ALPHANET-C		Pending	GUEST-ACC	666	0s
90-3C-92-06-5C-F3		0.0.0.0		ALPHANET-C		Pending	GUEST-ACC	666	0s
9C-D3-5B-97-D3-87		172.16.1.77		ALPHANET-C		Pending	GUEST-ACC	666	0s
9C-F3-87-4C-F6-F6		0.0.0.0		ALPHANET-C		Pending	GUEST-ACC	666	0s
A4-D1-D2-55-2D-CA		172.16.1.161		ALPHANET-C		Pending	GUEST-ACC	666	0s
C0-33-5E-2B-36-B7	StephenSurf	172.16.1.139	fe80::4081:b	ALPHANET-C		Success	GUEST-ACC	666	4h 15m 38s
C4-43-8F-F5-B2-F5		172.16.1.80		ALPHANET-C		Pending	GUEST-ACC	666	0s
D8-50-E6-7F-79-04		172.16.1.196		ALPHANET-C		Pending	GUEST-ACC	666	0s
E8-50-8B-80-CF-E0		172.16.1.111		ALPHANET-C		Pending	GUEST-ACC	666	0s

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 509 and Application Group on page 511.

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.

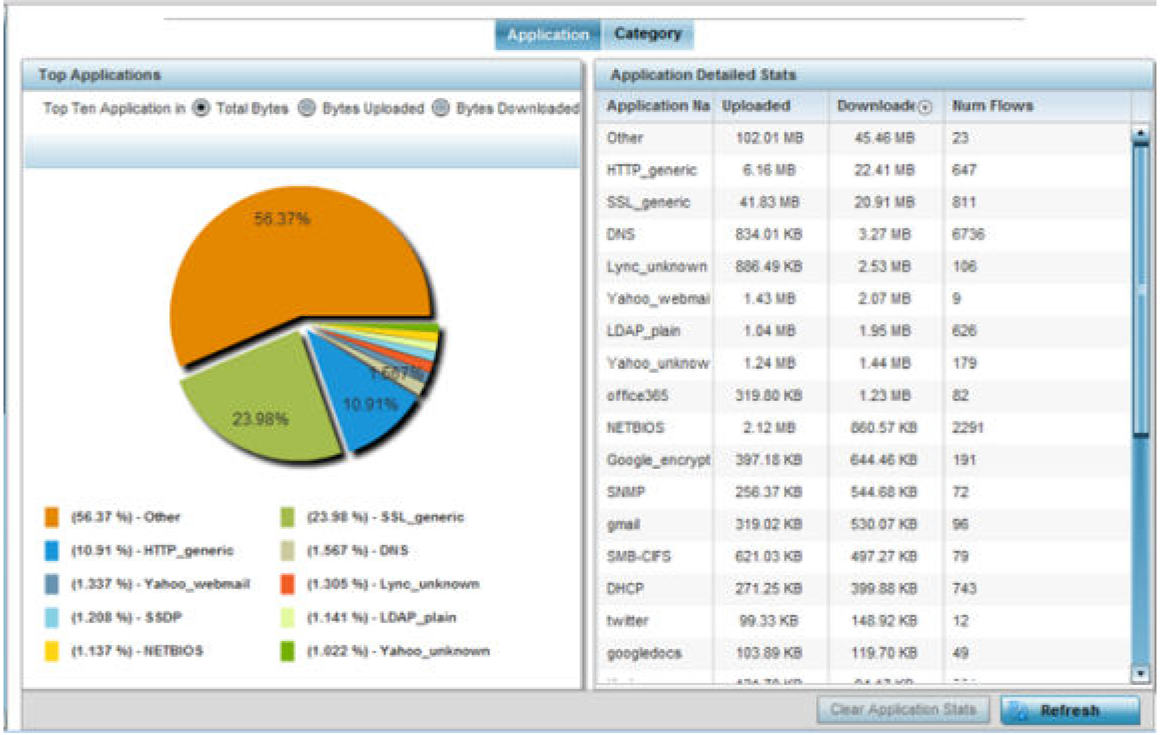
The **System** node expands to display the RF Domains created within the managed network.

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.


Application
Category
Top Applications
Top Ten Application in ● Total Bytes ○ Bytes Uploaded ○ Bytes Downloaded
56.37%
23.98%
10.91%
1.567%
🟧 (56.37 %) - Other
🟩 (23.98 %) - SSL_generic
🟦 (10.91 %) - HTTP_generic
▨ (1.567 %) - DNS
🟦 (1.337 %) - Yahoo_webmail
🟥 (1.305 %) - Lync_unknown
🟦 (1.208 %) - SSDP
🟩 (1.141 %) - LDAP_plain
🟨 (1.137 %) - NETBIOS
🟩 (1.022 %) - Yahoo_unknown
Application Detailed Stats
Clear Application Stats
Refresh

Application Na	Uploaded	Downloade	Num Flows
Other	102.01 MB	45.46 MB	23
HTTP_generic	6.16 MB	22.41 MB	647
SSL_generic	41.83 MB	20.91 MB	811
DNS	834.01 KB	3.27 MB	6736
Lync_unknown	886.49 KB	2.53 MB	106
Yahoo_webmai	1.43 MB	2.07 MB	9
LDAP_plain	1.04 MB	1.95 MB	626
Yahoo_unknow	1.24 MB	1.44 MB	179
office365	319.80 KB	1.23 MB	82
NETBIOS	2.12 MB	860.57 KB	2291
Google_encrypt	397.18 KB	644.46 KB	191
SNMP	256.37 KB	544.68 KB	72
gmail	319.02 KB	530.07 KB	96
SMB-CIFS	621.03 KB	497.27 KB	79
DHCP	271.25 KB	399.88 KB	743
twitter	99.33 KB	148.92 KB	12
googledocs	103.89 KB	119.70 KB	49

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).

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.

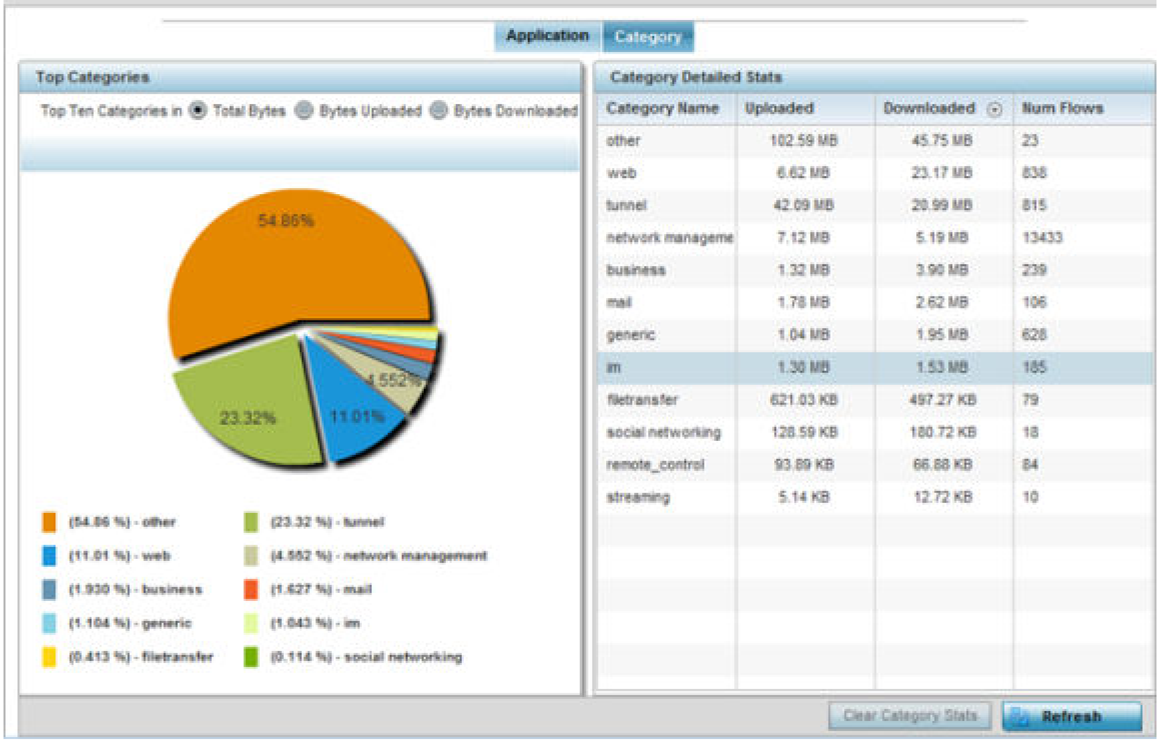
5 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment.

6 Periodically, click **Refresh** to update the statistics counters to their latest values.

7 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 509 and Application Group on page 511.

The **Application Visibility > Category** screen displays.



Category Detailed Stats

Category Name	Uploaded	Downloaded	Num Flows
other	102.59 MB	45.75 MB	23
web	6.62 MB	23.17 MB	838
tunnel	42.09 MB	20.99 MB	815
network manageme	7.12 MB	5.19 MB	13433
business	1.32 MB	3.90 MB	239
mail	1.78 MB	2.62 MB	106
generic	1.04 MB	1.95 MB	628
im	1.30 MB	1.53 MB	185
filetransfer	621.03 KB	497.27 KB	79
social networking	128.59 KB	180.72 KB	18
remote_control	93.89 KB	66.88 KB	84
streaming	5.14 KB	12.72 KB	10

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.

8. Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment.
9. Periodically, click **Refresh** to update the statistics counters to their latest values.

Coverage Hole Detection

Periodically refer to a selected RF Domain's coverage hole summary to assess the RF Domain member access point radios reporting coverage hole adjustments. 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 *(signal to noise 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:

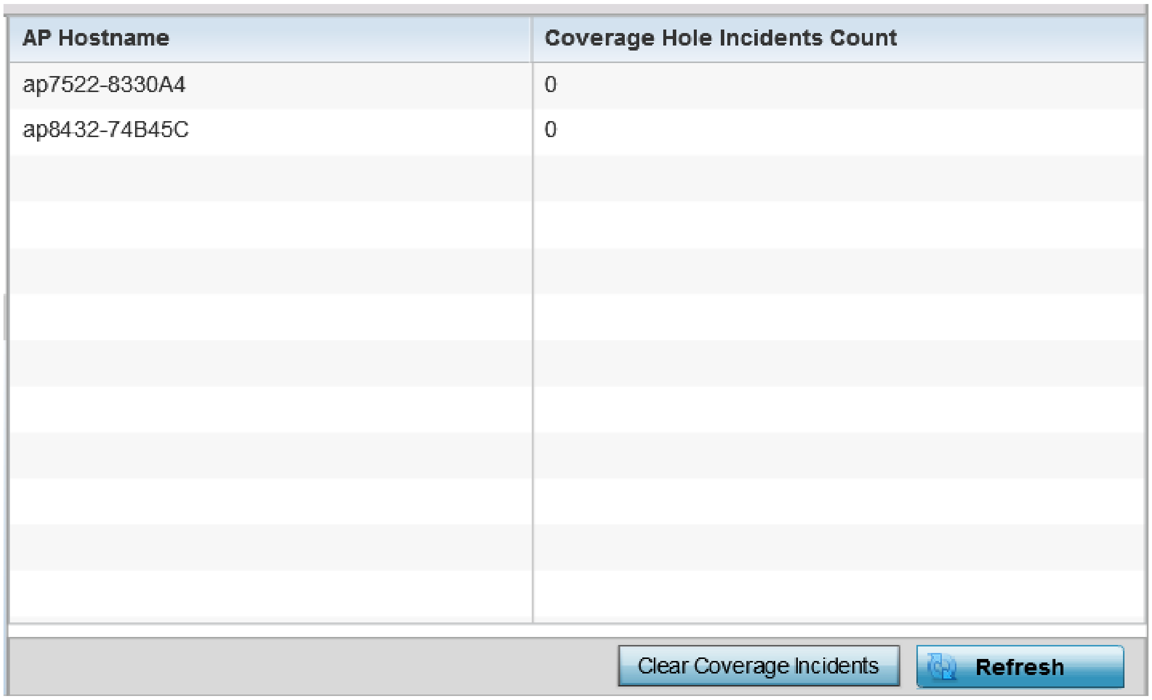
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node on the top, left-hand side of the screen.

   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.



AP Hostname	Coverage Hole Incidents Count
ap7522-8330A4	0
ap8432-74B45C	0

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.

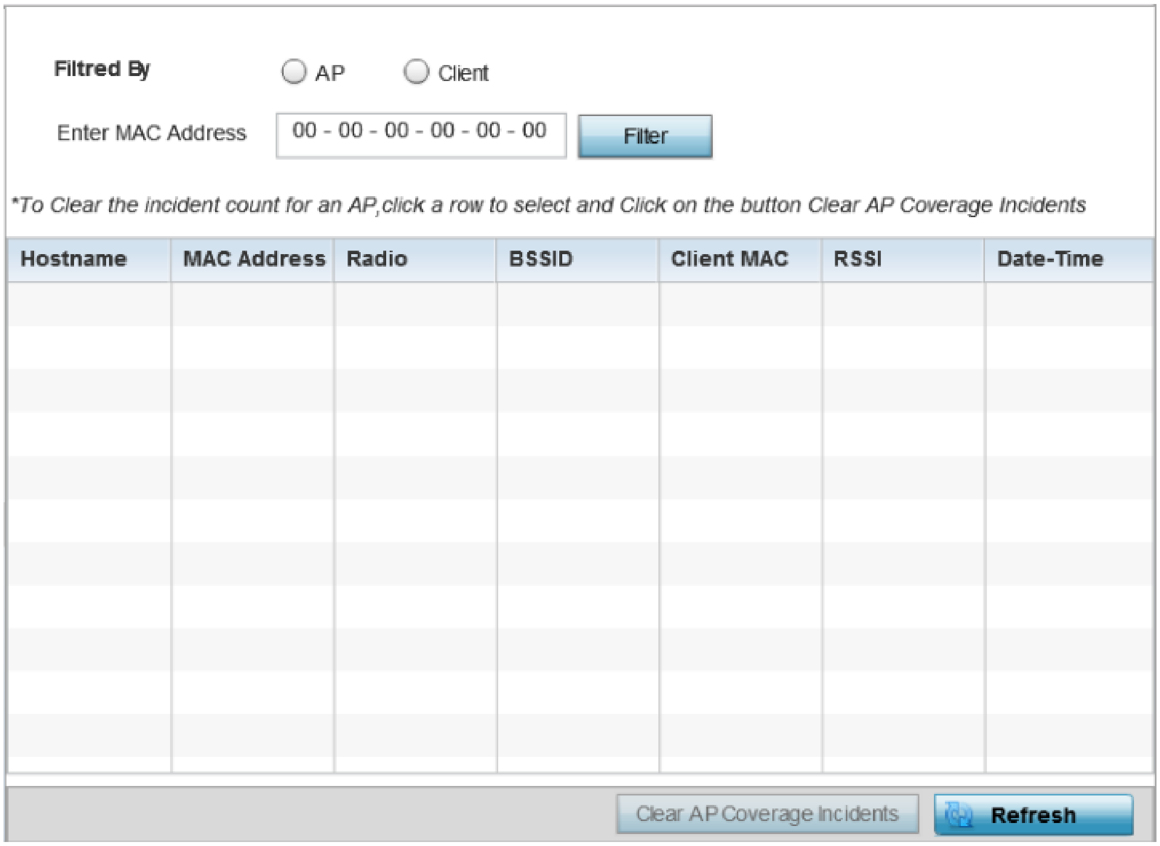
3 Select an **RF Domain** from the list.

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.


Filtred By
○ AP
○ Client
Enter MAC Address
00 - 00 - 00 - 00 - 00 - 00
Filter
*To Clear the incident count for an AP,click a row to select and Click on the button Clear AP Coverage Incidents
Hostname
MAC Address
Radio
BSSID
Client MAC
RSSI
Date-Time
Clear AP Coverage Incidents
Refresh

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.

Controller Statistics

The **Wireless Controller** screen displays information about peer controllers (or service platforms) and their connected APs. As members of a cluster, a controller or service platform manages its own network and is ready to assume the load of an offline peer when needed.

This screen displays detailed statistics, which include network health, device inventory, connected wireless clients, adopted APs, rogue APs and WLANs. For more information, refer to the following:

- Health
- Device
- Cluster Peers
- AP Upgrade
- Adoption
- AP Detection
- Wireless Clients
- Wireless LANs
- Policy Based Routing
- Radios
- Mesh
- Interfaces
- Power Status
- PPPoE
- OSPF
- L2TPv3
- VRRP
- Critical Resource
- Network
- DHCP Server
- Firewall

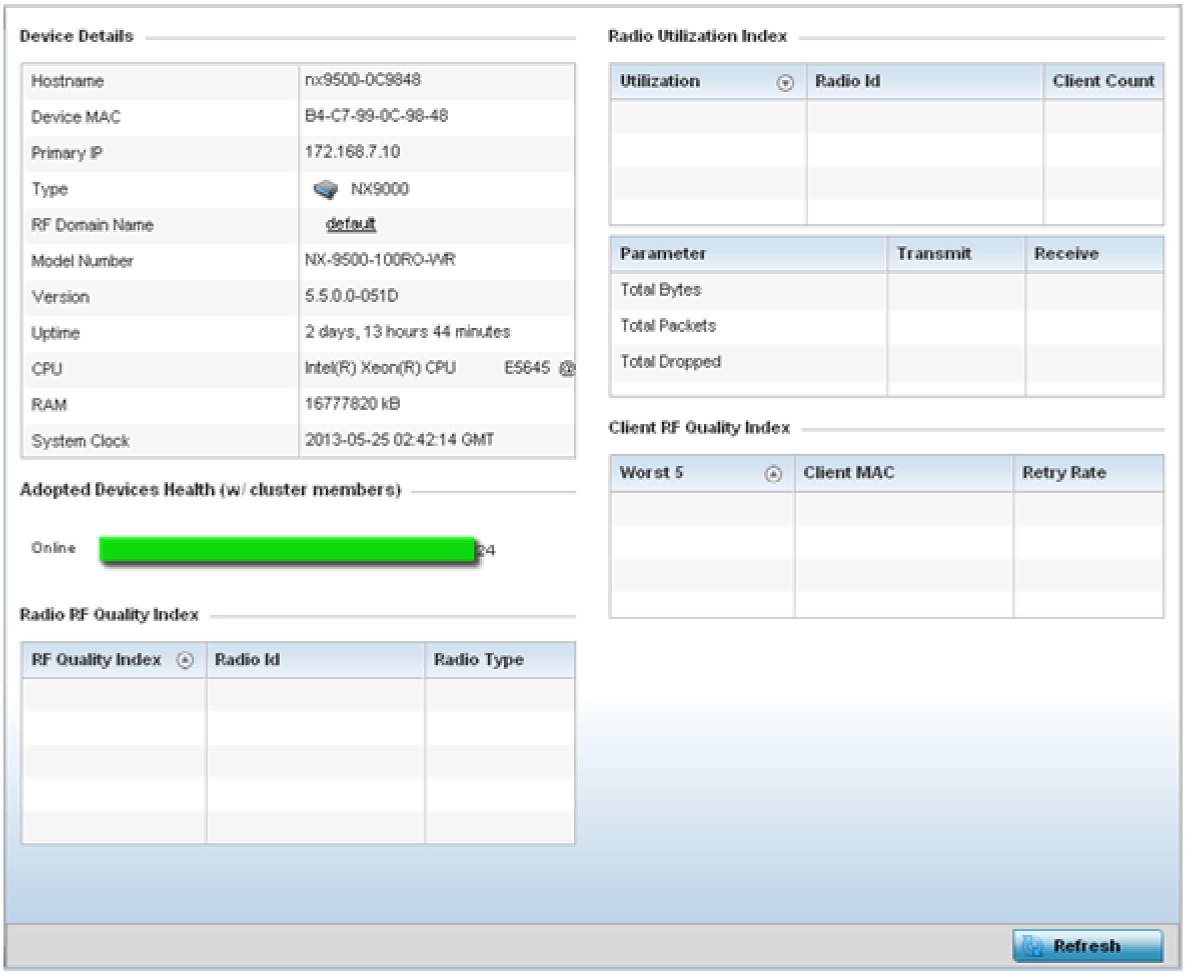
- VPN
- Viewing Certificate Statistics
- WIPS Statistics
- Sensor Server
- Captive Portal Statistics
- Network Time

Controller Health

The **Health** screen displays the hostname, device name, RF Domain name, radio RF quality and client RF quality of the selected RFS controller or NX series service platform.

To view health data:

1. Select the **Statistics** tab from the Web UI.
2. Select **System** from the navigation pane (on the left-hand side of the screen).
3. Expand the **RF Domain** node, and select one its connected **Wireless Controller/Service Platform**.
4. Select **Health** from the left-hand side of the UI.



Device Details

Hostname	nx9500-0C9848
Device MAC	B4-C7-99-0C-98-48
Primary IP	172.168.7.10
Type	NX9000
RF Domain Name	default
Model Number	NX-9500-100RO-WR
Version	5.5.0.0-051D
Uptime	2 days, 13 hours 44 minutes
CPU	Intel(R) Xeon(R) CPU E5645 @
RAM	16777820 kB
System Clock	2013-05-25 02:42:14 GMT

Adopted Devices Health (w/ cluster members)

Online 24

Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type

Radio Utilization Index

Utilization	Radio Id	Client Count

Parameter	Transmit	Receive
Total Bytes		
Total Packets		
Total Dropped		

Client RF Quality Index

Worst 5	Client MAC	Retry Rate

Review the different fields displayed on the **Controller > Health** screen.

The **Device Details** field displays the following:

Hostname	Displays the hostname of the controller or service platform.
Device MAC	Displays the MAC address of the controller or service platform.
Primary IP	Lists the network address used by this controller or service platform as a network identifier.
Type	Displays the controller type (for example, RFS 4000) or service platform type (for example, NX 9600).
RF Domain Name	Displays the controller's domain membership. The name displays in the form of a link that can be selected to display a detailed description of the RF Domain configuration.
Model Number	Displays the model number of the selected controller or service platform.
Version	Displays the version of the image running on the controller or service platform.
Uptime	Displays the cumulative time since the controller or service platform was last rebooted or lost power.
CPU	Displays the controller or service platform processor name.
RAM	Displays the CPU memory currently utilized.
System Clock	Displays the system clock information.

The **Adopted Devices Health (w/ cluster members)** chart shows how many managed devices are online versus offline. These cluster members directly managed by the wireless controller or service platform. This data does not include access points associated to other controllers or service platforms in the same cluster.

The **Radio RF Quality Index** field displays RF quality (overall effectiveness of the RF environment). Use this table to assess radio performance for improvement ideas. This field displays the following:

RF Quality Index	Displays the five radios with the lowest average quality.
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 measures how efficiently the traffic medium is used. It’s defined as the percentage of the current throughput relative to the maximum relative possible throughput:

Total Bytes	Displays the total bytes of data transmitted and received by the controller or service platform since the screen was last refreshed.
Total Packets	Lists the total number of data packets transmitted and received by the controller or service platform since the screen was last refreshed.
Total Dropped	List the number of dropped data packets by a controller or service platform managed access point radio since the screen was last refreshed.

The **Client RF Quality Index** field displays the RF quality of the clients. Use this table to troubleshoot radios not optimally performing:

Worst 5	Displays five client radios with the lowest quality indices of all of those managed by the controller or service platform.
Client MAC	Displays the hardware encoded MAC address of the client.
Retry Rate	Displays the excessive retry rate of each listed controller or service platform client.

5 Select **Refresh** to update the statistics counters to their latest values.

Controller Device

The Device screen provides detailed information about the selected device within the controller, service platform managed system.

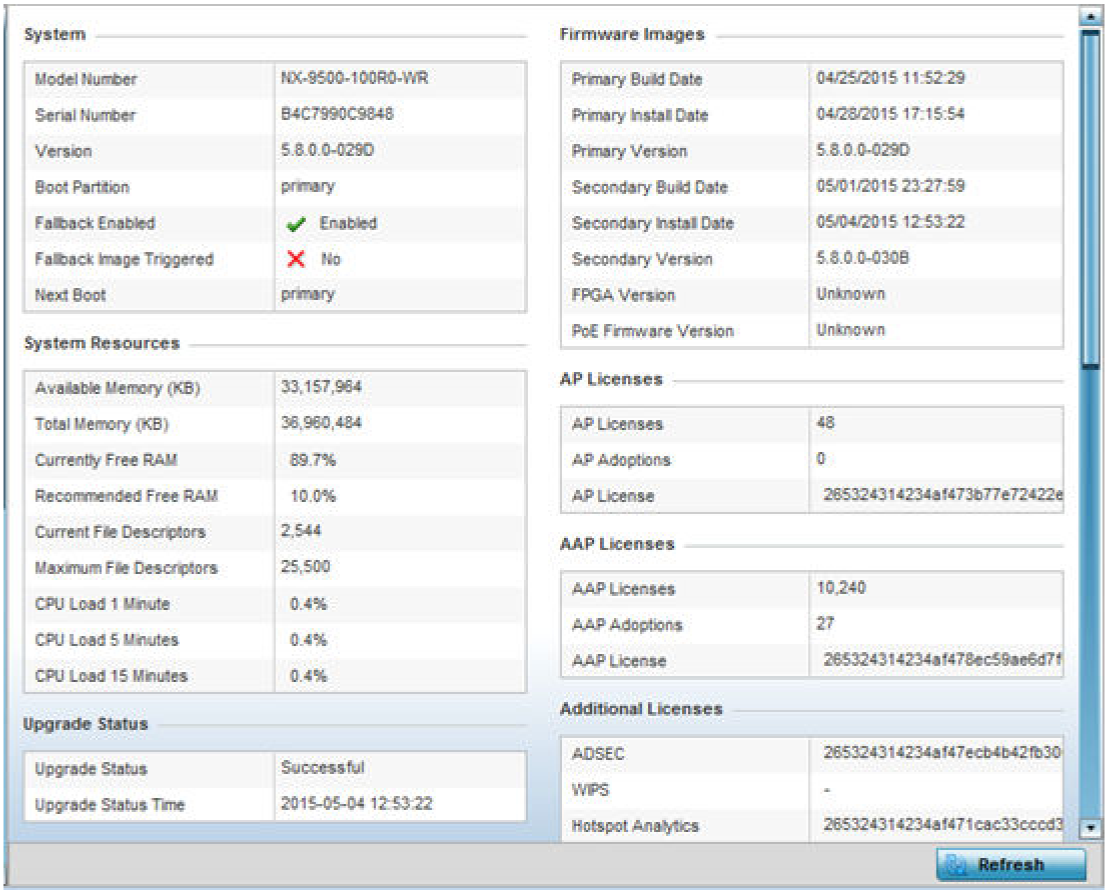
To view system device statistics:

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 its connected **Wireless Controller/Service Platform**.

4 Select **Device** from the left-hand side of the UI.



System

Model Number	NX-9500-100R0-WR
Serial Number	B4C7990C9848
Version	5.8.0.0-029D
Boot Partition	primary
Fallback Enabled	✓ Enabled
Fallback Image Triggered	✗ No
Next Boot	primary

System Resources

Available Memory (KB)	33,157,964
Total Memory (KB)	36,960,484
Currently Free RAM	89.7%
Recommended Free RAM	10.0%
Current File Descriptors	2,544
Maximum File Descriptors	25,500
CPU Load 1 Minute	0.4%
CPU Load 5 Minutes	0.4%
CPU Load 15 Minutes	0.4%

Upgrade Status

Upgrade Status	Successful
Upgrade Status Time	2015-05-04 12:53:22

Firmware Images

Primary Build Date	04/25/2015 11:52:29
Primary Install Date	04/28/2015 17:15:54
Primary Version	5.8.0.0-029D
Secondary Build Date	05/01/2015 23:27:59
Secondary Install Date	05/04/2015 12:53:22
Secondary Version	5.8.0.0-030B
FPGA Version	Unknown
PoE Firmware Version	Unknown

AP Licenses

AP Licenses	48
AP Adoptions	0
AP License	265324314234af473b77e72422e

AAP Licenses

AAP Licenses	10,240
AAP Adoptions	27
AAP License	265324314234af478ec59ae6d7f

Additional Licenses

ADSEC	265324314234af47ecb4b42fb30
WIPS	-
Hotspot Analytics	265324314234af471cac33cccd3

The System field displays the following:

Model Number	Displays the model number for the selected controller or service platform.
Serial Number	Displays the serial number factory encoded on the controller or service platform at the factory.
Version	Displays the unique alphanumeric firmware version name for the controller or service platform firmware.
Boot Partition	Displays the boot partitioning type (primary or secondary).
Fallback Enabled	Displays whether fallback is enabled. The fallback feature enables a user to store both a legacy and new firmware version in memory. You can test the new software and use an automatic fallback mechanism, which loads the old version, if the new version fails.
Fallback Image Triggered	Displays whether the fallback image has been triggered. The fallback is a legacy software image stored in device memory. This allows an user to test a new version and revert to the older version if needed.
Next Boot	Designates this version as the version used the next time the controller or service platform is booted.

The System Resources table displays the following:

Available Memory (MB)	Displays the available memory (in MB) available on the selected device (controller or service platform).
Total Memory (MB)	Displays the total memory resources available to the selected device.
Currently Free RAM	Displays the free RAM space available to the selected device. 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 current file description.
Maximum File Description	Displays the maximum file description.
CPU Load 1 Minute	Lists the typical device processor load over 1 minute.
CPU Load 5 Minutes	Lists the typical device processor load over 5 minutes.
CPU Load 15 Minutes	Lists the typical device processor load over 15 minutes.

The Upgrade Status field displays firmware upgrade statistics. The table provides the following:

Upgrade Status	Displays whether the image upgrade was successful.
Upgrade Status Time	Displays the time of the upgrade.

The IP Domain field displays the following:

IP Domain Name	Displays the name of the IP Domain service used with the selected device (controller or service platform).
IP Domain Lookup state	Lists the current state of the lookup operation.

The Fan Speed field displays the following:

Number	Displays the number of fans supported on the this controller or service platform.
Speed (Hz)	Displays the fan speed in Hz.

The **Temperature** field displays the following:

Number	Displays the number of temperature elements (gauges) utilized by the selected device (controller or service platform).
Temperature	Displays the current temperature (in Celsius) to assess a potential 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 device (controller or service platform.
Maximum Buffers	Lists the maximum buffers available to the selected device.

The **Firmware Images** field displays the following:

Primary Build Rate	Displays the build date when this version was created.
Primary Install Date	Displays the date this firmware version was installed on the controller or service platform.
Primary Version	Displays the primary version string.
Secondary Build Date	Displays the build date when this secondary version was created.
Secondary Install Date	Displays the date this secondary version was installed on the controller or service platform.
Secondary Version	Displays the secondary version string.
FGPA Version	Displays the FGPA version string.
PoE Firmware Version	Displays the version of the PoE *(Power Over Ethernet)* firmware if the PoE feature is available.

The **AP Licenses** field displays the following license information for access points:

AP Licenses	Displays the number of AP licenses currently available on the controller or service platform. This value represents the maximum number of licenses the controller or service platform can adopt.
AP Adoptions	Displays the number of APs adopted by this controller or service platform.
AP License	Displays the license string of the AP.

The **AAP Licenses** field displays the following license information for adaptive access points:

AAP Licenses	Displays the number of AAP *(adaptive access point)* licenses currently available. This value represents the maximum number of licenses the controller or service platform can adopt.
AAP Adoptions	Displays the number of AAPs adopted by this controller or service platform.
AAP License	Displays the license string of the AAP.

The **Additional Licenses** area displays the following information:

ADSEC	Displays the number of Advanced Security licenses. This enables the Role Based firewall and increases the number of IP Sec VPN tunnels. The maximum number of IP Sec VPN tunnels varies by platform.
WIPS	Displays the number of WIPS licenses utilized by the controller or service platform.
Hotspot Analytics	Displays whether an advanced hotspot analytics license is in use and applied to the controller or service platform.

The IP Name Servers table displays the following:

Name Server	Displays any custom Name Server mappings on the controller or service platform.
Type	Displays the type of DNS mapping, if any, on the controller or service platform.

The IPv6 Name Servers table displays the following:

Name Server	Displays any custom IPv6 formatted IP address Name Server mappings on the controller or service platform.
Type	Displays the type of DNS mapping, if any, on the controller or service platform.

The IPv6 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 Delegated Prefixes field displays the following:

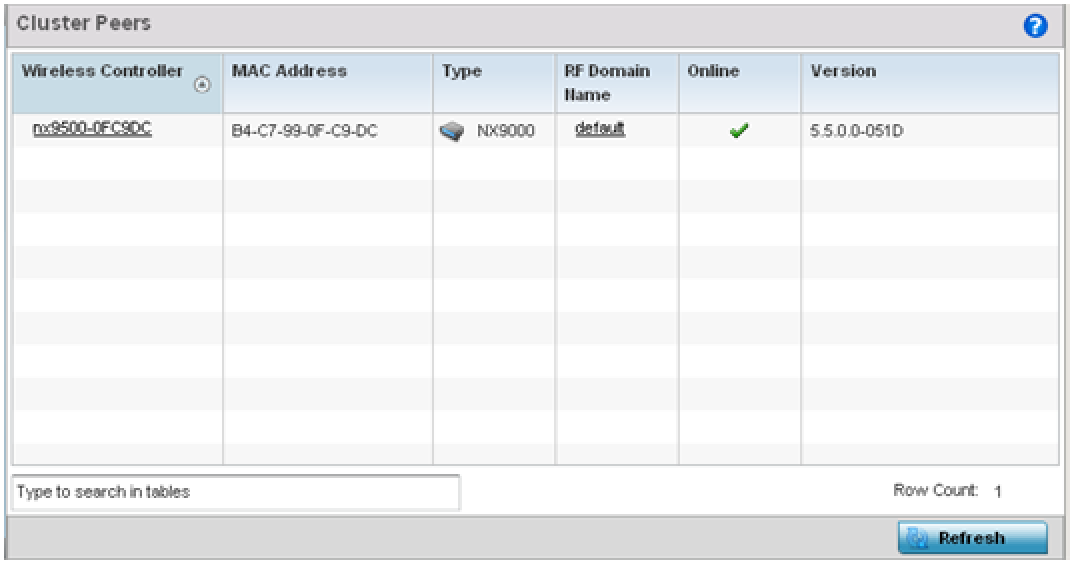
IPv6 Delegated Prefix	If IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix.
Prefix Name	Lists the 32 character maximum name for the IPv6 delegated prefix used as an easy to remember alias for an entire IPv6 address.
DHVPv6 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	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.

Cluster Peers

Refer to the Cluster Peers screen to review device address and version information for peer devices within a cluster.

To view cluster peer statistics:

1. Select the Statistics tab from the Web UI.
2. Expand the **RD Domain** node.
3. Select the Wireless Controller node from the left navigation pane.
4. Select Cluster Peers from the left-hand side of the UI.



Wireless Controller	MAC Address	Type	RF Domain Name	Online	Version
nx9500-0FC9DC	B4-C7-99-0F-C9-DC	NX9000	default	✓	5.5.0.0-051D

The Cluster Peers screen displays the following:

Wireless Controller	Displays the IP addresses of current cluster member controller or service platform. The name displays in the form of a link that can be selected to display a detailed description of the controller or service platform's configuration.
MAC Address	Displays the MAC addresses of current cluster members.
Type	Displays the type of cluster peer.
RF Domain Name	Displays each member's RF Domain name. The name displays in the form of a link that can be selected to display a detailed description of the RF Domain's configuration.
Online	Displays whether a cluster member is currently online. If online, a green check mark displays, if it is offline a red X displays.
Version	Displays the numeric firmware version currently running controller or service platform. Use this version as the basis for comparison on whether newer versions are available from the support site that may provide increased functionality and a broader feature set.
Refresh	Select to update the screen's statistics counters to their latest values.

Controller 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 controller or service platform. 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).

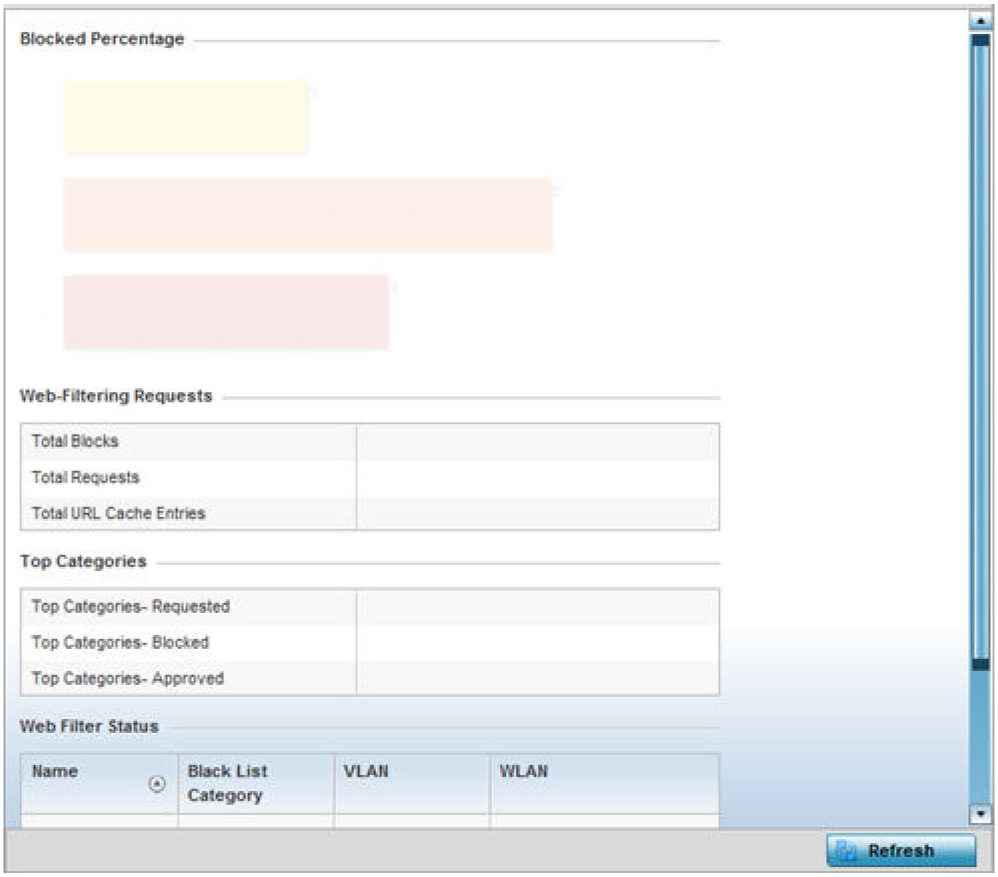
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**.

The selected device'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 > Controller/AP > Web-Filtering** screen is displayed.



5 Review the following Web-Filtering statistics:

The Web-Filtering Requests field displays the following:

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 controller or service platform.
Total URL Cache Entries	Displays the number of cached URL data entries made on this controller or service platform on the request of requesting clients requiring URL data managed by the controller or service platform 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 controller or service platform. 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 controller or service platform. 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 controller or service platform. 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 controller or service platform VLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category.
WLAN	Lists the impacted controller or service platform 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.

Controller Application Visibility (AVC)

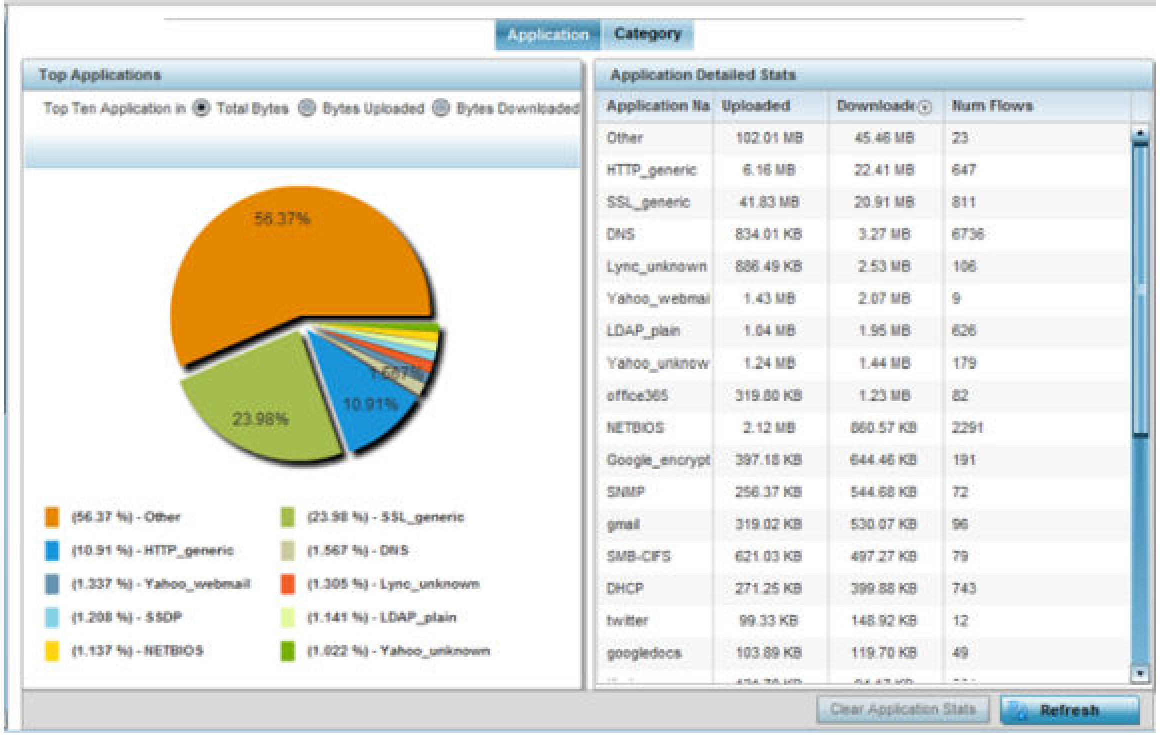
Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. For information on categorizing, filtering and logging the application data allowed to proliferate the controller or service platform managed network, refer to Application on page 509 and Application Group on page 511.

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, select a **controller or service platform**.

   The Controller's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.
4. Select **Application Visibility (AVC)** from the menu.

   The **Statistics** → **Controller/AP** → **Application Visibility (AVC)** → **Application** screen displays.



Application Detailed Stats

Application Na	Uploaded	Downloade	Num Flows
Other	102.01 MB	45.46 MB	23
HTTP_generic	6.16 MB	22.41 MB	647
SSL_generic	41.83 MB	20.91 MB	811
DNS	834.01 KB	3.27 MB	6736
Lync_unknown	886.49 KB	2.53 MB	106
Yahoo_webmai	1.43 MB	2.07 MB	9
LDAP_plain	1.04 MB	1.95 MB	626
Yahoo_unknow	1.24 MB	1.44 MB	179
office365	319.80 KB	1.23 MB	82
NETBIOS	2.12 MB	860.57 KB	2291
Google_encrypt	397.18 KB	644.46 KB	191
SNMP	256.37 KB	544.68 KB	72
gmail	319.02 KB	530.07 KB	96
SMB-CIFS	621.03 KB	497.27 KB	79
DHCP	271.25 KB	399.88 KB	743
twitter	99.33 KB	148.92 KB	12
googledocs	103.89 KB	119.70 KB	49

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 controller or service platform managed network. These are only the administrator allowed applications approved for proliferation within the controller or service platform managed network.
Bytes Uploaded	Displays the top ten applications in respect to total data bytes uploaded through the controller or service platform 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 controller or service platform 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).

Refer to the Application Detailed Stats table to assess specific application data utilization:

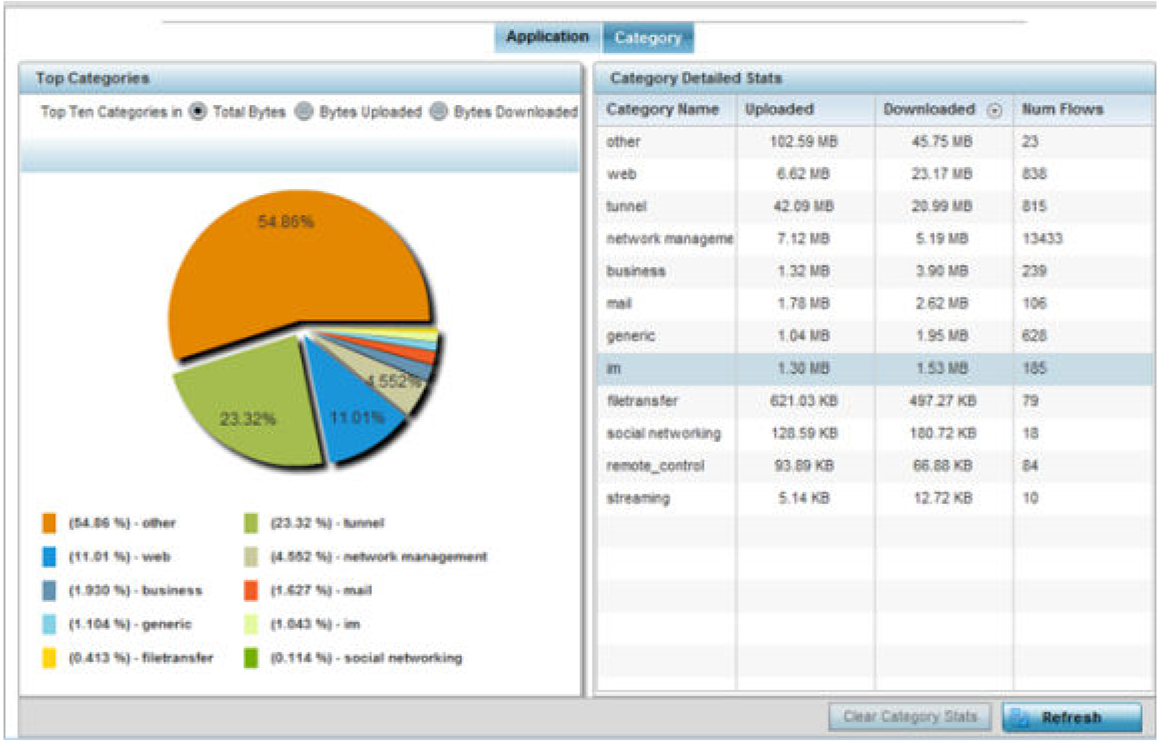
Application Name	Lists the allowed application name whose data (bytes) are passing through the controller or service platform managed network.
Uploaded	Displays the number of uploaded application data (in bytes) passing the through the controller or service platform managed network.
Downloaded	Displays the number of downloaded application data (in bytes) passing the through the controller or service platform managed network.
Num Flows	Lists the total number of application data flows passing through the controller or service platform 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.

5 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.

6 Click 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 509 and Application Group on page 511.

The **Statistics** → **Controller** → **Application Visibility** → **Category** screen displays.



Category Name	Uploaded	Downloaded	Num Flows
other	102.59 MB	45.75 MB	23
web	6.62 MB	23.17 MB	838
tunnel	42.09 MB	20.99 MB	815
network manageme	7.12 MB	5.19 MB	13433
business	1.32 MB	3.90 MB	239
mail	1.78 MB	2.62 MB	106
generic	1.04 MB	1.95 MB	628
im	1.30 MB	1.53 MB	185
filetransfer	621.03 KB	497.27 KB	79
social networking	128.59 KB	180.72 KB	18
remote_control	93.89 KB	66.88 KB	84
streaming	5.14 KB	12.72 KB	10

Refer to the Top Categories graph to assess the most prolific, and allowed, application data categories utilized by the controller or service platform.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the controller or service platform managed network. These are only the administrator allowed application categories approved for proliferation within the controller or service platform managed network.
Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the controller or service platform 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 controller or service platform 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 controller or service platform managed network.
Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the controller or service platform managed network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the controller or service platform managed network.
Num Flows	Lists the total number of application category data flows passing through controller or service platform managed 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.

7. 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.
8. Click **Refresh** to update the statistics counters to their latest values.

Controller 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.

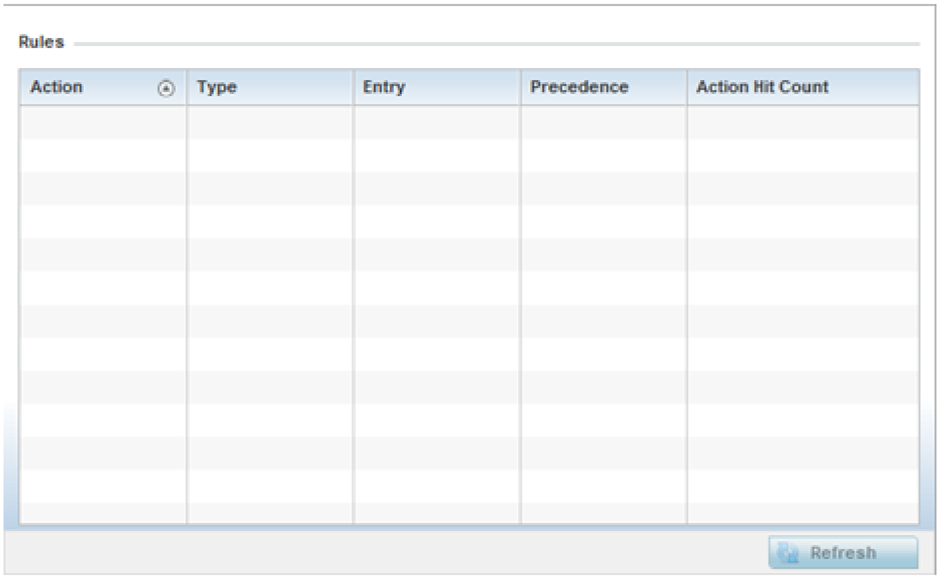
Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. Rate-limits create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

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, select a **controller or service platform**.

   The Controller'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** → **Controller** →**Application 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 controller or service platform.

Action	Displays the action executed on the listed application. • **`Allow`** - Allows packets for a specific application and its defined category type (social networking, etc.). This is the default setting. • **`Deny`** - Denies (restricts) the action applied to a specific application or a specific application category. • **`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.

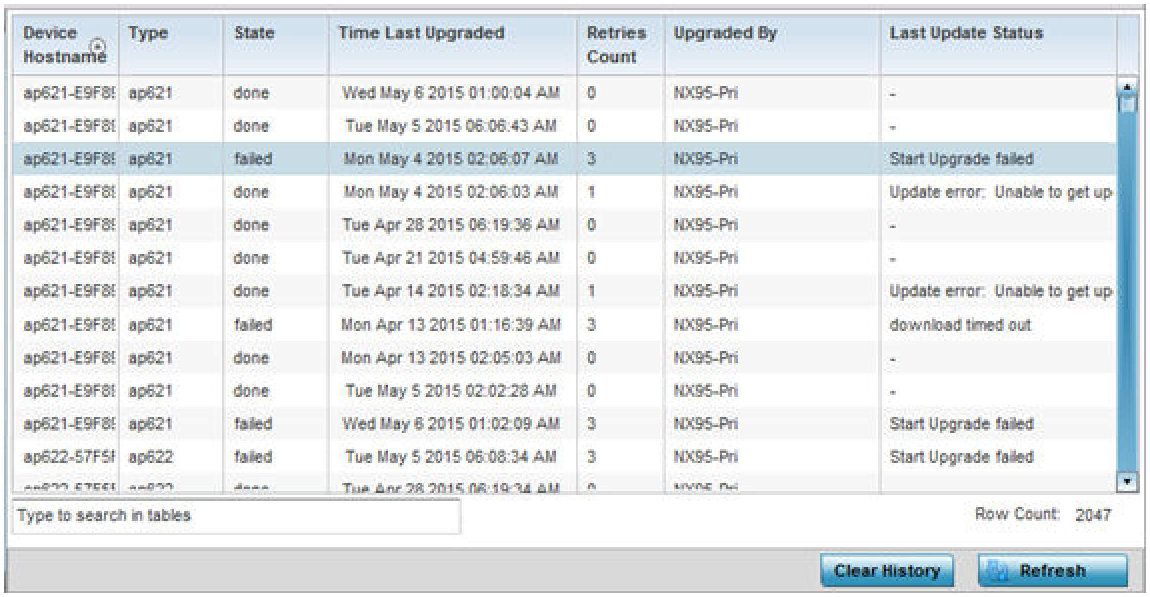
Device Upgrade

The Device Upgrade screen displays information about devices receiving updates within the controller or service platform managed network. Use this screen to gather version data, install firmware images, boot an image and upgrade status.

Controllers, service platforms or APs can be RF domain managers capable of receiving device firmware files from the NOC then provisioning other devices within their same RF domain. Controllers, service platforms and APs 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.

To view the device upgrade statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select the **Wireless Controller** node from the left navigation pane.
4 Select **Device Upgrade**.



Device Hostname	Type	State	Time Last Upgraded	Retries Count	Upgraded By	Last Update Status
ap621-E9F8	ap621	done	Wed May 6 2015 01:00:04 AM	0	NX95-Pri	-
ap621-E9F8	ap621	done	Tue May 5 2015 06:06:43 AM	0	NX95-Pri	-
ap621-E9F8	ap621	failed	Mon May 4 2015 02:06:07 AM	3	NX95-Pri	Start Upgrade failed
ap621-E9F8	ap621	done	Mon May 4 2015 02:06:03 AM	1	NX95-Pri	Update error: Unable to get up
ap621-E9F8	ap621	done	Tue Apr 28 2015 06:19:36 AM	0	NX95-Pri	-
ap621-E9F8	ap621	done	Tue Apr 21 2015 04:59:46 AM	0	NX95-Pri	-
ap621-E9F8	ap621	done	Tue Apr 14 2015 02:18:34 AM	1	NX95-Pri	Update error: Unable to get up
ap621-E9F8	ap621	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap621-E9F8	ap621	done	Mon Apr 13 2015 02:05:03 AM	0	NX95-Pri	-
ap621-E9F8	ap621	done	Tue May 5 2015 02:02:28 AM	0	NX95-Pri	-
ap621-E9F8	ap621	failed	Wed May 6 2015 01:02:09 AM	3	NX95-Pri	Start Upgrade failed
ap622-57F5	ap622	failed	Tue May 5 2015 06:08:34 AM	3	NX95-Pri	Start Upgrade failed

The Upgrade screen displays the following information:

Device Hostname	Displays the administrator-assigned hostname of the device receiving the update.
Type	Displays the model type of the device receiving a firmware update from the provisioning controller or service platform.
State	Displays the current state of the upgrade process (`done`, `failed`, etc.).
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.
Upgraded By	Displays the MAC address of the controller or service platform that performed the upgrade.
History ID	Displays a unique timestamp for the upgrade event.
Last Update Status	Displays the status of the last upgrade operation (`Start Upgrade`, `Update error`, etc.).

5 Click **Clear History** to clear the screen of its current status and begin a new data collection.
6 Click Refresh to update the screen's statistics counters to their latest values.

Adoption

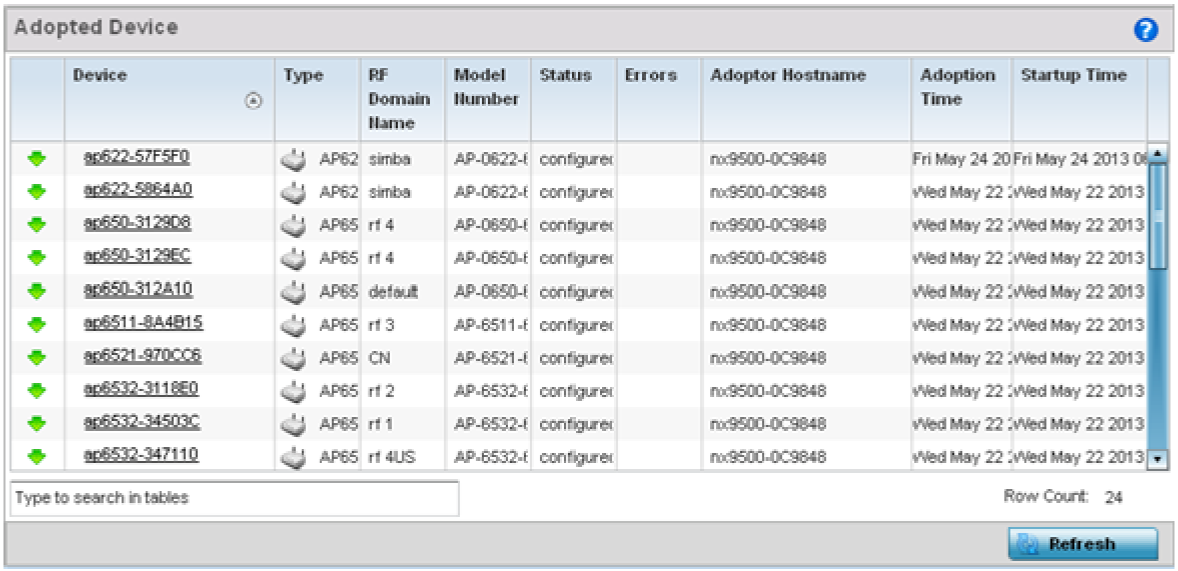
The Adoption screens lists devices adopted by the controller or service platform, and includes model, RF Domain membership, configuration status and device uptime information. For additional AP adoption information, including an adoption history and pending adoptions, see:

- Adopted Devices
- AP Adoption History
- Pending Adoption

Adopted Devices

To view adopted devices statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select the **Wireless Controller** node from the left navigation pane.
4. Expand the **Adoption** node in the left-hand side of the UI.
5. Select **Adopted Devices**.



	Device	Type	RF Domain Name	Model Number	Status	Errors	Adoptor Hostname	Adoption Time	Startup Time
	ap622-57F5F0	AP62	simba	AP-0622-	configure		nx9500-0C9848	Fri May 24 20	Fri May 24 2013 0
	ap622-5864A0	AP62	simba	AP-0622-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap650-3129D8	AP65	rf 4	AP-0650-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap650-3129EC	AP65	rf 4	AP-0650-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap650-312A10	AP65	default	AP-0650-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap6511-8A4B15	AP65	rf 3	AP-6511-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap6521-970CC6	AP65	CN	AP-6521-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap6532-3118E0	AP65	rf 2	AP-6532-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap6532-34503C	AP65	rf 1	AP-6532-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013
	ap6532-347110	AP65	rf 4US	AP-6532-	configure		nx9500-0C9848	Wed May 22	Wed May 22 2013

6. The Adopted Devices screen displays the following:

Device	Displays the name assigned to the adopted device by the WiNG management software. The device name displays as a link that can be selected to display configuration and network address information in greater detail.
Type	Lists the model type of each device managed by the selected controller.
RF Domain Name	Displays the RF Domain memberships of each listed adopted device.
Model Number	Displays the model number of the adopted device.

Status	Lists whether the adopted device has been configured (provisioned) by its connected controller or service platform.
Errors	Lists any errors encountered the adoption.
Adopter Hostname	Lists the hostname of the adopting controller or service platform.
Adoption Time	Displays a timestamp, for each listed device, showing the date and time of adoption.
Startup Time	Lists the time the adopted device was last started up and detected on the network.

7 Click **Refresh** to update the screen's statistics counters to their latest values.

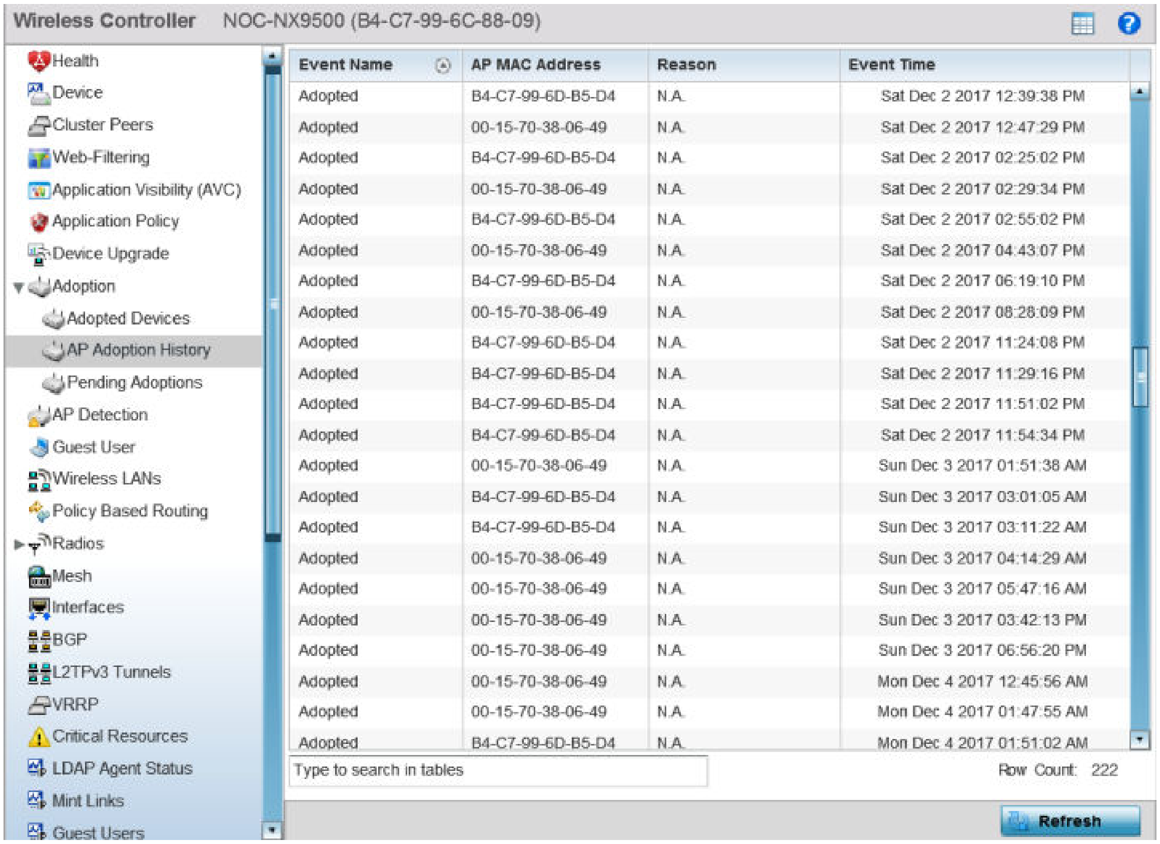
AP Adoption History

The AP Adoption History screen displays a list of devices adopted to the controller or service platform managed network. Use this screen to view a list of devices and their current status.

To view AP adoption history statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller** node from the left navigation pane.
4 Expand the **Adoption** node in the left-hand side of the UI.
5 Select **AP Adoption History**.

The **Statistics > Controller > Adoption > AP Adoption History** screen displays.



Wireless Controller NOC-NX9500 (B4-C7-99-6C-88-09)

Event Name	AP MAC Address	Reason	Event Time
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 12:39:38 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 12:47:29 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 02:25:02 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 02:29:34 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 02:55:02 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 04:43:07 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 06:19:10 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 08:28:09 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:24:08 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:29:16 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:51:02 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:54:34 PM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 01:51:38 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sun Dec 3 2017 03:01:05 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sun Dec 3 2017 03:11:22 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 04:14:29 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 05:47:16 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 03:42:13 PM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 06:56:20 PM
Adopted	00-15-70-38-06-49	N.A.	Mon Dec 4 2017 12:45:56 AM
Adopted	00-15-70-38-06-49	N.A.	Mon Dec 4 2017 01:47:55 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Dec 4 2017 01:51:02 AM

Row Count: 222

The AP Adoption History screen displays the following:

Event Name	Displays the current adoption status of each AP as either **`adopted`** or **`un-adopted`**.
AP MAC Address	Displays the hardware-encoded MAC *(Media Access Control)* address of each AP the controller or service platform has attempted to adopt.
Reason	If in case of failure to adopt, the reason for failure is displayed in this column.
Event Time	Displays *day*, *date* and *time* for each AP adoption attempt made by the controller or service platform.

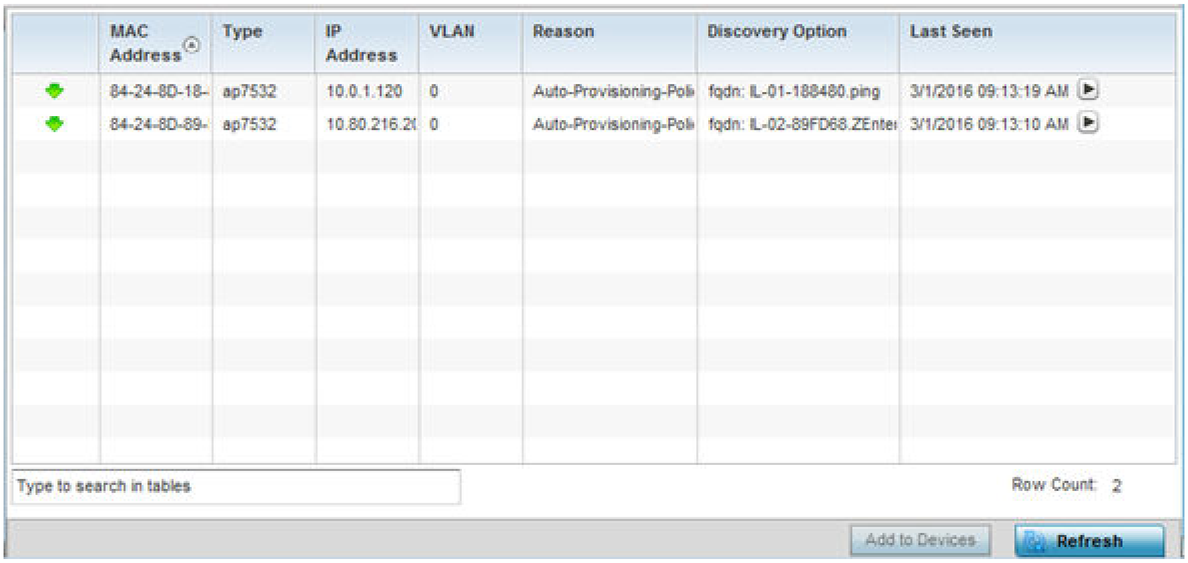
6 Click **Refresh** to update the screen's statistics counters to their latest values.

Pending Adoptions

The Pending Adoptions screen displays devices still pending (awaiting) adoption to the controller or service platform managed network. Review this data to assess whether adoption is still beneficial and to troubleshoot issues preventing adoption.

To view pending adoption AP statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller** node from the left navigation pane.
4 Expand the **Adoption** node in the left-hand side of the UI.
5 Select **Pending Adoptions**.



	MAC Address	Type	IP Address	VLAN	Reason	Discovery Option	Last Seen
	84-24-8D-18-	ap7532	10.0.1.120	0	Auto-Provisioning-Poli	fqdn: IL-01-188480.ping	3/1/2016 09:13:19 AM
	84-24-8D-89-	ap7532	10.80.216.2(	0	Auto-Provisioning-Poli	fqdn: IL-02-89FD68.ZEnte	3/1/2016 09:13:10 AM

Row Count: 2

The Pending Adoptions screen provides the following information:

MAC Address	Displays the MAC address of the device pending adoption.
Type	Displays the AP model type. The supported AP models are: 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.
IP Address	Displays the current IP Address of the device pending adoption.
VLAN	Displays the current VLAN number of the device pending adoption.
Reason	Displays the status code as to why the device is still 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 device from amongst those displayed and select **Add to Devices** to validate the adoption of the selected device and begin the process of connecting the device to the controller or service platform managed network.

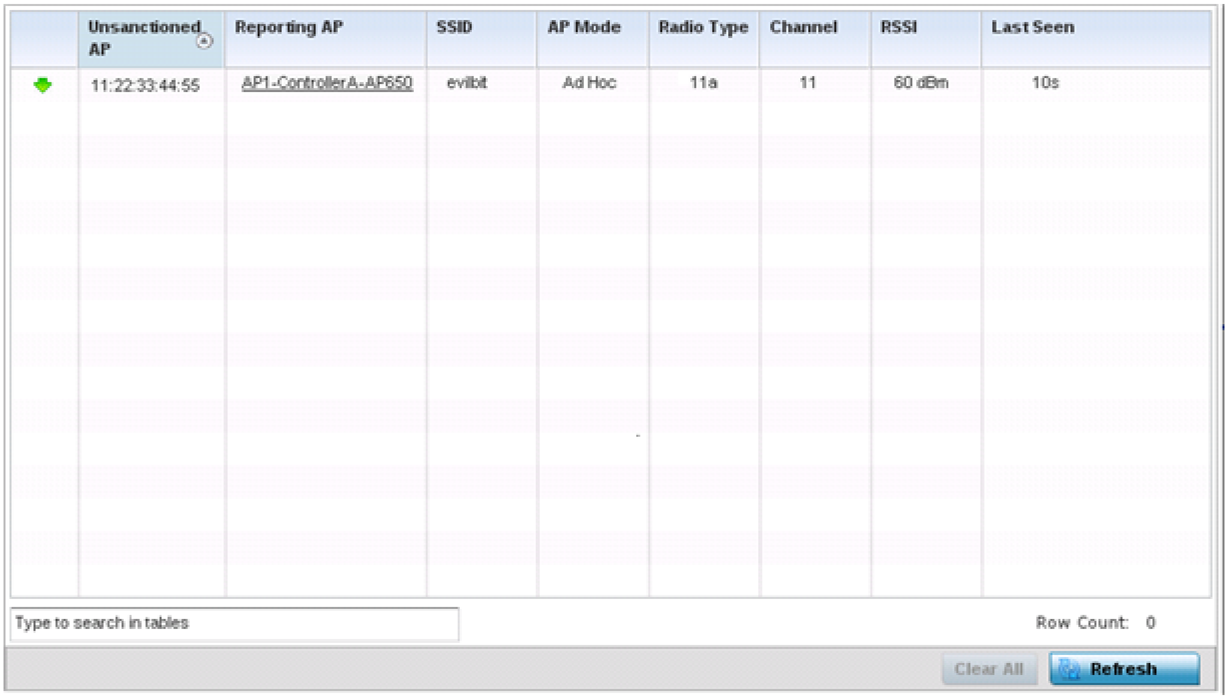
6 Select **Refresh** to update the statistics counters to their latest values.

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 AP hacking into the network.

To view the controller or service platform AP detection statistics:

1 Select the Statistics menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a Wireless Controller.
4 Select AP Detection from the left-hand side of the UI.



	Unsanctioned AP	Reporting AP	SSID	AP Mode	Radio Type	Channel	RSSI	Last Seen
↓	11:22:33:44:55	AP1-ControllerA-AP650	evilbit	Ad Hoc	11a	11	60 dBm	10s

The AP Detection screen displays the following:

Unsanctioned AP	Displays the MAC address of unsanctioned APs detected within the controller or service platform radio coverage area. Unsanctioned APs are detected APs without deployment approval (sanction).
Reporting AP	Lists the AP whose radio detected the unsanctioned AP. The AP displays as a link that you can select to view configuration and network address information in greater detail.

SSID	Displays the SSID of each unsanctioned AP.
AP Mode	Displays the operating mode of the unsanctioned device.
Radio Type	Displays the unsanctioned AP's radio type. The radio can be `802.11b`, `802.11bg`, `802.1bgn`, `802.11a` or `802.11an`.
Channel	Displays the channel where the unsanctioned AP was detected.
RSSI	Lists the RSSI *(Received Signal Strength Indicator)* for each listed AP.
Last Seen	Displays when the unsanctioned AP was last seen (observed within the network) by the detecting AP.

5 Click **Clear All** to clear all the screen's statistic counters and begin detecting new access points.
6 Click **Refresh** to update the statistics counters to their latest values.

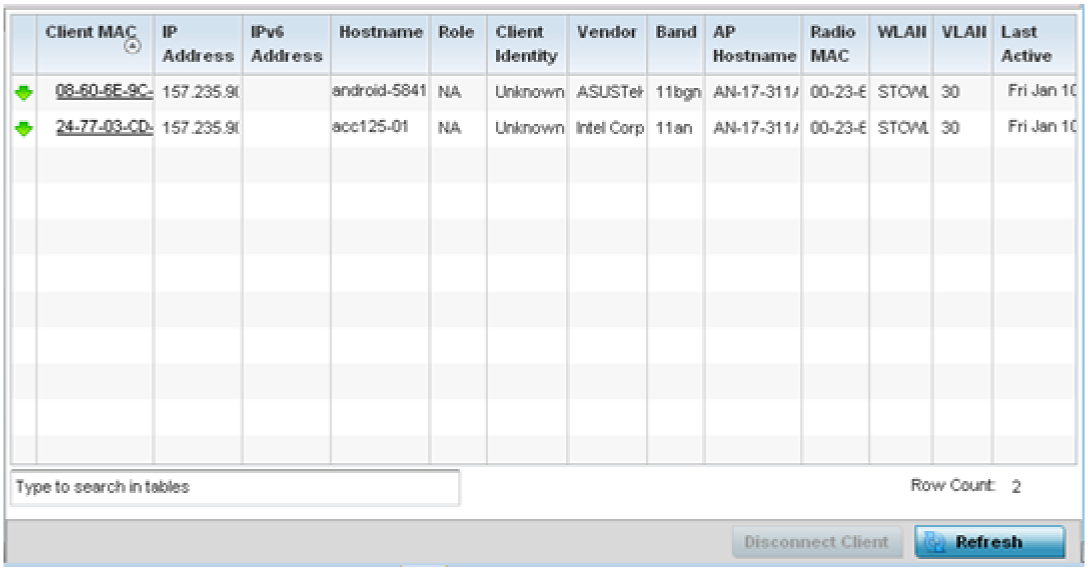
Guest User - Clients

The Guest User screen displays read-only device information for guest clients associated with the selected controller or service platform. Use this information to assess if configuration changes are required to improve performance.

To view a controller or service platform's connected guest user client 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). The System node expands to display the RF Domains created within the managed network.
3. Expand the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Select **Guest User** from the left-hand side of the UI.

   The **Statistics** → **Controller** → **Guest User** screen displays.



Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
08-60-6E-9C-	157.235.9		android-5841	NA	Unknown	ASUSTe	11bgn	AN-17-311	00-23-	STCW	30	Fri Jan 1
24-77-03-CD-	157.235.9		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311	00-23-	STCW	30	Fri Jan 1

The Guest User screen displays the following:

Client MAC	Displays the hard coded MAC address assigned to the guest client at the factory and can not be modified. The address displays as a link that you can select to view configuration and network address information in greater detail.
IP Address	Displays the unique IP address of the guest 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 IP *(Internet Protocol)* 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 guest clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail.
Role	Lists the guest client's defined role within the controller or service platform managed network.
Client Identity	Displays the Client Identity for this device. Client Identity is a set of unique fingerprints used to identify a class of devices. This information is then used to configure the permissions and access rules for the class of devices in the network.
Vendor	Displays the name of the manufacturer of the device.
Band	Displays the **2.4** or **5** GHz radio band on which the listed guest client operates.
AP Hostname	Displays the administrator assigned hostname of the access point to which this guest client is associated.
Radio MAC	Displays the MAC address of the radio which the guest client is connected
WLAN	Displays the name of the WLAN the guest client is currently assigned for its AP interoperation. Use this information to determine if the client/WLAN placement best suits the intended operation and the client's coverage area.
VLAN	Displays the VLAN ID the guest client's connected AP has defined as a virtual interface.
Last Active	Displays the time when this guest client was last seen (or detected) by a device within the controller or service platform managed network.

6. Click **Disconnect Client** to terminate this guest client's connection to its controller or service platform connected access point radio.
7. Click **Refresh** to update the statistics counters to their latest values.

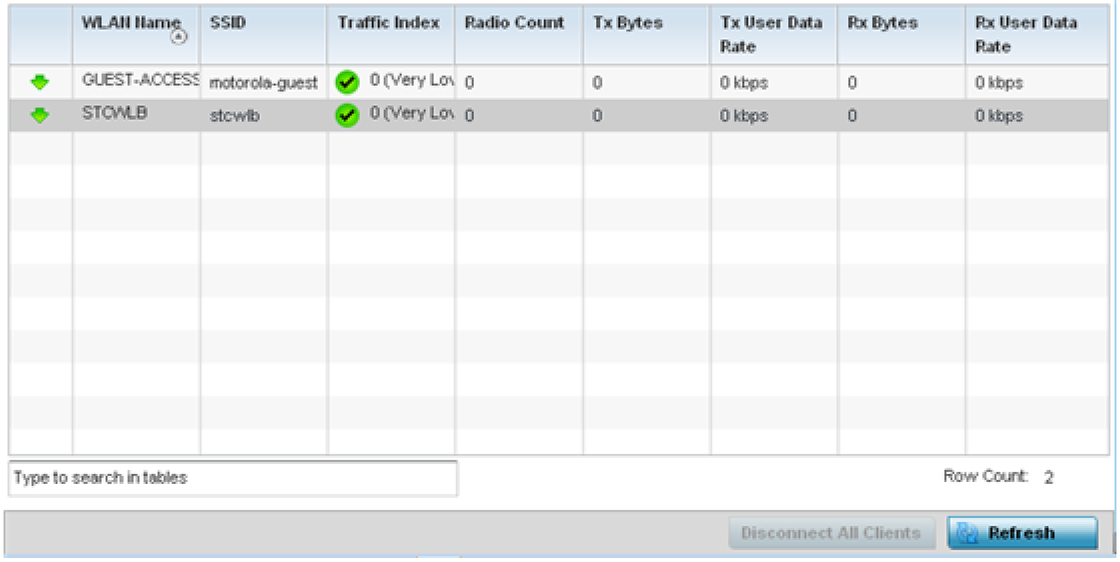
Wireless LANs

The Wireless LANs screen displays performance statistics for each WLAN managed by the controller or service platform. Use this information to assess if configuration changes are required to improve connected AP and client performance.

To view the wireless LAN statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select the **Wireless Controller** node from the left navigation pane.
4. Select **Wireless LANs** from the left-hand side of the UI.

   The **Statistics > Controller > Wireless LANs** screen displays.



	WLAN Name	SSID	Traffic Index	Radio Count	Tx Bytes	Tx User Data Rate	Rx Bytes	Rx User Data Rate
⬇	GUEST-ACCES	motorola-guest	✓ 0 (Very Lo	0	0	0 kbps	0	0 kbps
⬇	STCWLB	stcwlb	✓ 0 (Very Lo	0	0	0 kbps	0	0 kbps

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name of the WLANs the controller or service platform is currently utilizing for client connections and QoS segregation.
SSID	Displays the SSID each listed WLAN is using as an identifier on the wireless network.
Traffic Index	Displays the traffic utilization 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. Traffic indices are: • **`0 – 20`** (very low utilization) • **`20 – 40`** (low utilization) • **`40 – 60`** (moderate utilization) • **`60 and above`** (high utilization)
Radio Count	Displays the number of radios currently in use by device utilizing the listed controller or service platform managed WLAN.
Tx Bytes	Displays data transmit activity (in bytes) on each listed WLAN.
Tx User Data Rate	Displays the average user data rate for packets transmitted by controller or service platform connected devices using this WLAN.
Rx Bytes	Displays the total number of bytes received on each listed WLAN.
Rx User Data Rate	Displays the average user data rate for packets received by controller or service platform connected devices using this WLAN.

5 Click **Disconnect All Clients** to terminate the all client WLAN memberships.

6 Click **Refresh** to update the statistics counters to their latest values.

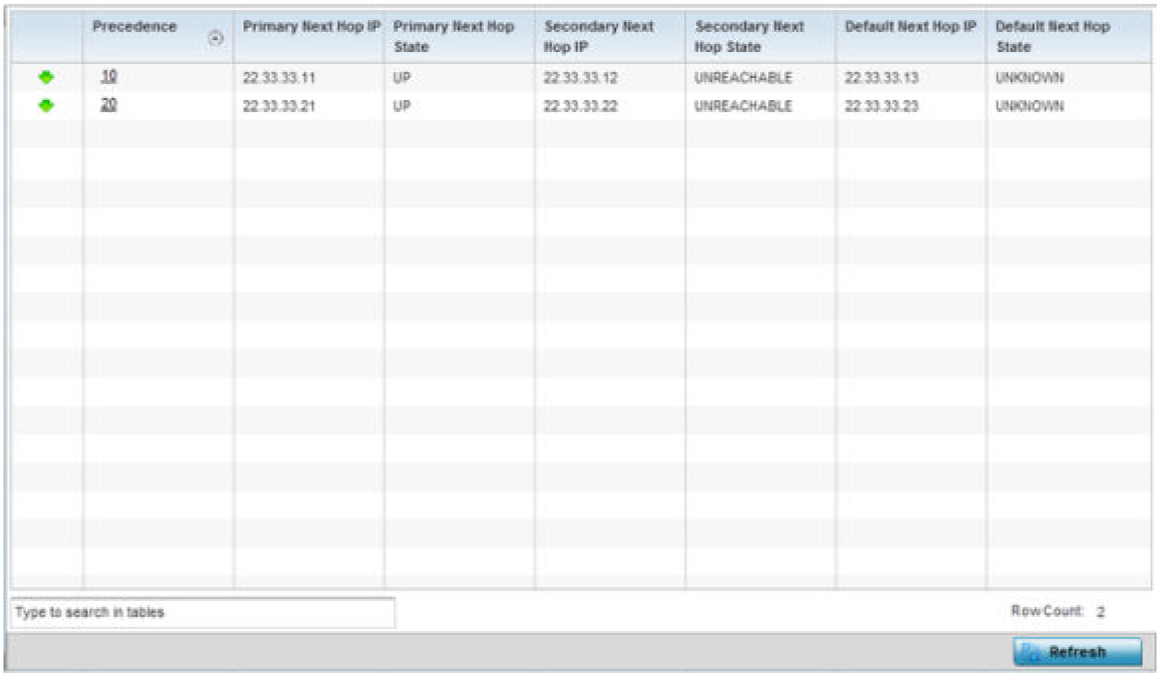
Policy Based Routing

The PBR *(Policy Based Routing)* screen displays statistics for packet path redirections. PBR can optionally mark traffic for preferential services (QoS). PBR is applied to incoming routed packets, and 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. Route-maps are configurable under a global policy called *routing-policy*, and applied to profiles and managed client devices.

To review PBR statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **Policy Based Routing** from the left-hand side of the UI.

   The **Statistics > Controller > Policy Based Routing** screen displays.



	Precedence	Primary Next Hop IP	Primary Next Hop State	Secondary Next Hop IP	Secondary Next Hop State	Default Next Hop IP	Default Next Hop State
●	10	22.33.33.11	UP	22.33.33.12	UNREACHABLE	22.33.33.13	UNKNOWN
●	20	22.33.33.21	UP	22.33.33.22	UNREACHABLE	22.33.33.23	UNKNOWN

The Policy Based Routing 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 being applied to incoming routed packets.
Secondary Next Hop IP	If the defined primary hop is unavailable, a alternative second 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 the destination, the configured default 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 Click **Refresh** to update the screen's statistics counters to their latest values.

Radios

The **Radios** statistics screens provide radio association data, including radio ID, connected APs, radio type, quality index and SNR *(Signal to Noise Ratio)*. This data is reported to the managing controller or service platform from connected AP radios and should be refreshed periodically.

For more information, see

- Radio Status on page 1083.
- Radio RF Statistics on page 1084.
- Radio Traffic Statistics on page 1085.

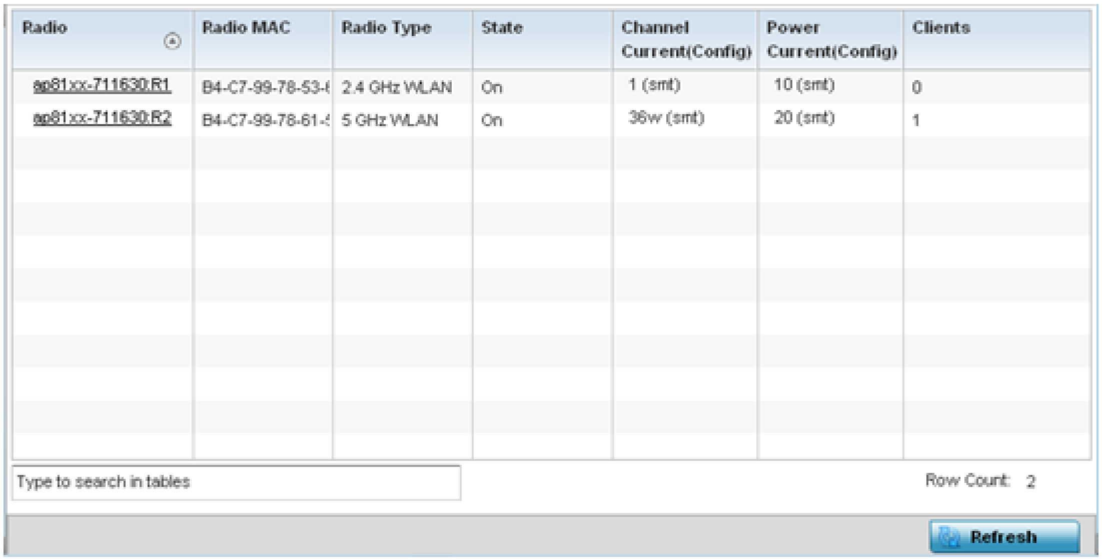
Radio Status

The radio **Status** screen provides radio association data, including radio ID, connected APs, radio type, quality index and SNR.

To view the radio status statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Expand the **Radios** node from the left-hand side of the UI.

The **Statistics > Controller > Radio > Status** screen displays by default.



Radio	Radio MAC	Radio Type	State	Channel Current(Config)	Power Current(Config)	Clients
ap81xx-711630:R1	B4-C7-99-78-53-	2.4 GHz WLAN	On	1 (smt)	10 (smt)	0
ap81xx-711630:R2	B4-C7-99-78-61-	5 GHz WLAN	On	36w (smt)	20 (smt)	1

The Radios Status screen provides the following information:

Radio	Displays the model and numerical value assigned to the radio as its unique identifier. Optionally, select the listed radio (it displays as a link) to display radio configuration information in greater detail.
Radio MAC	Displays the MAC address assigned to the radio as its unique hardware identifier.
Radio Type	Defines whether the radio is operating in the **`2.4 GHz`** or **`5 GHz`** radio band.
access point	Displays the administrator-assigned system name of each listed AP. Optionally, select the listed AP's link to view configuration information in greater detail.
AP Type	Lists the model type of the AP housing the listed radio.
State	Displays the current operational state of each radio.
Channel Current (Config)	Displays the administrator configured channel each listed radio is broadcasting on.
Power Current (Config)	Displays the administrator configured power level the radio is using for its transmissions.
Clients	Displays the number of wireless clients associated with each listed radio. This value helps assess whether the client load is optimally distributed amongst available AP radios.

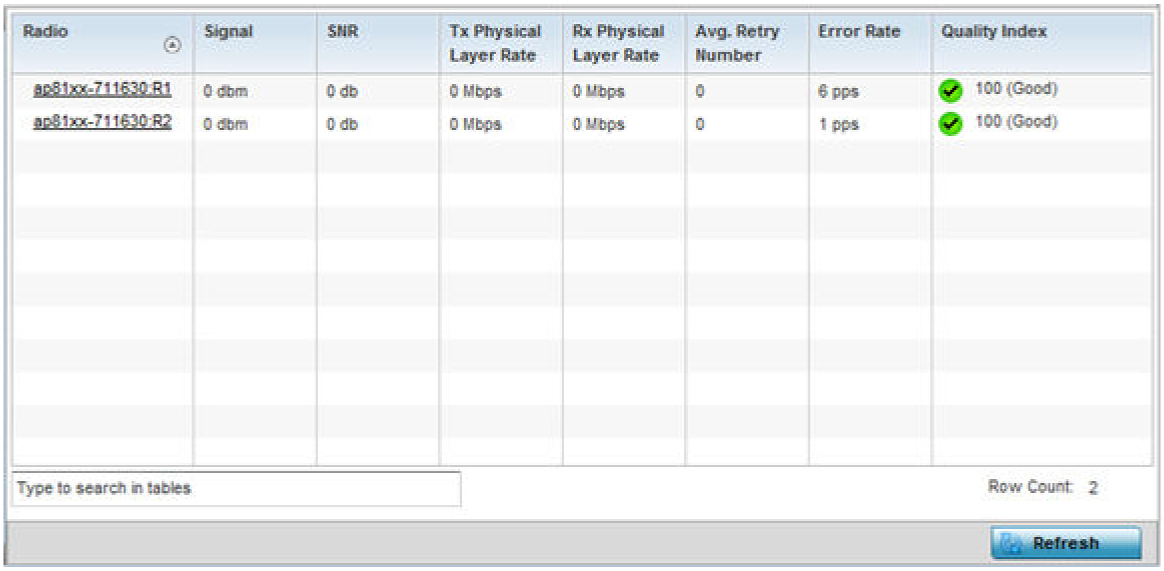
5 Click **Refresh** to update the statistics counters to their latest values.

Radio RF Statistics

To view connected radio RF statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Expand the **Radios** node from the left-hand side of the UI.
5. Select **RF Statistics**.

The **Statistics > Controller > Radios > RF Statistics** screen displays.



Radio	Signal	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Avg. Retry Number	Error Rate	Quality Index
ap81xx-711630:R1	0 dbm	0 db	0 Mbps	0 Mbps	0	6 pps	✓ 100 (Good)
ap81xx-711630:R2	0 dbm	0 db	0 Mbps	0 Mbps	0	1 pps	✓ 100 (Good)

The RF Statistics screen provides the following information:

Radio	Displays the name assigned to each listed radio. Each radio name displays as a link that can be selected to display radio information in greater detail.
Signal	Displays the power of each listed radio signals in dBm.
SNR	Displays the signal to noise ratio of each listed radio. SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A ratio higher than 1:1 indicates more signal than noise.
Tx Physical Layer Rate	Displays the data transmit rate for each managed radio's physical layer. The rate is displayed in Mbps.
Rx Physical Layer Rate	Displays the data receive rate for each managed radio's physical layer. The rate is displayed in Mbps.
Avg Retry Rate	Displays the average number of retries for each radio.
Error Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems requiring administration to improve performance.
Quality Index	Displays the client'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 rate and the error rate. RF quality index value can be interpreted as: • `0 – 20` — very poor quality • `20 – 40` — poor quality • `40 – 60` — average quality • `60 – 100` — good quality

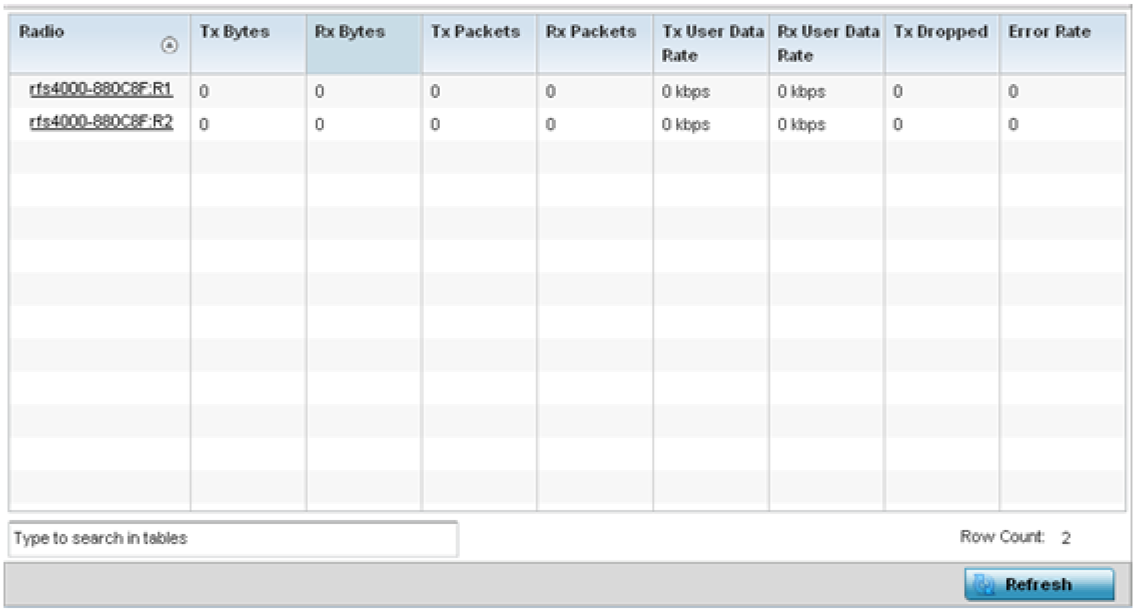
6. Click **Refresh** to update the screen's statistics counters to their latest values.

Radio Traffic Statistics

To view the radio traffic statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Expand the **Radios** node from the left-hand side of the UI.
5. Select **Traffic Statistics**.

   The **Statistics > Controller > Radios > Traffic Statistics** screen displays.



Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Error Rate
rfs4000-880C8F:R1	0	0	0	0	0 kbps	0 kbps	0	0
rfs4000-880C8F:R2	0	0	0	0	0 kbps	0 kbps	0	0

The Traffic Statistics screen provides the following information:

Radio	Displays the name assigned to each listed radio. Each radio name displays as a link that you can select to view radio configuration and network address information in greater detail.
Tx Bytes	Displays the total amount of transmitted data in bytes for each radio.
Rx Bytes	Displays the total amount of received data in bytes for each radio.
Tx Packets	Displays the total number of transmitted data in packets for each radio.
Rx Packets	Displays the total number of received data in packets for each radio.
Tx User Data Rate	Displays the average speed in kbps of data transmitted to users for each radio.
Rx User Data Rate	Displays the average speed in kbps of data received from users for each radio.
Tx Dropped	Displays the number of transmissions (packets) dropped by each listed radio. An excessive number of drops and a high error rate could be an indicator to lighten the radio’s current load.
Traffic Index	Displays the traffic utilization index of each listed radio, 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: • **`0 – 20`** (very low utilization) • **`20 – 40`** (low utilization) • **`40 – 60`** (moderate utilization) • **`60 and above`** (high utilization)

6 Click **Refresh** to update the statistics counters to their latest values.

Mesh

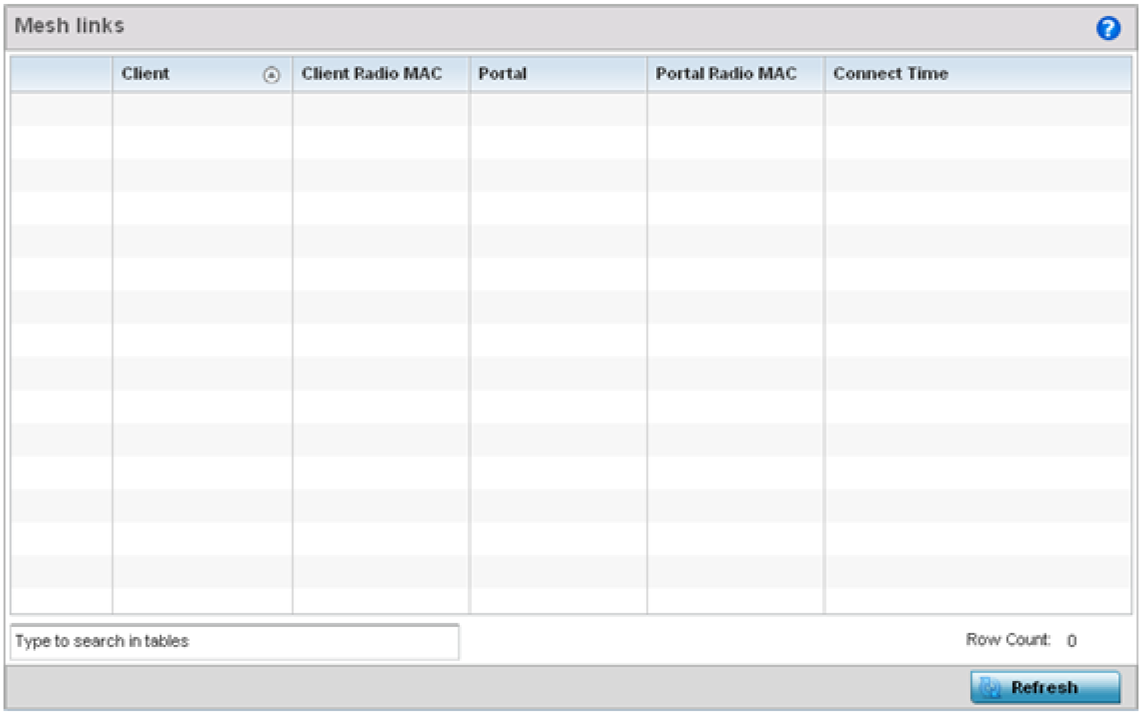
The Mesh screen provides detailed statistics on each of Mesh capable client in the selected controller or service platform radio coverage area.

A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.

To view Mesh statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **Mesh** from the left-hand side of the UI.

The **Statistics > Controller > Mesh** screen displays.



The Mesh screen displays the following:

Client	Displays the name assigned to each mesh client when added to the controller or service platform managed network.
Client Radio MAC	Displays the factory encoded Media Access Control (MAC) address of each device within the controller or service platform managed mesh network.
Portal	Mesh portals are mesh enabled devices connected to an external network that forward traffic in and out. Mesh devices 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 APs serving as mesh portals.
Connect Time	Displays the total (elapsed) connection time for each client within the controller or service platform managed mesh network.

5 Click **Refresh** to update the statistics counters to their latest value.

Interfaces

The **Interface** screen provides detailed statistics on each of the interfaces available on the selected controller or service platform. Use this screen to review the statistics for each interface. Interfaces vary amongst supported hardware model controllers and service platforms.

The Interface Statistics supports the following:

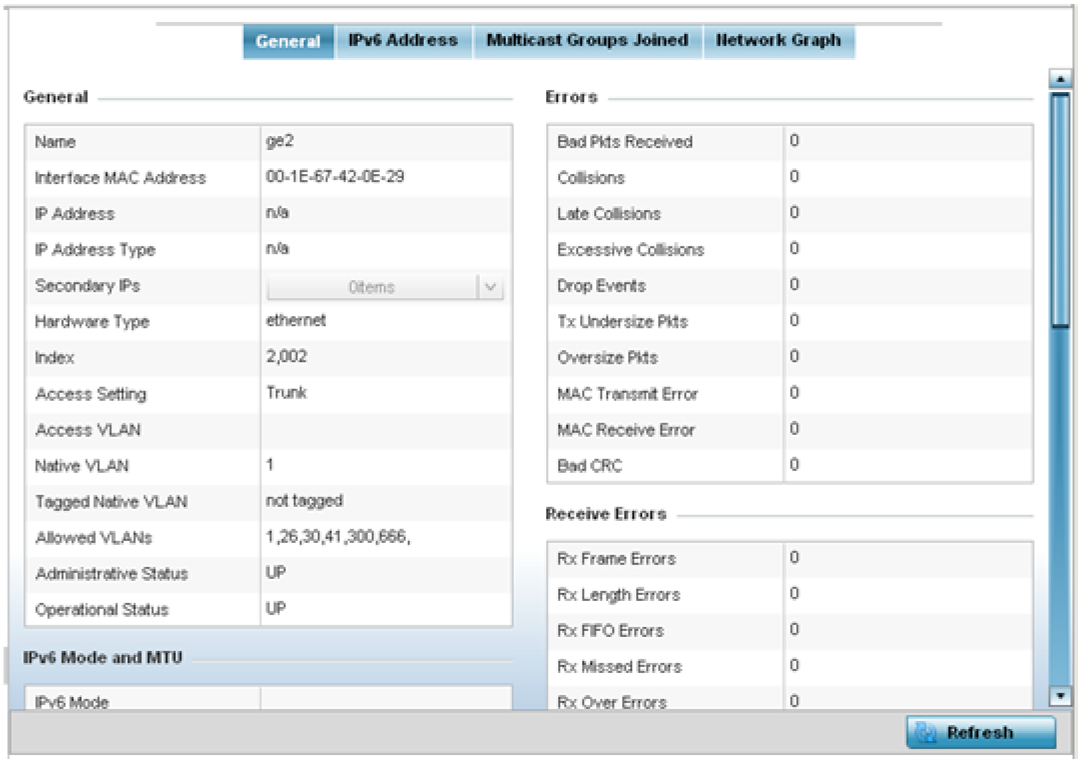
- Controller General Interface Details on page 1088
- IPv6 Address on page 1091
- Multicast Groups Joined on page 1095
- Network Graph on page 1096

Controller General Interface Details

To review general interface 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. Expand the **RF Domain** node.
4. Select a **Wireless Controller**
5. Select **Interfaces** from the left-hand side of the UI.

   The **Statistics > Controller > Interfaces > General** screen displays by default in the right-hand pane.



General

Name	ge2
Interface MAC Address	00-1E-67-42-0E-29
IP Address	n/a
IP Address Type	n/a
Secondary IPs	0items
Hardware Type	ethernet
Index	2,002
Access Setting	Trunk
Access VLAN	
Native VLAN	1
Tagged Native VLAN	not tagged
Allowed VLANs	1,26,30,41,300,666,
Administrative Status	UP
Operational Status	UP

IPv6 Mode and MTU

IPv6 Mode	

Errors

Bad Pkts Received	0
Collisions	0
Late Collisions	0
Excessive Collisions	0
Drop Events	0
Tx Undersize Pkts	0
Oversize Pkts	0
MAC Transmit Error	0
MAC Receive Error	0
Bad CRC	0

Receive Errors

Rx Frame Errors	0
Rx Length Errors	0
Rx FIFO Errors	0
Rx Missed Errors	0
Rx Over Errors	0

The **General** tab provides information on a selected controller interface such as its MAC address, type and TX/RX statistics.

Name	Displays the name of the interface ge1, up 1 etc. RFS series controllers and NX series service platforms each have a unique set of interfaces.
Interface MAC Address	Displays the MAC address of the interface.
IP Address	IP address of the interface.
IP Address Type	Displays the IP address type, either IPv4 or IPv6.
Secondary IPs	Displays a list of secondary IP resources assigned to this interface.
Hardware Type	Displays the networking technology.
Index	Displays the unique numerical identifier for the interface.
Access VLAN	Displays the tag assigned to the native VLAN.
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.
Tagged Native VLAN	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.
Access Setting	Displays the VLAN mode as either **`Access`** or **`Trunk`**.
Allowed VLANs	Displays the list of allowed virtual interface(s) on this interface.
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 information:

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 table displays the following information:

Media Type	Displays the physical connection type of the interface. Medium types include: • **`Copper`** - Used on RJ-45 Ethernet ports • **`Optical`** - Used on fibre optic gigabit Ethernet ports
Protocol	Displays the routing protocol used by the interface.
MTU	Displays the *maximum transmission unit* (MTU) 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: • **`Access`** – The Ethernet interface accepts packets only from native VLANs. • **`Trunk`** – The 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 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 table displays the following information:

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 Packets Sent	Displays the number of good packets transmitted.
Good Packets Received	Displays the number of good packets received.
Mcast Pkts Sent	Displays the number of multicast packets sent through the interface.
Mcast Pkts Received	Displays the number of multicast packets received through the interface.
Ucast Pkts Sent	Displays the number of unicast packets sent through the interface.
Ucast Pkts Received	Displays the number of unicast packets received through the 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 table displays the following information:

Bad Pkts Received	Displays the number of bad packets received through the interface.
Collisions	Displays the number of collisions over the selected interface.
Late Collisions	Displays the number of late collisions. Late collisions occur after the first 64 octets of data has been sent. Late collisions are not normal, and 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 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 failed transmits due to an internal MAC sublayer error (that’s not a late collision), due to excessive collisions or a carrier sense error.

MAC Receive Error	Displays the number of received packets that failed due to an internal MAC sublayer (that's not a late collision), an excessive number of collisions or a carrier sense error.
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.

The **Receive Errors** table displays the following information:

Rx Frame Errors	Displays the number of frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
Rx Length Errors	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was either less or over the Ethernet standard.
Rx FIFO Errors	Displays the number of *First-in First-out* (FIFO) errors received at the interface. FIFO 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 packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
Rx Missed Errors	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.
Rx Over Errors	Displays the number of overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following information:

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 bad cabling.
Tx FIFO Errors	Displays the number of FIFO errors transmitted at the interface. FIFO 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.
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) 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.

6 Click **Refresh** to update the statistics counters to their latest value.

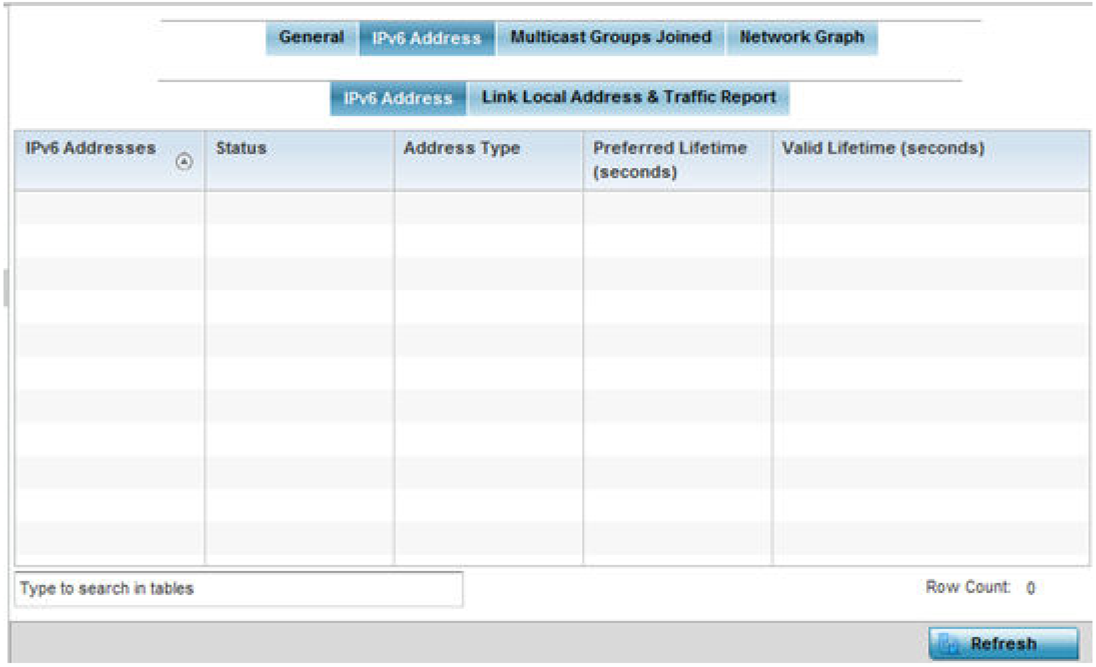
IPv6 Address

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.

To review IPv6 Address interface statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**
4. Select **Interfaces** from the left-hand side of the UI.
5. Select the **IPv6 Address** tab.

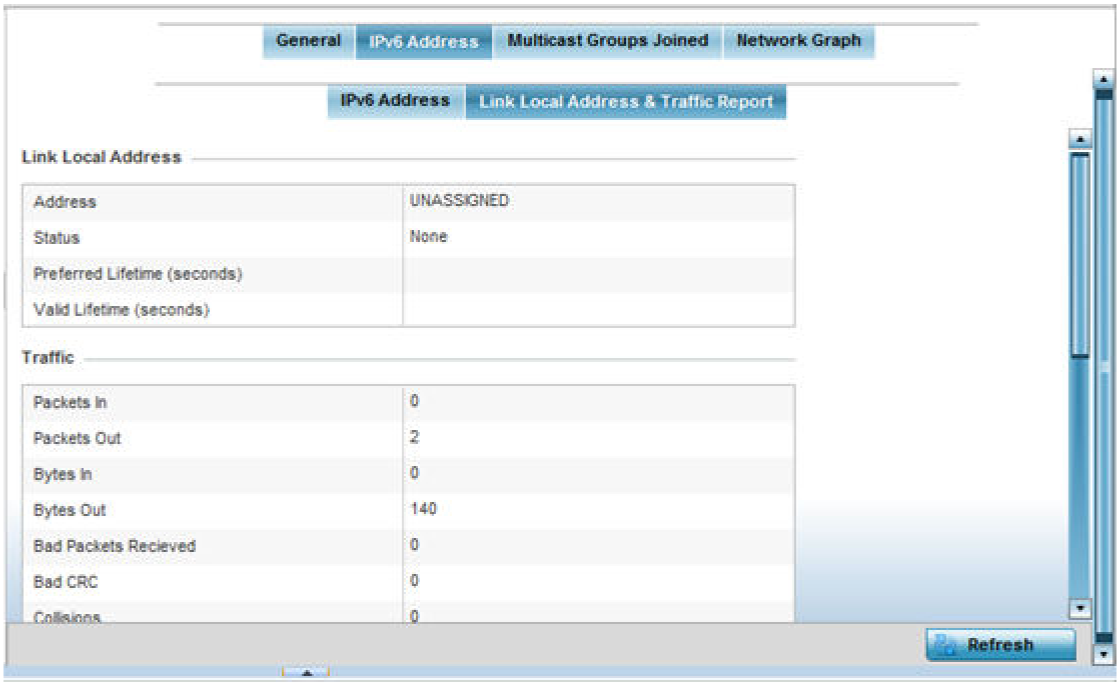
   The **Statistics > Controller > Interfaces > IPv6 Address > IPv6 Address** screen displays by default in the right-hand pane.



The IPv6 Address table displays the following sections:

IPv6 Addresses	Lists the IPv6 formatted addresses currently utilized by the controller or service platform in the selected interface.
Status	Lists the current utilization status of each IPv6 formatted address currently in use by this controller or service platform's selected interface.
Address Type	Lists whether the address is *unicast* or *multicast* in its utilization over the selected controller or service platform 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.



Link Local Address

Address	UNASSIGNED
Status	None
Preferred Lifetime (seconds)	
Valid Lifetime (seconds)	

Traffic

Packets In	0
Packets Out	2
Bytes In	0
Bytes Out	140
Bad Packets Recieved	0
Bad CRC	0
Collisions	0

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 controller or service platform interface since the screen was last refreshed.
Packets Out	Lists the number of IPv6 formatted data packets transmitted on the selected controller or service platform 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.

Multicast Groups Joined

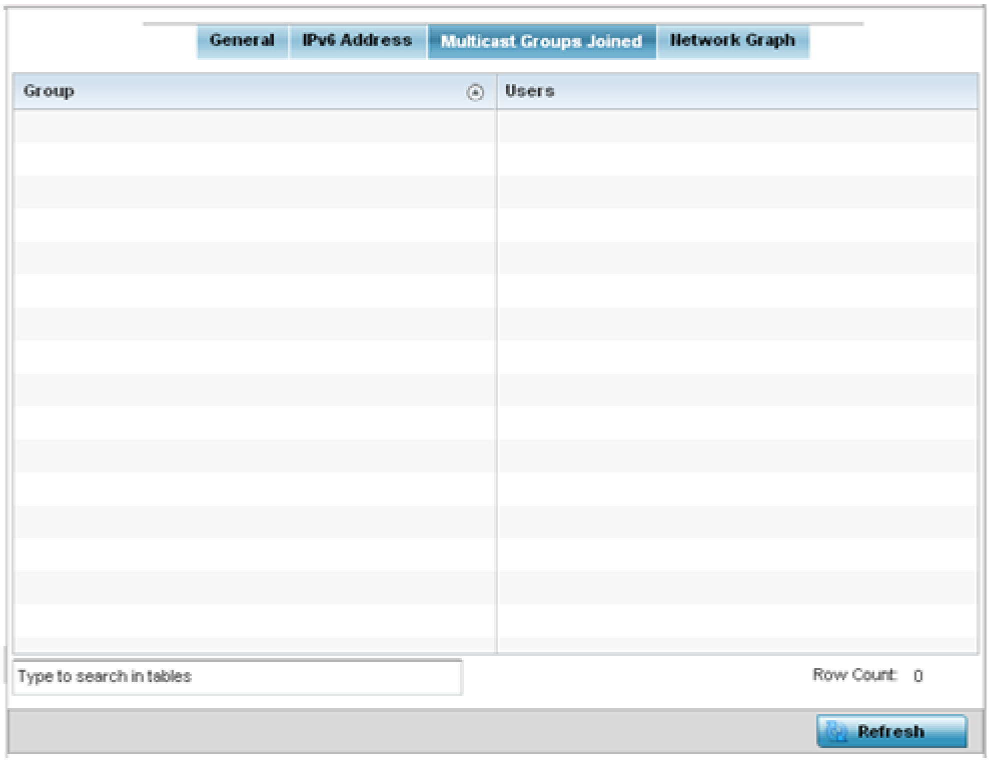
Multicast groups scale to a larger set of destinations by not requiring prior knowledge of who or how many destinations there are. Multicast devices use their infrastructure efficiently by requiring the source to send a packet only once, even if delivered to a large number of devices. Devices replicate a packet to reach multiple receivers only when necessary.

Controllers and service platforms 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 review Multicast Groups that the selected controller or service platform has joined:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **Interfaces** from the left-hand side of the UI.
5. Select the **Multicast Groups Joined** tab.

   The **Statistics > Controller > 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.

6 Periodically, click **Refresh** to update the screen's counters to their latest values.

Network Graph

The Network Graph tab displays statistics the controller or service platform 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:

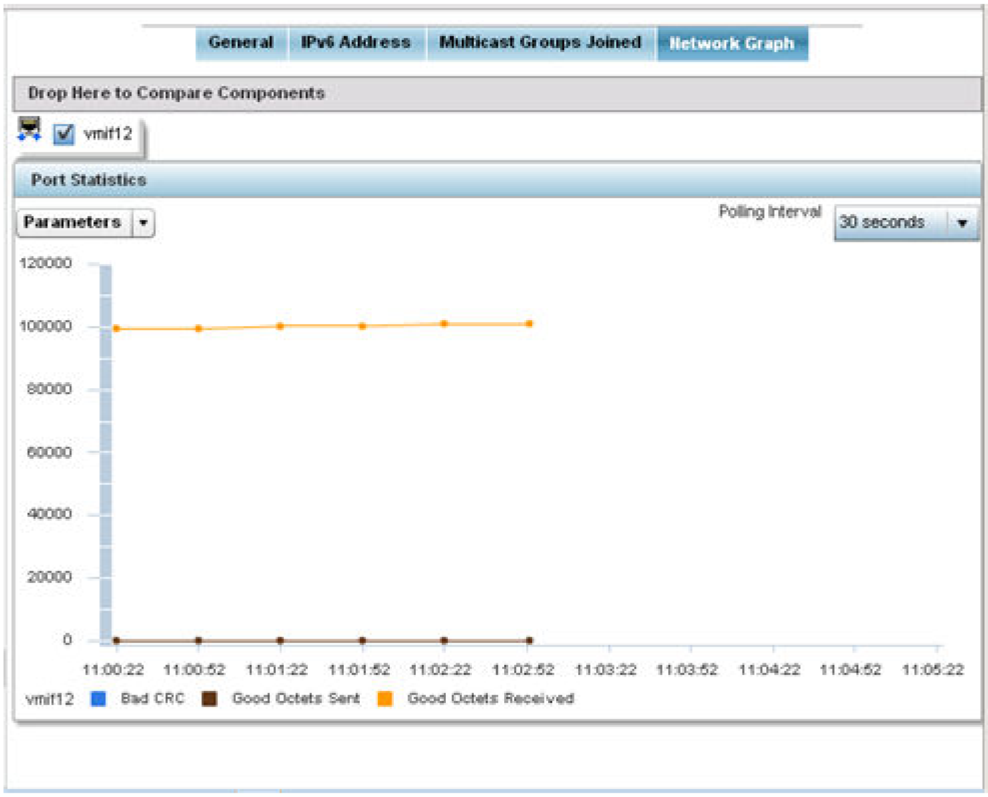
1 Select the **Statistics** menu from the Web UI.
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
3 Expand the **RF Domain** node.

4 Select a **Wireless Controller**.

5 Select **Interfaces**from the left-hand side of the UI.

6 Select the **Network Graph** tab.

The **Statistics > Controller > Interfaces > Network Graph** screen displays in the right-hand pane.



7 Use the **Parameters** drop-down menu to specify what is trended in the graph.

RAID Statistics

RAID statistics are available to assist an administrator in assessing the status of the service platform RAID array, including each physical drive. The information within the RAID statistics screen is polled by the service platform from the RAID controller hardware, then forwarded to the WiNG operating system.

RAID controller drive arrays are available within NX 7510 and NX 95XX models only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

For information on setting the service platform drive array configuration as well as the diagnostic behavior of its member drives, refer to RAID on page 970.

To view RAID statistics:

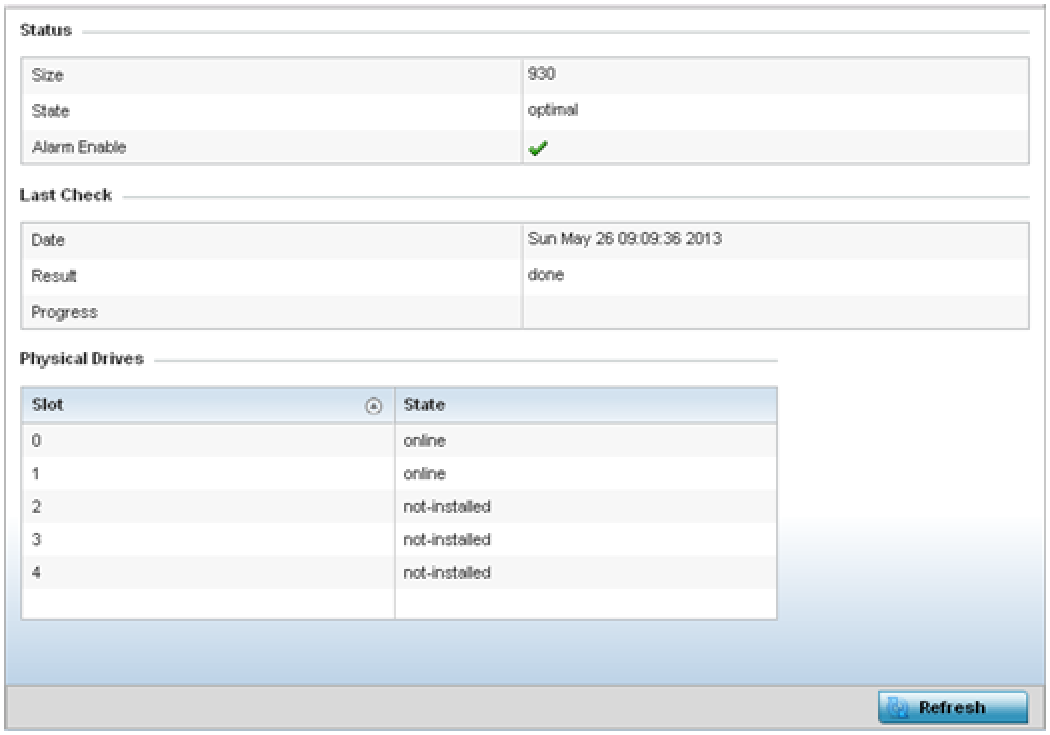
1 Select the **Statistics** menu from the Web UI.

2 Expand the **RF Domain** node.

3 Select **Wireless Controller** .

4 Select **RAID** from the left-hand side of the UI.

The **Statistics** → **Controller** → **RAID** screen displays.



Status

Size	930
State	optimal
Alarm Enable	✓

Last Check

Date	Sun May 26 09:09:36 2013
Result	done
Progress	

Physical Drives

Slot	State
0	online
1	online
2	not-installed
3	not-installed
4	not-installed

The Status field displays the following information:

Size	Lists the size of the RAID drive array. The size is the total physical memory space available on the two physical drives comprising the active RAID controller.
State	Displays whether the drive array is currently in an optimal operation state or degraded, and in need of administration to perform diagnostics and perhaps prepare a standby drive for hot spare replacement.
Alarm Enabled	Displays whether the RAID alarm has been enabled to sound the service platform's chassis alarm upon detection of a RAID controller degradation event. The RAID alarm is enabled by default.

Refer to the Last Check field to assess the time, progress and results of the RAIS array's most recent consistency check:

Date	Lists the date and time of the RAID controller's most recent consistency check on the integrity of the drive array.
Result	Displays true for a successful RAID array consistency check and false for a failed consistency check. A false indication would trigger the service platform's chassis alarm if RAID alarm is enabled.
Progress	Displays the progress of an in process consistency check in both percentage completed and minutes utilized (for example, 78%/116min).

Use the Physical Drives field to assess the RAID array's drive utilization and whether the drives are currently online:

Slot	Lists RAID array's drive slot utilization. Since there is only one RAID array controller reporting status to the service platform, its important to know if other drive slots house hot spare drives available as additional resources should one of the dedicated drives fail.
State	Displays whether a physical slot within the RAID array has a drive installed, and whether the drive is currently online.

5 Select **Refresh** at any time to update either the screen's statistic counters to their latest value.

Power Status

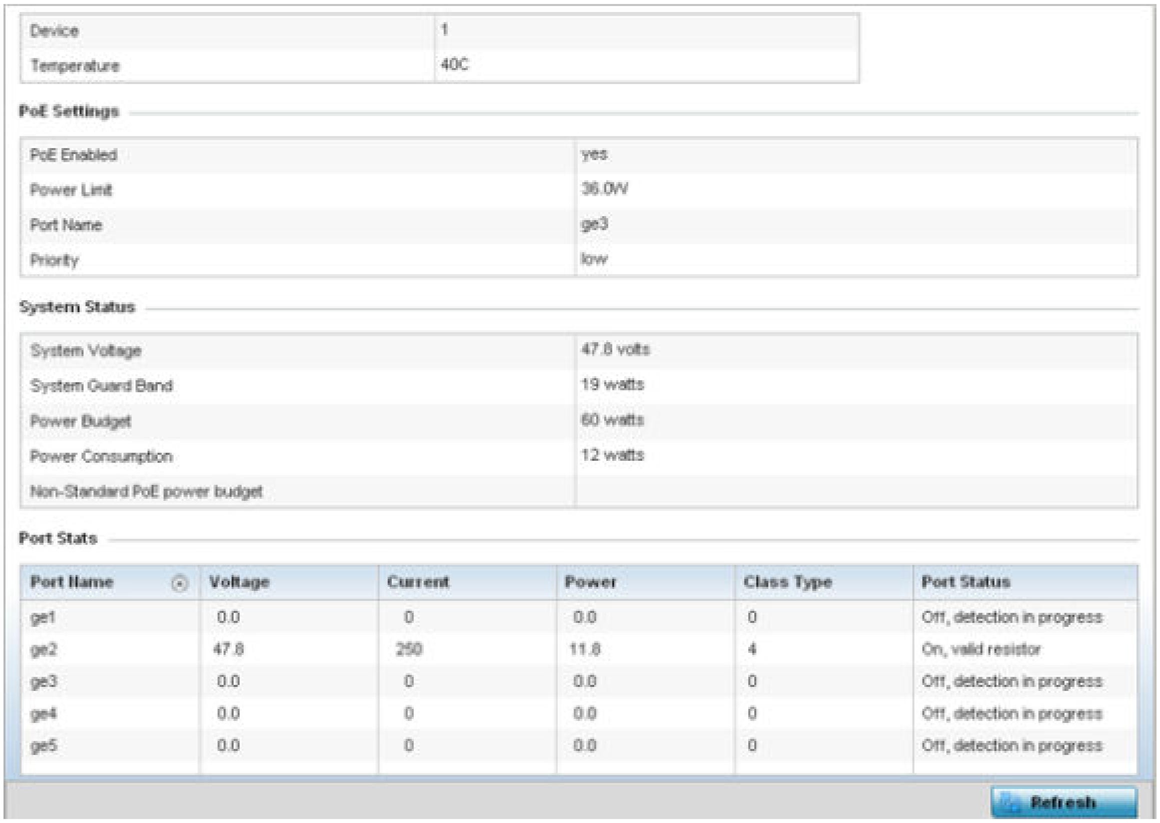
Periodically review the controller or service platform power status to assess the power budget and PoE capability (if supported).

PoE is supported on WiNG model wireless controller. PoE allows users to monitor port power consumption and configure power usage limits and priorities for each GE port.

To view power status statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **Power Status** from the left-hand side of the UI.

The **Statistics** → **Controller** → **Power Status** screen displays.



Device	1
Temperature	40C

PoE Settings

PoE Enabled	yes
Power Limit	36.0W
Port Name	ge3
Priority	low

System Status

System Voltage	47.8 volts
System Guard Band	19 watts
Power Budget	60 watts
Power Consumption	12 watts
Non-Standard PoE power budget	

Port Stats

Port Name	Voltage	Current	Power	Class Type	Port Status
ge1	0.0	0	0.0	0	Off, detection in progress
ge2	47.8	250	11.8	4	On, valid resistor
ge3	0.0	0	0.0	0	Off, detection in progress
ge4	0.0	0	0.0	0	Off, detection in progress
ge5	0.0	0	0.0	0	Off, detection in progress

This screen provides the following information for supported controllers:

Device	Displays the administrator assigned device name for the listed controller or service platform.
Temperature	Displays the internal system temperature for the controller or service platform.
PoE Enabled	Displays whether or not PoE *(Power over Ethernet)* is enabled for the controller. 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. PoE is supported on RFS 4000 model controllers.
Power Limit	Displays the total watts available for Power over Ethernet support. The value should be between 0 - 40 watts.
Port Name	Displays the GE port name on the controller.
Priority	Displays the power priority for the listed port as either **`Critical`**, **`High`** or **`Low.`** This is the priority assigned to this port versus the power requirements of the other ports.
System Voltage	Displays the total current system voltage.
System Guard Band	Displays the amount of voltage allocated to a System Guard Band. A System Guard Band is an amount of voltage allocated to prevent power loss or cycling on connected PoE devices when the power draw goes above the PoE Power Budget.
Power Budget	Displays the total amount of voltage allocated for use in Power over Ethernet.
Power Consumption	Displays the current amount of power being consumed by PoE devices managed by the controller or service platform.
Non-Standard PoE power budget	Displays the amount of voltage allocated to non 802.3af or 802.3at PoE devices.
Port Name	Displays the GE port name for each PoE capable port.
Voltage	Displays the voltage in use by each PoE capable port.
Current	Displays the amount of current in milliwatts being used by each PoE capable port.
Power	Displays whether or not each PoE capable port is providing power for potential requesting devices.
Class Type	Displays the PoE class type including 802.3af, 802.3at and non-standard PoE types.
Port Status	Displays the status of each PoE capable port on the controller. It will display either **`Enabled`** or **`Disabled`**.

5 Select **Refresh** to update the statistics counters to their latest value.

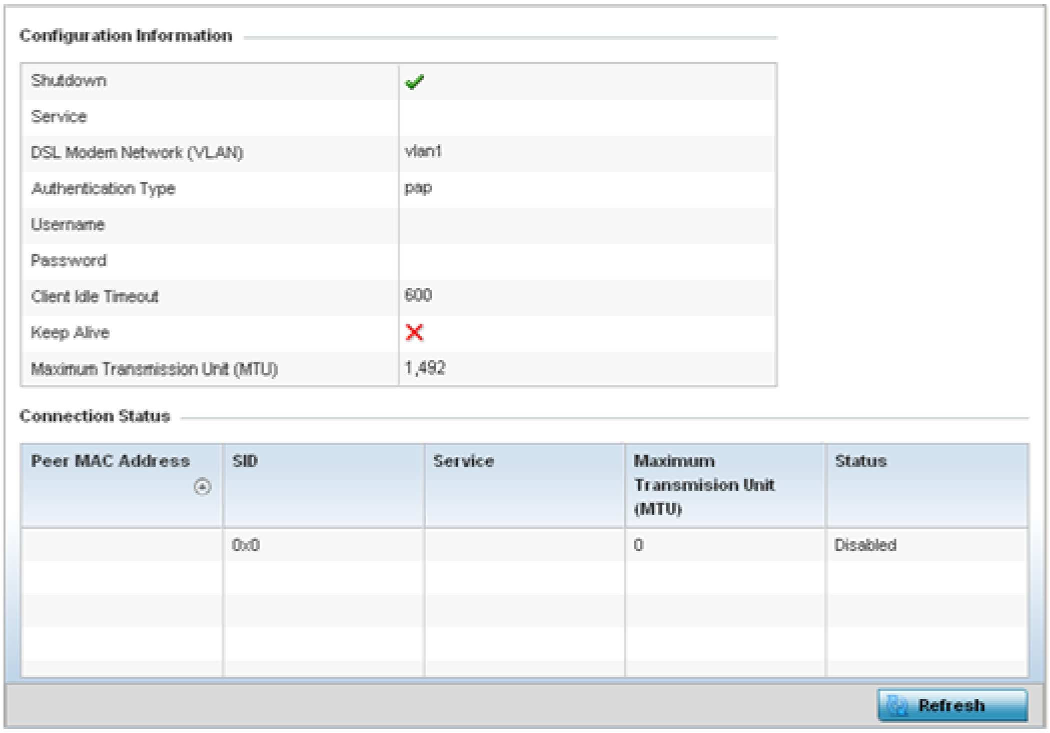
PPPoE

The PPPoE statistics screen displays stats derived from access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables point-to-points connection to an ISP over existing Ethernet interface.

Power over Ethernet is supported on RFS 4000 model controllers. When enabled, the controller supports 802.3af PoE on each of its ge ports.

To review a selected controller or service platform's PPPoE statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a Wireless Controller.
4 Select PPPoE from the left-hand side of the UI.



Configuration Information

Shutdown	✓
Service	
DSL Modem Network (VLAN)	vlan1
Authentication Type	pap
Username	
Password	
Client Idle Timeout	600
Keep Alive	✗
Maximum Transmission Unit (MTU)	1,492

Connection Status

Peer MAC Address	SID	Service	Maximum Transmision Unit (MTU)	Status
	0x0		0	Disabled

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. A green checkmark defines the connection as enabled. A red X defines the connection as shutdown.
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. 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 controller or service platform uses the listed timeout so it does not sit idle waiting for input from a PPPoE client and the server that may never come.

Keep Alive	If a keep alive is utilized (enabled displays a green checkmark, disabled a red X) the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
Maximum Transmission Unit (MTU)	Displays 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.

5 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 Wired WAN were to fail

6 Select **Refresh** to update the screen's statistics counters to their latest values.

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:

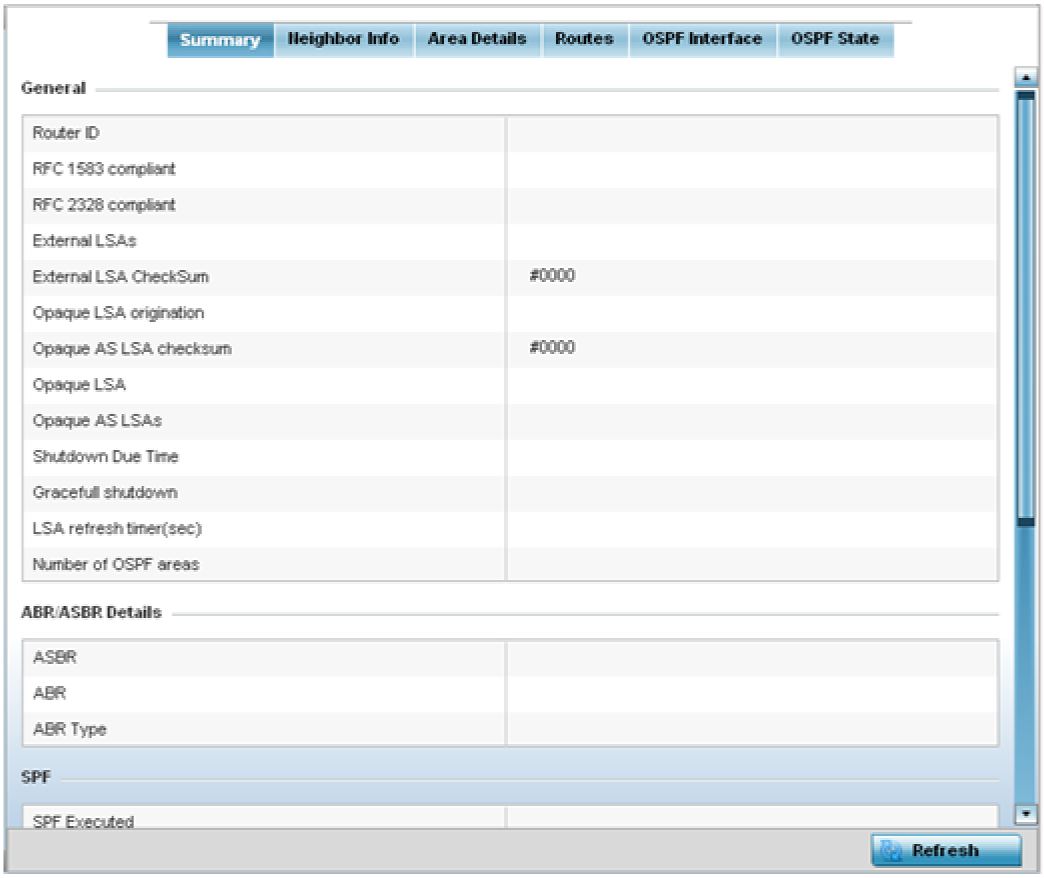
- OSPF Summary on page 1102
- OSPF Neighbors on page 1104
- OSPF Area Details on page 1105
- AP OSPF Route Statistics on page 1257
- OSPF Interface on page 1110
- OSPF State on page 1111

OSPF Summary

To view OSPF summary statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.

The **Statistics > Controller > OSPF > Summary** screen displays by default.



General

Router ID	
RFC 1583 compliant	
RFC 2328 compliant	
External LSAs	
External LSA CheckSum	#0000
Opaque LSA origination	
Opaque AS LSA checksum	#0000
Opaque LSA	
Opaque AS LSAs	
Shutdown Due Time	
Gracefull shutdown	
LSA refresh timer(sec)	
Number of OSPF areas	

ABR/ASBR Details

ASBR	
ABR	
ABR Type	

SPF

SPF Executed	

This screen describes the following data 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.

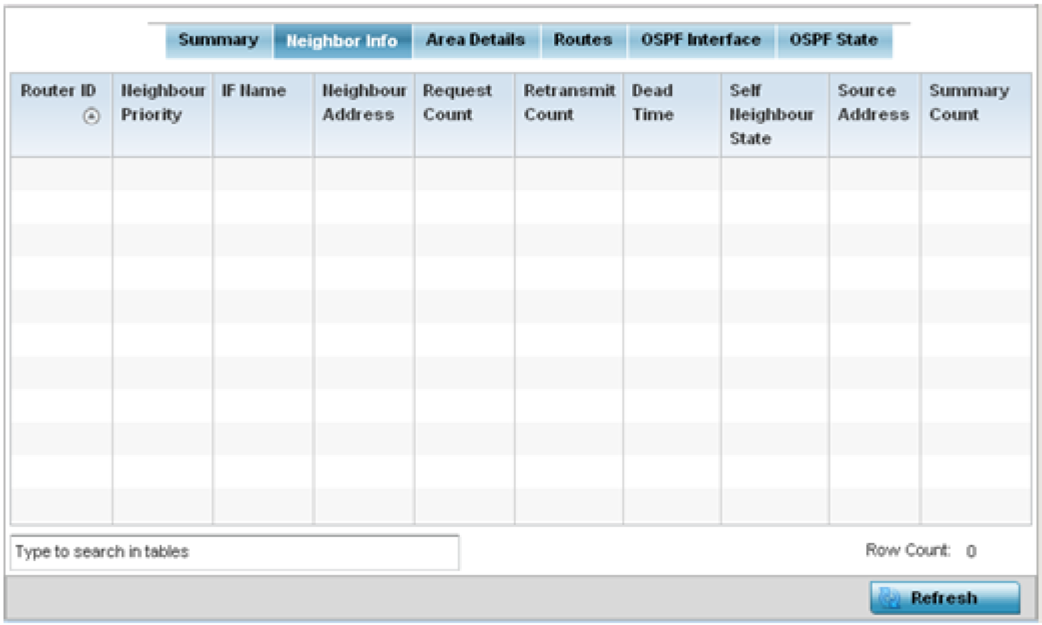
OSPF Neighbors

OSPF establishes neighbor relationships to exchange routing updates with other routers. A controller or service platform 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 **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.
5 Select the Neighbor Info tab.

The **Statistics > Controller > OSPF > Neighbor Info** screen displays.



Router ID	Neighbour Priority	IF Name	Neighbour Address	Request Count	Retransmit Count	Dead Time	Self Neighbour State	Source Address	Summary Count

The screen provides the following information:

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.

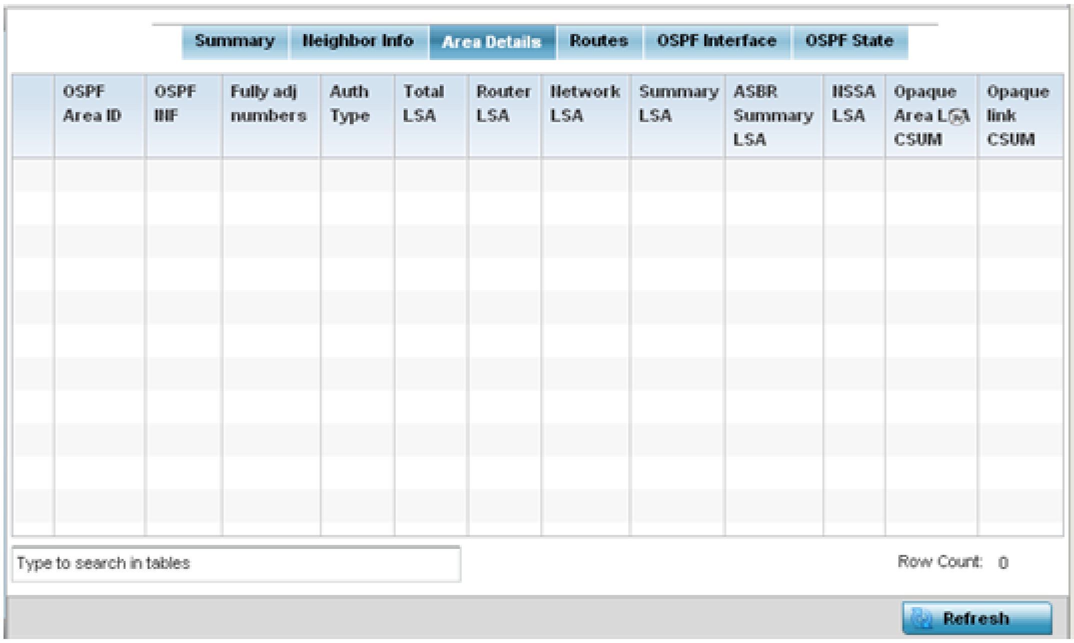
OSPF Area Details

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 a 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 *(Link State Advertisements)* 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 **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **OSPF** from the left-hand side of the UI.
5. Select the **Area Details** tab.

   The **Statistics > Controller > OSPF > Area Details** screen displays.



This screen provides the following information:

OSPF Area ID	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router.
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 Link State Advertisements of all entities using the dynamic route (in any direction) in the listed area ID.
Router LSA	Lists the Link State Advertisements 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 *Not-so-stubby-area* (NSSA) 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. 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.
Opaque link CSUM	Displays the Type-10 opaque link checksum with the complete contents of the LSA.

6 Select **Refresh** to update the statistics counters to their latest values.

Controller OSPF Route Statistics

Refer to the Routes tab to assess the status of OSPF

- Border Routes on page 1107.
- AP OSPF External Routes on page 1258.
- AP OSPF Network Routes on page 1259.
- AP OSPF Router Routes on page 1260.

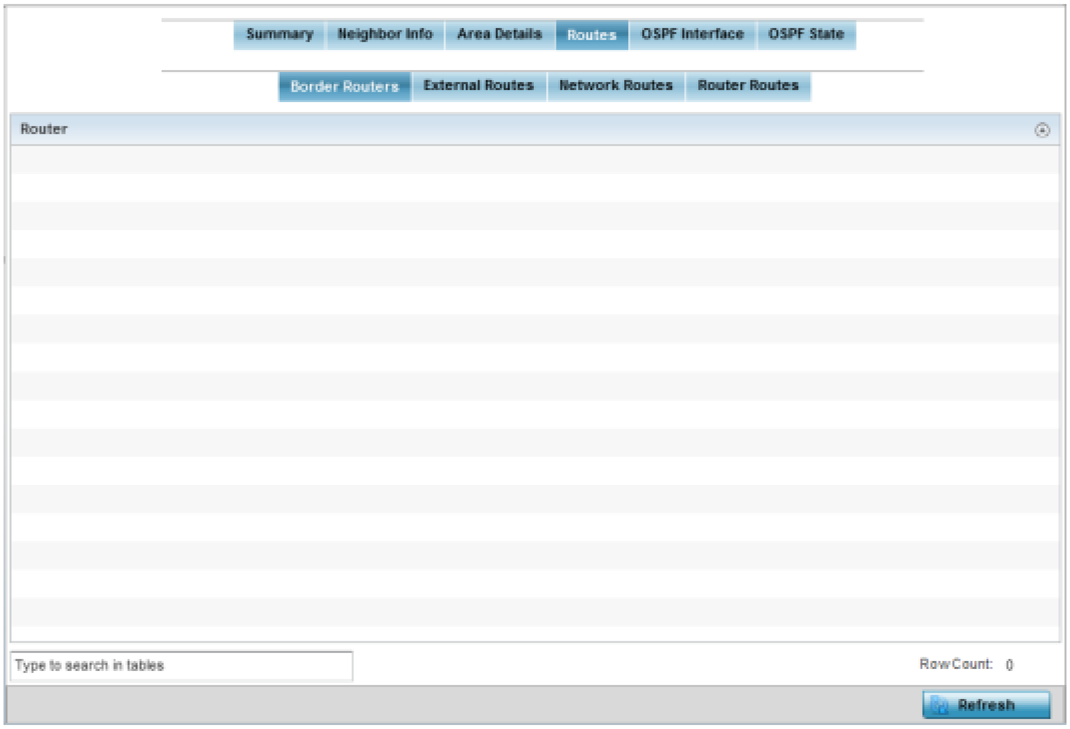
.

Border Routes

To view OSPF border route statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.
5 Select the **Routes** tab.

The **Statistics > Controller > OSPF > Routes > Border Routers** screen displays by default.



An ABR 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 routes 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.

External Routes

To view OSPF external route statistics:

1 Select the Statistics menu from the Web UI.

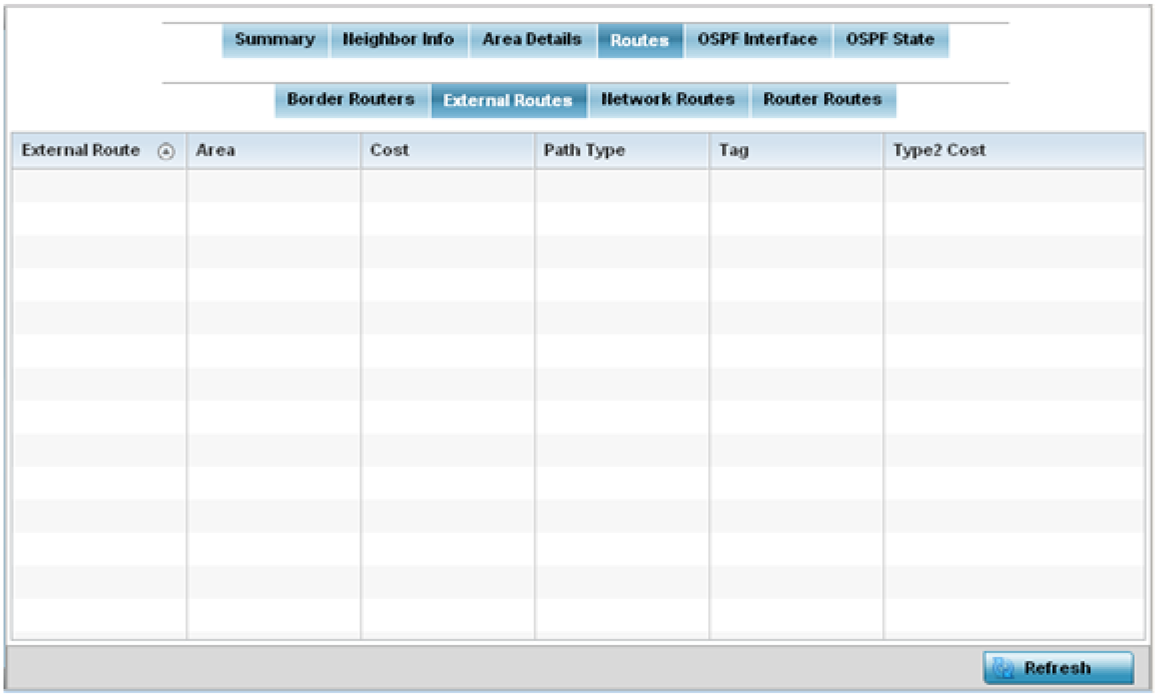
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller** or **service platform**, and select one of its connected **access points**. The selected device's statistics menu displays in the right-hand side of the screen, with the Health tab selected by default.

4 Expand the **OSPF** from the left-hand side of the UI.

5 Select the **Routes > External Routes** tab.

The **Statistics > Controller > OSPF > Routes > External Routes** screen displays.



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.

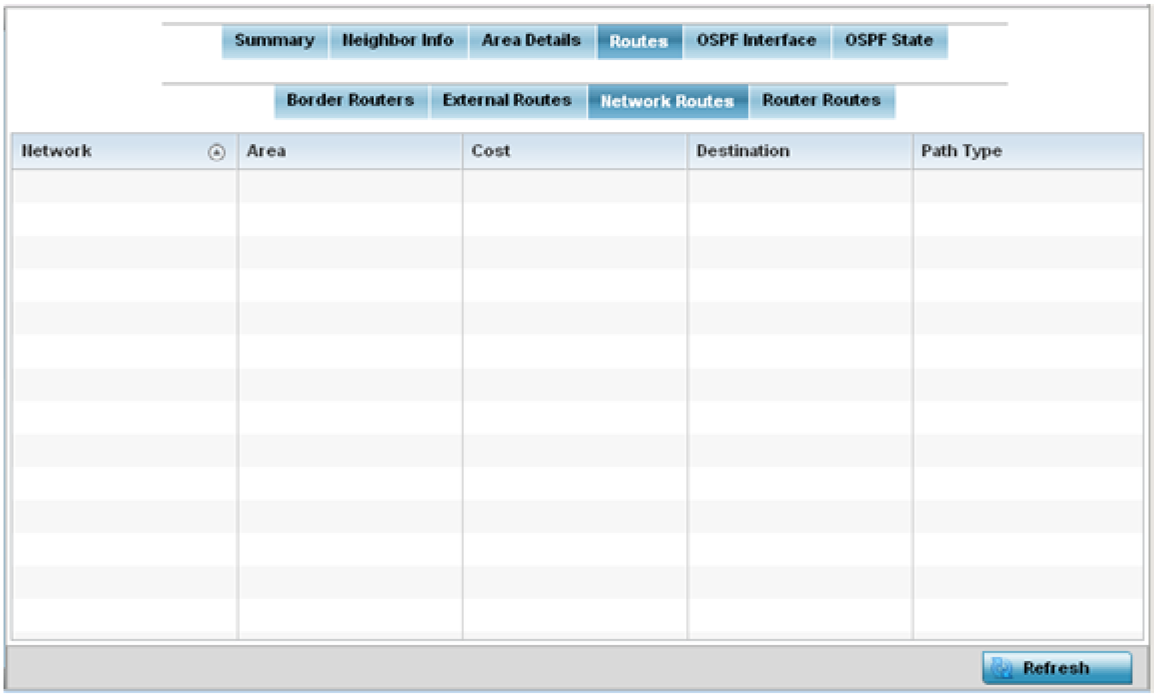
6 Select **Refresh** to update the statistics counters to their latest values.

Network Routes

To view OSPF network route statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.
5 Select the **Routes > Network Routes** tab.

The **Statistics > Controller > OSPF > Routes > Network Routers** screen displays.



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*.

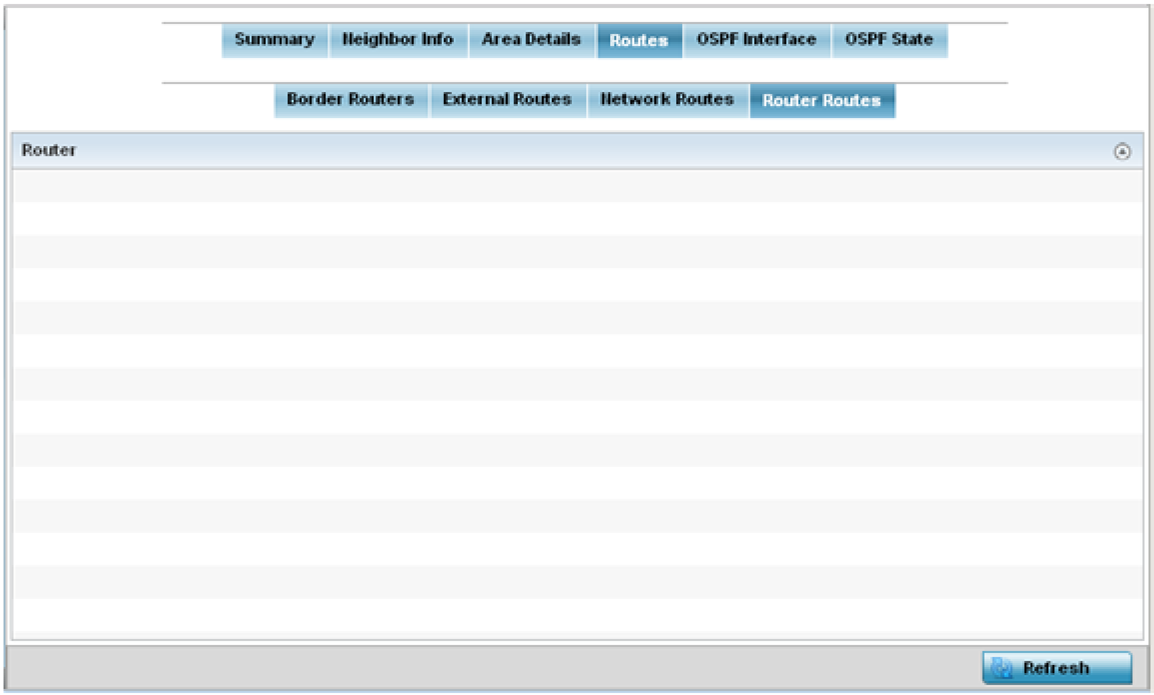
6 Select **Refresh** to update the statistics counters to their latest values.

Router Routes

To view OSPF router route statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.
5 Select the **Router Routes > Router Routes**tab.

The **Statistics > Controller > OSPF > Routes > Router Routes** screen displays.



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.

6 Select **Refresh** to update the statistics counters to their latest values.

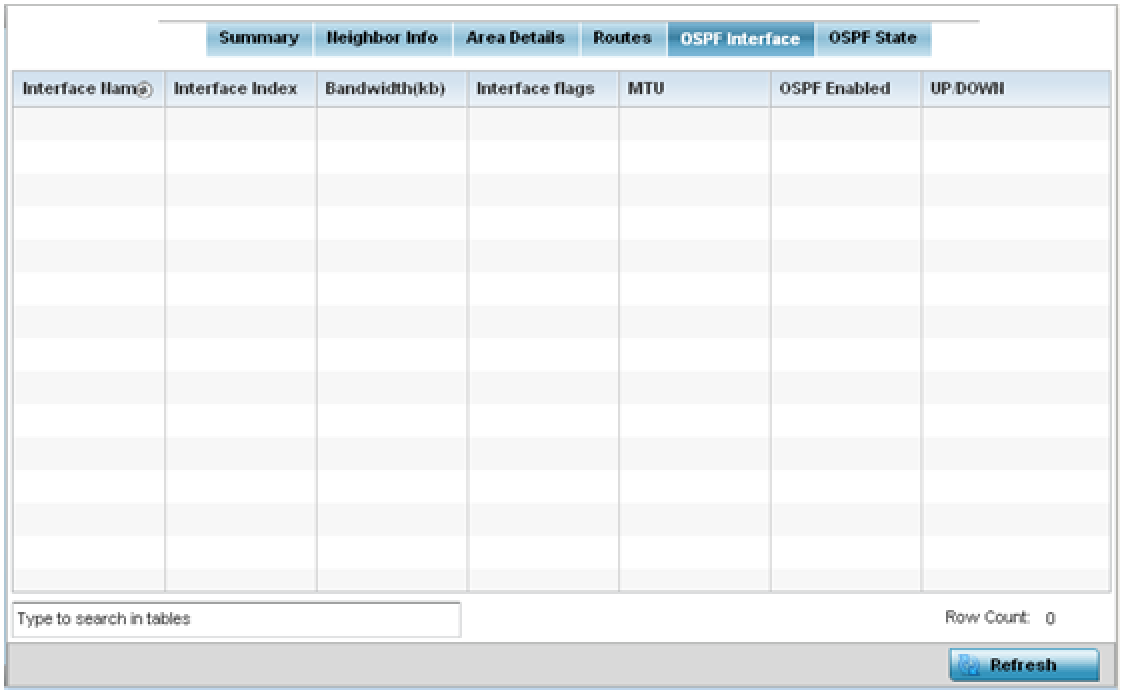
OSPF Interface

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 **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **OSPF** from the left-hand side of the UI.
5 Select the **OSPF Interface** tab.

The **Statistics > Controller > OSPF > OSPF Interface** screen displays.



This screen provides the following information:

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) from 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 *(maximum transmission unit)* 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.

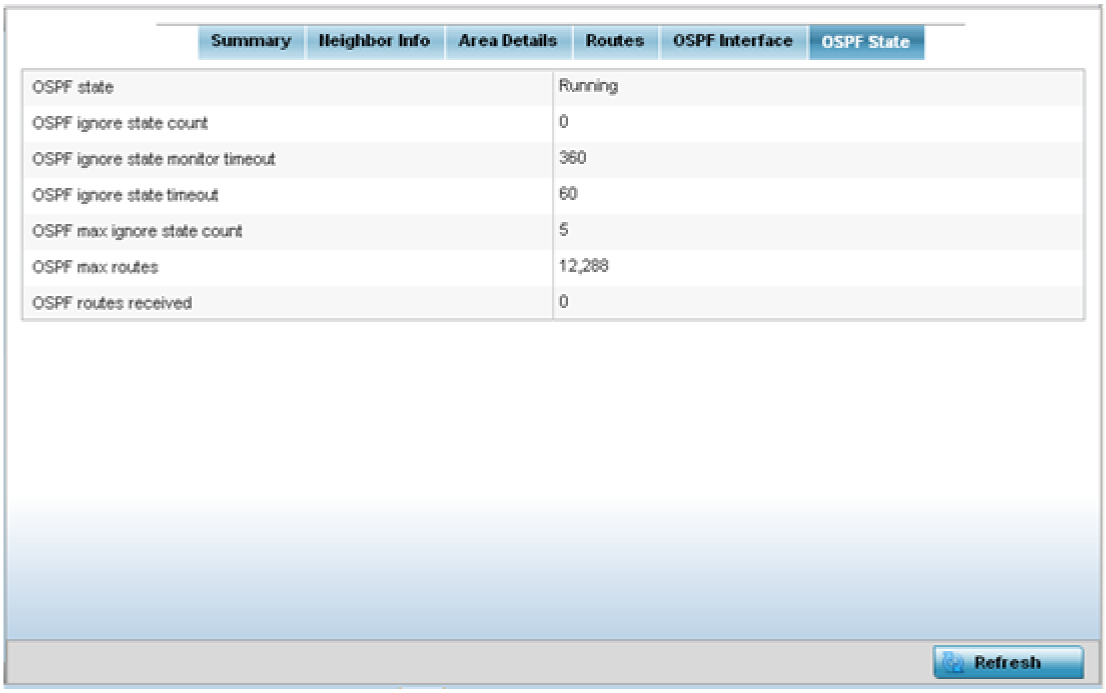
OSPF State

An OSPF enabled controller or service platform sends hello packets to discover neighbors and elect a designated router for dynamic links. The hello packet includes link *state* data periodically updated on all OSPF members. The controller tracks link state information to help assess the health of the OSPF dynamic route.

To view OSPF state statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **OSPF** from the left-hand side of the UI.
5. Select the **OSPF State** tab.

The **Statistics > Controller > OSPF > OSPF State** screen displays.



OSPF state	Running
OSPF ignore state count	0
OSPF ignore state monitor timeout	360
OSPF ignore state timeout	60
OSPF max ignore state count	5
OSPF max routes	12,288
OSPF routes received	0

This screen provides the following information:

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 controller and its peers within this OSPF supported broadcast domain.
OSPF ignore state monitor timeout	Displays the timeout that, when exceeded, prohibits the controller 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.

BGP

BGP *(Border Gateway Protocol)* is an inter-ISP routing protocol which establishes routes between ISPs. ISPs use BGP to exchange routing and reachability information between AS *(Autonomous Systems)* on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An AS is a set of routers under the same administration that use IGP *(Interior Gateway Protocol)* and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a graceful close (all outstanding data is delivered before the connection is closed).

Use BGP statistics to assess status of the controller/service platforms' BGP feature and its neighbor BGP peers. Much of the configuration information can be filtered from the Route Filters screen.

Note
BGP is only supported on NX 95XX and NX 96XX model controllers and service platforms.

The BGP statistics page displays the following information:

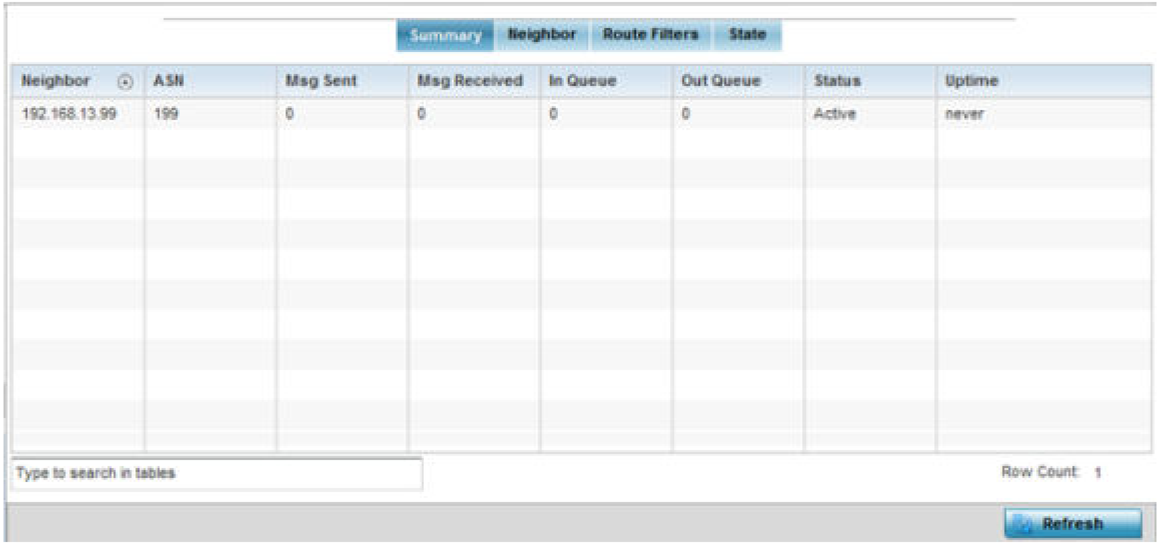
- BGP Summary on page 1113
- BGP Neighbor on page 1114
- BGP Route Filters on page 1117
- BGP State on page 1121

BGP Summary

To review BGP statistics summary:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **BGP** from the left-hand side of the UI.

   The **Statistics > Controller > BGP > Summary** screen displays by default in the right-hand pane.



Neighbor	ASN	Msg Sent	Msg Received	In Queue	Out Queue	Status	Uptime
192.168.13.99	199	0	0	0	0	Active	never

The Summary screen displays the following information:

Neighbor	Lists the IP address of neighbor BGP supported devices.
ASN	Lists the ASN *(Autonomous System Number)* assigned to each listed neighbor BGP peer. ASN is a set of routers under the same administration that use IGP *(Interior Gateway Protocol)* and common metrics to define how to route packets.
Msg Sent	Lists the number of messages sent out of this BGP peer.
Msg Received	Lists the number of messages received by this BGP peer.
In Queue	Lists the number of messages in the controller or service platform queue that have not yet been read (processed).
Out Queue	Lists the number of messages in the controller or service platform queue that have not yet been sent.
Status	Displays the status of each listed BGP neighbor as **`Active`** or **`Disabled`**.
Uptime	Displays the time duration in HH:MM:SS format since the connection to this neighbor BGP peer was established.

5 Periodically, click **Refresh** to update the screen’s counters to their latest value.

BGP Neighbor

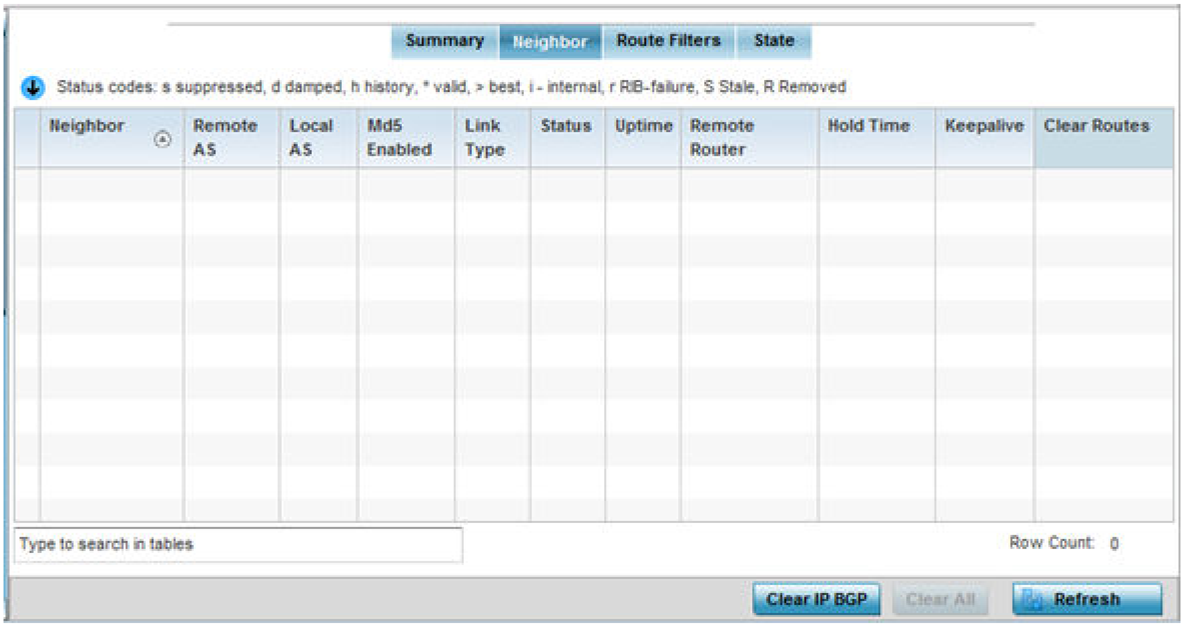
To review BGP Neighbor statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **BGP** from the left-hand side of the UI.

The BGP Summary screen is displayed by default in the right-hand pane.

5 Select the **Neighbor** tab.

The **Statistics > Controller > BGP > Neighbor** screen displays.



Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, R Removed

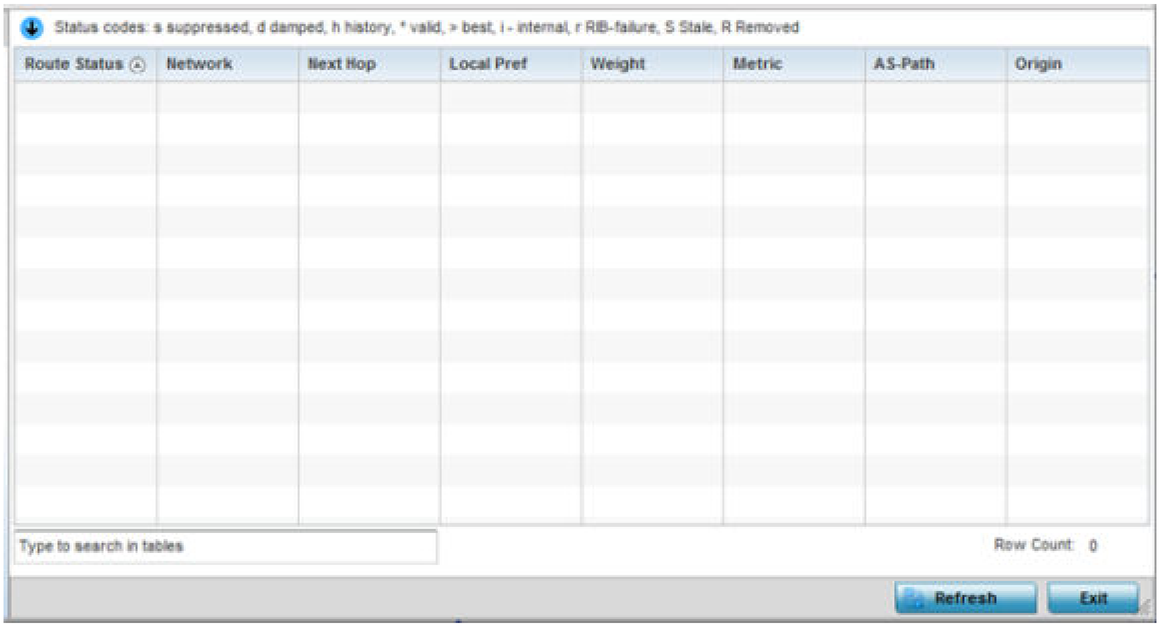
Neighbor	Remote AS	Local AS	Md5 Enabled	Link Type	Status	Uptime	Remote Router	Hold Time	Keepalive	Clear Routes

This screen displays the following information:

Neighbor	Lists the IP address of neighbor BGP supported peer controllers or service platforms. Each IP address displays as a link to display BGP supported device data in greater detail.
Remote	Lists the AS number configured on this BGP neighbor. An AS is a set of routers under the same administration that use IGP and common metrics to define how to route packets within the AS.
Local AS	Lists the AS number (1 - 4,294,967,295) configured on this BGP wireless controller or service platforms.
Md5 Enabled	A green check defines MD5 authentication enabled on the listed BGP neighbor. A red X means disabled. 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.
Link Type	Lists the type of BGP link. Displays internal if the link type is iBGP. Displays external if the link type is eBGP. iBGP exchanges routing table information between routers within an autonomous system. eBGP exchanges routing table information between hosts outside an autonomous system.
Status	Displays the current Active or Inactive state of each listed BGP neighbor device.
Uptime	Displays the uptime for each listed BGP neighbor.
Remote Router	Lists the IP address used by the BGP remote router resource as a network identifier.
Hold Time	Displays the duration, in seconds, for the hold (delay) of packet transmissions to each listed BGP neighbor device.

Keepalive	Displays the duration, in seconds, for the keep alive timer used to maintain the connection to each listed BGP neighbor device.
Clear Routes	Select this option (within the table) to reset and clear all routes received from this BGP neighbor.

6 Optionally select the IP address of a listed BGP neighbor device to launch the following screen for more granular device information for the selected peer device:



Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, R Removed

The BGP neighbor Statistics screen displays route information for the following kinds of routes:

- *Advertised* – Displays route information for routes advertised to the selected neighbor device.
- *Received* – Displays route information for routes received from the selected neighbor device.
- *Routes* – Displays the route information for routes learned from the selected neighbor device.

7 Refer to the following for details on the displayed route. The fields are common to all the screens.

Route Status	Displays the status of this route. Route statuses include: • **`Suppressed`** – This route has been suppressed. • **`Damped`** – This route has been damped due to flapping. • **`History`** - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. • **`Valid`** – This route is a valid route. • **`Best`** – This route is the best route of all the routes utilized. • **`RIB Failure`** - A route with better administrative distance is already present, a memory failure exists or the number of routes in VPN routing/forwarding (VRF) exceeds the route-limit configured under the VRF instance. • **`Removed`** – This route has been removed from the routes list and is no longer available to BGP supported neighbor devices.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop in this route.

Local Pref	Lists the IP address of this controller or service platform's preferred next hop for the route.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure (metric) of the quality of the path. A lower value indicates a better path.
AS-Path	Displays the AS Path information for this route.
Origin	Displays the IP address of the route's origin.

8 Periodically, select **Refresh** to update the screen's counters to their latest value.

BGP Route Filters

To review BGP Route statistics:

1 Select the **Statistics** menu from the Web UI.

2 Expand the **RF Domain** node.

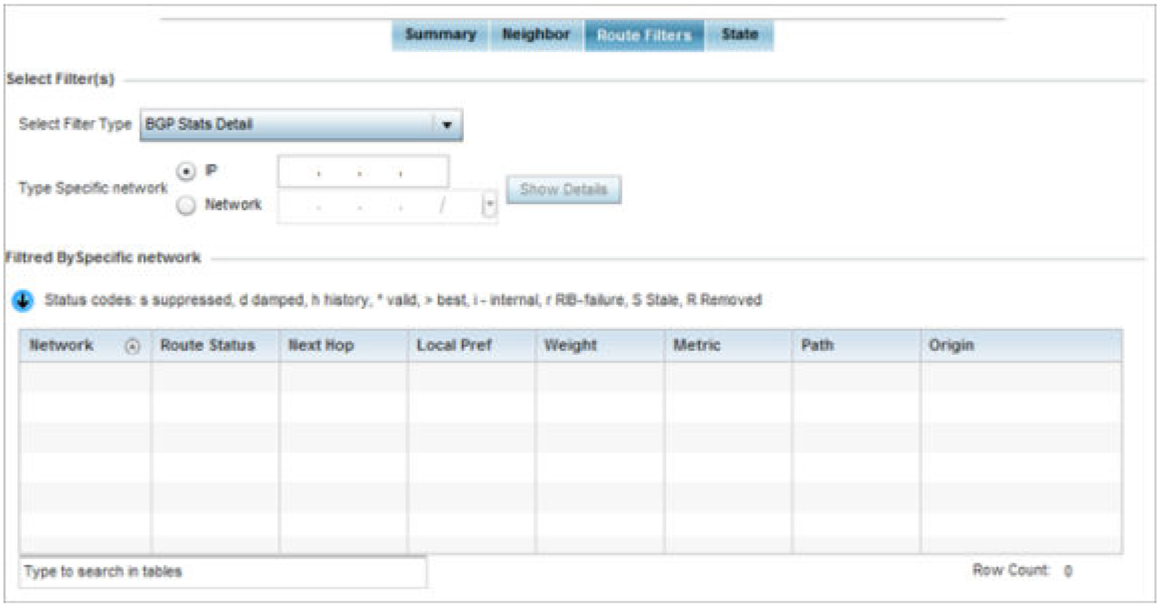
3 Select a **Wireless Controller**.

4 Select **BGP** from the left-hand side of the UI.

The BGP Summary screen displays by default in the right-hand pane.

5 Select the **Route Filters** tab.

The **Statistics > Controller > BGP > Route Filters** screen displays



Select Filter Type: BGP Stats Detail

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, R Removed

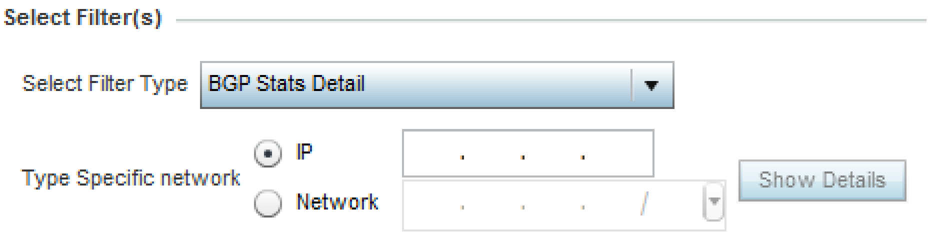
Network	Route Status	Next Hop	Local Pref	Weight	Metric	Path	Origin

6 In the Select Filter(s) area, use the **Select Filter Type** drop-down menu to specify a filter. Route statistics can be filtered on the basis of the following eight (8) different parameters:

- **`BGP Stats Details`** – Routes are filtered on BGP statistics details.
- **`Community List`** – Routes are filtered on the community lists included in each route.
- **`Community`** – Routes are filtered on the community information included in each route.

- **`Expanded Community List`** – Routes are filtered on the expanded community information included in each route.
- **`Prefix List`** – Routes are filtered on the prefix list included in each route.
- **`Filter List`** – Routes are filtered on the filter list included in each route.
- **`Regular Expression`** – Routes are filtered based on regular expressions.
- **`Route Map`** – Routes are filtered on the route map information included in each route.

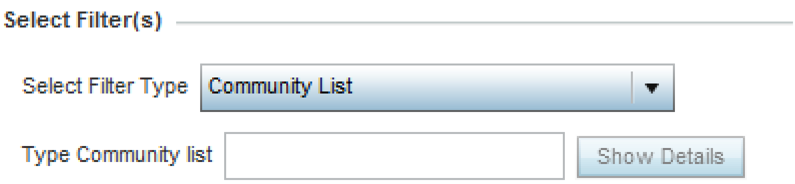
7 Select the **BGP Stats Detail** from the Select Filter Type list.



8 Use the **Type Specific Network** field to filter statistics based on the provided **IP** or **Network** information. Select **Show Details** to display the list of filtered routes.

Route Status	Displays the status of this route. Route status options include: • **`Suppressed`** – This route has been suppressed. • **`Damped`** – This route has been damped due to flapping. • **`History`** - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. • **`Valid`** – This route is a valid route. • **`Best`** – This route is the best route of all routes. • **`RIB Failure`** – A route with better administrative distance is already present, a memory failure exists or the number of routes in VRF *(VPN routing/forwarding)* exceeds the route-limit configured under the VRF instance. • **`Removed`** – This route has been removed from the routes list.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop resource utilized in this route.
Local Pref	Lists the IP address of this controller or service platform's preferred next hop for this route. The local preference indicates the preferred path when there are multiple paths to the same destination. The path having the highest preference value is preferred. The preference value is sent to all routers and access servers in the local AS.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure (metric) of the quality of the path. A lower value indicates a better path. This value is the MED *(Multi Exit Discriminator)* evaluated by BGP during the best path selection process.
Path	Displays path information for this route.
Origin	Displays the IP address of the origin for this route.

9 Select **Community List** from the Select Filter Type list.



Select Filter(s)

Select Filter Type: Community List

10 Use the **Type Community List** field to filter the statistics based on the community type of the route. Select **Show Details** to display the list of filtered routes.

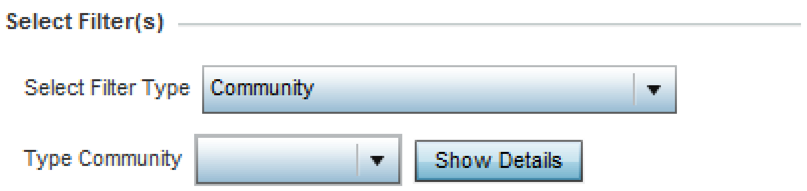
Note

The following table is common to these filter types:

- Community List
- Community
- Prefix List
- Filter List
- Regular Expression
- Route Map

Route Status	Displays the status of this route. Route status options include: • **`Suppressed`** – This route has been suppressed. • **`Damped`** – This route has been damped due to flapping. • **`History`** - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. • **`Valid`** – This route is a valid route. • **`Best`** – This route is the best route of all routes. • **`RIB Failure`** – A route with better administrative distance is already present, a memory failure exists or the number of routes in VRF exceeds the route-limit configured under the VRF instance. • **`Removed`** – This route has been removed from the routes list.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop resource utilized in this route.
Local Pref	Lists the IP address of this controller or service platform's preferred next hop for this route. The local preference indicates the preferred path when there are multiple paths to the same destination. The path having the highest preference value is preferred. The preference value is sent to all routers and access servers in the local AS.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure (metric) of the quality of the path. A lower value indicates a better path. This value is the MED evaluated by BGP during the best path selection process.
AS-Path	Displays AS path information for this route.
Origin	Displays the IP address of the origin for this route.

11 Select **Community** from the Select Filter Type list.



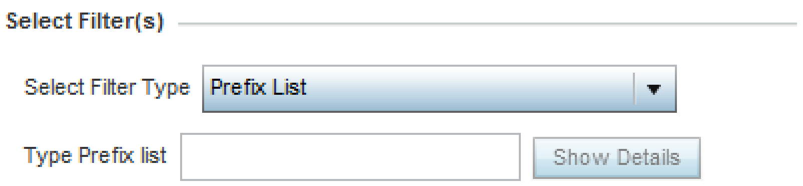
Select Filter Type Community

12 Use the **Type Community** drop-down menu to filter the statistics based on the community of the route. Routes can be filtered on:

- `local-AS` - Displays routes that prevent the transmission of packets outside the local AS.
- `no-advertise` - Displays routes not advertised to any peer, either internal or external.
- `no-export` - Displays routes not advertised to BGP peers, keeping this route within an AS.
- `aa:nn` - Filters routes based on the AS Number specified. The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number. Routes matching this number are filtered.

13 Select **Show Details** to display the list of filtered routes.

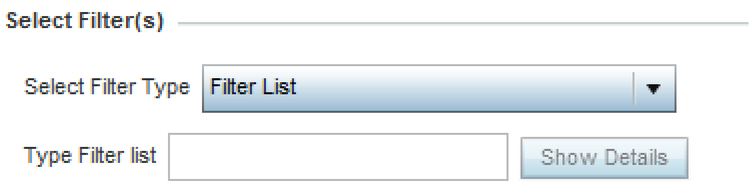
14 Select **Prefix List** from the Select Filter Type list.



Select Filter Type Prefix List

15 Use the **Type Prefix list field** to filter the statistics based on the prefix of the route. Select Show Details to display the list of filtered routes.

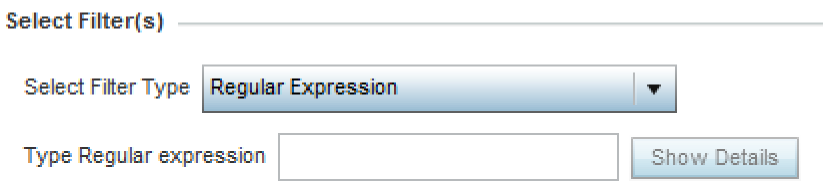
16 Select **Filter List** from the Select Filter Type list.



Select Filter Type Filter List

17 Use the **Type Filter List field** to filter the statistics based on the filter list of the route. Select Show Details to display the list of filtered routes.

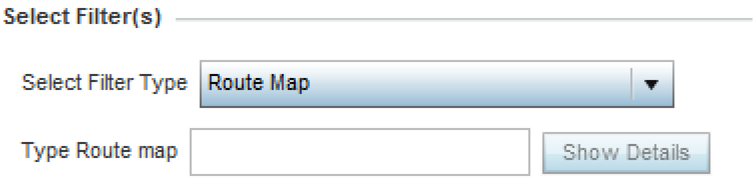
18 Select **Regular Expression** from the Select Filter Type list.



Select Filter Type Regular Expression

19 Use the **Type Regular Expression** field to filter the routes based on regular expressions. Select Show Details to display the list of filtered routes.

20 Select **Route Map** from the **Select Filter Type** list.



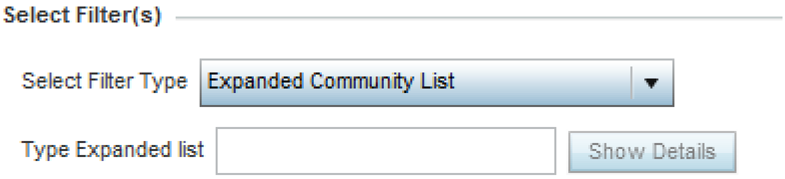
Select Filter(s)

Select Filter Type: Route Map

Type Route map

21 Use the **Type Route Map** field to filter the routes based on route maps (enhanced packet filters). Select Show Details to display the list of filtered routes.

22 Select **Expanded Community List** from the Select Filter Type list.



Select Filter(s)

Select Filter Type: Expanded Community List

Type Expanded list

23 Use the **Type Expanded list** to filter routes based on route-maps. Select Show Details to display a list of filtered routes.

24 Periodically, select **Refresh** to update the screen's counters to their latest value.

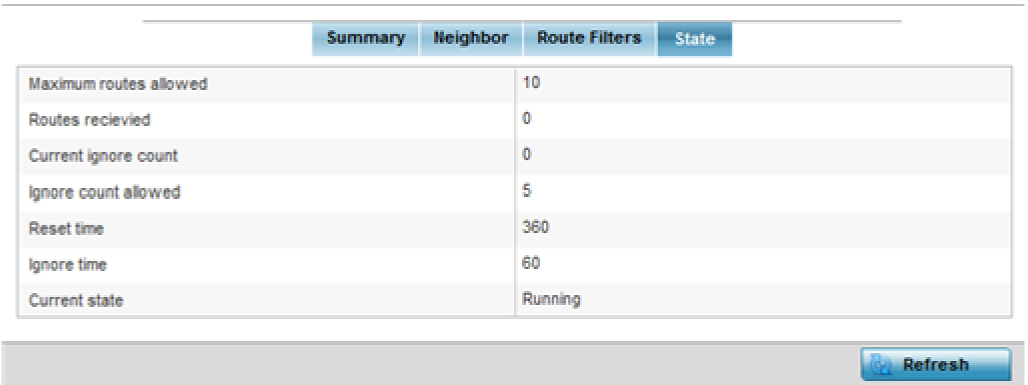
BGP State

To view BGP State statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **BGP** from the left-hand side of the UI.

   The BGP Summary screen displays by default in the right-hand pane.
5. Select the **State** tab.

   The **Statistics > Controller > BGP > State** screen displays.



Maximum routes allowed	10
Routes recievied	0
Current ignore count	0
Ignore count allowed	5
Reset time	360
Ignore time	60
Current state	Running

The State screen displays the following:

Maximum Routes Allowed	Lists the maximum number of routes allowed on the selected BGP wireless controller or service platforms.
Routes Received	Lists the number of routes received from all the BGP peers.
Current Ignore Count	Lists the number of times the BGP daemon has been put in the Ignore state.
Ignore Count Allowed	Lists the maximum number of times the BGP daemon can be put in an Ignore state before entering permanent ignore state.
Reset Time	Lists the time after which ignore state count is reset to 0 and BGP daemon continues in the state it was in previously.
Ignore Time	Lists the time duration after which BGP daemon shall exit the Ignore state.
Current State	Lists the current state of this BGP route utilized on the wireless controller or service platforms.

6 Periodically, select **Refresh** to update the screen’s counters to their latest value.

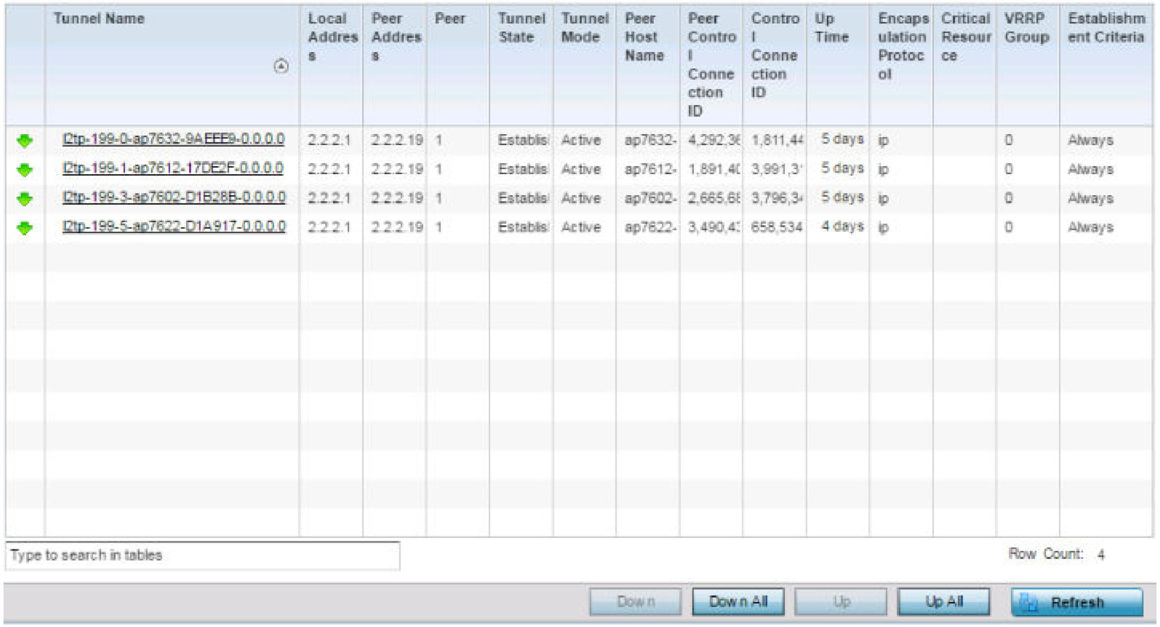
L2TPv3 Tunnels

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables a controller or service platform 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.

To review a selected controller or service platform's L2TPv3 statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **L2TPv3 Tunnels** in the left-hand side of the UI.

The **Statistics** → **Controller** → **L2TPv3 Tunnels** screen displays in the right-hand pane.



	Tunnel Name	Local Address	Peer Address	Peer	Tunnel State	Tunnel Mode	Peer Host Name	Peer Control Connection ID	Control Connection ID	Up Time	Encapsulation Protocol	Critical Resource	VRRP Group	Establishment Criteria
⬇	l2tp-199-0-ap7632-9AEEE9-0.0.0.0	2.2.2.1	2.2.2.19	1	Establis	Active	ap7632-	4,292,36	1,811,44	5 days	ip		0	Always
⬇	l2tp-199-1-ap7612-17DE2F-0.0.0.0	2.2.2.1	2.2.2.19	1	Establis	Active	ap7612-	1,891,40	3,991,3	5 days	ip		0	Always
⬇	l2tp-199-3-ap7602-D1B28B-0.0.0.0	2.2.2.1	2.2.2.19	1	Establis	Active	ap7602-	2,665,68	3,796,34	5 days	ip		0	Always
⬇	l2tp-199-5-ap7622-D1A917-0.0.0.0	2.2.2.1	2.2.2.19	1	Establis	Active	ap7622-	3,490,43	658,534	4 days	ip		0	Always

Row Count: 4

The following table describes the L2TPv3 statistics information:

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 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 the following format- **`Days`**: **`Hours`**: **`Minutes`**: **`Seconds`**: format. If the up time is displayed as - D:0 H:0 M: 0 S:0, it means 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	Displays monitored critical resources. Critical resources are device IP addresses or interface destinations interoperated as critical to the health of the network. Critical resources allow for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends.
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 the **Refresh** button to update the screen's statistics counters to their latest value.
6. Click the **Tunnel Name** link, to view per-session statistics for a specific L2TPv3 tunnel. The sessions for the selected L2TPv3 tunnel are displayed.
7. Click the **VLAN ID** of the desired session to view session statistics.

8 Select an L2TPV3 tunnel, and click **Down** to terminate it.
9 Select **Down All** to terminate all configured L2TPv3 Tunnels.
10 Select an L2TPV3 tunnel, and click **Up** to bring it up.
11 Select **Up All** to bring up all configured L2TPv3 Tunnels.

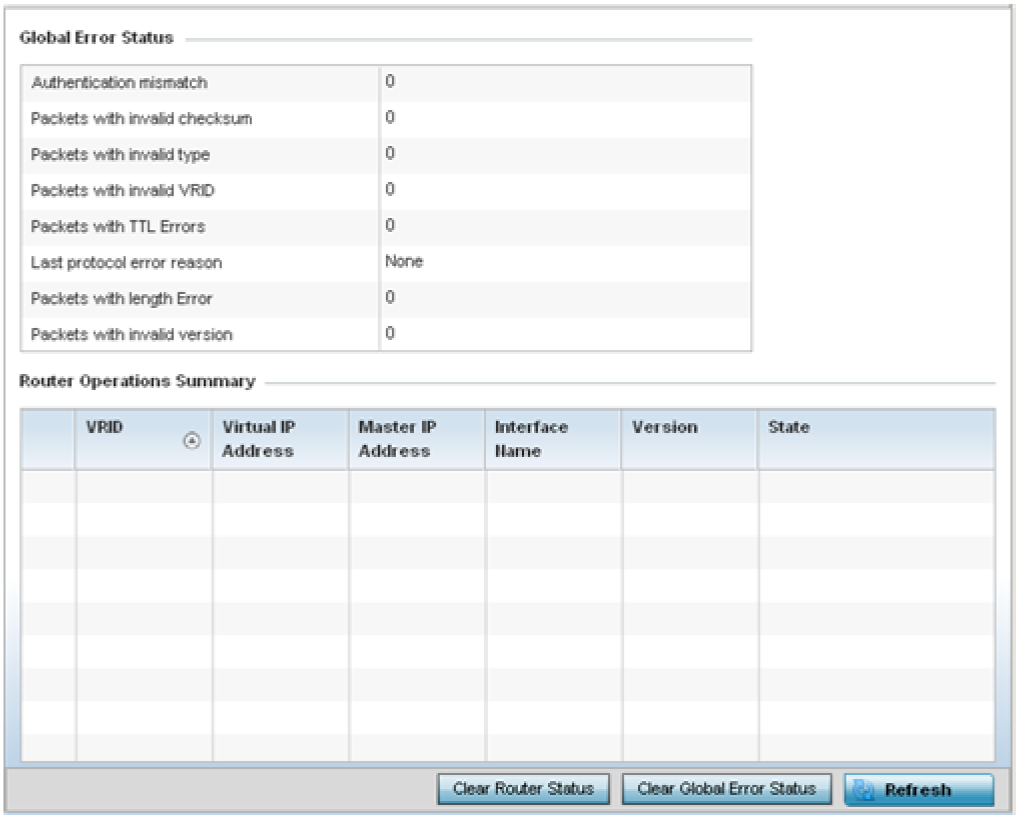
VRRP

The VRRP statistics screen displays VRRP *(Virtual Router Redundancy Protocol)* configuration statistics supporting router redundancy in a wireless network requiring high availability.

To review a selected controller or service platform's VRRP statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **VRRP** from the controller statistics menu.

The **Statistics** → **Controller** → **VRRP** screen displays in the right-hand pane.



Global Error Status

Authentication mismatch	0
Packets with invalid checksum	0
Packets with invalid type	0
Packets with invalid VRID	0
Packets with TTL Errors	0
Last protocol error reason	None
Packets with length Error	0
Packets with invalid version	0

Router Operations Summary

	VRID	Virtual IP Address	Master IP Address	Interface Name	Version	State

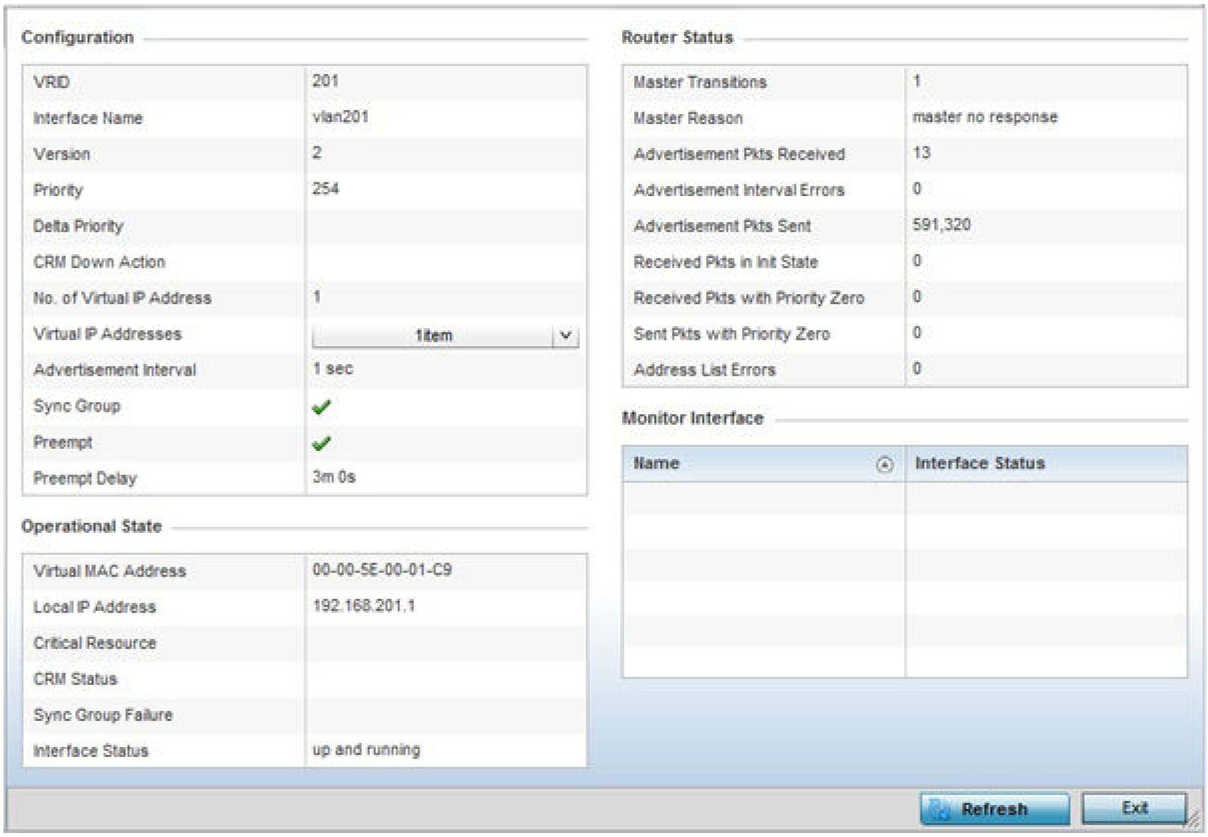
Refer to the Global Error Status field to review the various sources of packet errors logged during the implementation of the virtual route.

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.

Refer to the Router Operations Summary area 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 address associated with the virtual router and accepts packets addressed to the IP address associated with the virtual router.
Interface Name	Displays the interfaces selected 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.

5 Optionally select a **VRID** to list the ID's VRRP information in greater detail.



Configuration

VRID	201
Interface Name	vlan201
Version	2
Priority	254
Delta Priority	
CRM Down Action	
No. of Virtual IP Address	1
Virtual IP Addresses	1 item
Advertisement Interval	1 sec
Sync Group	✓
Preempt	✓
Preempt Delay	3m 0s

Operational State

Virtual MAC Address	00-00-5E-00-01-C9
Local IP Address	192.168.201.1
Critical Resource	
CRM Status	
Sync Group Failure	
Interface Status	up and running

Router Status

Master Transitions	1
Master Reason	master no response
Advertisement Pkts Received	13
Advertisement Interval Errors	0
Advertisement Pkts Sent	591,320
Received Pkts in Init State	0
Received Pkts with Priority Zero	0
Sent Pkts with Priority Zero	0
Address List Errors	0

Monitor Interface

Name	Interface Status

The Configuration area displays the following information:

VRID	Lists this selected ID's assigned ID. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
Interface	Displays the interfaces selected to supply VRRP redundancy failover support.
Version	Displays the VRRP version scheme used with the configuration. 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).
Priority	Lists the ID's 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.
Delta Priority	Displays the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.
CRM Down Action	Lists the critical resource down action applied to this listed VRID.
No. of Virtual IP Address	Lists the number of virtual interface IP address used as the redundant gateway address for the virtual route.
Virtual IP Addresses	Lists the virtual interface IP address set as the redundant gateway address for the virtual route.
Advertisement Interval	Lists the interval for unsolicited router assignments. The advertisement interval is the minimum interval between sending router updates. Sending too many updates creates flapping of routes leading to possible disruption.
Sync Group	Lists whether a VRRP sync group is assigned to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group.
Preempt	Lists whether preempt is enabled for the selected ID. Preempt ensures 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 preemption. 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 preempt is enabled, this item lists the delay interval (in seconds) for preemption.

The **Operation State** area displays the following information:

Virtual MAC Address	Lists the alpha numeric virtual MAC address utilized by the selected VRID.
Local IP Address	This address represents an alternative to an interface IP address. The last byte of the address (XX) is the VRID, which is different for each virtual router in the network.
Critical Resource	Displays the critical resource currently utilized by the selected VRID.
CRM Status	Lists operational network status of the critical resource used by this VRID.
Sync Group Failure	Lists any sync failures detected with the sync group of virtual IP addresses.
Interface Status	Lists the operational network status of the interfaces selected to supply VRRP redundancy failover support.

The Router Status area displays the following information:

Master Transitions	Lists the number of transitions to master router designation that have occurred with this VRID's router.
Master Reason	Displays an event message in respect the dedicated VRRP router's availability.
Advertisement Pkts Received	Lists the number of router advertisements received by this selected VRID. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.
Advertisement Interval Errors	Lists this VRID's number of advertisement prefix errors for link determination, address configuration and maximum hop limits.
Advertisement Pkts Sent	Lists the number of router advertisements sent by this selected VRID. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.
Received Pkts in Init State	Lists the number of packets received by the selected VRID when a router receives a hello packet but the local router ID is not listed in the received neighbor field. This means bidirectional communication is not been established.
Received Pkts with Priority Zero	Lists this VRID's number of received packets with a value of zero.
Sent Pkts with Priority Zero	Lists this VRID's number of sent packets with a value of zero.
Address List Errors	Lists the number of router event errors detected where an address that could not be resolved and bidirectional communication could not be established.

6. Refer to the Monitor Interface field to assess the names of this VRID's interface utilization and their respective statuses.
7. Select **Clear Router Status** to clear the Router Operations Summary table values 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.

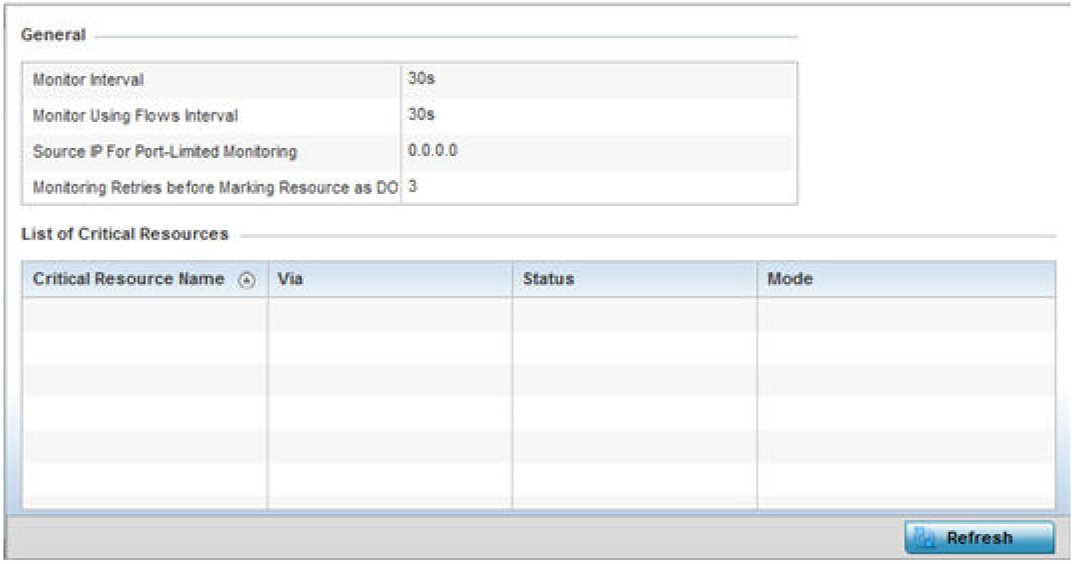
Critical Resource

The Critical Resources statistics screen displays a list of device network IP addresses (gateways, routers etc.) defined as critical to the health of the controller, service platform or access point managed network. Critical resources are pinged regularly to ensure availability. If there is a connectivity issue, an event is generated stating a critical resource is unavailable.

To view Critical Resource statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Select **Critical Resource** from the left-hand side of the UI.

   The **Statistics > Controller > Critical Resource** screen is displayed in the right-hand pane.



General

Monitor Interval	30s
Monitor Using Flows Interval	30s
Source IP For Port-Limited Monitoring	0.0.0.0
Monitoring Retries before Marking Resource as DO	3

List of Critical Resources

Critical Resource Name	Via	Status	Mode

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	Displays the name of the critical resource being monitored.
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.

LDAP Agent Status

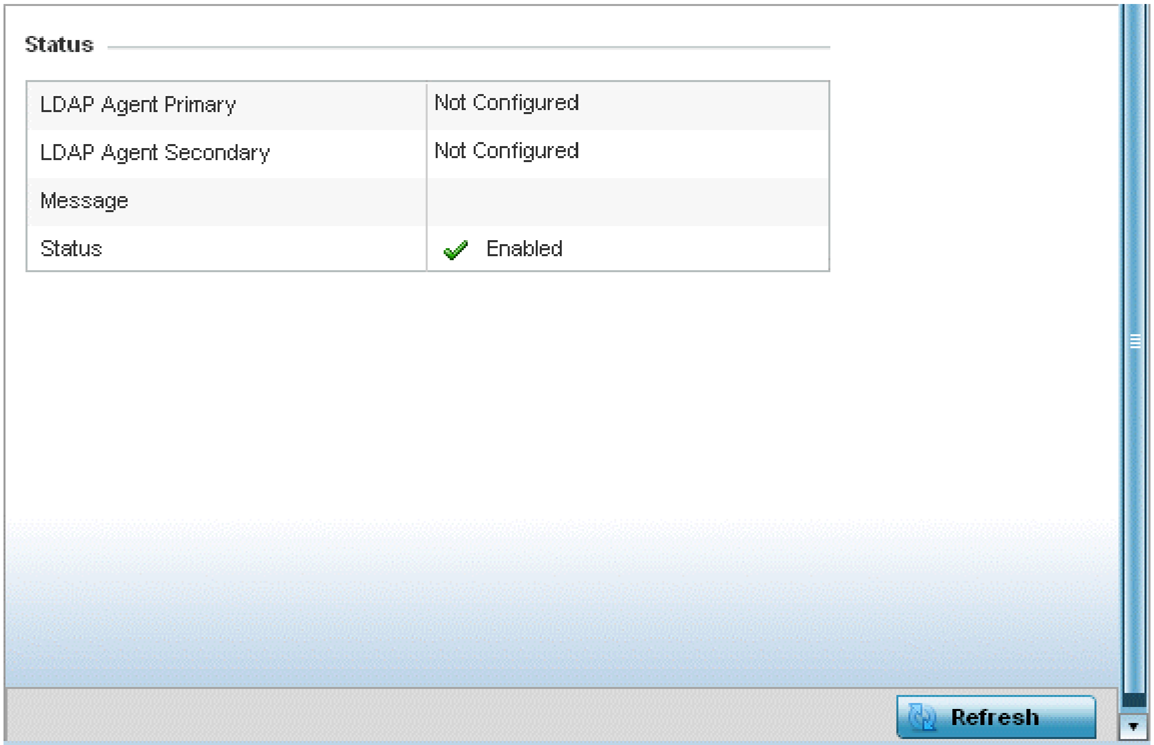
When LDAP has been specified as an external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary 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 RADIUS Server Policies on page 892 .

To view controller or service platform LDAP agent statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **LDAP Agent Status** from the left-hand side of the UI.

The **Statistics** → **Controller** → **LDAP Agent Status** screen is displayed in the right-hand pane.



Status

LDAP Agent Primary	Not Configured
LDAP Agent Secondary	Not Configured
Message	
Status	✓ Enabled

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.

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 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. MiNT links can be established over a VLAN (Among access points on a VLAN) or IP (remote access point to controller).

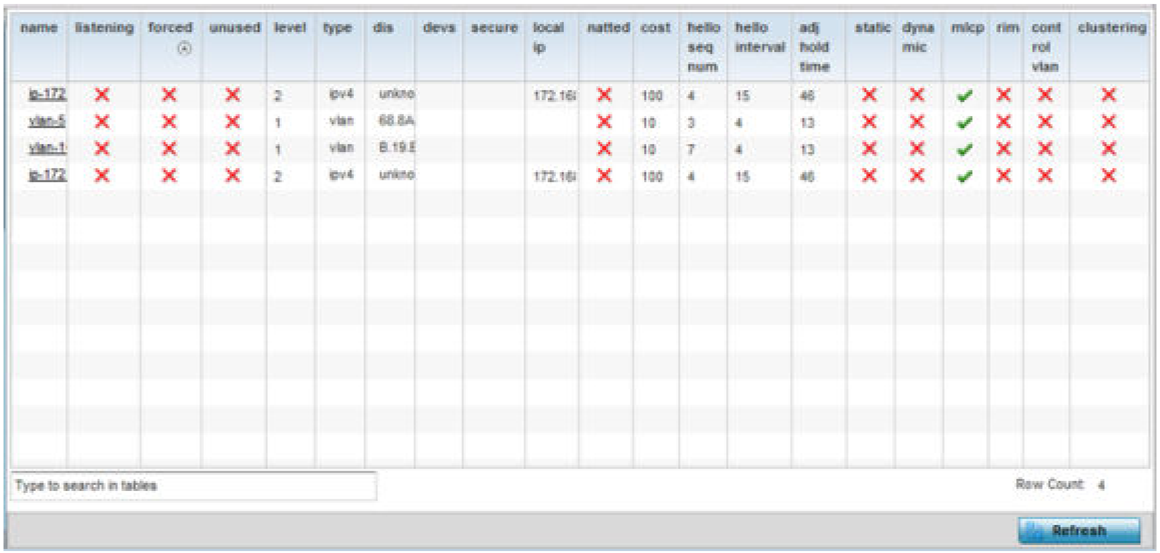
MiNT Links are automatically created between controllers and APs during adoption using MLCP *(MiNT Link Creation Protocol)*. They can also be manually created between a controller and AP (or) between two APs. MiNT links are manually created between controllers while configuring a cluster.

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 controller or service platform Mint link statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Select **Mint Links** from the left-hand side of the UI.

The **Statistics > Controller > MiNT Links** stats is displayed in the right-hand pane.



name	listening	forced	unused	level	type	dis	devs	secure	local ip	natted	cost	hello seq num	hello interval	adj hold time	static	dynamic	mlcp	rim	control vlan	clustering
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗
vlan-5	✗	✗	✗	1	vlan	68.8A				✗	10	3	4	13	✗	✗	✓	✗	✗	✗
vlan-1	✗	✗	✗	1	vlan	B.19.E				✗	10	7	4	13	✗	✗	✓	✗	✗	✗
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗

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.

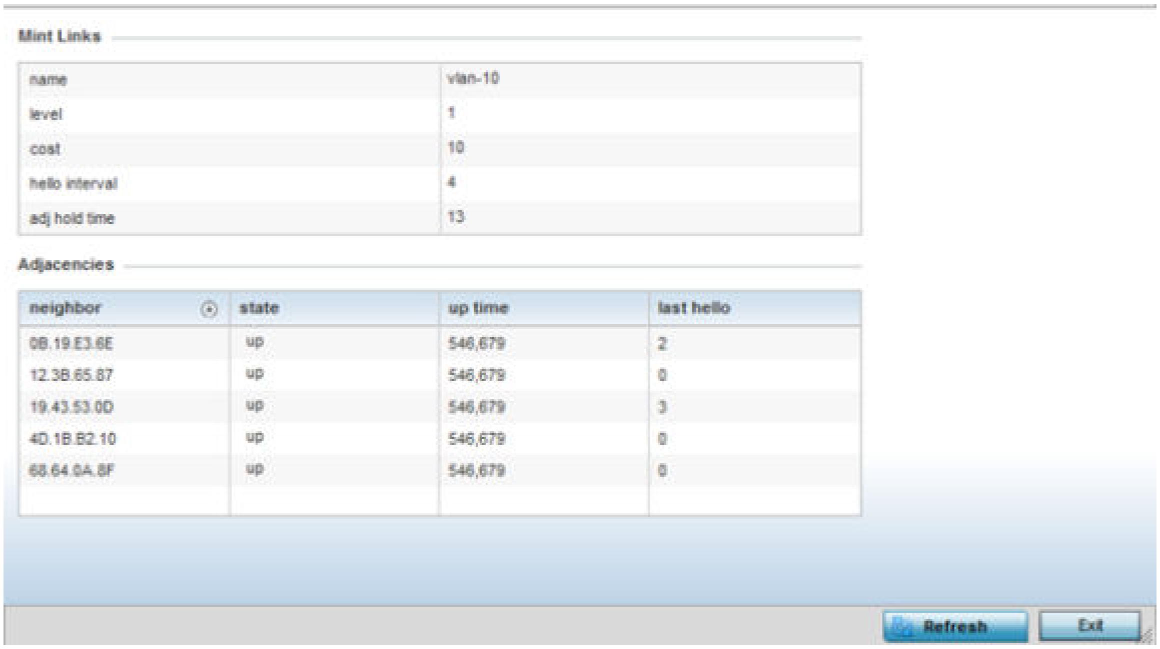
Refer to the secure column to assess whether the listed links are isolated between peers. The local ip column lists the IP address assigned as the link's end point address, not the interface's IP address.

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.



name	vlan-10
level	1
cost	10
hello interval	4
adj hold time	13

neighbor	state	up time	last hello
0B.19.E3.6E	up	546,679	2
12.3B.65.87	up	546,679	0
19.43.53.0D	up	546,679	3
4D.1B.B2.10	up	546,679	0
68.64.0A.8F	up	546,679	0

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.

Guest Users

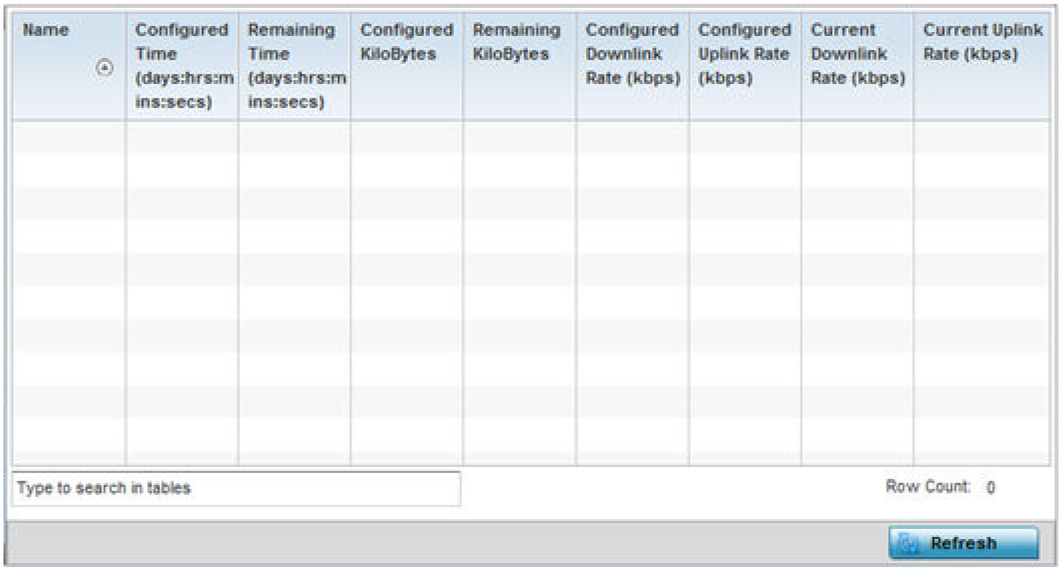
A captive portal is an access policy for providing guests temporary and restrictive access to the wireless network. A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's 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 controller or service platform managed network or provide access without limitations.

For information on setting captive portal duration and authentication settings, refer to Captive Portal Policies on page 834.

To view the controller or service platform guest user utilization:

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.
4. Select a **Wireless Controller**.
5. Select **Guest Users** from the left-hand side of the UI.

   The **Statistics** → **Controller** → **Guest Users** screen displays in the right-hand pane:



Name	Configured Time (days:hrs:mins:secs)	Remaining Time (days:hrs:mins:secs)	Configured KiloBytes	Remaining KiloBytes	Configured Downlink Rate (kbps)	Configured Uplink Rate (kbps)	Current Downlink Rate (kbps)	Current Uplink Rate (kbps)

This screen describes the following:

Name	Lists the administrator assigned name of the client utilizing the controller or service platform 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 controller or service platform.
Remaining Time (days:hrs:mins:secs)	Displays the time each listed client has remaining in their captive portal guest user session with this managing controller or service platform.

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 888.
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 toDefining User Pools on page 888 .
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 888.
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 to Defining User Pools on page 888 .

6. Select **Refresh** to update the screen's statistics counters to their latest value.

GRE Tunnel

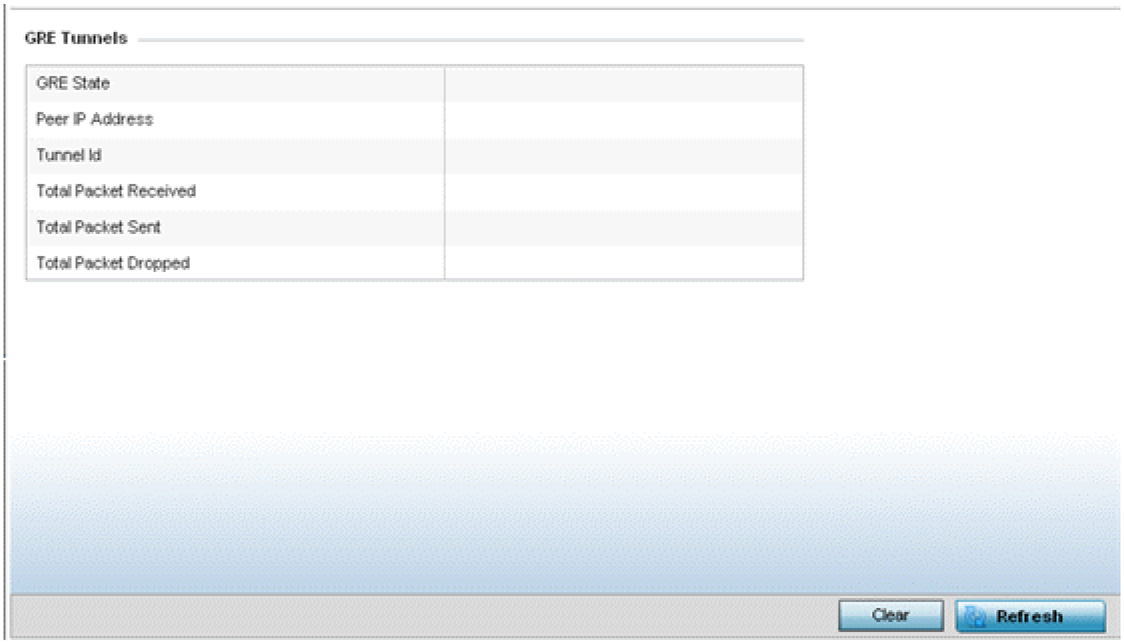
GRE *(Generic Routing Encapsulation)* is one of the available tunneling mechanisms, which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

Use the GRE Tunnel screen to view information on the traffic flow in a GRE tunnel.

To view the 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Select **GRE Tunnels**.

   The **Statistics > Controller > GRE Tunnels** screen displays in the right-hand pane.



GRE Tunnels

GRE State	
Peer IP Address	
Tunnel Id	
Total Packet Received	
Total Packet Sent	
Total Packet Dropped	

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

6 Select **Clear** to revert the screen counters to zero and begin a new data collection.

7 Select **Refresh** to update the screen's statistics counters to their latest value.

Dot1x

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.

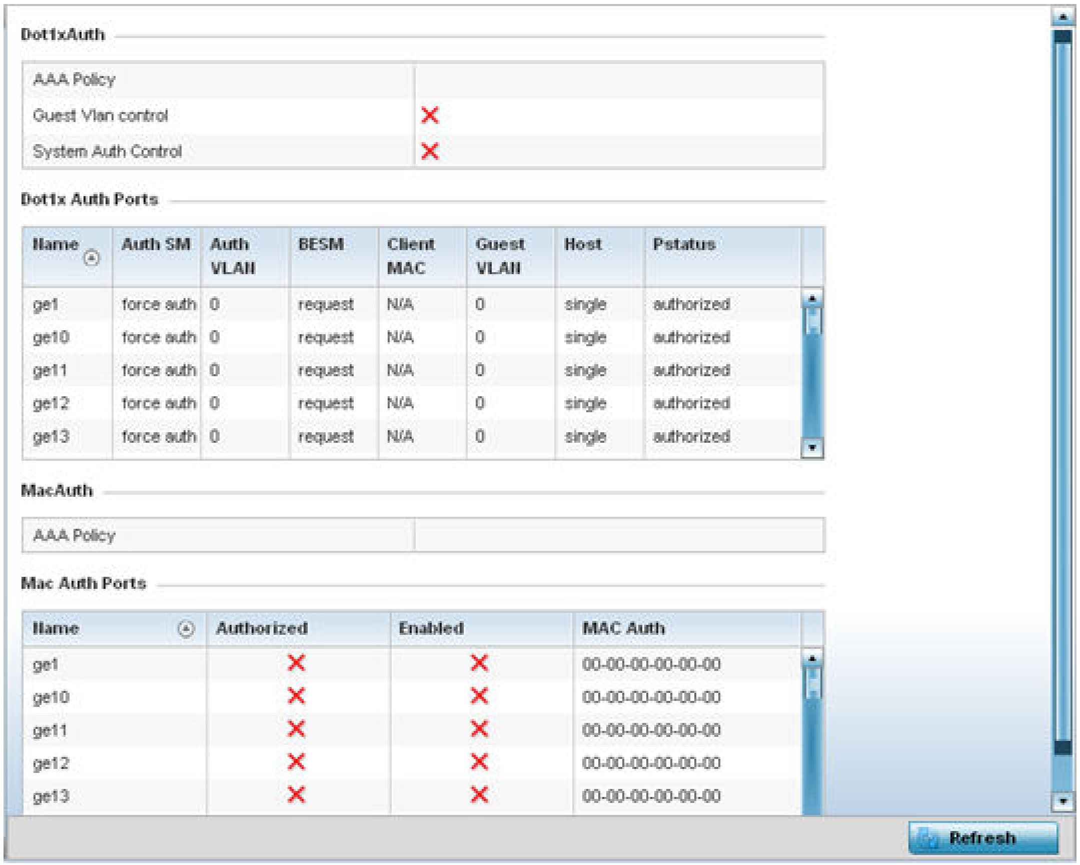
To view the Dot1x statistics:

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 the **RF Domain** node.

4 Select a **Wireless Controller**.

5 Select **Dot1x** from the left-hand side of the UI.

The Statistics > Controller > Dot1x screen displays in the right-hand pane.



Dot1xAuth

AAA Policy	
Guest Vlan control	✗
System Auth Control	✗

Dot1x Auth Ports

Name	Auth SM	Auth VLAN	BESM	Client MAC	Guest VLAN	Host	Pstatus
ge1	force auth	0	request	N/A	0	single	authorized
ge10	force auth	0	request	N/A	0	single	authorized
ge11	force auth	0	request	N/A	0	single	authorized
ge12	force auth	0	request	N/A	0	single	authorized
ge13	force auth	0	request	N/A	0	single	authorized

MacAuth

AAA Policy	

Mac Auth Ports

Name	Authorized	Enabled	MAC Auth
ge1	✗	✗	00-00-00-00-00-00
ge10	✗	✗	00-00-00-00-00-00
ge11	✗	✗	00-00-00-00-00-00
ge12	✗	✗	00-00-00-00-00-00
ge13	✗	✗	00-00-00-00-00-00

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.

6 Select **Refresh** to update the screen’s statistics counters to their latest value.

Network

Use the Network set of management screens to view information for *ARP*, *DHCP*, *Routing* and *Bridging*. Each of these screens provides enough data to troubleshoot issues related to the following:

- ARP Entries
- Route Entries
- Bridge
- IGMP
- DHCP Options
- Cisco Discovery Protocol
- Link Layer Discovery Protocol

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.

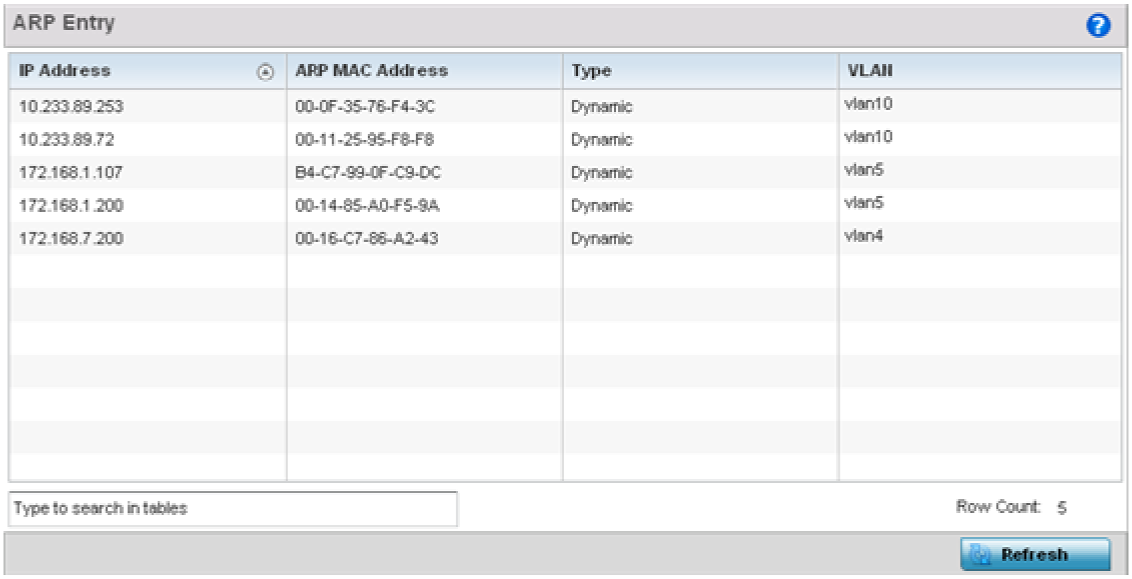
To view the ARP entries on the network statistics screen:

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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Networks** menu from the left-hand side of the UI.
6 Select **ARP Entries**.

The **Statistics > Controller > ARP Entries** stats is displayed in the right-hand pane.



IP Address	ARP MAC Address	Type	VLAN
10.233.89.253	00-0F-35-76-F4-3C	Dynamic	vlan10
10.233.89.72	00-11-25-95-F8-F8	Dynamic	vlan10
172.168.1.107	B4-C7-99-0F-C9-DC	Dynamic	vlan5
172.168.1.200	00-14-85-A0-F5-9A	Dynamic	vlan5
172.168.7.200	00-16-C7-86-A2-43	Dynamic	vlan4

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.

7 Select the **Refresh** button to update the screen's statistics counters to their latest values.

Route Entries

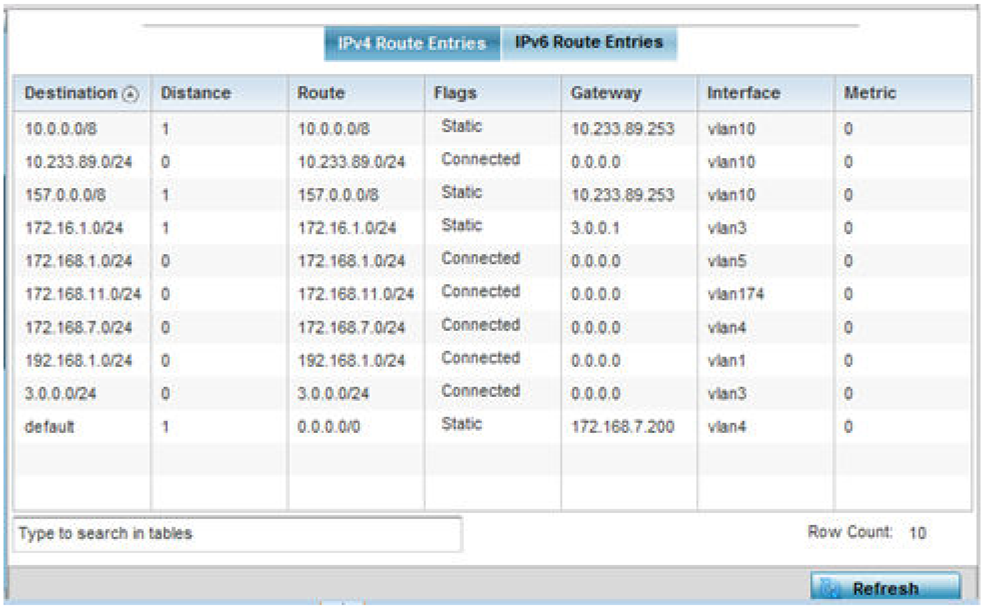
The Route Entries screen displays data for routing packets to a defined destination. When an existing destination subnet does not meet the needs of the network, add a new destination subnet, subnet mask and gateway.

To view the 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Network** menu from the left-hand side of the UI.

6 Select **Route Entries**.

The **Statistics > Controller > IPv4 Route Entries** stats display by default in the right-hand pane.



Destination	Distance	Route	Flags	Gateway	Interface	Metric
10.0.0.0/8	1	10.0.0.0/8	Static	10.233.89.253	vlan10	0
10.233.89.0/24	0	10.233.89.0/24	Connected	0.0.0.0	vlan10	0
157.0.0.0/8	1	157.0.0.0/8	Static	10.233.89.253	vlan10	0
172.16.1.0/24	1	172.16.1.0/24	Static	3.0.0.1	vlan3	0
172.168.1.0/24	0	172.168.1.0/24	Connected	0.0.0.0	vlan5	0
172.168.11.0/24	0	172.168.11.0/24	Connected	0.0.0.0	vlan174	0
172.168.7.0/24	0	172.168.7.0/24	Connected	0.0.0.0	vlan4	0
192.168.1.0/24	0	192.168.1.0/24	Connected	0.0.0.0	vlan1	0
3.0.0.0/24	0	3.0.0.0/24	Connected	0.0.0.0	vlan3	0
default	1	0.0.0.0/0	Static	172.168.7.200	vlan4	0

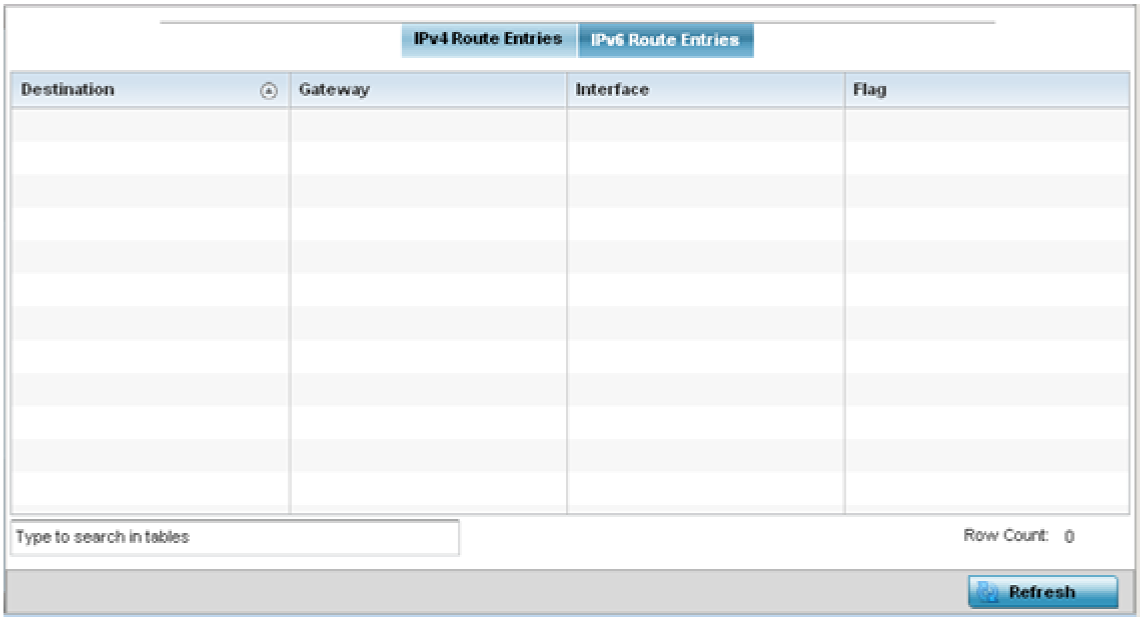
Row Count: 10

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.

7 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.

8 Select **Refresh** to update the display to the latest values.

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.

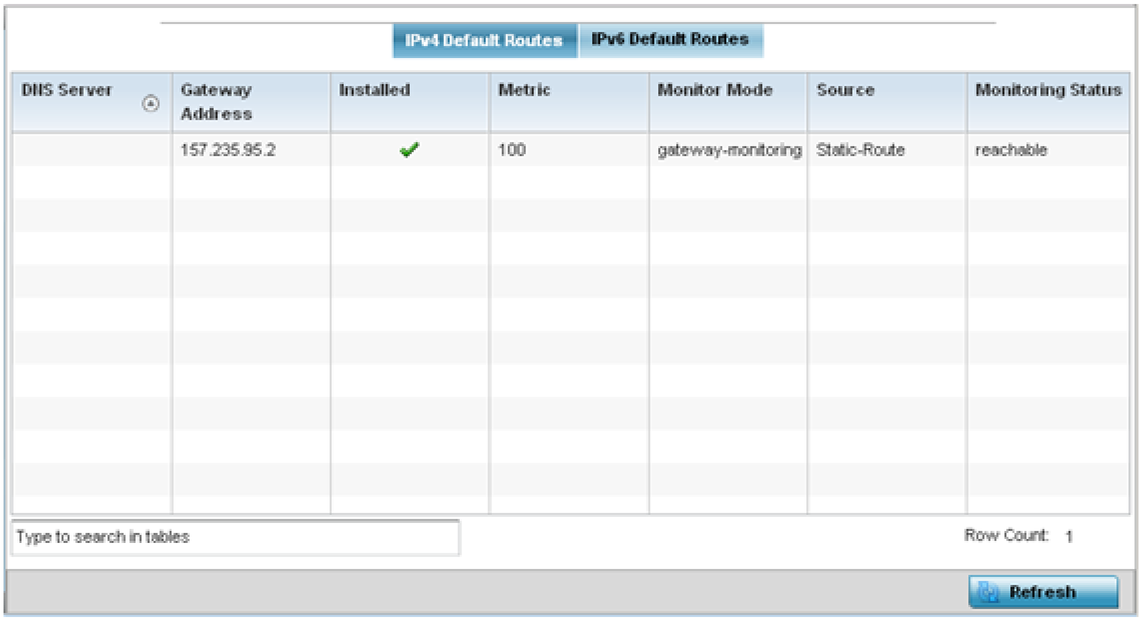
Static routes are manually configured. They work fine in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.

To view controller or service platform 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Network** menu from the left-hand side of the UI.

6 Select **Default Routes**.

The **Statistics > Controller > IPv4 Default Routes** stats is displayed by default in the right-hand pane.



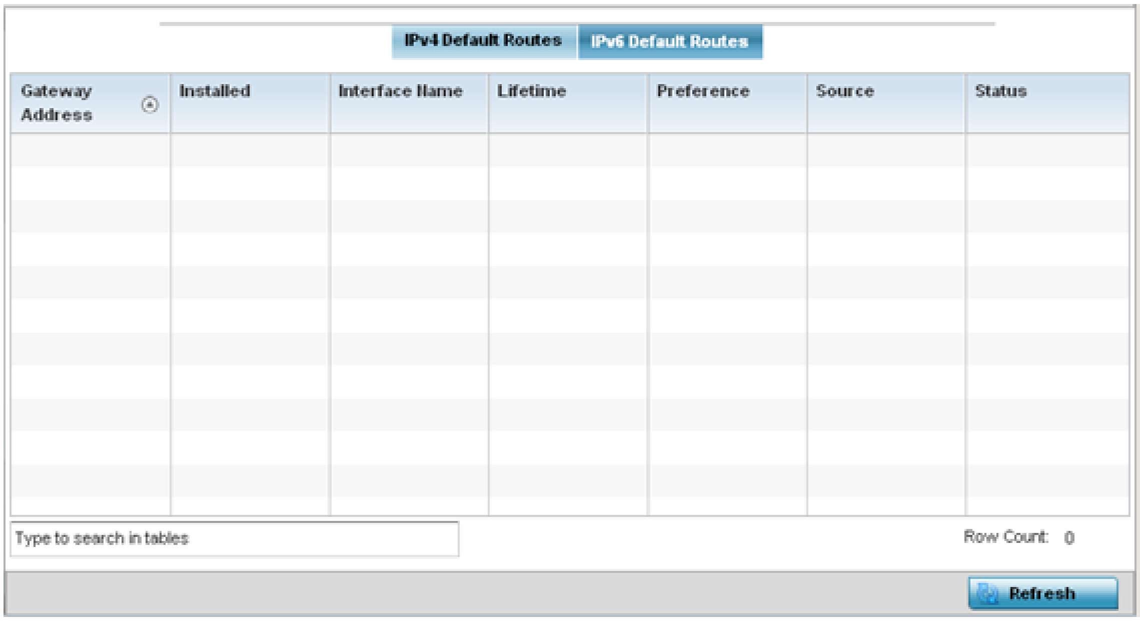
DNS Server	Gateway Address	Installed	Metric	Monitor Mode	Source	Monitoring Status
	157.235.95.2	✓	100	gateway-monitoring	Static-Route	reachable

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 controller or service platform.
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 controller or service platform. 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 controller or service platform managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.

7 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

The IPv6 Default Routes stats is displayed by default in the right-hand pane.



The 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 controller or service platform. 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 controller or service platform managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.

8 Select **Refresh** to update the display to the latest values.

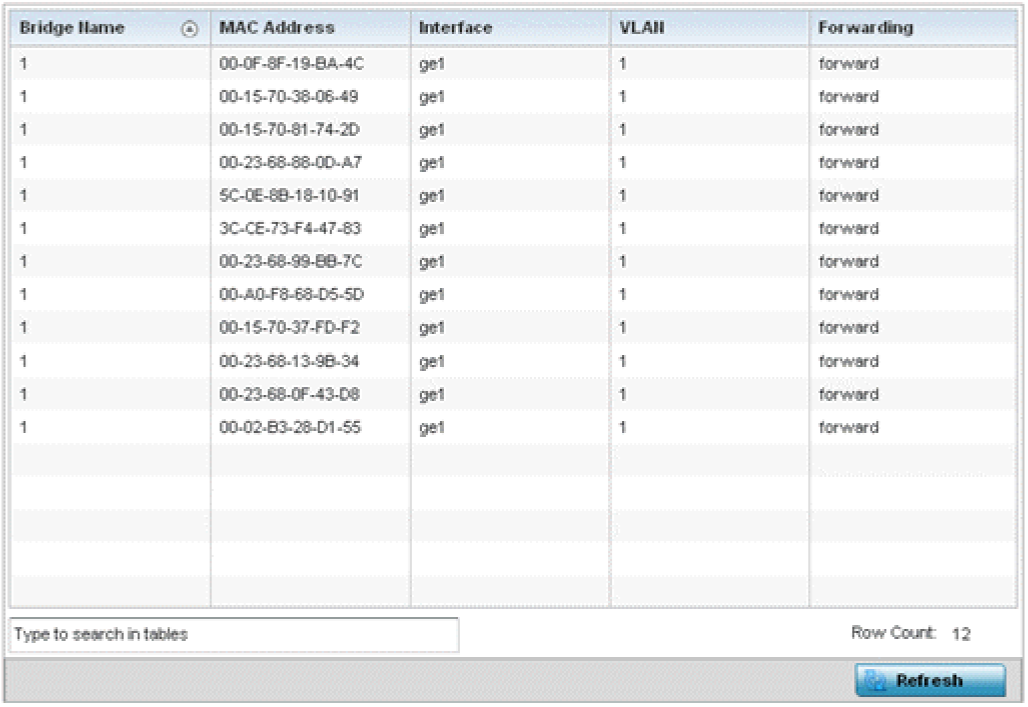
Bridge

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.

To view network bridge 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Network** menu from the left-hand side of the UI.
6 Select **Bridge**.

The **Statistics > Controller > Bridge** stats is displayed in the right-hand pane.



Bridge Name	MAC Address	Interface	VLAN	Forwarding
1	00-0F-8F-19-BA-4C	ge1	1	forward
1	00-15-70-38-06-49	ge1	1	forward
1	00-15-70-81-74-2D	ge1	1	forward
1	00-23-68-88-0D-A7	ge1	1	forward
1	5C-0E-8B-18-10-91	ge1	1	forward
1	3C-CE-73-F4-47-83	ge1	1	forward
1	00-23-68-99-BB-7C	ge1	1	forward
1	00-A0-F8-68-D5-5D	ge1	1	forward
1	00-15-70-37-FD-F2	ge1	1	forward
1	00-23-68-13-9B-34	ge1	1	forward
1	00-23-68-0F-43-D8	ge1	1	forward
1	00-02-B3-28-D1-55	ge1	1	forward

Row Count: 12

This screen displays the following:

Bridge Name	Displays the numeric ID of the network bridge.
MAC Address	Displays the MAC address of each listed bridge.
Interface	Displays the controller or service platform physical port interface the bridge uses to transfer packets. Interface availability is slightly different amongst supported controller and service platform models.
VLAN	Displays the VLAN the bridge is using as a virtual interface within the network.
Forwarding	Displays whether the bridge is forwarding packets and in a forwarding state.

7 Select **Refresh** to update the statistics counters to the latest values.

IGMP

IGMP *(Internet Group Management Protocol)* is a protocol used for managing members of IP multicast groups. The access point listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the access point floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To view network IGMP 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.

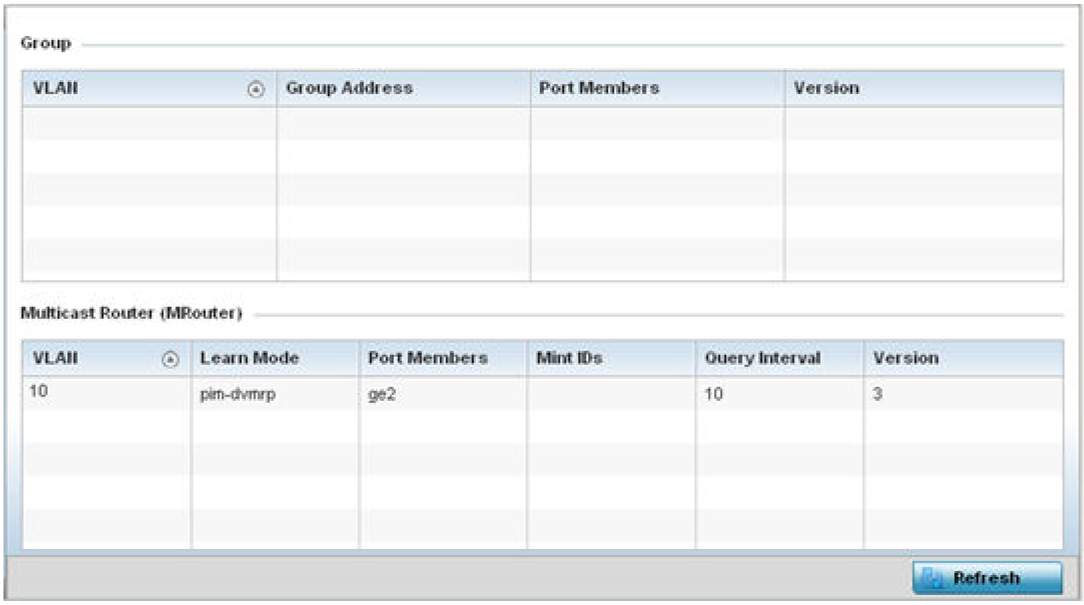
3 Expand the **RF Domain** node.

4 Select a **Wireless Controller**.

5 Expand the **Network** menu from the left-hand side of the UI.

6 Select **IGMP**.

The **Statistics > Controller > IGMP** stats is displayed in the right-hand pane.



Group

VLAN	Group Address	Port Members	Version

Multicast Router (MRouter)

VLAN	Learn Mode	Port Members	Mint IDs	Query Interval	Version
10	pim-dvmrp	ge2		10	3

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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

MLD

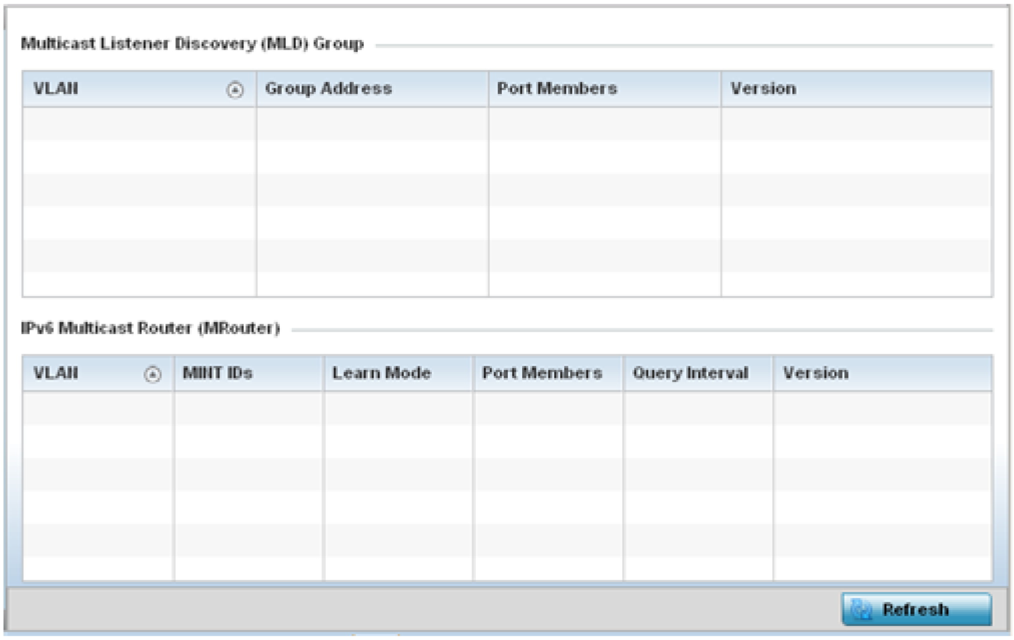
MLD *(Multicast Listener Discovery)* snooping enables a controller, service platform or access point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD 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 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Network** menu from the left-hand side of the UI.
6 Select **MLD**.

The **Statistics > Controller > MLD** stats is displayed in the right-hand pane.



Multicast Listener Discovery (MLD) Group

VLAN	Group Address	Port Members	Version

IPv6 Multicast Router (MRouter)

VLAN	MINT IDs	Learn Mode	Port Members	Query Interval	Version

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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

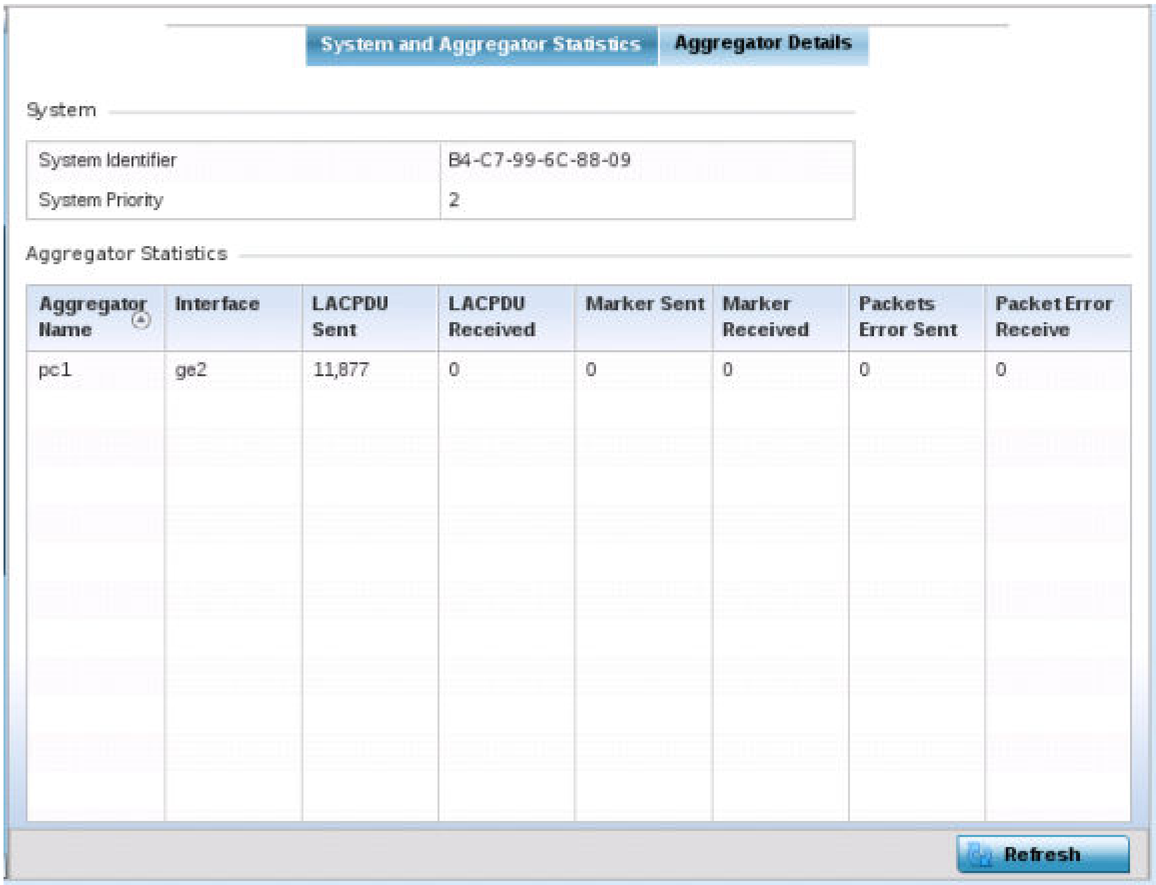
LACP

LACP *(Link Aggregation Control Protocol)* is used to dynamically determine if link aggregation is possible and then to automatically configure the aggregation. LACP is a part of the IEEE 802.1ad standard and allows the switch to dynamically reconfigure the LAGs *(link aggregation groups)*. A LAG is enabled only if the LACP determines that the remote device is also using LACP and is able to join the LAG.

To view the LACP statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **LACP**.

The **Statistics > Controller > System and Aggregator Statistics** tab displays by default in the right-hand pane.



System

System Identifier	B4-C7-99-6C-88-09
System Priority	2

Aggregator Statistics

Aggregator Name	Interface	LACPDU Sent	LACPDU Received	Marker Sent	Marker Received	Packets Error Sent	Packet Error Receive
pc1	ge2	11,877	0	0	0	0	0

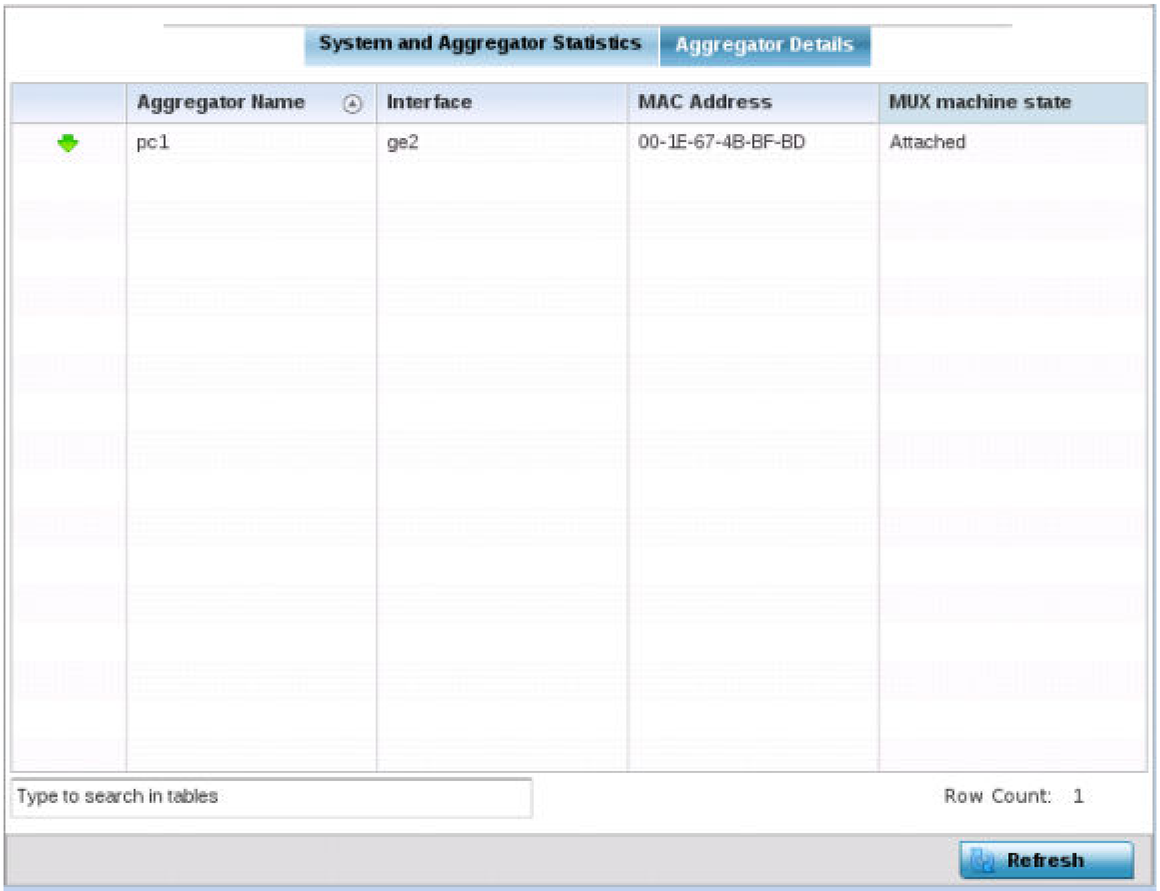
The System field describes the following:

System Indentifier	Displays the MAC address of the device.
System Priority	Displays the system's LACP priority value.

The Aggregator Statistics field describes the following:

Aggregator Name	Displays the name of the port channel configured on this device.
Interface	Displays the name of the interface for which these statistics are being displayed.
LACPUD Sent	Displays the number of LACPDUs *(Link Aggregation Control Protocol Data Units)* sent from this device.
LACPDU Received	Displays the number of LACPDUs received by this device.
Marker Sent	Displays the number of marker packets sent. Marker packets are sent to the remote device to ensure that all frames transmitted through the link have been received.
Marker Received	Displays the number of marker packet responses received from the remote device.
Packets Error Sent	Displays the total number packets transmitted with error
Packets Error Received	Displays the total number packets received with error.

6 Select the **Aggregator Details** tab. This field describes the following:



	Aggregator Name	Interface	MAC Address	MUX machine state
▼	pc1	ge2	00-1E-67-4B-BF-BD	Attached

Aggregator Name	Displays the name of the LAG.
Interface	Displays the name of the interface that is a member of the LAG.

MAC Address	Displays the MAC address of the physical interface.
Mux Machine State	Displays the state of the multiplexer state machine for the aggregation port. The values are: • **`attached`** – Displays the state as attached, when the multiplexer state machine is initiating the process of attaching the port to the selected aggregator. • **`detached`** – Displays the state as detached, when the multiplexer state machine is initiating the process of detaching the port from the aggregator. • **`collecting/distributing`** – Displays the state as collecting/distributing. Collecting and distributing states are merged together to form a combined state (coupled control). Because independent control is not possible, the coupled control state machine does not wait for the partner to signal that collection has started before enabling both collection and distribution.

7. Select **Refresh** to update the screen's statistics counters to their latest values.

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 1148.
- Traffic Shaping - Statistics on page 1148.

Traffic Shaping - Status

To view network the controller or service platform's traffic shaping status:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select the **Wireless Controller** node from the left navigation pane.
4. Expand the **Network** menu from the left-hand side of the UI.
5. Select **Traffic Shaping**.

   The **Statistics > Controller > Traffic Shaping > Status** screen displays by default.

   The status screen simply lists the controller or service platform's current traffic shaping operational status.
6. Select **Refresh** to update the screen's statistics counters to their latest values.

Traffic Shaping - Statistics

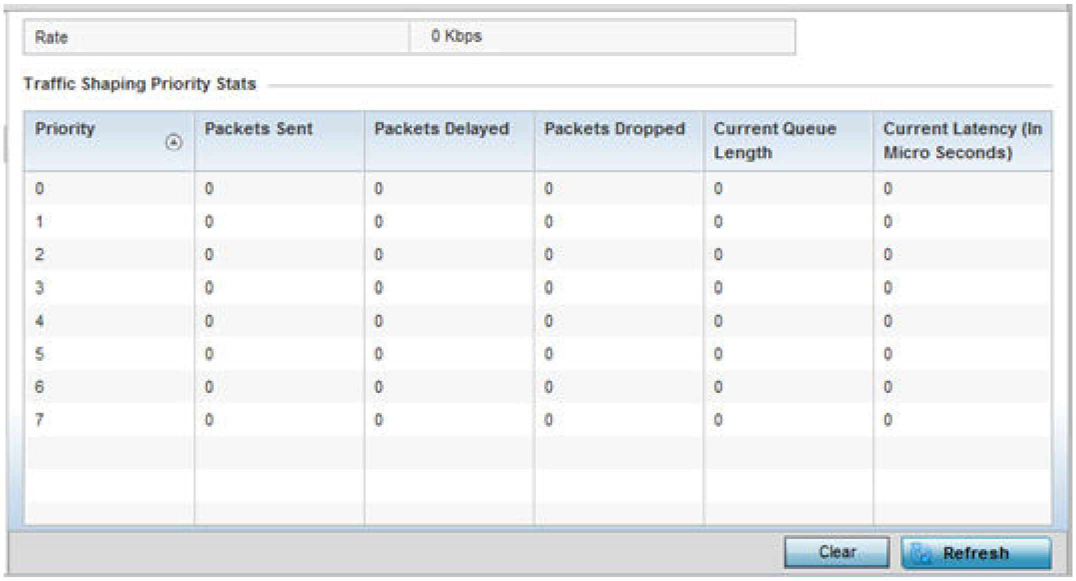
To view network the controller or service platform's traffic shaping statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select the **Wireless Controller** node from the left navigation pane.
4 Expand the **Network** menu from the left-hand side of the UI.
5 Select **Traffic Shaping**.

The Status screen displays by default.

6 Select the **Statistics** tab.

The **Statistics > Controller > Traffic Shaping > Statistics** screen displays.



Rate: 0 Kbps

Traffic Shaping Priority Stats

Priority	Packets Sent	Packets Delayed	Packets Dropped	Current Queue Length	Current Latency (In Micro Seconds)
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0

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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

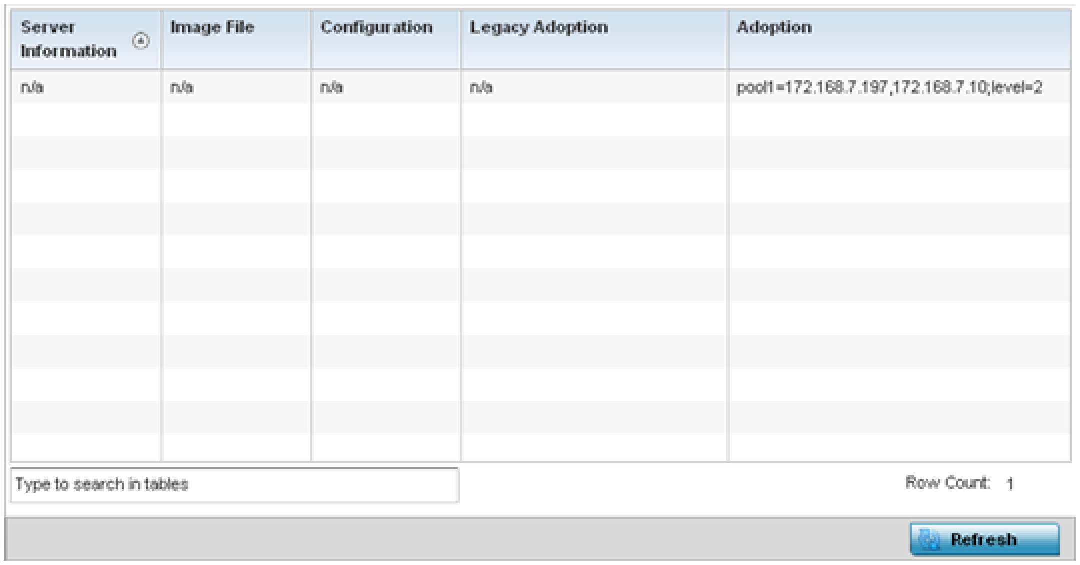
DHCP Options

Controllers and service platforms contain an internal DHCP *(Dynamic Host Configuration Protocol)* server. The DHCP server can provide the dynamic assignment of IP addresses automatically to requesting clients. This 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 include IP address, gateway and network mask.

To view network 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Network** menu from the left-hand side of the UI.
6 Select **DHCP Options**.

The **Statistics > Controller > Network > DHCP Options** screen displays.



Server Information	Image File	Configuration	Legacy Adoption	Adoption
n/a	n/a	n/a	n/a	pool1=172.168.7.197,172.168.7.10;level=2

This screen describes the following:

Server Information	Lists server information specific to each DHCP server resource available to requesting clients for the dynamic assignment of IP addresses.
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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

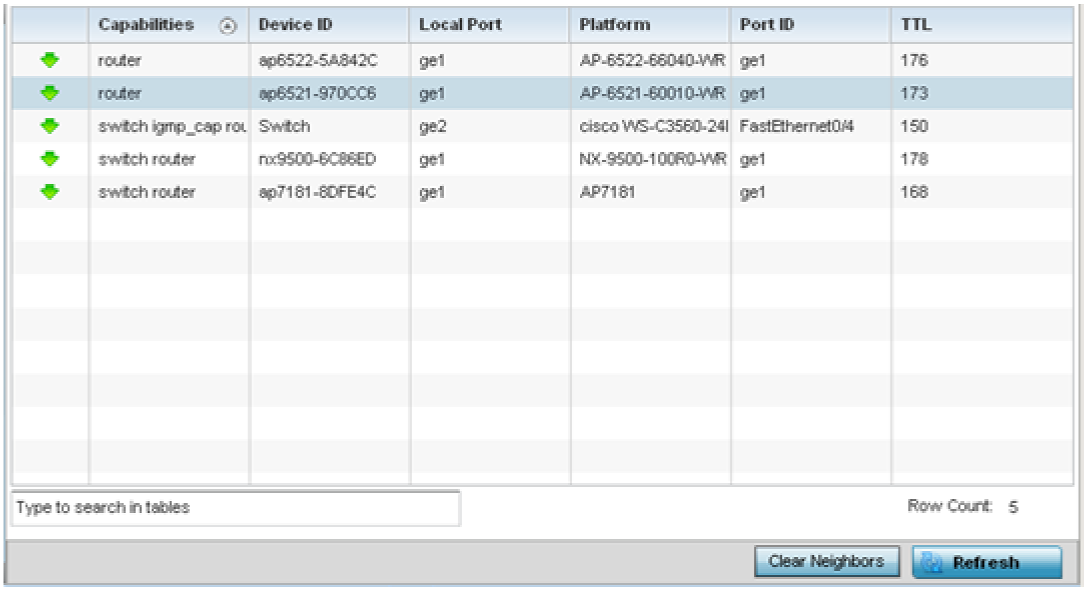
Cisco Discovery Protocol

CDP *(Cisco Discovery Protocol)* is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To view a selected controller's or service platform'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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Network** menu from the left-hand side of the UI.
6. Select **Cisco Discovery Protocol**.

   The **Statistics > Controller > Network > Cisco Discovery Protocol** screen displays in the right-hand pane.



	Capabilities	Device ID	Local Port	Platform	Port ID	TTL
⬇	router	ap6522-5A842C	ge1	AP-6522-66040-WR	ge1	176
⬇	router	ap6521-970CC6	ge1	AP-6521-60010-WR	ge1	173
⬇	switch igmp_cap rou	Switch	ge2	cisco WS-C3560-24I	FastEthernet0/4	150
⬇	switch router	nx9500-6C86ED	ge1	NX-9500-100R0-WR	ge1	178
⬇	switch router	ap7181-8DFE4C	ge1	AP7181	ge1	168

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 for each CDP capable device.
Platform	Displays the model number of the CDP capable device.

Port ID	Displays the identifier for the local port.
TTL	Displays the TTL *(time to live)* for each CDP connection.

7. Click **Clear Neighbors** to remove all known CDP neighbors from the table.
8. Select **Refresh** to update the screen's statistics counters to their latest values.

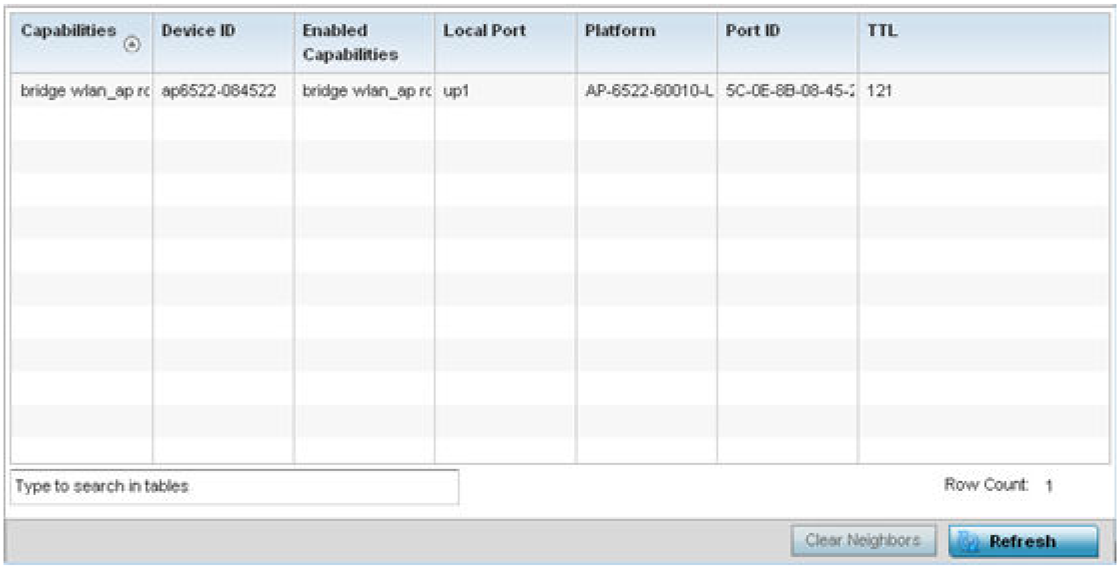
Link Layer Discovery Protocol

The LLDP *(Link Layer Discovery Protocol)* 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 Link Layer Discovery Protocol statistics:

1. Select the **Statistics** menu from the Web UI.
2. Expand the **RF Domain** node.
3. Select a **Wireless Controller**.
4. Expand the **Network** menu from the left-hand side of the UI.
5. Select **Link Layer Discovery Protocol**.

   The **Statistics > Controller > Network > Link Layer Discovery Protocol** screen displays in the right-hand pane.



Capabilities	Device ID	Enabled Capabilities	Local Port	Platform	Port ID	TTL
bridge wlan_ap r	ap6522-084522	bridge wlan_ap r	up1	AP-6522-60010-L	5C-0E-8B-08-45-	121

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 capabilities are currently in utilization by the listed device.
Local Port	Displays the local port name for each LLDP capable device.
Platform	Displays the model number of the LLDP capable device.

Port ID	Displays the identifier for the local port.
TTL	Displays the TTL *(time to live)* 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.

IPv6 Neighbor Discovery

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.

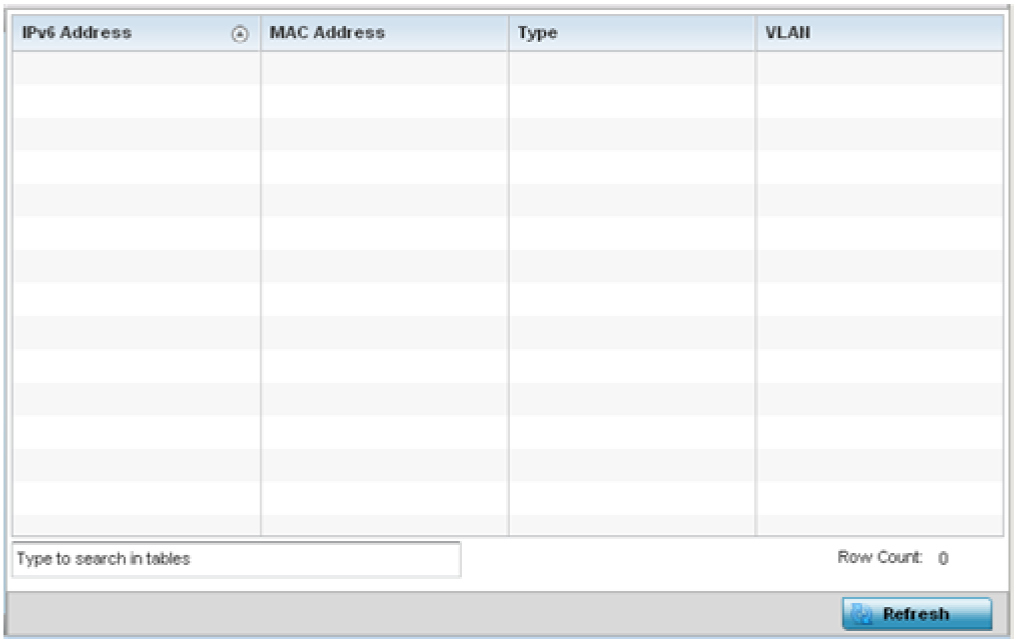
Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

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 a controller or service platform'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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Network** menu from the left-hand side of the UI.
6 Select **IPv6 Neighbor Discovery**.

The **Statistics > Controller > 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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

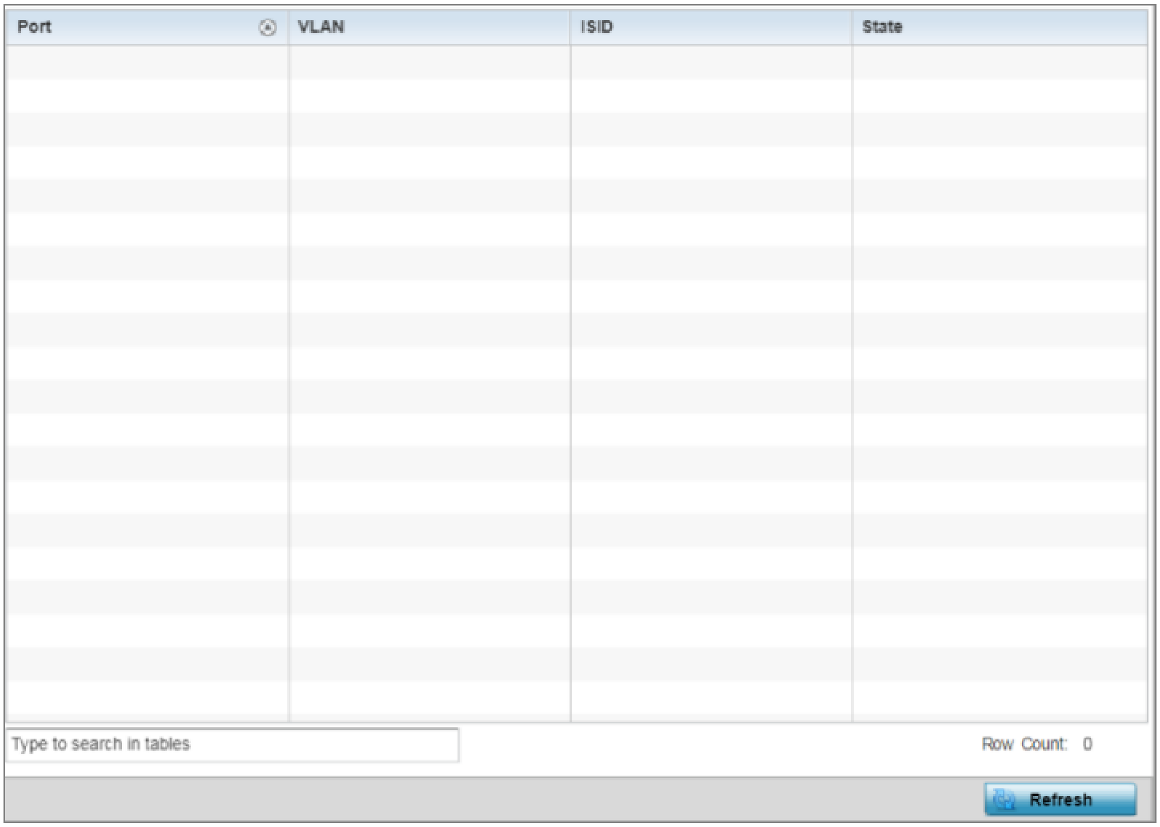
Fabric Attach

Displays the current status of FA *(Fabric Attach)* VLAN to Individual Service Identifier (I-SID) assignments for all ports.

To view a controller or service platform's FA statistics:

1 Select the **Statistics** → **Wireless Controller/Service Platform** menu from the Web UI.

2 Expand the **Network** menu and select **Fabric Attach**.



Port	VLAN	ISID	State

Figure 404: Statistics → Controller → Fabric Attach screen

3 Review the following Fabric Attach details.

Port	Displays the current status of FA *(Fabric Attach)* VLAN to I-SID *(Individual Service Identifier)* assignments for all ports.
VLAN	Displays the VLAN number
ISID	Displays the ISID assigned to the above displayed VLAN
State	Displays the status of VLAN to I-SID mappings, if configured, on the Ethernet ports of an FA Client. The status displays as: • active – If the VLAN to I-SID mapping is accepted by the FA Server and applied to the VLAN traffic from the client. • pending – If the VLAN to I-SID mapping acceptance is not achieved (i.e, pending acceptance)

4 Select **Refresh** to update the screen with latest FA related information.

MSTP

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.

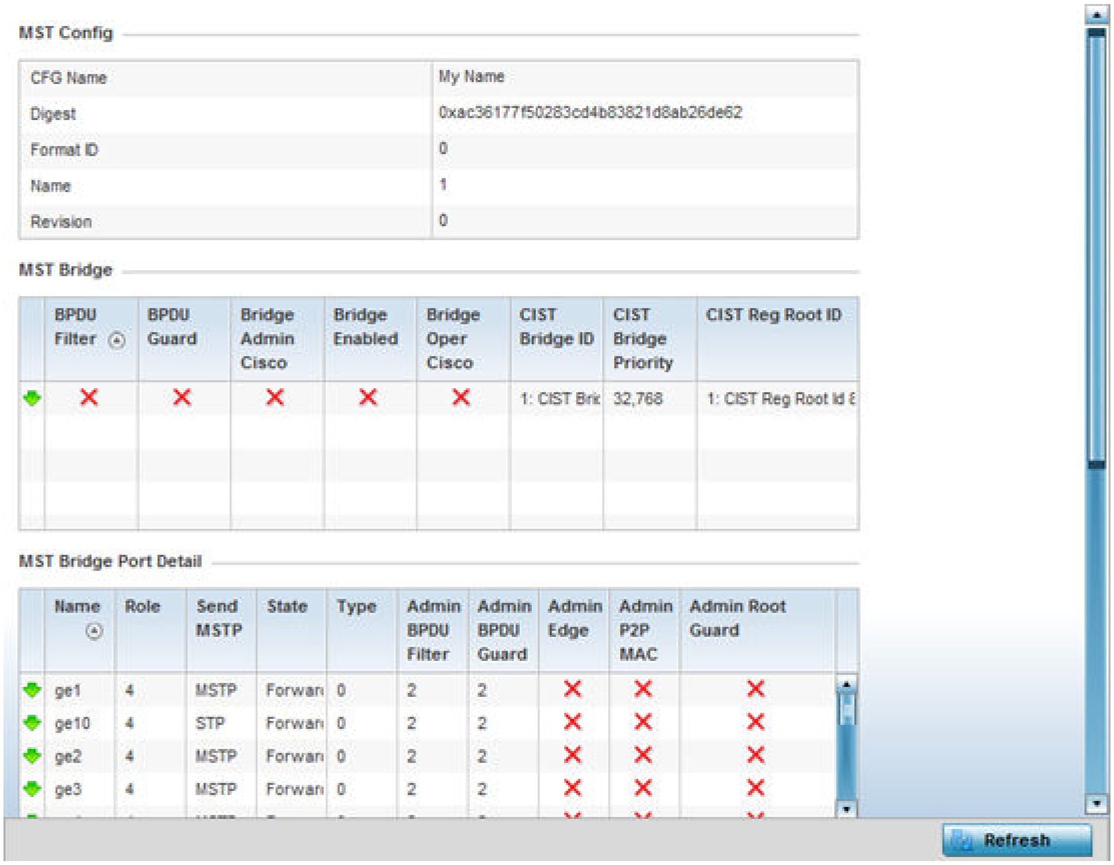
If there's just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP includes all of its spanning tree information in a single BPDU *(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 view a controller or service platform'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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Network** menu from the left-hand side of the UI.
6. Select **MSTP**.

   The **Statistics > Controller > Network > MSPT** stats is displayed in the right-hand pane.



MST Config

CFG Name	My Name
Digest	0xac36177f50283cd4b83821d8ab26de62
Format ID	0
Name	1
Revision	0

MST Bridge

	BPDU Filter	BPDU Guard	Bridge Admin Cisco	Bridge Enabled	Bridge Oper Cisco	CIST Bridge ID	CIST Bridge Priority	CIST Reg Root ID
⬇	✗	✗	✗	✗	✗	1: CIST Bri	32,768	1: CIST Reg Root Id

MST Bridge Port Detail

	Name	Role	Send MSTP	State	Type	Admin BPDU Filter	Admin BPDU Guard	Admin Edge	Admin P2P MAC	Admin Root Guard
⬇	ge1	4	MSTP	Forwar	0	2	2	✗	✗	✗
⬇	ge10	4	STP	Forwar	0	2	2	✗	✗	✗
⬇	ge2	4	MSTP	Forwar	0	2	2	✗	✗	✗
⬇	ge3	4	MSTP	Forwar	0	2	2	✗	✗	✗

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.

7 Select **Refresh** to update the screen’s statistics counters to their latest values.

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 controller or service platform's DHCPv6 relay configuration:

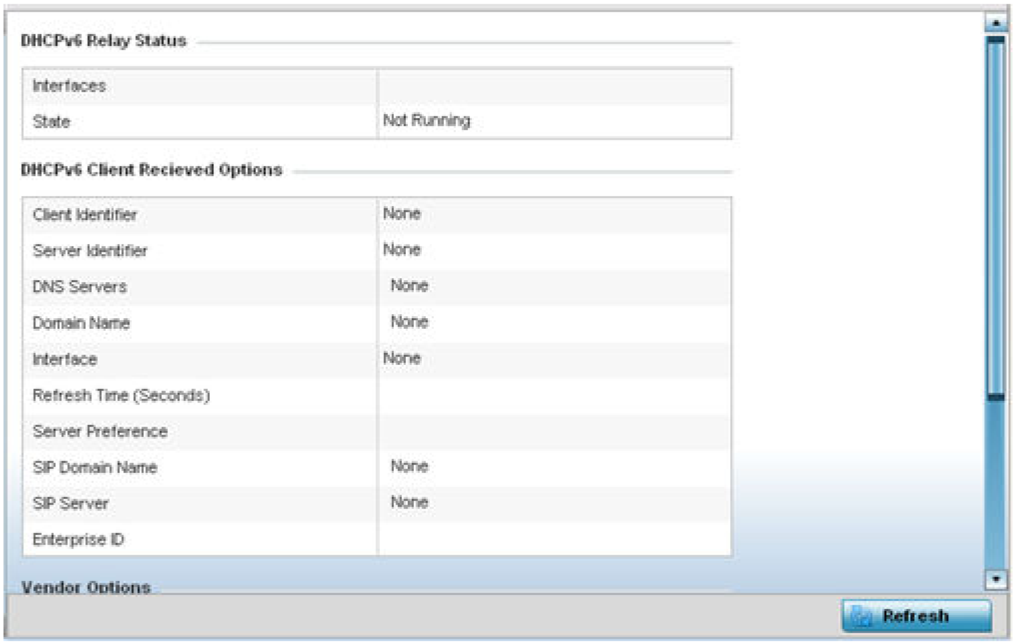
1 Select the **Statistics** menu from the Web UI.

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 the **RF Domain** node.

4 Select the **Wireless Controller** node from the left navigation pane.
5 Select **DHCP Relay & Client** from the left-hand side of the UI.

The **Statistics > Controller > DHCP Relay & Client** screen displays in the right-hand pane.



DHCPv6 Relay Status

Interfaces	
State	Not Running

DHCPv6 Client Recieved Options

Client Identifier	None
Server Identifier	None
DNS Servers	None
Domain Name	None
Interface	None
Refresh Time (Seconds)	
Server Preference	
SIP Domain Name	None
SIP Server	None
Enterprise ID	

Vendor Options

The DHCP Relay Status table defines the following:

Interfaces	Displays the controller or service platform 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.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

DHCP Server

Controllers and service platforms contain an internal DHCP *(Dynamic Host Configuration Protocol)* server. DHCP can provide IP addresses automatically to requesting devices. 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 host.

To review DHCP server statistics, refer to the following:

- Viewing General DHCP Information
- Viewing DHCP Binding Information
- Viewing DHCP Server Networks Information

Viewing General DHCP Information

To view General DHCP status and binding information:

1 Select the Statistics menu from the Web UI.

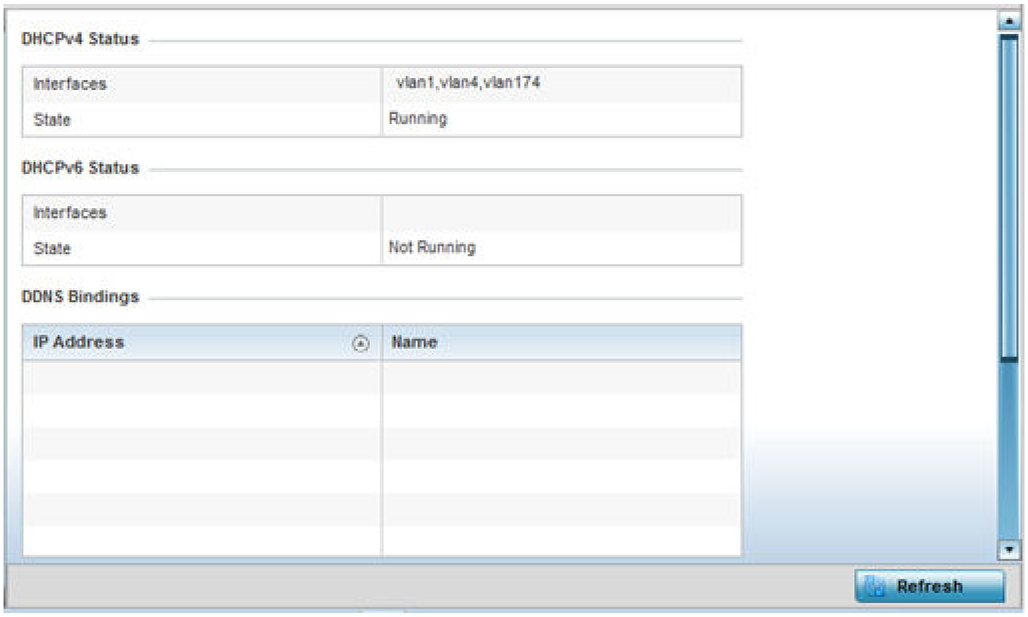
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand the **RF Domain** node.

4 Select a Wireless Controller.

5 Expand the DHCP Server menu from the left-hand side of the UI.

The **Statistics > Controller > DHCP Server > General** screen displays by default in the right-hand pane.



DHCPv4 Status

Interfaces	vlan1,vlan4,vlan174
State	Running

DHCPv6 Status

Interfaces	
State	Not Running

DDNS Bindings

IP Address	Name

The **DHCPv4 Status** and **DHCPv6 Status tables** defines the following:

Interfaces	Displays the controller or service platform 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.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

Viewing DHCP Binding Information

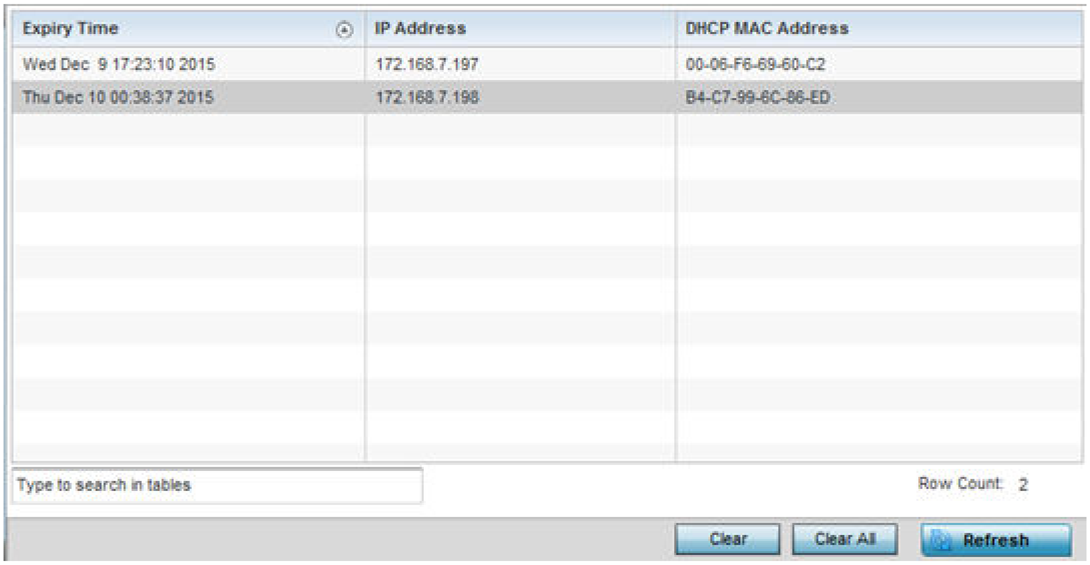
The **DHCP Binding** screen displays DHCP binding information such as expiry time, client IP addresses and their MAC address.

Controllers and service platforms build and maintain a DHCP snooping table (DHCP binding database). A controller or service platform 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 the DHCP 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **DHCP Server** menu from the left-hand side of the UI.
6 Select **Bindings.**

The **Statistics > Controller > DHCP Server > Bindings** screen displays by default in the right-hand pane.



Expiry Time	IP Address	DHCP MAC Address
Wed Dec 9 17:23:10 2015	172.168.7.197	00-06-F6-69-60-C2
Thu Dec 10 00:38:37 2015	172.168.7.198	B4-C7-99-6C-86-ED

Row Count: 2

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.

7 Select a table entry and select **Clear** to remove the client from the list of devices requesting DHCP services.
8 Select **Clear All** to remove all listed clients from the list of requesting clients.
9 Select the **Refresh** button to update the screen's statistics counters to their latest values.

Viewing DHCP Server Networks Information

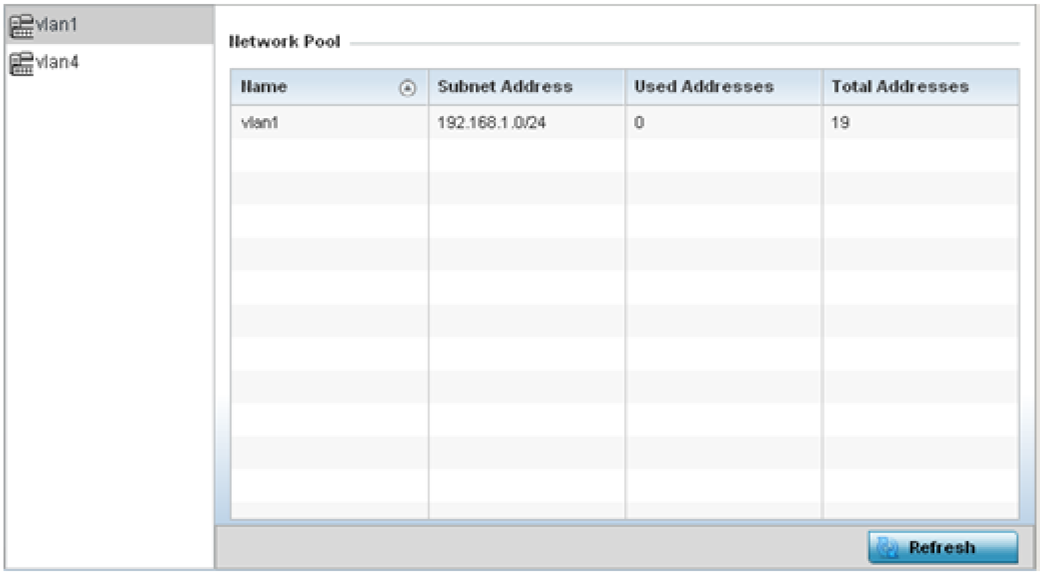
The DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers, etc). On receiving a valid client request, the server assigns the computer an IP address, a lease (the validity of time), and other IP configuration parameters.

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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **DHCP Server** menu from the left-hand side of the UI.
6. Select **Networks**.

   The **Statistics > Controller > DHCP Server > Networks** screen displays in the right-hand pane.



Name	Subnet Address	Used Addresses	Total Addresses
vlan1	192.168.1.0/24	0	19

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.

7. Select **Refresh** to update the screen's statistics counters to their latest values.

Firewall

A firewall is a part of a computer system or network designed to block unauthorized access while permitting authorized communications. It’s a device or set of devices configured to permit or deny access to the controller or service platform managed network based on a defined set of rules.

This screen is partitioned into the following:

- Viewing Packet Flow Statistics
- Viewing Denial of Service Statistics
- IP Firewall Rules
- MAC Firewall Rules

- NAT Translations
- Viewing DHCP Snooping Statistics

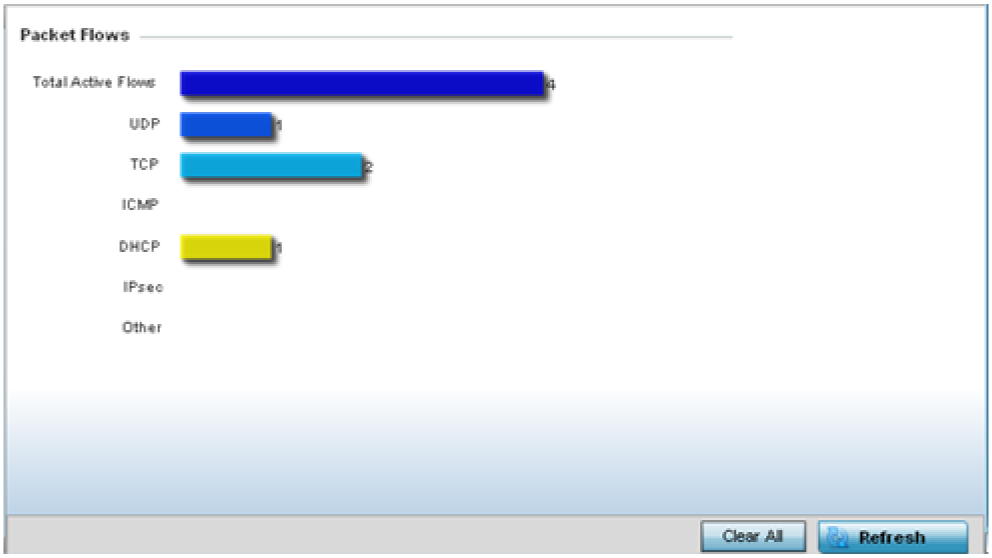
Viewing Packet Flow Statistics

The Packet Flows screen displays data traffic packet flow utilization. The chart lists 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 field displays the total number of flows supported by the controller.

To view the packet flow 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Firewall** menu from the left-hand side of the UI.
6. Select **Packets Flows**.

   The **Statistics > Controller > Firewall > Packet Flows** screen displays in the right-Hand pane.



7. 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.

Viewing Denial of Service Statistics

A DoS attack *(denial-of-service 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 a concerted effort to prevent an Internet site or service from functioning efficiently.

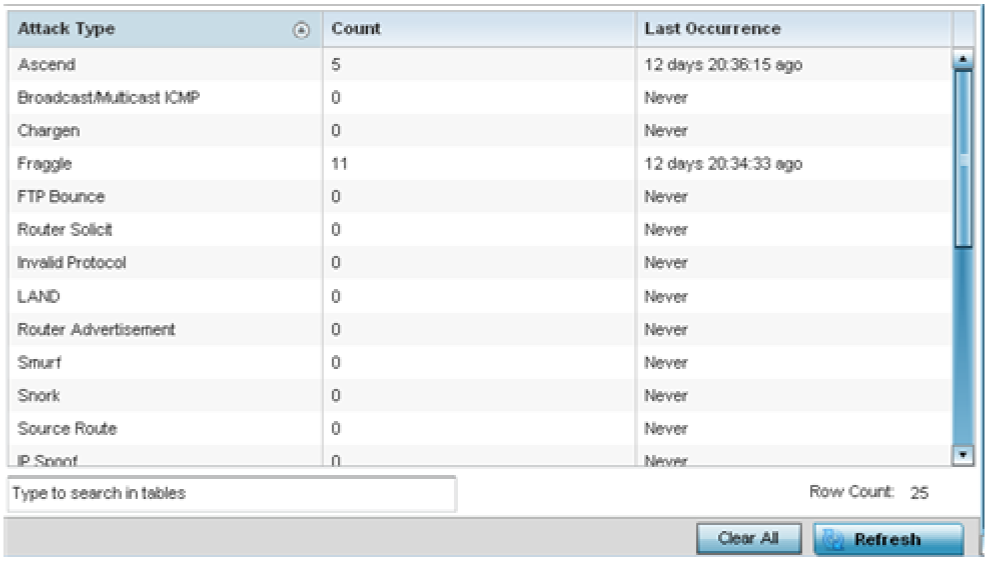
One common attack involves saturating the target's (victim's) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service.

The *Denial of Service* screen displays attack type, number of occurrences, and time of last occurrence.

To view the denial of 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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **Firewall** menu from the left-hand side of the UI.
6 Select **Denial of Service**.

The **Statistics > Controller > Firewall > Denial of Service** screen displays in the right-hand pane.



Attack Type	Count	Last Occurrence
Ascend	5	12 days 20:36:15 ago
Broadcast/Multicast ICMP	0	Never
Chargen	0	Never
Fraggle	11	12 days 20:34:33 ago
FTP Bounce	0	Never
Router Solicit	0	Never
Invalid Protocol	0	Never
LAND	0	Never
Router Advertisement	0	Never
Smurf	0	Never
Snork	0	Never
Source Route	0	Never
IP Spoof	0	Never

This screen displays the following:

Attack Type	Displays the DoS attack type. Controllers and service platforms support `enabling` or `disabling` 24 different DoS attack filters.
Count	Displays the number of times each DoS attack was observed by the controller or service platform's firewall.
Last Occurrence	Displays when the DoS attack was last observed by the controller or service platform's firewall.

7 Select **Clear All** to revert the statistics counters to zero and begin a new data collection.
8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

IP Firewall Rules

Create firewall rules to let any computer send IPv4 traffic to, or receive traffic from, programs, system services, computers or users. Firewall rules can be created to provide one of the three actions listed below that match the rule's criteria:

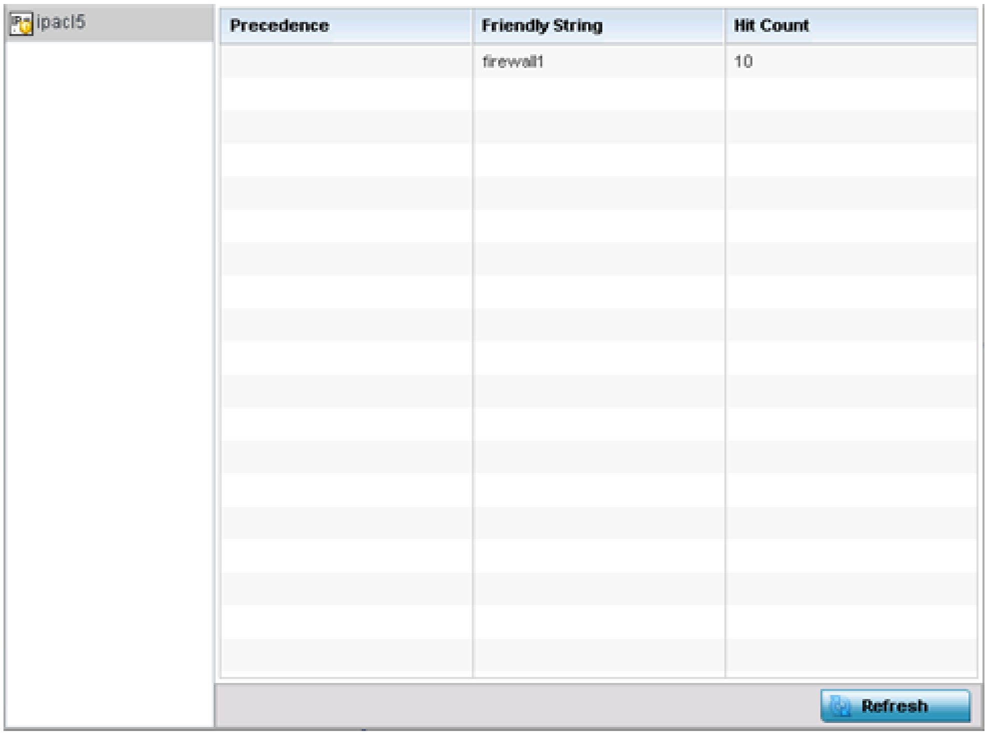
- *Allow a connection*.
- *Allow a connection only if it is secured through the use of Internet Protocol security*.
- *Block a connection*.

Rules can be created for either *inbound* or *outbound* traffic.

To view a controller or service platform's IPv4 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Firewall** menu from the left-hand side of the UI.
6. Select **IP Firewall Rules.**

   The **Statistics > Controller > Firewall > IP Firewall Rule** screen displays in the right-hand pane.



Precedence	Friendly String	Hit Count
	firewall1	10

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.

7. Select **Refresh** to update the screen's statistics counters to their latest values.

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 *(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.

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 a controller or service platform'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.

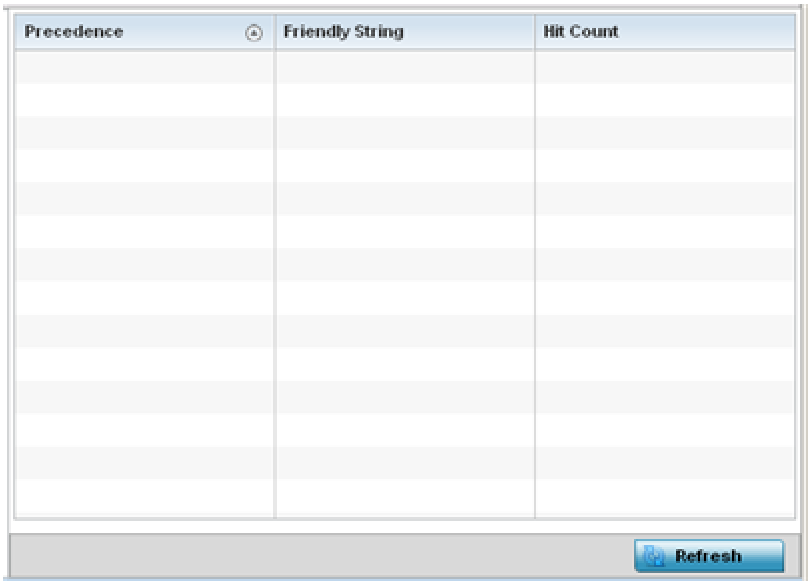
3 Expand the **RF Domain** node.

4 Select a **Wireless Controller**.

5 Expand the **Firewall** menu from the left-hand side of the UI.

6 Select **IPv6 Firewall Rules**.

The **Statistics > Controller > Firewall > IPv6 Firewall Rule** 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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

MAC Firewall Rules

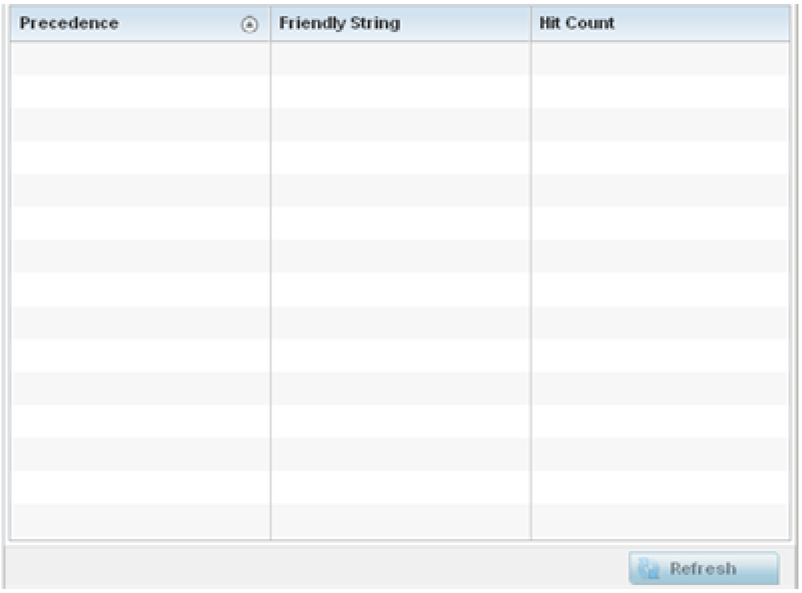
The ability to **`allow`** or **`deny`** client access by MAC address ensures malicious or unwanted users are unable to bypass security filters. Firewall rules can use one of the three following actions based on a rule criteria:

- *Allow a connection*.
- *Allow a connection only if it is secured through the MAC firewall security*.
- *Block a connection*.

To view a controller or service platform'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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Firewall** menu from the left-hand side of the UI.
6. Select **MAC Firewall Rules**.

   The **Statistics > Controller > 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 *(Access Control Entries)* 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.

7 Select **Refresh** to update the screen’s statistics counters to their latest values.

NAT Translations

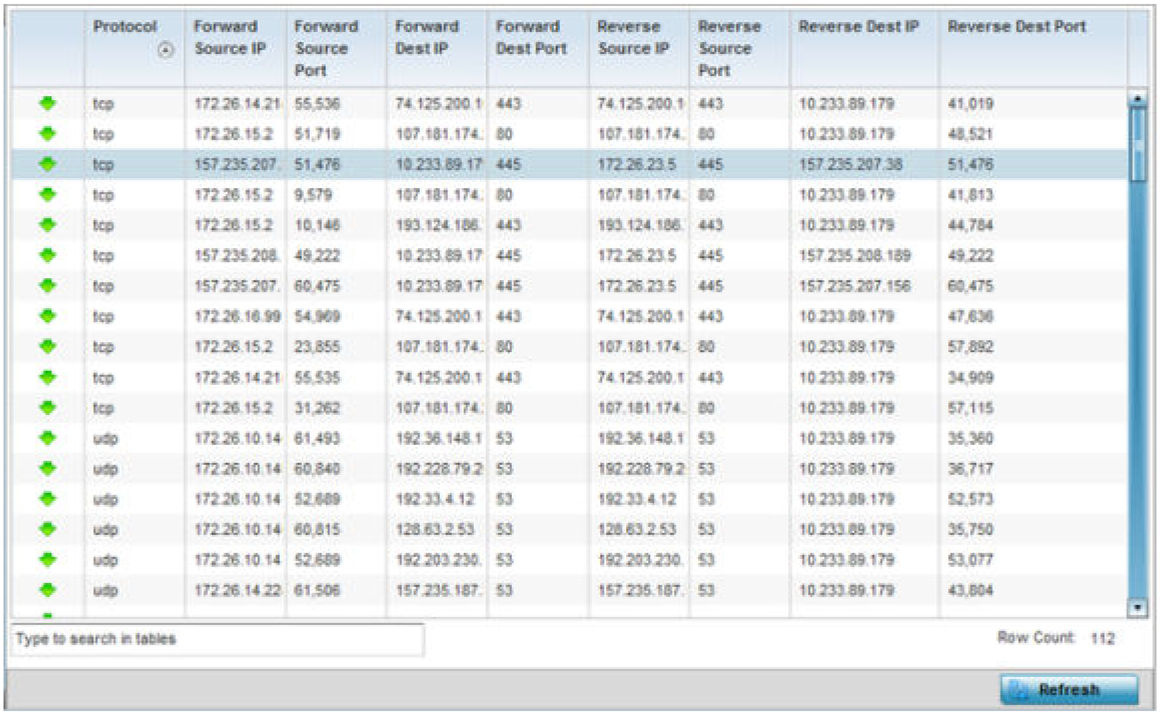
NAT *(Network address translation)* is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading 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 assess a controller or service platform's NAT 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Firewall** menu from the left-hand side of the UI.
6. Select **NAT Translations.**

   The **Statistics > Controller > Firewall > NAT Translations** screen displays in the right-hand pane.



Protocol	Forward Source IP	Forward Source Port	Forward Dest IP	Forward Dest Port	Reverse Source IP	Reverse Source Port	Reverse Dest IP	Reverse Dest Port
tcp	172.26.14.21	55,536	74.125.200.1	443	74.125.200.1	443	10.233.89.179	41,019
tcp	172.26.15.2	51,719	107.181.174.	80	107.181.174.	80	10.233.89.179	48,521
tcp	157.235.207.	51,476	10.233.89.17	445	172.26.23.5	445	157.235.207.38	51,476
tcp	172.26.15.2	9,579	107.181.174.	80	107.181.174.	80	10.233.89.179	41,813
tcp	172.26.15.2	10,146	193.124.186.	443	193.124.186.	443	10.233.89.179	44,784
tcp	157.235.208.	49,222	10.233.89.17	445	172.26.23.5	445	157.235.208.189	49,222
tcp	157.235.207.	60,475	10.233.89.17	445	172.26.23.5	445	157.235.207.156	60,475
tcp	172.26.16.99	54,969	74.125.200.1	443	74.125.200.1	443	10.233.89.179	47,636
tcp	172.26.15.2	23,855	107.181.174.	80	107.181.174.	80	10.233.89.179	57,892
tcp	172.26.14.21	55,535	74.125.200.1	443	74.125.200.1	443	10.233.89.179	34,909
tcp	172.26.15.2	31,262	107.181.174.	80	107.181.174.	80	10.233.89.179	57,115
udp	172.26.10.14	61,493	192.36.148.1	53	192.36.148.1	53	10.233.89.179	35,360
udp	172.26.10.14	60,840	192.228.79.2	53	192.228.79.2	53	10.233.89.179	36,717
udp	172.26.10.14	52,689	192.33.4.12	53	192.33.4.12	53	10.233.89.179	52,573
udp	172.26.10.14	60,815	128.63.2.53	53	128.63.2.53	53	10.233.89.179	35,750
udp	172.26.10.14	52,689	192.203.230.	53	192.203.230.	53	10.233.89.179	53,077
udp	172.26.14.22	61,506	157.235.187.	53	157.235.187.	53	10.233.89.179	43,804

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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

DHCP Snooping Statistics

When DHCP servers are allocating IP addresses to requesting clients, DHCP snooping can further strengthen the security on the LAN by allowing only clients with specific IP/MAC addresses.

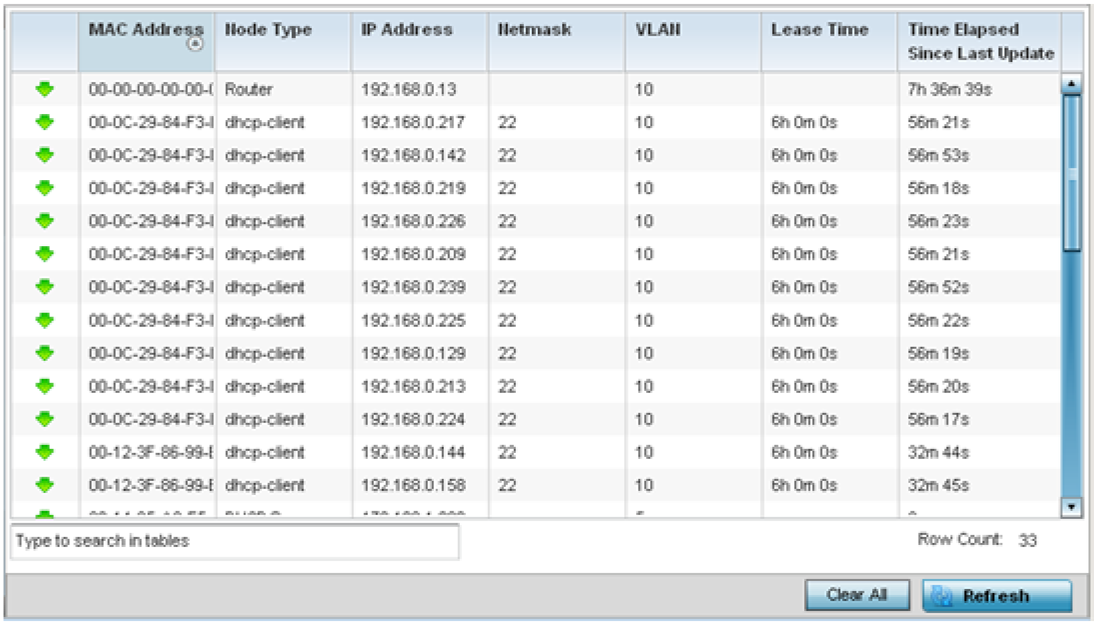
To view the DHCP snooping statistics:

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 the **RF Domain** node.
4 Select a **Wireless Controller**.

5 Expand the **Firewall** menu from the left-hand side of the UI.

6 Select **DHCP Snooping.**

The **Statistics > Controller > Firewall > DHCP Snooping** screen displays in the right-hand pane.



MAC Address	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since Last Update
00-00-00-00-00-	Router	192.168.0.13		10		7h 36m 39s
00-0C-29-84-F3-	dhcp-client	192.168.0.217	22	10	6h 0m 0s	56m 21s
00-0C-29-84-F3-	dhcp-client	192.168.0.142	22	10	6h 0m 0s	56m 53s
00-0C-29-84-F3-	dhcp-client	192.168.0.219	22	10	6h 0m 0s	56m 18s
00-0C-29-84-F3-	dhcp-client	192.168.0.226	22	10	6h 0m 0s	56m 23s
00-0C-29-84-F3-	dhcp-client	192.168.0.209	22	10	6h 0m 0s	56m 21s
00-0C-29-84-F3-	dhcp-client	192.168.0.239	22	10	6h 0m 0s	56m 52s
00-0C-29-84-F3-	dhcp-client	192.168.0.225	22	10	6h 0m 0s	56m 22s
00-0C-29-84-F3-	dhcp-client	192.168.0.129	22	10	6h 0m 0s	56m 19s
00-0C-29-84-F3-	dhcp-client	192.168.0.213	22	10	6h 0m 0s	56m 20s
00-0C-29-84-F3-	dhcp-client	192.168.0.224	22	10	6h 0m 0s	56m 17s
00-12-3F-86-99-	dhcp-client	192.168.0.144	22	10	6h 0m 0s	32m 44s
00-12-3F-86-99-	dhcp-client	192.168.0.158	22	10	6h 0m 0s	32m 45s

This screen displays the following information:

MAC Address	Displays the MAC address of the client.
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 controller or service platform virtual interface ID 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.

7 Select **Clear All** to revert the counters to zero and begin a new data collection.

8 Select **Refresh** to update the screen's counters to their latest values

IPv6 Neighbor Snooping

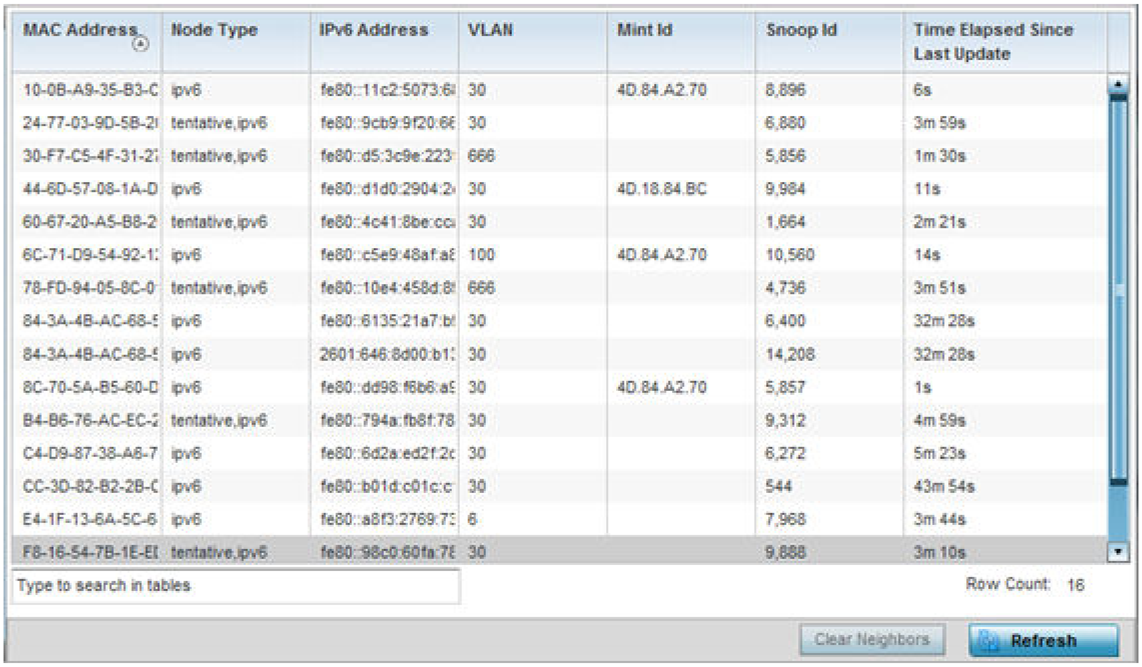
IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 ND *(neighbor discovery)* inspection, IPv6 address gleaning and IPv6 device tracking. When IPv6 ND is configured on a device, packet capture instructions redirect the ND protocol and DHCP for IPv6 traffic up to the controller for 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.

To review IPv6 neighbor snooping statistics:

1 Select the **Statistics** menu from the Web UI.
2 Expand the **RF Domain** node.
3 Select a **Wireless Controller**.
4 Expand the **Firewall** menu from the left-hand side of the UI.
5 Select **IPv6 Neighbor Snooping**.

The **Statistics > Controller > Firewall > IPv6 Neighbor Snooping** screen displays in the right-hand pane.



MAC Address	Node Type	IPv6 Address	VLAN	Mint Id	Snoop Id	Time Elapsed Since Last Update
10-0B-A9-35-B3-C	ipv6	fe80::11c2:5073:6	30	4D.84.A2.70	8,896	6s
24-77-03-9D-5B-2	tentative,ipv6	fe80::9cb9:9f20:6	30		6,880	3m 59s
30-F7-C5-4F-31-2	tentative,ipv6	fe80::d5:3c9e:223	666		5,856	1m 30s
44-6D-57-08-1A-D	ipv6	fe80::d1d0:2904:2	30	4D.18.84.BC	9,984	11s
60-67-20-A5-B8-2	tentative,ipv6	fe80::4c41:8be:cc	30		1,664	2m 21s
6C-71-D9-54-92-1	ipv6	fe80::c5e9:48af:a	100	4D.84.A2.70	10,560	14s
78-FD-94-05-8C-0	tentative,ipv6	fe80::10e4:458d:8	666		4,736	3m 51s
84-3A-4B-AC-68-	ipv6	fe80::6135:21a7:b	30		6,400	32m 28s
84-3A-4B-AC-68-	ipv6	2601:646:8d00:b1	30		14,208	32m 28s
8C-70-5A-B5-60-D	ipv6	fe80::dd98:f6b6:a	30	4D.84.A2.70	5,857	1s
B4-B6-76-AC-EC-	tentative,ipv6	fe80::794a:fb8f:78	30		9,312	4m 59s
C4-D9-87-38-A6-7	ipv6	fe80::6d2a:ed2f:2	30		6,272	5m 23s
CC-3D-82-B2-2B-	ipv6	fe80::b01d:c01c:c	30		544	43m 54s
E4-1F-13-6A-5C-6	ipv6	fe80::a8f3:2769:7	6		7,968	3m 44s
F8-16-54-7B-1E-E	tentative,ipv6	fe80::98c0:60fa:7	30		9,888	3m 10s

Row Count: 16

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 a numeric snooping ID associated with each packet inspection snooping session conducted by the controller or service platform.
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.

VPN

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 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 *(security associations)* 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 *(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 pre-configuration.

VPN statistics are partitioned into the following:

- IKESA
- IPSec

IKESA

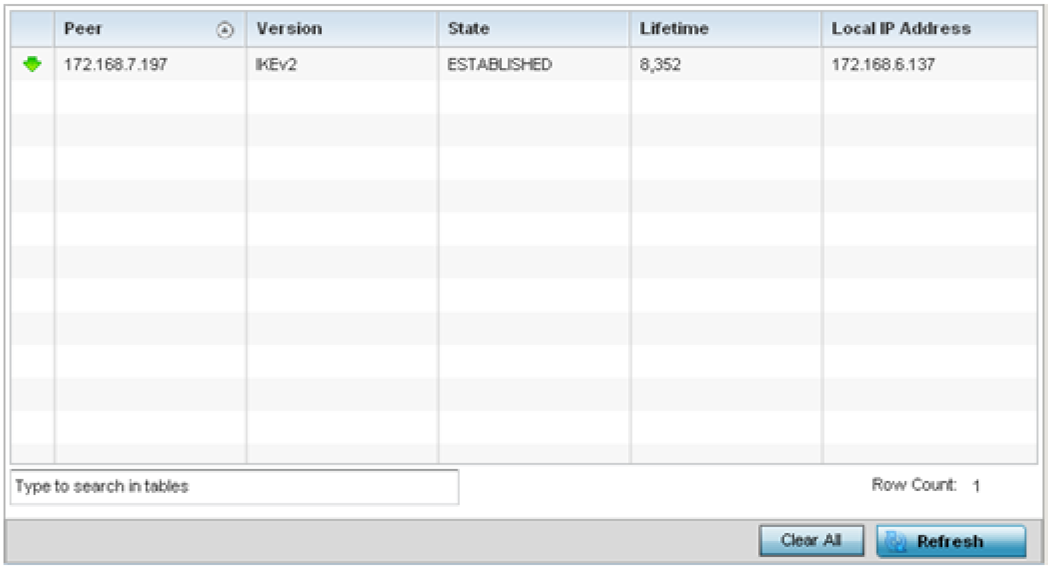
The IKESA screen allows for the review of individual peer security association statistics.

To view controller or service platform'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 the **RF Domain** node.

4 Select a **Wireless Controller**.
5 Expand the **VPN** menu.
6 Select **IKESA**.

The **Statistics > Controller > VPN > IKESA** screen displays in the right-hand pane.



	Peer	Version	State	Lifetime	Local IP Address
●	172.168.7.197	IKEv2	ESTABLISHED	8,352	172.168.6.137

Type to search in tables

Row Count: 1

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.

7 Select a IKE peer configuration and click **Clear** to remove the peer from the table.
8 Select **Clear All** to clear each peer of its current status and begin a new data collection.
9 Select **Refresh** to update the screen's statistics counters to their latest values.

IPSec

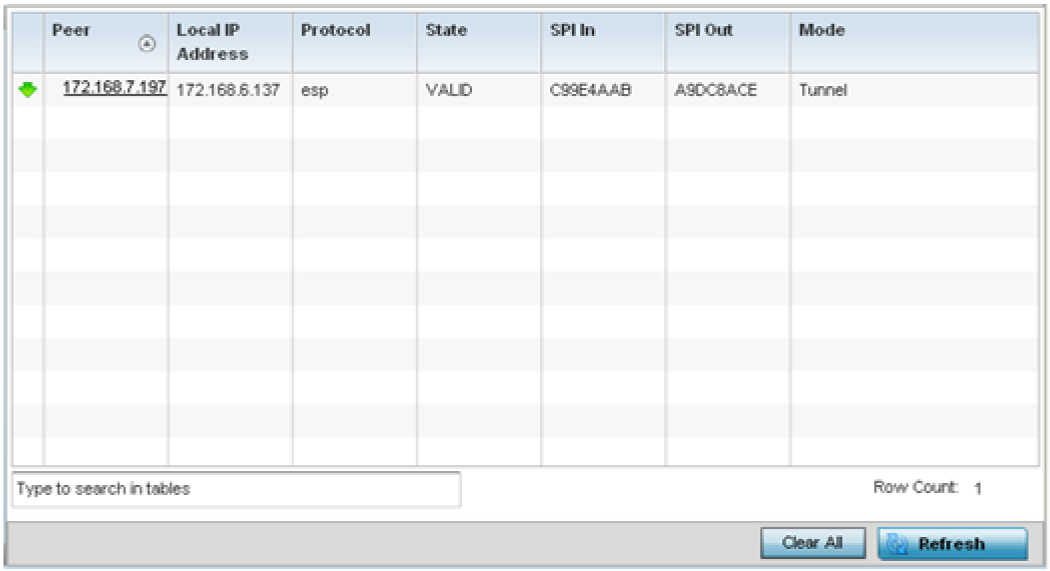
IPSec provides a secure tunnel between two networked peer controllers or service platforms. Administrators can define which packets are sent within the tunnel, and how they are protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Use the IPSec VPN screen to assess the tunnel status between networked peers.

To view IPSec VPN status for tunneled peers:

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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **VPN** menu.
6. Select **IPSec**.

   The **Statistics > Controller > VPN > IPsec** screen displays in the right-hand pane.



	Peer	Local IP Address	Protocol	State	SPI In	SPI Out	Mode
◆	172.168.7.197	172.168.6.137	esp	VALID	C99E4AAB	A9DC8ACE	Tunnel

Type to search in tables

Row Count: 1

   Review the following VPN peer security association statistics:

Peer	Lists IP addresses 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 *(stateful packet inspection)* 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.

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.

Certificate Statistics

The SSL *(Secure Socket Layer)* protocol ensures secure transactions between Web servers and browsers. This protocol uses a third-party, a certificate authority, to identify one end or both ends of the transactions. A browser checks the certificate issued by the server before establishing a connection.

For more information, see:

- Trustpoints on page 1175
- RSA Key Details on page 1177

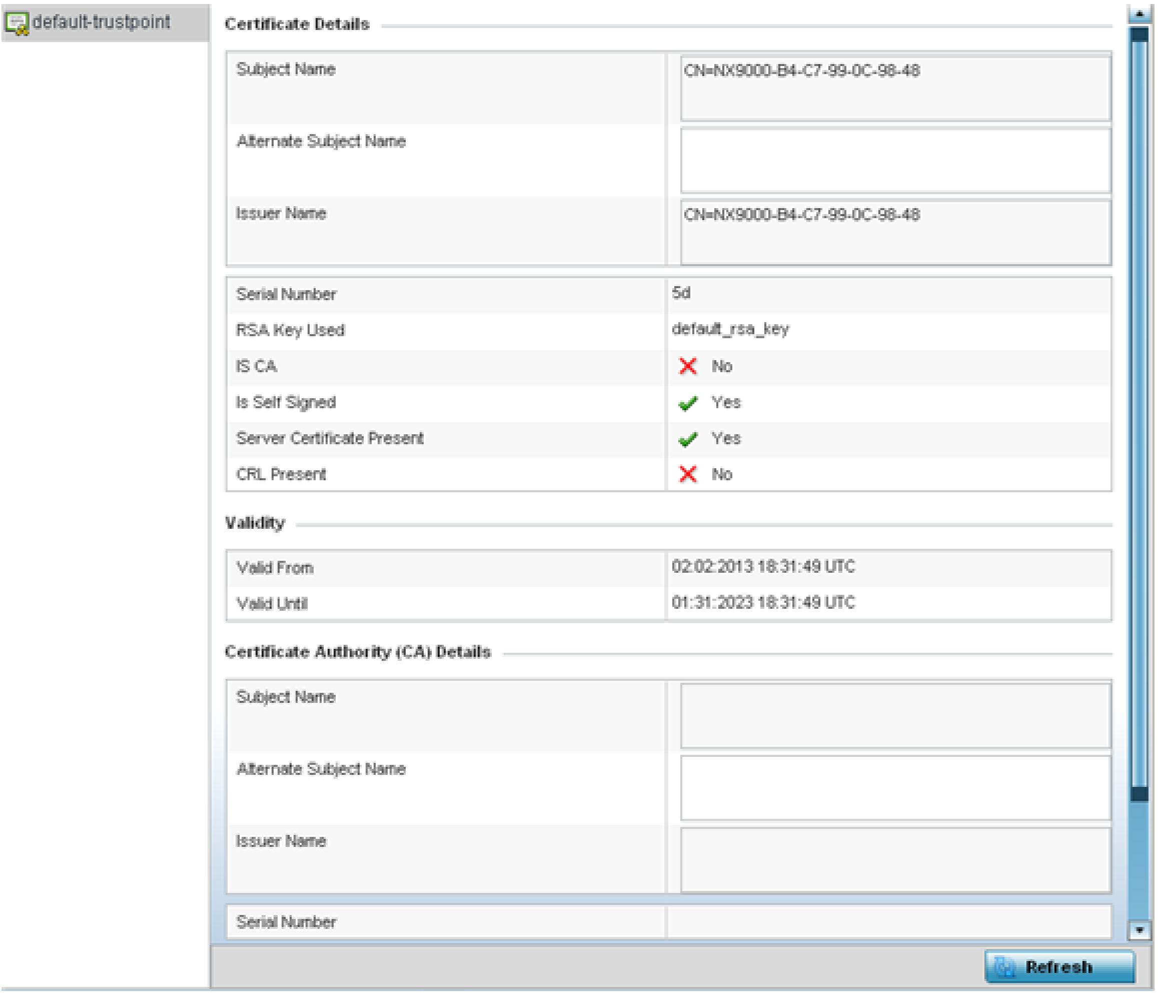
Trustpoints

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.

To view trustpoint 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Certificate** menu.
6. Select **Trustpoint**.

   The **Statistics > Controller > Certificates > Trustpoints** screen displays in the right-hand pane.



Certificate Details

Subject Name	CN=NX9000-B4-C7-99-0C-98-48
Alternate Subject Name	
Issuer Name	CN=NX9000-B4-C7-99-0C-98-48

Serial Number	5d
RSA Key Used	default_rsa_key
IS CA	✗ No
Is Self Signed	✓ Yes
Server Certificate Present	✓ Yes
CRL Present	✗ No

Validity

Valid From	02:02:2013 18:31:49 UTC
Valid Until	01:31:2023 18:31:49 UTC

Certificate Authority (CA) Details

Subject Name	
Alternate Subject Name	
Issuer Name	
Serial Number	

This screen has the following elements:

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 *(Certificate Revocation List)* 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.

7. Select **Refresh** to update the screen's statistics counters to their latest values.

RSA Key Details

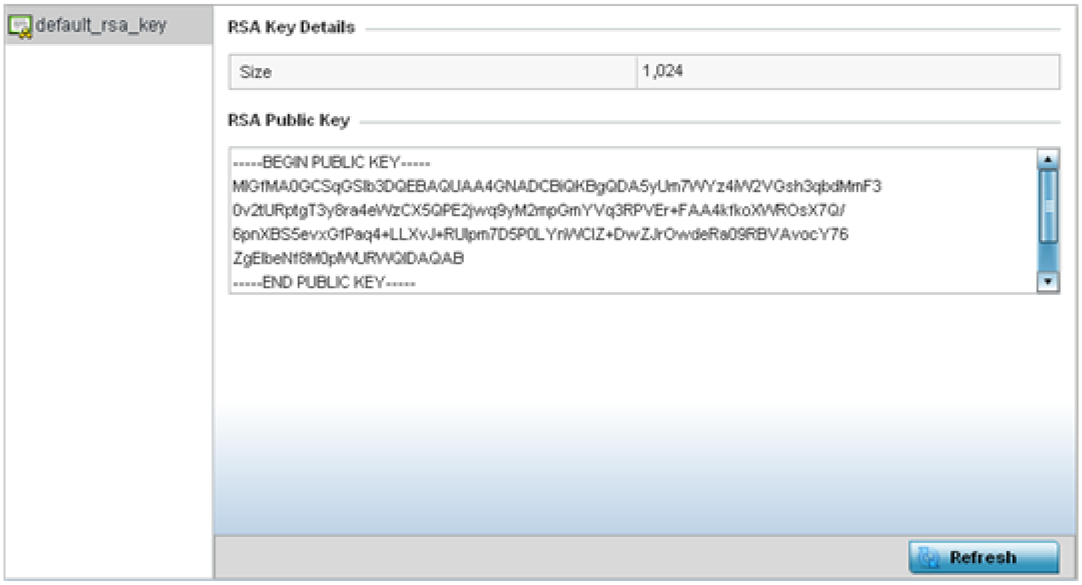
RSA *(Rivest, Shamir, and Adleman)* is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing as well as encryption.

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 controller or service platform'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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Certificate** menu.
6. Select **RSA Keys**.

The **Statistics > Controller > Certificates > RSA Key** screen displays.



RSA Key Details

Size	1,024

RSA Public Key

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5yUm7WYz4W2VGsh3qbdMmF3
0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4kfkoXWROsX7Q/
6pnXBS5evxG1Paq4+LLXvJ+RUlpm7D5P0LYnWCIZ+DwZJrOwdeRa09RBVAvocY76
ZgElbeNf8M0pMURWQIDAQAB
-----END PUBLIC KEY-----
```

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.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

WIPS Statistics

A WIPS *(Wireless Intrusion Protection System)* detects the presence of unauthorized access points. Unauthorized attempts to access the WLAN is generally accompanied by intruding clients finding network vulnerabilities. Basic forms of this behavior can be monitored and reported without a dedicated WIPS deployment. When the parameters exceed a configurable threshold, the controller or service platform generates a SNMP trap and reports the result via the management interfaces. Basic WIPS functionality does not require monitoring APs and does not perform off-channel scanning.

For more information, see:

- Client Blacklist on page 1178
- WIPS Event Statistics on page 1179

Client Blacklist

The Client Blacklist screen displays blacklisted clients detected using WIPS. Blacklisted clients are not allowed to associate to connected devices within the controller or service platform managed network.

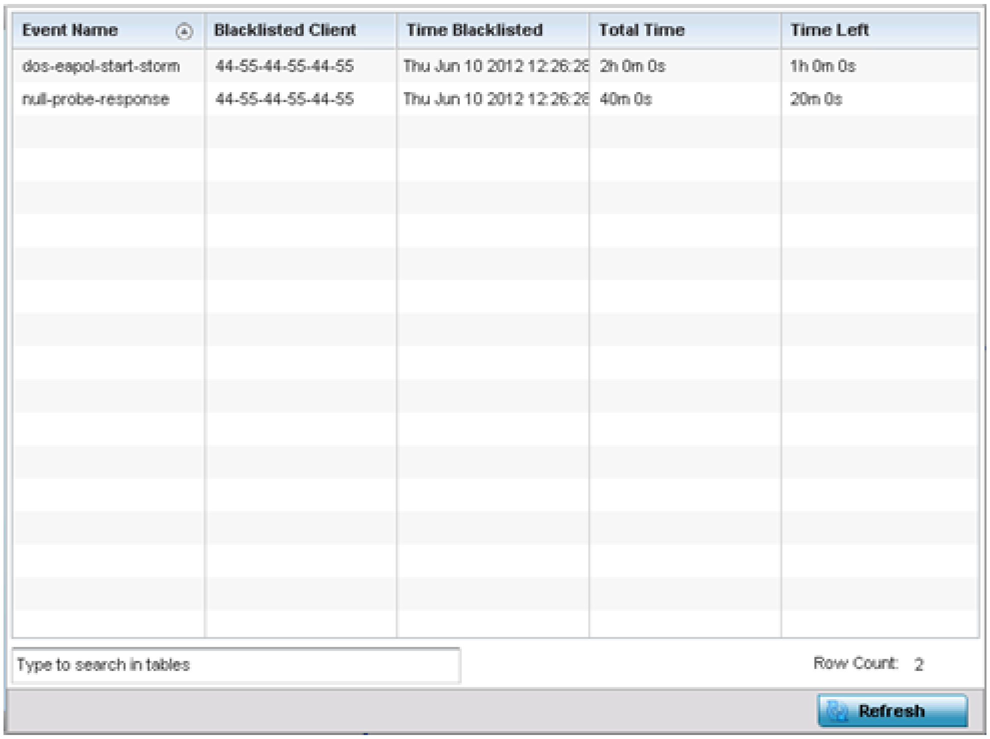
To view the controller or service platform's client blacklist screen:

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 the **RF Domain** node.
4 Select a **Wireless Controller**.
5 Expand the **WIPS** menu.
6 Select **Client Blacklist**.

The **Statistics > Controller > WIPS > Client Blacklist** screen displays in the right-hand pane.



Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-eapol-start-storm	44-55-44-55-44-55	Thu Jun 10 2012 12:26:2	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2012 12:26:2	40m 0s	20m 0s

This screen displays the following:

Event Name	Displays the name of the detected wireless intrusion resulting in a blacklisting of the client from controller or service platform resources.
Blacklisted Client	Displays the MAC address of the intruding client device pending exclusion from the controller or service platform managed network.
Time Blacklisted	Displays the time this client was blacklisted from interoperating with known and trusted devices within the wireless network.
Total Time	Displays the duration the unauthorized device remained in the WLAN before being blacklisted.
Time Left	Displays the time the blacklisted client remains on the list.

7 Select **Refresh** to update the screen's statistics counters to their latest values.

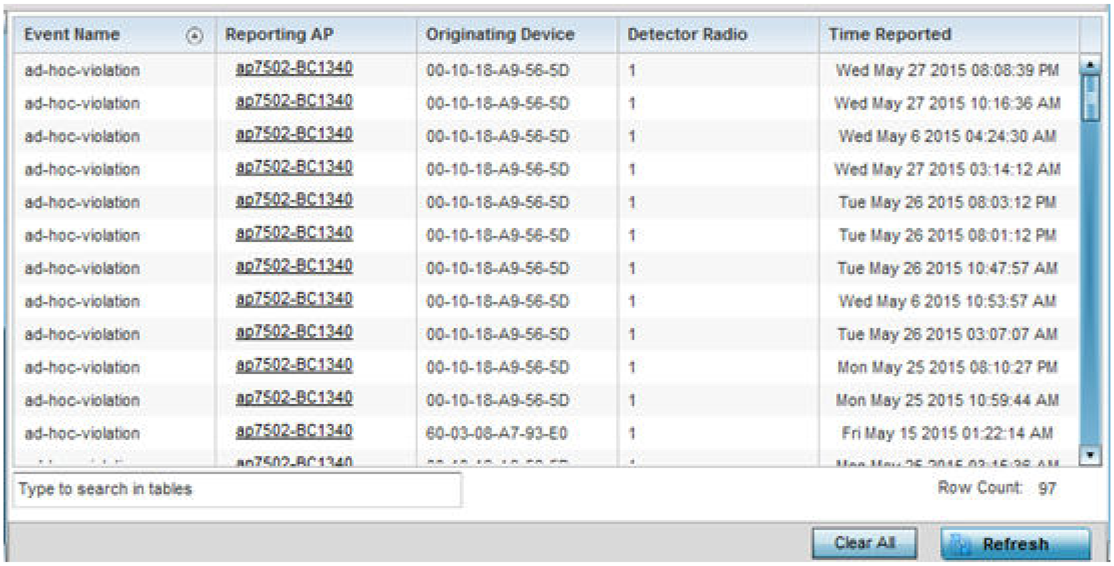
WIPS Event Statistics

The WIPS Events screen displays event information for rogue access point intrusions within the controller or service platform managed network.

To view WIPS event 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **WIPS** menu.
6. Select **WIPS Events**.

   The **Statistics > Controller > WIPS > WIPS Events** screen displays in the right-hand pane.



Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	ap7502-BC1340	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

Type to search in tables

Row Count: 97

This screen displays the following information:

Event Name	Displays the name of the detected 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 which AP radio is making the intrusion detection.
Time Reported	Displays the time when the intrusion event was detected.

7. Select **Clear All** to reset the statistics counters to zero and begin a new data collection.
8. Select **Refresh** to update the screen's statistics counters to their latest values.

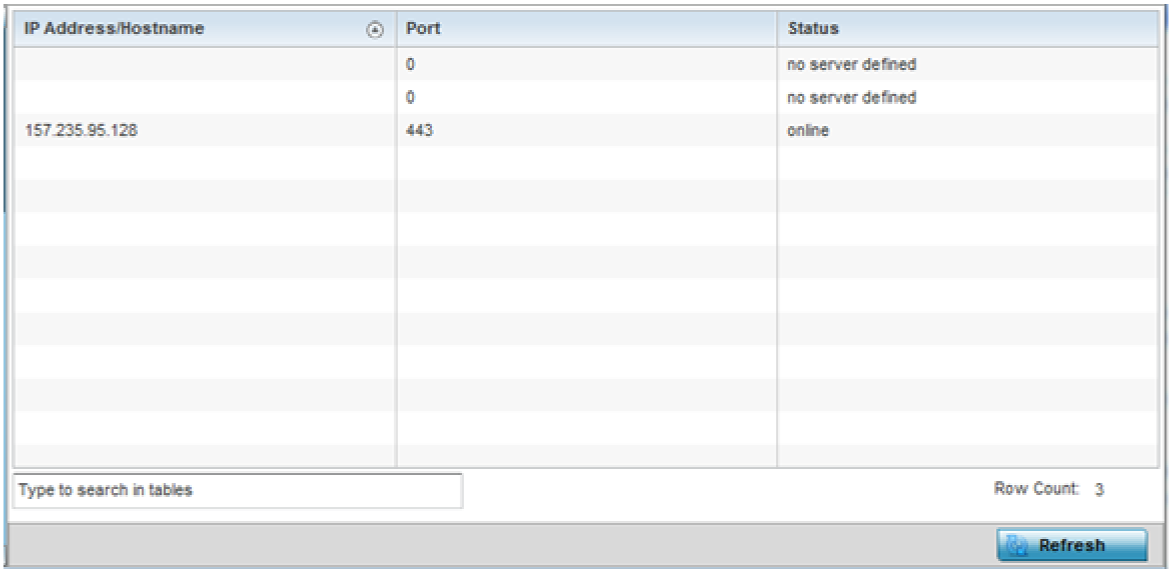
Sensor Server

Sensor servers allow the monitor and download of device authorization data from multiple sensors and remote locations using Ethernet, TCP/IP or serial connections. Repeaters are available to extend the transmission range and combine sensors with various frequencies on the same receiver, thus extending the Advanced WIPS supported reporting range.

To view the Sensor Server statistics:

1. Select the **Statistics** → **System** menu from the Web UI.
2. Expand **RF Domain** and select **Wireless Controller**.
3. Select **Sensor Servers** from the left-hand side of the UI.

   The Sensor Servers screen displays.



IP Address/Hostname	Port	Status
	0	no server defined
	0	no server defined
157.235.95.128	443	online

4. Review the following configuration details:

IP Address	Displays a list of sensor server IP addresses. These are sensor resources available to the controller or service platform.
Port	Displays the port on which this server is listening.
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

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:

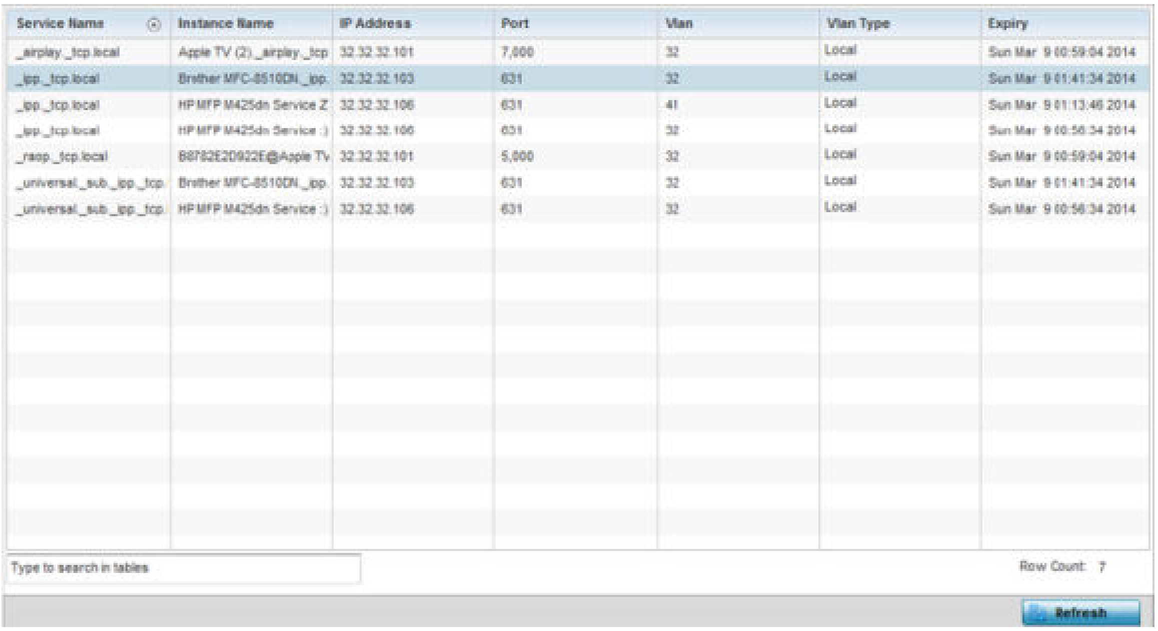
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node from the navigation pane (on the left-hand side of the screen).

   The System node expands to display the RF Domains created within the managed network.
3. Expand the **RF Domain** node.

4 Select a **Wireless Controller**.

5 Select **Bonjour Services** from the left-hand side of the UI.

The **Statistics > Controller > Bonjour Services** screen displays.



Service Name	Instance Name	IP Address	Port	Vlan	Vlan Type	Expiry
_airplay._tcp.local	Apple TV (2)._airplay._tcp	32.32.32.101	7,000	32	Local	Sun Mar 9 00:59:04 2014
_ipp._tcp.local	Brother MFC-8510DN._ipp.	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_ipp._tcp.local	HP MFP M425dn Service Z	32.32.32.106	631	41	Local	Sun Mar 9 01:13:46 2014
_ipp._tcp.local	HP MFP M425dn Service :)	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014
_raop._tcp.local	B8782E2D922E@Apple Tv	32.32.32.101	5,000	32	Local	Sun Mar 9 00:59:04 2014
_universal._sub._ipp._tcp	Brother MFC-8510DN._ipp.	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_universal._sub._ipp._tcp	HP MFP M425dn Service :)	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014

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.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

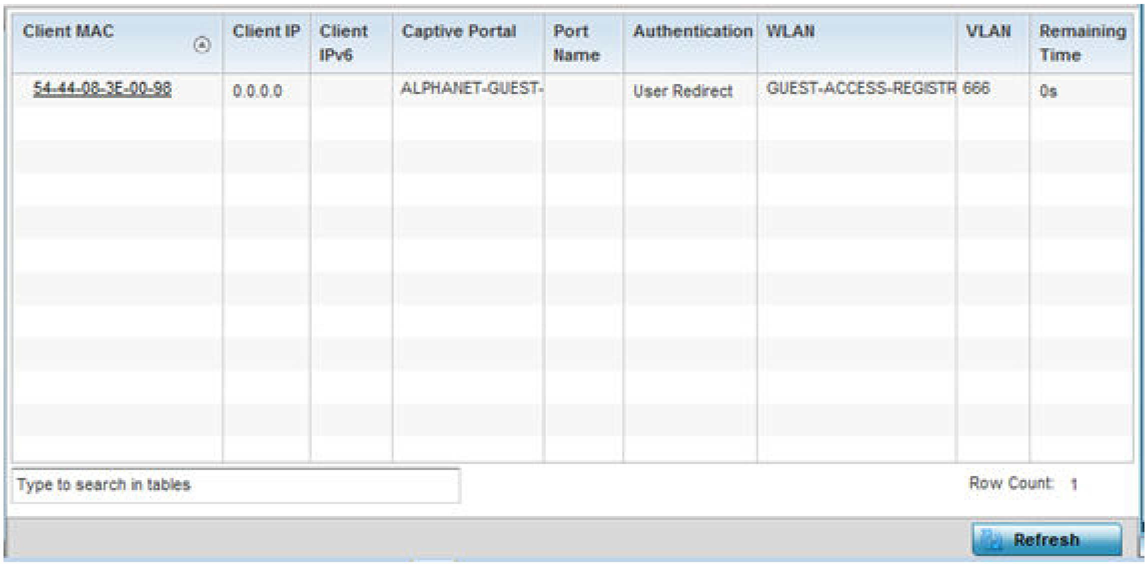
Captive Portal Statistics

A captive portal redirects an HTTP client to a Web page (usually for authentication purposes) before authenticating for Internet access. A captive portal turns a Web browser into an authenticator. This is done by intercepting packets (regardless of the address or port) until the user opens a browser and attempts to access the Internet. At that time, the browser is redirected to a Web page requiring authentication.

To view the 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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **WIPS** menu.
6. Select **Captive Portal** from the left-hand side of the controller UI.

   The **Statistics > Controller > Captive Portal** screen displays.



Client MAC	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
54-44-08-3E-00-98	0.0.0.0		ALPHANET-GUEST-		User Redirect	GUEST-ACCESS-REGISTR	666	0s

Row Count: 1

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 formatted address.
Client IPv6	Displays the requesting client's IPv6 formatted address.
Captive Portal	Displays the captive portal name that each listed client is utilizing for guest access to network 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 a virtual interface for captive portal sessions.
Remaining Time	Displays the time after which the client is disconnected from the captive portal managed Internet.

7. Select **Refresh** to update the screen's statistics counters to their latest values.

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:

- NTP Status on page 1184.
- NTP Association on page 1185.

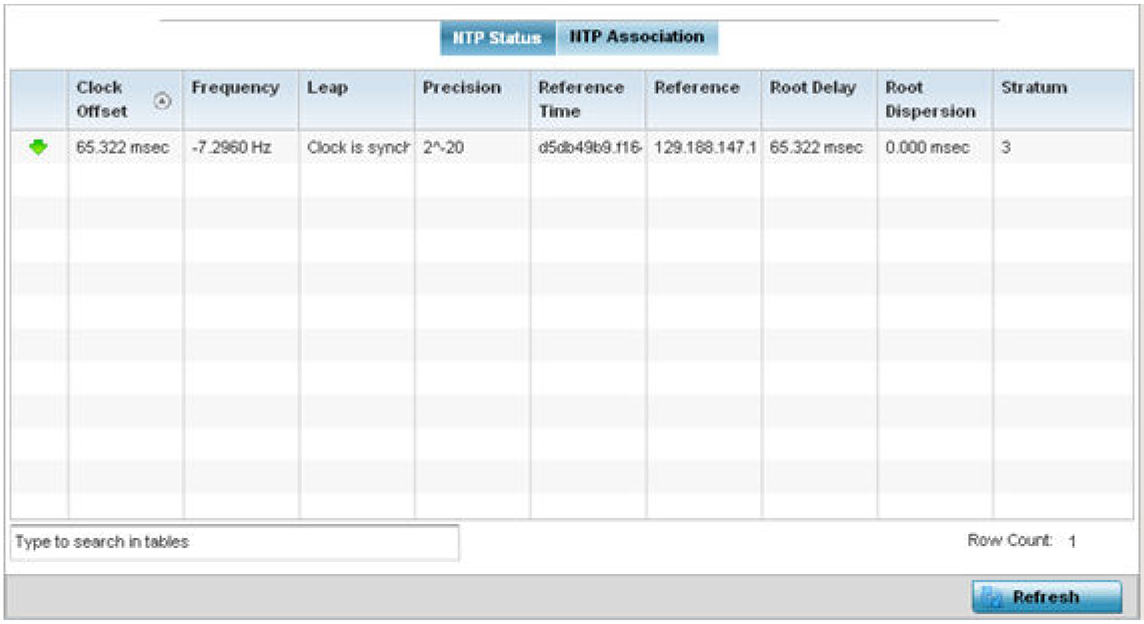
NTP Status

The **NTP Status** screen displays performance (status) information relative to the NTP association status. Verify NTP status to assess the controller or service platform's current NTP resource.

To view the NTP status of a controller or service platform managed network:

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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Network Time** menu.

   The **Statistics > Controller > Network Time > NTP Status** screen displays by default.



	Clock Offset	Frequency	Leap	Precision	Reference Time	Reference	Root Delay	Root Dispersion	Stratum
	65.322 msec	-7.2960 Hz	Clock is synch	2^-20	d5db49b9.f16-	129.188.147.1	65.322 msec	0.000 msec	3

Refer to the NTP Status table to review the accuracy and performance of the synchronization with a NTP server resource.

Clock Offset	Displays the time differential between the controller or service platform time and the NTP resource's time.
Frequency	An SNTP server clock's skew (difference) for the controller or service platform and the dedicated NTP resource.
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 local clock was last set or corrected.
Reference	Displays the address of the time source the controller or service platform 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 it's reference clock. The reference clock is the clock used by the NTP server to set its own clock.
Stratum	Displays how many hops the controller or service platform is from its current NTP time source.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

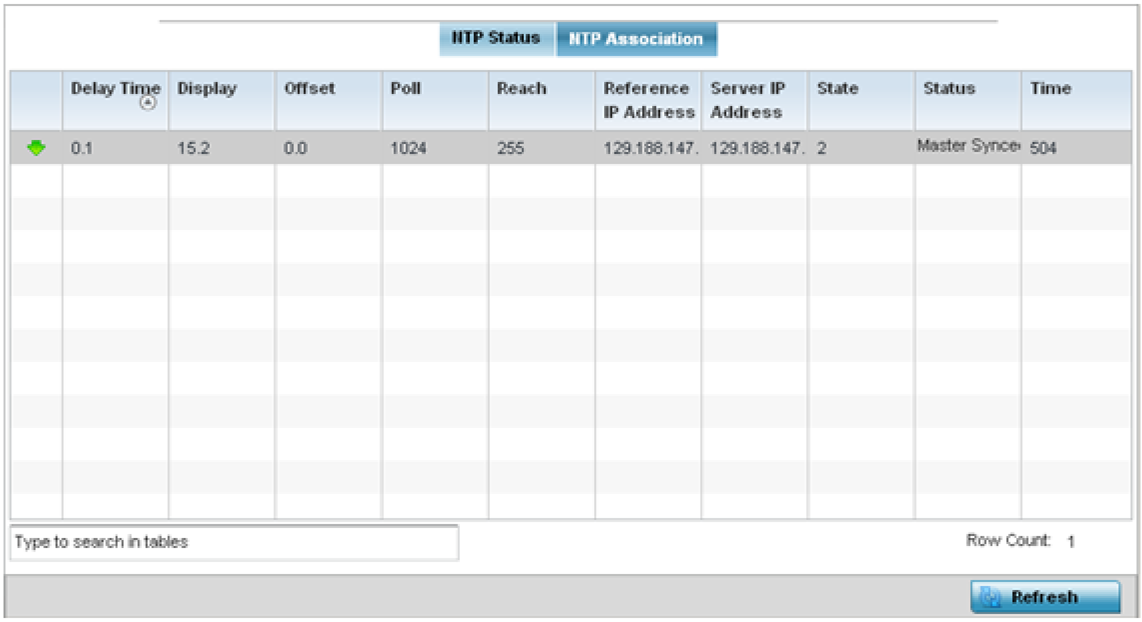
NTP Association

The interaction between the controller or service platform and a SNTP server constitutes an *association*. SNTP associations can be either *peer* associations (a controller or service platform synchronizes to another system or allows another system to synchronize to it), or a *server* associations (only the controller or service platform synchronizes to the SNTP resource, not the other way around).

To view the controller or service platform's NTP associations:

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 the **RF Domain** node.
4. Select a **Wireless Controller**.
5. Expand the **Network Time** and expand the menu to reveal its sub menu items.
6. Select **NTP Association**.

The **Statistics > Controller > Network Time > NTP Association** screen displays.



	Delay Time	Display	Offset	Poll	Reach	Reference IP Address	Server IP Address	State	Status	Time
▼	0.1	15.2	0.0	1024	255	129.188.147.	129.188.147.	2	Master Synce	504

Row Count: 1

This screen provides the controller or service platform's current NTP associations:

Delay Time	Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP server and the controller or service platform.
Display	Displays the time difference between the peer NTP server and the onboard wireless controller clock.
Offset	Displays the calculated offset between the controller and the SNTP server. The controller adjusts its clock to match the server's time. The offset gravitates towards zero overtime, 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 IP address of the time source the controller or service platform is synchronized to.
Server IP Address	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the controller or service platform.
State	Displays the NTP association status. The state can be one of the following: • `Synced` – Indicates the controller or service platform is synchronized to this NTP server. • `Unsynced` – Indicates the controller or service platform has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC. • `Selected` – Indicates this NTP master server will be considered the next time the controller or service platform chooses a new master to synchronize with. • `Candidate` – Indicates this NTP master server may be considered for selection the next time the controller or service platform chooses a NTP master server. • `Configured` – Indicates this NTP server is a configured server.

Status	Displays the NTP peer's current status.
Time	Displays the timestamp of the last NTP packet received from the NTP peer.

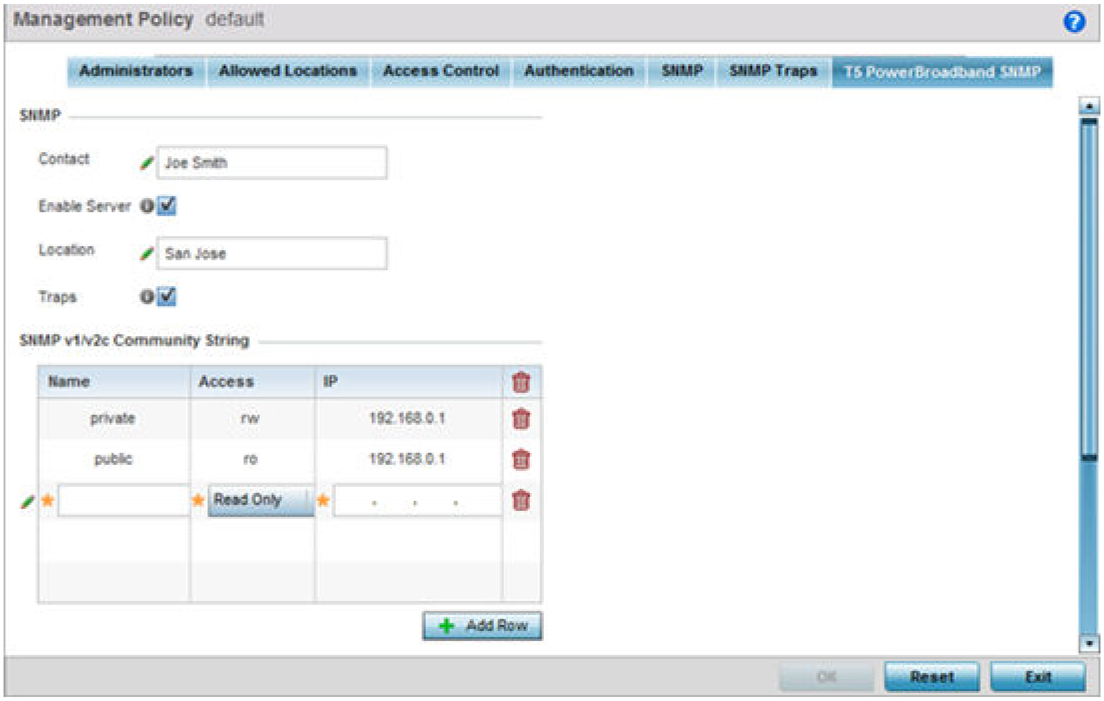
7 Select **Refresh** to update the screen's statistics counters to their latest values

Setting T5 PowerBroadband SNMP Configuration

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

To define a T5 controller power broadband SNMP configuration:

1 Select the T5 Power Broadband tab.



SNMP

Contact: Joe Smith

Enable Server ☑

Location: San Jose

Traps ☑

SNMP v1/v2c Community String

Name	Access	IP
private	rw	192.168.0.1
public	ro	192.168.0.1
	Read Only	. . .

2 Set the following SNMP settings:

Contact	Set a 64 character maximum contact name for the administration of T5 controller SNMP events.
Enable Server	Select this option to enable SNMP event management for the T5 controller. This setting is disabled by default.
Location	Set a 64 character maximum location for the SNMP resource dedicated to T5 controller support.
Traps	Select this option for SNMP trap support for the T5 controller. 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.

3. Set the SNMP v1/v2c Community String configuration for T5 controller usage. 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	Set a 32 character maximum SNMP community string.
Access	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: Read Only - Allows a remote device to retrieve information. Read-Write - Allows a remote device to modify settings.
IP	Set the IP address of the SNMP manager.

4. Use the **Host** table to define up to 4 SNMP receiver resource IP addresses.
5. Select **OK** to update the configuration. Select **Reset** to revert to the last saved configuration.

T5 Device

To view device statistics for a selected T5 model controller:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Device** from the left-hand side of the UI.

The System field displays the following:

Hostname	Lists the administrator assign hostname of the T5 controller applied to the device upon initial administration.
MAC	Lists the factory encoded MAC address of the T5 controller as its hardware identifier.
Type	Indicates the type of controller reporting system data.
RF Domain Name	Lists the RF Domain to which the T5 controller belongs. The RF Domain displays as a link that's selectable to display RF Domain data in greater detail.
System Clock	Displays T5 controller system time, as reported from the controller itself or its remote NTP time resource.
Uptime	Displays the duration the T5 controller has remained active since last offline or booted,
Application Version	Displays the version of the firmware running on this device.
Bootloader Version	Displays the version of the Boot Loader software available on this device.

The Temperature field displays the following:

Current Temperature	Displays the current T5 controller temperature in Celsius.
Fans at Variable Speed in (C)	Lists the temperature of the T5 controller as reported by the controller's fans operating at variable speed.
Fans at Full Speed in (C)	Lists the temperature of the T5 controller as reported by the controller's fans operating at full speed.

The Firmware Images field displays the following:

Primary Version	Displays the primary version string available for an upgrade.
Secondary Version	Displays the secondary version string available as a backup (secondary) upgrade resource.

The Upgrade Status field displays firmware upgrade statistics. The table provides the following:

Upgrade Status	Displays whether the image upgrade was successful.

4 Select **Refresh** to update the statistics counters to their latest values.

T5 Wireless Client

The T5 Wireless Clients screen displays read only device information for wireless clients associated with the selected T5 controller and its connected CPE device radios. Use this information to assess if configuration changes are required to improve client performance.

To view wireless client's statistics

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select **Wireless Clients** from the left-hand side of the UI.

The Wireless Clients screen displays the following:

Device	Lists the name of the T5 controller managed CPE device radio detecting and reporting client information.
MAC Address	Displays the factory encoded hardware MAC address assigned to the client as hardware identifier.
SSID	Displays each listed client’s SSID *(service set id)* used as a network identifier.
Last RSSI	Lists a RSSI *(relative signal strength indication)* in dBm for client devices connected to the selected T5 controller and its managed CPE radios.
Rx Packets	Displays the number of packets received by the listed T5 controller managed client.
Tx Packets	Displays the number of packets transmitted by the listed T5 controller managed client.
Association Status	Displays the association status of the wireless client.
Authentication Status	Displays the authentication status of the wireless client.
Retry Percentage	Displays the retry percentage for packets sent this wireless client. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 WLAN QoS

T5 controller WLAN utilization can be administered from one screen to assess how different data traffic is being utilized.

To administrate T5 controller WLAN QoS utilization:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Wireless LANs** from the left-hand side of the UI. The **Quality of Service** tab displays by default.

   Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN(s) utilized by the selected T5 controller.
Rx Background Packets	Lists the number of background (low priority) packets received on each listed T5 controller managed WLAN since the screen was last refreshed.
Rx Best Effort Packets	Lists the number of best effort packets received on each listed T5 controller managed WLAN since the screen was last refreshed.
Tx Background Packets	Lists the number of background (low priority) packets transmitted out of each listed T5 controller managed WLAN since the screen was last refreshed.
Tx Best Effort Packets	Lists the number of best effort packets transmitted out of each listed T5 controller managed WLAN since the screen was last refreshed.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 WLAN Rates

An administrator can assess a T5 controller's WLAN utilization data rate to determine WLAN performance speed is being optimized in both the transmit and receive directions.

To assess T5 controller WLAN data rates:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Wireless LANs** from the left-hand side of the UI.
4. Select the **Rates** tab.

   Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN member devices reporting the listed transmit and receive statistics for the T5 WLAN.
Rx Packets (1Mbps)	Lists the number of data packets received in the WLAN that have been relegated to a 1 Mbps data rate.
Rx Packets (54Mbps)	Lists the number of data packets received in the WLAN by T5 controller connected devices at 54Mbps.
Tx Packets (1Mbps)	Lists the number of data packets transmitted out of the WLAN that have been relegated to a 1 Mbps data rate.
Tx Packets (54Mbps)	Lists the number of data packets transmitted out of the WLAN at 54Mbps.

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 WLAN Sizes

T5 controller managed WLANs can be administrated to assess packets sizes both received and transmitted out of the WLAN.

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **Size** tab.

   Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN(s) utilized by the selected T5 controller.
Rx Packets (>1024 Bytes)	Lists the number of data packets received in each listed WLAN greater then 1024 bytes.
Tx Packets (>1024 Bytes)	Lists the number of data packets transmitted on each listed WLAN greater then 1024 bytes.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 MAC Table

The T5 MAC Table screen displays a dynamic list of MAC addresses learned by the T5 controller over its ethernet interfaces. Use this information to identify devices and the interfaces on which they can be found.

To view T5 MAC table:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **MAC Table** from the left-hand side of the UI.

   The MAC Table screen displays the following:

MAC Address	Displays the MAC address of the discovered client device.
Interface Name	Displays the interface on which the device can be found.
Device MAC	Displays the MAC address of the T5 controller that found the client device.
Vendor	Displays the Vendor (manufacturer) of the T5 discovered client device.
VLAN	Displays the T5 's VLAN (virtual interface) on which the device was discovered.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE System

The T5 controller CPE System screen displays device hardware and SKU information for T5 controller managed CPE devices. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.

To view CPE system information:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select and expand the **CPE** menu item to display its sub menu items.
4. Select **System**.

   The CPE System screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Product Type	Displays the model (product) type of each T5 controller managed CPE.
Serial Number	Displays the hardware encoded serial number appended to each T5 controller managed CPE. The serial number is different from the MAC address and is not configurable in the user interface.
SKU	Lists each T5 managed CPE's SKU information to assess hardware product revision.
Hardware Version	Lists a hardware revision number for each listed CPE.
MAC	Lists each CPE's factory encoded MAC address used as the CPE's hardware identifier within the user interface.

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio Statistics

The T5 controller Radios screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5’s management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Radios** from the left-hand side of the UI.
4. Select the **Statistics** tab.

   The Statistics tab displays the following for T5 controller managed CPE radio devices:

Name	Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Rx (Kbps)	Displays the listed CPE radio's receive data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.

Rx Octets	Displays the number of octets (bytes) received with no errors by the listed T5 controller managed CPE radio.
Rx Packets	Lists the number of data packets received for the listed T5 managed CPE radio since this screen was last refreshed.
Tx (Kpbs)	Displays the listed CPE radio's transmit data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
Tx Octets	Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE radio.
Tx Packets	Lists the number of data packets transmitted from the listed T5 managed CPE radio since this screen was last refreshed.

5 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio Summary

The T5 controller Radios screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio information:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select **Radios** from the left-hand side of the UI.

The Summary tab displays the following for T5 controller managed CPE radio devices: :

Name	Name Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Operational Status	Lists whether the selected radio is currently up or down in its ability be a radio coverage resource for its managing T5 controller.
MAC	MAC Displays the factory encoded Media Access Control (MAC) address of each listed CPE device radio managed by the selected T5 controller.
Transmit Power	Lists each T5 controller managed CPE radio's configured transmit power.
Channel	Lists each CPE radio's current transmit channel. Auto defines the radio as having an automatic channel assignment.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio WLAN Map

The T5 controller Radios screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio WLAN memberships:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Radios** from the left-hand side of the UI.
4. Select the **WLAN Map** tab.

   Refer to the following WLAN map membership data for T5 controller managed CPE radio devices:

Name	Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Status	Lists whether a CPE radio is currently enabled or disabled as a radio resource for the WLAN(s) the CPE radio has been mapped to.
WLAN-Radio Mapping	Displays the managed WLAN(s) each listed radio has been mapped to.

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Interface Ethernet Counter

A T5 controller can have its Ethernet ports reviewed for transmit and receive packet throughput.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2

To view T5 controller Ethernet port counter statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Interface** from the left-hand side of the UI.
4. Select **Ethernet Ports**. The **Counter** tab displays by default.

   Review the following T5 controller Ethernet port counter data:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Rx Octets	Displays the number of octets (bytes) received by the listed T5 controller Ethernet port.
Rx Packets	Lists the number of data packets received for the listed T5 Ethernet port since this screen was last refreshed.

Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received on this port since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted by the listed T5 controller Ethernet port.
Tx Packets	Lists the number of data packets transmitted from the listed T5 Ethernet port since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted on this port since this screen was last refreshed.

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Interface Ethernet Description

T5 controller Ethernet ports can have numeric ID and descriptions applied for differentiation.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port descriptions:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Interface** from the left-hand side of the UI and expand it to display it sub menu items.
4. Select **Ethernet Ports**.
5. Select the **Description** tab.

   Review the following T5 controller Ethernet port descriptions:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Interface Index	Lists the numeric index assignable to each T5 controller ge Ethernet port.
Description	Displays the 64 character maximum description an administrator assigns to each ge port as its unique description string.

6. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Interface Ethernet Status

T5 controller Ethernet ports can have be reviewed to assess link operational status, link speed and duplexing.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port link status:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select **Interface** from the left-hand side of the UI and expand it to display it sub menu items.

4 Select **Ethernet Ports**.

5 Select the **Status** tab.

Review the following T5 controller Ethernet port status:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Operational Status	Lists whether each Ethernet port link is currently up or down as a T5 controller transmit and receive resource.
Duplex	Lists either half, full or automatic as the duplex. Half duplex sends 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. Full duplex transmits data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Automatic enables the controller to dynamically duplex as port performance needs dictate.
Speed (MB)	Speed (MB) Lists each port's current speed in MB.
Pause	Lists whether pause packet utilization is currently off or on for the port.
Admin Status	Displays

6 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Interface Ethernet Utilization

T5 controller Ethernet ports can have be reviewed to assess link utilization efficiency.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port link status:

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select **Interface** from the left-hand side of the UI and expand it to display it sub menu items.

4 Select the **Utilization** tab.

Review the following T5 controller Ethernet port status:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Rx (Kpbs)	Displays the listed T5 controller ge Ethernet port receive data rate (in Kbps).
RX (p/s)	Lists a packet per second Ethernet port receive rate.
Rx Utilization (%)	Lists each port's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed T5 controller Ethernet port transmit data rate (in Kbps).
Tx (p/s)	Lists a packet per second Ethernet port transmit rate.
Tx Utilization (%)	Lists each port's transmit direction utilization as a percentage of available transmit bandwidth available.

5 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Counter

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view CPE DSL counter statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **DSL** menu item. The **Counter** tab displays by default.

   The DSL Counter screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Rx Octets	Displays the number of octets (bytes) received with no errors by the listed T5 controller managed CPE DSL.
Rx Packets	Lists the number of data packets received for the listed T5 managed CPE DSL since this screen was last refreshed.
Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received for the listed T5 managed CPE DSL since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE DSL.
Tx Packets	Lists the number of data packets transmitted from the listed T5 managed CPE DSL since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted from the listed T5 managed CPE DSL since this screen was last refreshed.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Custom

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view **Custom** CPE DSL counter statistics:

1. Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select the **DSL** menu item. Select the **Custom** tab displays by default.

The Custom DSL screen displays the following:

Average Response Time	List each DSL's average response time in microseconds.
Maximum (peak) Response Time	List each DSL's maximum (best to date since the screen was refreshed) response time in microseconds.
Downstream Errored Seconds	List the number of seconds downstream DSL transmissions were negatively impacted by code violations.
Downstream Severely Errored Seconds	List the number of seconds downstream DSL transmissions were severely negatively impacted by code violations.
Upstream Errored Seconds	List the number of seconds upstream DSL transmissions were negatively impacted by code violations.
Upstream Severely Errored Seconds	List the number of seconds upstream DSL transmissions were severely negatively impacted by code violations.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Description

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view CPE DSL description data:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select the **DSL** menu item. Select the **Description** tab.

The DSL Description screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Interface Index	Lits the numeric index assigned to each CPE DSL upon its initial management and configuration.
Description	Displays the administrator assigned description for further delineation amongst T5 controller managed CPE DSLs.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Status

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view CPE DSL status:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **DSL** menu item. Select the **Status** tab.

   The DSL Description screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Link Status	Displays whether each listed CPE DSL is currently enabled or disabled for utilization by its connected T5 controller.
Downstream Rate (Mbps)	Downstream Rate (Mbps) Lists each connected CPE DSL downstream data rate in Mbps.
Downstream Margin (dB)	Displays the DSL downstream power minus the attenuation (in dB).
Upstream Rate (Mbps)	Lists each connected CPE DSL upstream data rate in Mbps.
Upstream Margin (dB)	Displays the DSL upstream power minus the attenuation (in dB).
Power	Lists each DSL's wattage utilization.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Errors

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view CPE DSL error data:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **DSL** menu item. Select the **Errors** tab.

   The DSL Errors screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Line Downstream Fecs	Lists the number of Fecs detected in the downstream direction. Forward Error Correction (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels
Downstream Coding Violations	Lists the number of CPE DSL coding violations (badly coded packets) detected in the downstream direction.
Line Upstream Fecs	Lists the number of Fecs detected in the upstream direction. Forward Error Correction (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels
Upstream Coding Violations	Lists the number of CPE DSL coding violations (badly coded packets) detected in the upstream direction.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Radio DSL Utilization

A T5 controller uses the operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The Customer Premises Equipment (CPEs) are the T5 controller managed radio devices using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices. These CPEs use a Digital Subscriber Line (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To view CPE DSL utilization:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select the **DSL** menu item. Select the **Utilization** tab.
The DSL Utilization screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Rx (Kpbs)	Displays the listed CPE DSL's receive data rate (in Kbps).
RX (p/s)	Lists a packet per second DSL receive rate.
Rx Utilization (%)	Lists each DSL's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed CPE DSL's transmit data rate (in Kbps).
Tx (p/s)	List a packet per second DSL transmit rate.
Tx Utilization (%)	Lists each DSL's transmit direction utilization as a percentage of available transmit bandwidth available.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Fast Ethernet Counter

A T5 controller can have its Ethernet ports reviewed for transmit and receive packet throughput.

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up ton 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port counter statistics:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select the **Interface** menu item and expand it to display it sub menu items. Select **Fast Ethernet**. The **Counter** tab displays by default.

Review the following T5 controller connected CPE fe port counter data:

Name	Displays the name of each listed T5 controller controller connected CPE fe Ethernet port.
Rx Octets	Displays the number of octets (bytes) received by the listed CPE fe port.
Rx Packets	Lists the number of data packets received for the listed CPE fe port since this screen was last refreshed.
Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received on this port since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted by the listed CPE fe Ethernet port.
Tx Packets	Lists the number of data packets transmitted from the listed CPE fe port since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted on this port since this screen was last refreshed.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Fast Ethernet Description

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up ton 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port descriptions:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select the **Interface** menu item and expand it to display it sub menu items. Select **Fast Ethernet**. Select the **Description** tab.

Review the following CPE fe port descriptions:

Name	Displays the name of the selected CPE fe Ethernet port.
Interface Index	Lists the numeric index assignable to each CPE fe Ethernet port.
Description	Displays the 64 character maximum description an administrator assigns to each CPE fe port as its unique description string.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Fast Ethernet Status

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up ton 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port status:

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select the **Interface** menu item and expand it to display it sub menu items. Select **Fast Ethernet**. Select the **Status** tab.

Review the following CPE fe port descriptions:

Name	Displays the name of the selected CPE fe Ethernet port.
Operational Status	Lists whether each Ethernet port link is currently up or down as a transmit and receive resource.
Duplex	Lists either half, full or automatic as the duplex. Half duplex sends 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. Full duplex transmits data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Automatic enables the controller to dynamically duplex as port performance needs dictate.
Speed (MB)	Lists each port's current speed in MB.
Pause	Lists whether pause packet utilization is currently off or on for the port.
Admin Status	Admin Status Displays whether each listed port had been placed in an enabled or disabled state by the administrator.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 Fast Ethernet Utilization

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up ton 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port utilization:

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select the **Interface** menu item and expand it to display it sub menu items. Select **Fast Ethernet**. Select the **Utilization** tab.

Review the following CPE fe Ethernet port utilization data:

Name	Displays the name of the selected CPE fe Ethernet port.
Rx (Kpbs)	Displays the listed CPE fe Ethernet port receive data rate (in Kbps).
RX (p/s)	Lists a packet per second Ethernet port receive rate.
Rx Utilization (%)	Lists each port's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed CPE ge Ethernet port transmit data rate (in Kbps).
Tx (p/s)	Lists a packet per second fe Ethernet port transmit rate.
Tx Utilization (%)	Lists each fe port's transmit direction utilization as a percentage of available transmit bandwidth available.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Address

The T5 controller CPE Address screen lists the selected T5 controller's managed CPE radio devices. Use this screen to verify each CPE address credentials and whether their currently disconnected or ready for radio coverage area support.

To view CPE address data:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **CPE** menu item and expand it to display it sub menu items. Select **Address**.

   The CPE Address screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Status	Displays whether each T5 controller managed CPE is disconnected (offline) or ready to provide radio coverage area support for the T5 controller.
IP Address	Lists each CPE's current IP address used as its network identifier.
MAC Address	Displays each CPE hardware encoded MAC address used as a device hardware identifier.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Boot

The T5 controller CPE Boot screen lists the primary and secondary firmware versions available to each CPE, along with upgrade status form each device's most recent upgrade operation.

To view CPE boot configurations:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **CPE** menu item and expand it to display it sub menu items. Select **Boot**.

   The CPE Boot screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Primary Version	Lists the primary version of CPE firmware currently queued for each listed T5 controller managed CPE.
Secondary Version	Lists the secondary (alternate) version of CPE firmware currently queued for each listed T5 controller managed CPE.
Next Boot	Lists whether the next boot of each listed CPE is going to utilize either the primary or secondary firmware version.
Upgrade Process	Displays a completion percentage for any pending firmware upgrade operation impacting a listed T5 controller managed CPE device.
Upgrade Status	Lists the upgrade status of T5 controller managed CPEs. If a device is not undergoing an upgrade, its status is None.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Reset

The T5 controller CPE Reset screen lists the number times a T5 controller managed CPE has been reset.

To view CPE reset status:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **CPE** menu item and expand it to display it sub menu items. Select **Reset**.

   The CPE **Reset** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Resets	Lists the number of times each T5 controller managed CPE has been reset since this screen was last refreshed. Resetting a CPE temporarily renders the CPE offline until the reset is complete.

4. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE LED

The T5 controller CPE LED screen lists whether T5 controller managed CPE devices currently have their LEDs enabled or disabled. In places like hospitals, its not uncommon for Access Points to be operational, but their LEDs off as to not disturb patients.

To view CPE LED status:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select the **CPE** menu item and expand it to display it sub menu items. Select **LED**.

   The CPE **LED** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
LED Status	A green checkmark defines the listed CPE as having its LEDs on and illuminated. A red X defines the listed CPE as having its LEDs off.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Reset

The T5 controller CPE Reset screen lists the number times a T5 controller managed CPE has been reset.

To view CPE reset status:

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select the **CPE** menu item and expand it to display it sub menu items. Select **Reset**.

The CPE **Reset** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Resets	Lists the number of times each T5 controller managed CPE has been reset since this screen was last refreshed. Resetting a CPE temporarily renders the CPE offline until the reset is complete.

4 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE System

The T5 controller CPE System screen displays device hardware and SKU information for T5 controller managed CPE devices. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.

To view CPE system information:

1 Select the **Statistics** menu from the Web UI.

2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

3 Select and expand the **CPE** menu item to display its sub menu items.

4 Select **System**.

The CPE System screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Product Type	Displays the model (product) type of each T5 controller managed CPE.
Serial Number	Displays the hardware encoded serial number appended to each T5 controller managed CPE. The serial number is different from the MAC address and is not configurable in the user interface.

SKU	Lists each T5 managed CPE's SKU information to assess hardware product revision.
Hardware Version	Lists a hardware revision number for each listed CPE.
MAC	Lists each CPE's factory encoded MAC address used as the CPE's hardware identifier within the user interface.

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Uptime

The CPE Uptime screen lists the time each T5 controller manage CPE device has been actively deployed and operational.

To view CPE device uptimes:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select and expand the **CPE** menu item to display its sub menu items.
4. Select **Uptime**.

   The CPE Uptime screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Uptime	Lists the time each listed T5 controller has been deployed without interruption (reboot etc.).

5. Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Version

The CPE Version screen lists the application and boot versions utilized by T5 controller managed CPE devices.

To view CPE device version data:

1. Select the **Statistics** menu from the Web UI.
2. Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3. Select and expand the **CPE** menu item to display its sub menu items.
4. Select **Version**.

   The CPE Version screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Application Verison	Lists the firmware version currently utilized and deployed with each listed T5 controller managed CPE.
Boot Loader Version	Displays the firmware version queued as the boot version for each listed T5 controller managed CPE.

5 Select **Refresh** to update the screen's statistics counters to their latest values.

T5 CPE Port Status

The T5 controller CPE Port Status screen lists the status of the ports for the T5 controller managed CPE devices.

To view CPE device version data:

1 Select the **Statistics** menu from the Web UI.
2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
3 Select and expand the **CPE** menu item to display its sub menu items.
4 Select **Port Status**.

The CPE Port Status screen displays the following:

CPE Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
CPE MAC	Lists the MAC address of the T5 controller managed CPE device.
Interface	Lists the interface on which the T5 controller managed CPE device is found.
Operation Status	Lists the operational status of the T5 controller managed CPE device.
Speed (Mbps)	Lists the interface speed of the CPE device in Mbps.
Duplex	Displays the interface as either half duplex, full duplex or unknown.

5 Select **Refresh** to update the screen's statistics counters to their latest values.

EX3500 Statistics

Use the EX3500 switch's statistics screens to assess switch throughput and error rates in both the transmit and receive directions. Expand the topics in this section as needed to review individual Ethernet port performance utilizations.

EX3500 System

Refer to the System screen to assess EX3500 switch system data as well as switch fan utilization and device upgrade information.

Use the System field to assess the administrator assigned System Name for the switch,System Object ID (numeric identifier), administrative System Contact, System Description, System Location and System Up Time. The factory encoded MAC Address of the switch displays as the unit's hardware identifier. The System field also displays the switch's dedicated Web server port, whether Web Server functionality is enabled, the Web Server Secure Port and whether Web Secure Server is enabled for optimized Web server security. Additionally, assess whether Telnet Server functionality has been enabled and over which Telnet Server Port. Lastly, assess whether support for Jumbo Frames with more than 1500 bytes of payload has been enabled or disabled.

Refer to the Fan table to review the Fan and Unit index of each EX3500 switch fan utilized and their current Fan Status.

The Upgrade table lists the queued file for the upgrade operation, its Path (file location) and Status and Reload Status.

The Temperature table displays the current temperature (in degrees) to assess a potential overheat condition.

Periodically select **Refresh** to update the screen to its latest information.

w

EX3500 Version

The EX3500 switch Version screen lists hardware and switch software version information utilized for the selected EX3500 switch. Use this information when reporting any issues to Support or when assessing whether an update would improve switch performance.

To view EX3500 switch version information:

- Refer to the Unit ID and Serial Number items to assess the switch numeric identifier and serial number.
- The Hardware Version lists hardware version of the EX3500 switch main board.
- Refer to the EPLD Version to check the EPLD *(erasable programmable logic device)* comprising an array of PLD *(programmable logic devices)* that do not come pre-connected with the switch.
- The Number of Ports field lists built-in port utilization. The EX3524 and EX3548 are Gigabit Ethernet Layer 2 switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP *(Small Form Factor Pluggable)* transceiver slots for fiber connectivity.
- Refer to the Main Power Status item to assess the status of the internal power supply.
- Refer to the Role table item to review the switch's current defined network role (**`master`** or **`slave`**).
- The Loader Version item displays the version number of the switch loader code.
- The Operation Code Version lists the version number of the switch's runtime code.
- The Adopted Version lists the version of the management agent used by the switch to adopt to a WiNG controller.
- The Linux Version lists the version of the Linux operating system utilized on the switch.

Periodically select **Refresh** to update the screen to its latest information.

EX3500 Directory Information

The Directory Information screen helps an administrator Opcode and Configuration files currently residing on the EX3500 switch and whether their currently designated as boot files.

Refer to the following directory information for the selected EX3500:

- Refer to the Unit ID item to list the ID associated with each listed configuration or opcode file.
- The File Name item lists the files available for utilization on the switch currently. Select **Whichboot** (from the upper left) to filter this list to just the files queued for switch boot operations.
- The Type item lists whether each listed file is a **`OpCode`** (switch runtime code) or **`Config`** (switch configuration) file.
- The Startup item lists Y/N as to whether the listed file is invoked at switch startup.
- The Modify Time parameter lists the last time the listed file was modified on this EX3500 switch.
- The Size (Bytes) item lists the byte size of the listed operation code (Opcode) or configuration file.

Periodically select **Refresh** to update the screen to its latest information.

EX3500 Interface

Use the EX3500 switch's Ethernet and interface statistics screens to assess switch throughput and error rates in both the transmit and receive directions. Expand the topics in this section as needed to review individual Ethernet port performance utilizations.

EX3500 Ether

Refer to the Ether-LIKE screen to assess a variety of errors that may be negatively impacting the performance of each listed EX3500 switch interface.

Review the following error conditions for each listed EX3500 switch interface:

- Interface - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stats.
- Alignment Errors - Lists frames received that are not an integral number of bytes long and that fail the FCS check.
- FCS Errors - Lists each interface's FCS *(frame check sequence)* errors. refers to the extra error-detecting code added to a frame in a communications protocol.
- Single Collision Frames - Displays each interface's number of collisions over the selected interface.
- Multiple Collision Frames - Displays each interface's number of frames transmitted that met with more than one collision before the 64-bytes traversed the connection.
- SQE Test Errors - Lists each interface's SQE TEST ERROR message. SQEs are **`Signal Quality Errors`**, and are also referred as an Ethernet **`heartbeat`**.
- Deferred Transmissions - The number of frames that were ultimately sent after the system initially deferred them (the first transmission attempt was delayed because the medium was busy). This number does not include frames involved in any collisions.
- Late Collisions - Lists each interface's late collisions. 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.
- Excessive Collisions - Displays each interface's number of excessive collisions. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently.
- Internal MAC Transmit Errors - Lists each interface's error count due to to an internal MAC sublayer transmit error. This number does not include alignment, FCS, or frame-too-long errors.
- Internal MAC Receive Errors - Lists each interface's error count due to an internal MAC sublayer receive error. This number does not include alignment, FCS, or frame-too-long errors.
- Frames Too Long - Lists each interface's error count due from exceeding the standard Ethernet size limitation but had a valid CRC. Without jumbo frames enabled, these are frames over 1518 bytes or

1522 bytes for VLAN frames. With jumbo frames enabled, these are frames over 9018 bytes or 9022 bytes for VLAN frames.

- Carrier Sense Errors - Lists each interface's errors that occur when an interface attempts to transmit a frame, but no carrier is detected, and the frame cannot be transmitted.

Periodically select **Refresh** to update the data to the latest values.

EX3500 Interface Extended IF

The EX3500 Interface Extended IF screen lists multicast and broadcast traffic utilization in both the transmit and receive directions.

Review the following extended interface information for the selected EX3500 switch:

- Interface - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- Multicast Input - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast address at this sub-layer.
- Multicast Output - Lists each port's number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
- Broadcast Input - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
- Broadcast Output - Lists each port's The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Periodically select **Refresh** to update the screen to its latest information.

EX3500 Interface IF

Refer to the Interface Table for octet utilization and reported errors for each listed EX3500 switch port.

The table includes the following:

- Interface - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- Octets Input - Lists the total number of octets received on the listed switch port, including framing characters.
- Octets Output - Lists the total number of octets transmitted out of the listed switch port, including framing characters.
- Unicast Input - Lists the number of subnetwork-unicast packets delivered to each listed interface.
- Unicast Output - Lists each port's number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address.
- Discard Input - Number of input frames discarded because they did not conform to the general validation rules or specific usage rules defined for the listed port.
- Discard Output - Number of output frames discarded because they did not conform to the general validation rules or specific usage rules defined for the listed.
- Error Input - Lists each port's total number of erroneous input frames that could not be received.
- Error Output - Lists each port's total number of erroneous output frames that could not be transmitted and forwarded to their destination.
- Unknown Protos Input - Lists each port's number of packets received and discarded because of an unknown or unsupported protocol.

Periodically select **Refresh** to update the screen to its latest information.

EX3500 Interface Port Utility

Refer to the Port Utilization Statistics screen to assess packet throughput per listed switch port.

Review the following EX3500 switch port utilizations stats:

- Interface - Lists the impacted physical EX3500 Ethernet Port reporting the listed stat.
- Octet Input Per Second - Number of octets entering the listed port in kbits/second.
- Packet Input Per Second - Lists each port's received packet total per second.
- Input Utilization - The input utilization rate for each listed port.
- Octet Output Per Second - Number of octets leaving each listed port in kbits/second.
- Packet Output Per Second - Number of packets leaving each listed port per second.
- Output Utilization - The output utilization rate for this listed port interface.

Periodically select **Refresh** to update the statistic counters to their latest values.

EX3500

EX3500 Interface Extended IF

The EX3500 Interface Extended IF screen lists multicast and broadcast traffic utilization in both the transmit and receive directions.

Review the following extended interface information for the selected EX3500 switch:

- Interface - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- Multicast Input - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast address at this sub-layer.
- Multicast Output - Lists each port's number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
- Broadcast Input - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
- Broadcast Output - Lists each port's The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Periodically select **Refresh** to update the screen to its latest information.

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 AP505, AP510 and AP560 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

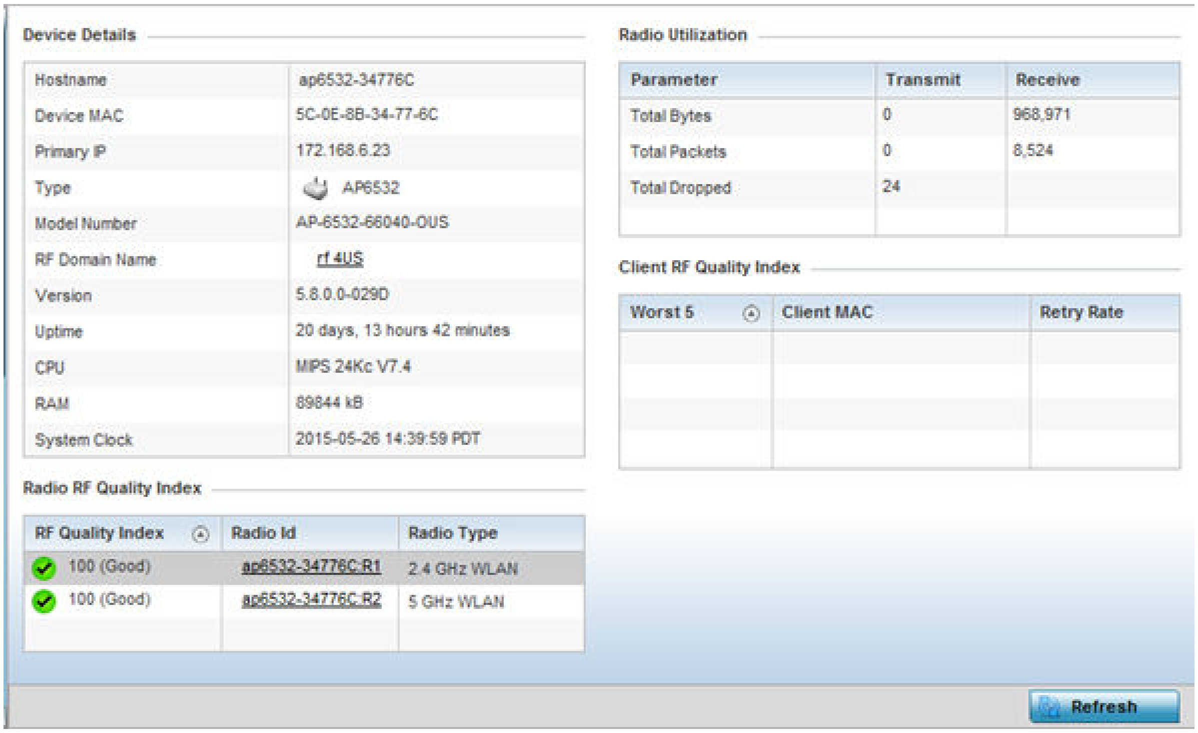
The **Health** screen displays a selected access point's hardware and software version. Use this information to refine the performance of an access point. The Health screen should also be the starting point for troubleshooting an access point, since it displays a high level overview of access point performance 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, select a **controller or service platform**, and select one of its connected **access points**.

4 Select **Health** from the left-hand side of the UI.



Device Details

Hostname	ap6532-34776C
Device MAC	5C-0E-8B-34-77-6C
Primary IP	172.168.6.23
Type	AP6532
Model Number	AP-6532-66040-OUS
RF Domain Name	rf 4US
Version	5.8.0.0-029D
Uptime	20 days, 13 hours 42 minutes
CPU	MIPS 24Kc V7.4
RAM	89844 kB
System Clock	2015-05-26 14:39:59 PDT

Radio Utilization

Parameter	Transmit	Receive
Total Bytes	0	968,971
Total Packets	0	8,524
Total Dropped	24	

Client RF Quality Index

Worst 5	Client MAC	Retry Rate

Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type
✓ 100 (Good)	ap6532-34776C:R1	2.4 GHz WLAN
✓ 100 (Good)	ap6532-34776C:R2	5 GHz WLAN

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: • 0 – 50 (poor) • 50 – 75 (medium) • 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.

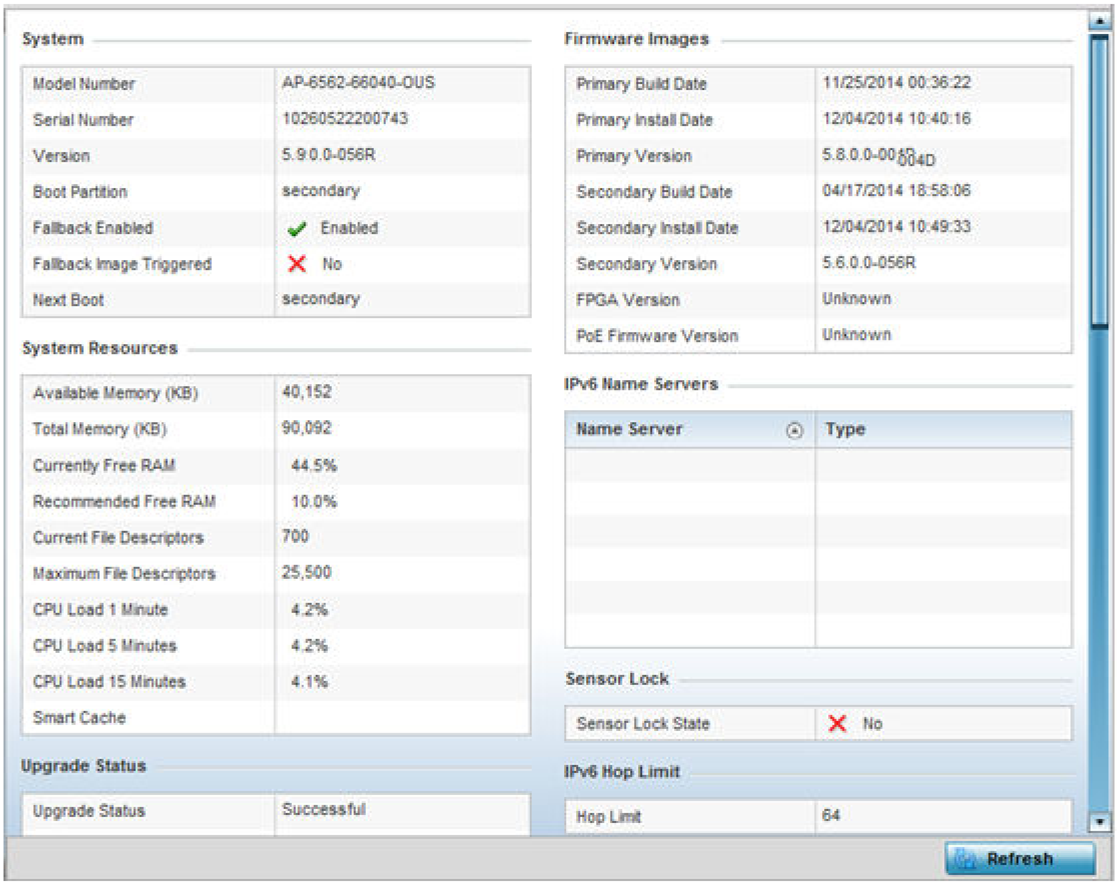
5. Select **Refresh** as needed to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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**.



System

Model Number	AP-6562-66040-OUS
Serial Number	10260522200743
Version	5.9.0.0-056R
Boot Partition	secondary
Fallback Enabled	✓ Enabled
Fallback Image Triggered	✗ No
Next Boot	secondary

System Resources

Available Memory (KB)	40,152
Total Memory (KB)	90,092
Currently Free RAM	44.5%
Recommended Free RAM	10.0%
Current File Descriptors	700
Maximum File Descriptors	25,500
CPU Load 1 Minute	4.2%
CPU Load 5 Minutes	4.2%
CPU Load 15 Minutes	4.1%
Smart Cache	

Upgrade Status

Upgrade Status	Successful

Firmware Images

Primary Build Date	11/25/2014 00:36:22
Primary Install Date	12/04/2014 10:40:16
Primary Version	5.8.0.0-004D
Secondary Build Date	04/17/2014 18:58:06
Secondary Install Date	12/04/2014 10:49:33
Secondary Version	5.6.0.0-056R
FPGA Version	Unknown
PoE Firmware Version	Unknown

IPv6 Name Servers

Name Server	Type

Sensor Lock

Sensor Lock State	✗ No

IPv6 Hop Limit

Hop Limit	64

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:

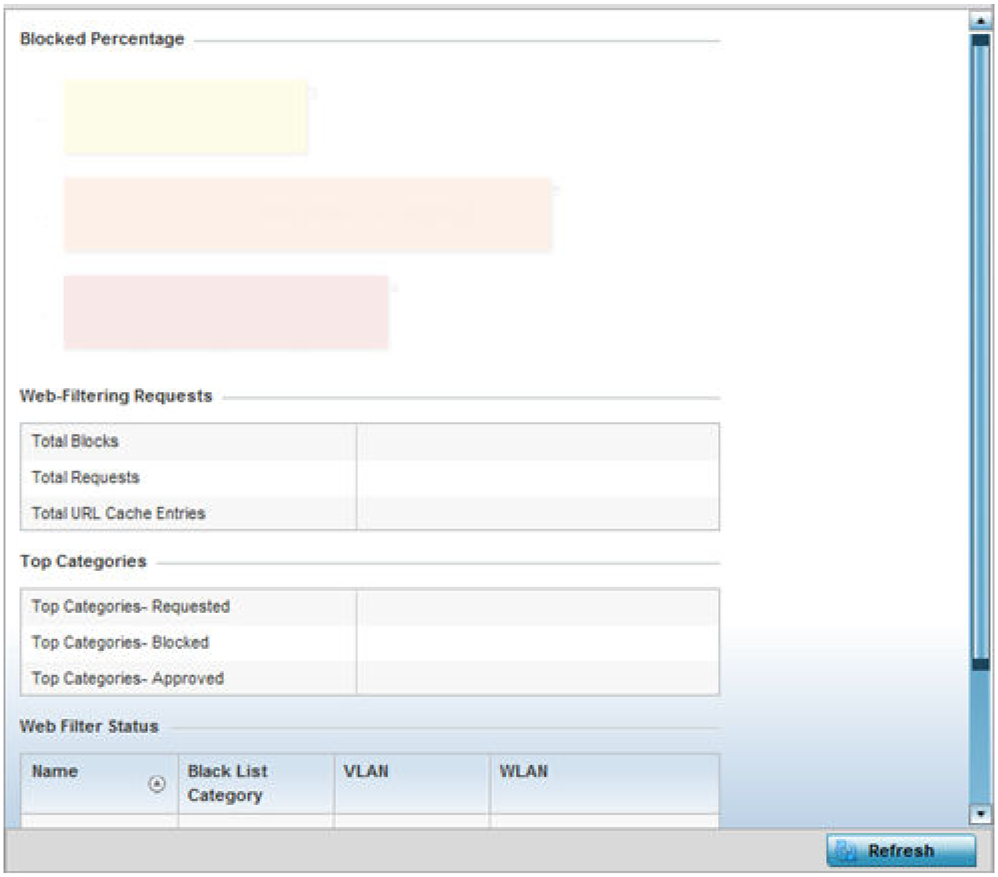
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node from the navigation pane (on the left-hand side of the screen).

   The System node expands to display the RF Domains created within the managed network.
3. Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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)

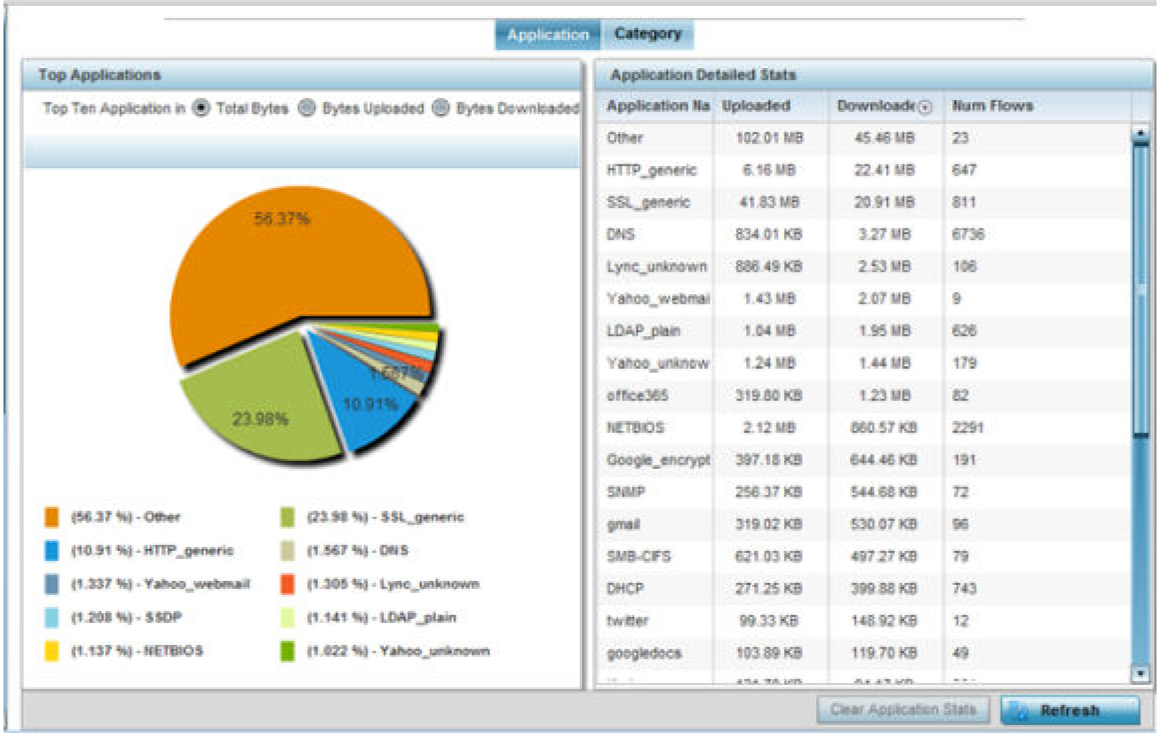
Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application.

1. Select the **Statistics** → **System** tab from the Web UI.
2. Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

   The Controller'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.



Application Na	Uploaded	Downloade	Num Flows
Other	102.01 MB	45.46 MB	23
HTTP_generic	6.16 MB	22.41 MB	647
SSL_generic	41.83 MB	20.91 MB	811
DNS	834.01 KB	3.27 MB	6736
Lync_unknown	886.49 KB	2.53 MB	106
Yahoo_webmai	1.43 MB	2.07 MB	9
LDAP_plain	1.04 MB	1.95 MB	626
Yahoo_unknow	1.24 MB	1.44 MB	179
office365	319.80 KB	1.23 MB	82
NETBIOS	2.12 MB	860.57 KB	2291
Google_encrypt	397.18 KB	644.46 KB	191
SNMP	256.37 KB	544.68 KB	72
gmail	319.02 KB	530.07 KB	96
SMB-CIFS	621.03 KB	497.27 KB	79
DHCP	271.25 KB	399.88 KB	743
twitter	99.33 KB	148.92 KB	12
googledocs	103.89 KB	119.70 KB	49

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.

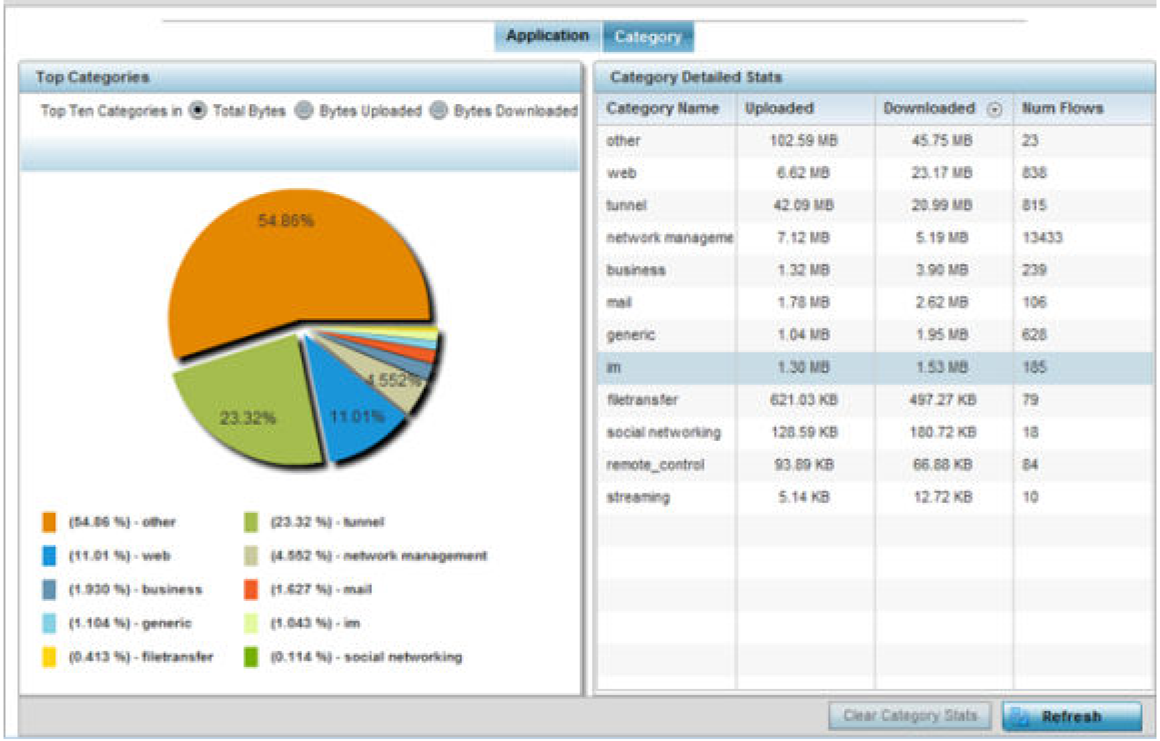
Downloaded	Displays the number of downloaded application data (in bytes) passing the through the access point managed network.
Num Flows	Lists the total number of application data flows passing through the access point for each listed application. An application flow can consist of packets in a specific 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.



Top Ten Categories in ● Total Bytes ○ Bytes Uploaded ○ Bytes Downloaded

Category Detailed Stats

Category Name	Uploaded	Downloaded	Num Flows
other	102.59 MB	45.75 MB	23
web	6.62 MB	23.17 MB	838
tunnel	42.09 MB	20.99 MB	815
network manageme	7.12 MB	5.19 MB	13433
business	1.32 MB	3.90 MB	239
mail	1.78 MB	2.62 MB	106
generic	1.04 MB	1.95 MB	628
im	1.30 MB	1.53 MB	185
filetransfer	621.03 KB	497.27 KB	79
social networking	128.59 KB	180.72 KB	18
remote_control	93.89 KB	66.88 KB	84
streaming	5.14 KB	12.72 KB	10

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.

1 Select the **Statistics** tab from the Web UI.

2 Expand the **System** node on the top, left-hand side of the screen.

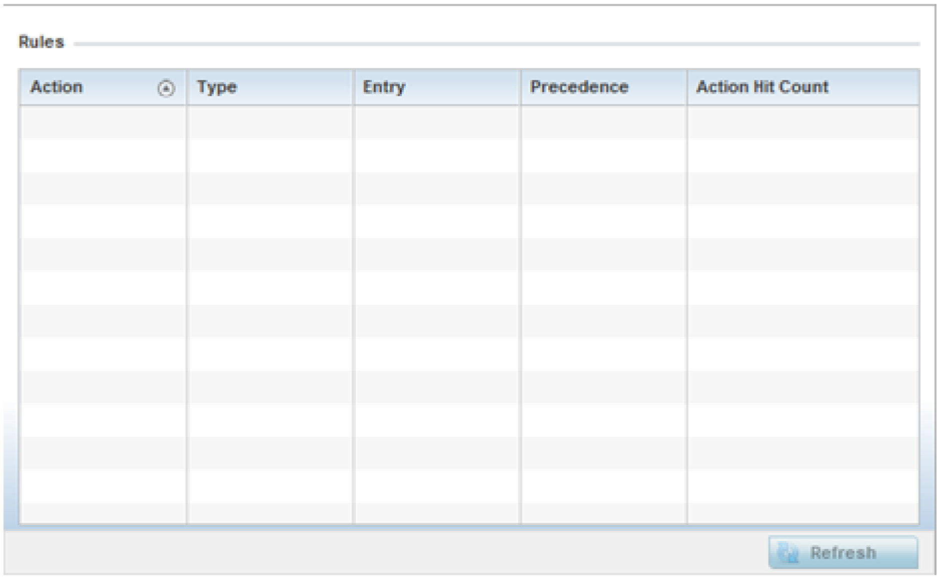
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Controller'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. • `Allow` - Allows packets for a specific application and its defined category type (social networking etc.). This is the default setting. • `Deny` - Denies (restricts) the action applied to a specific application or a specific application category. • `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.

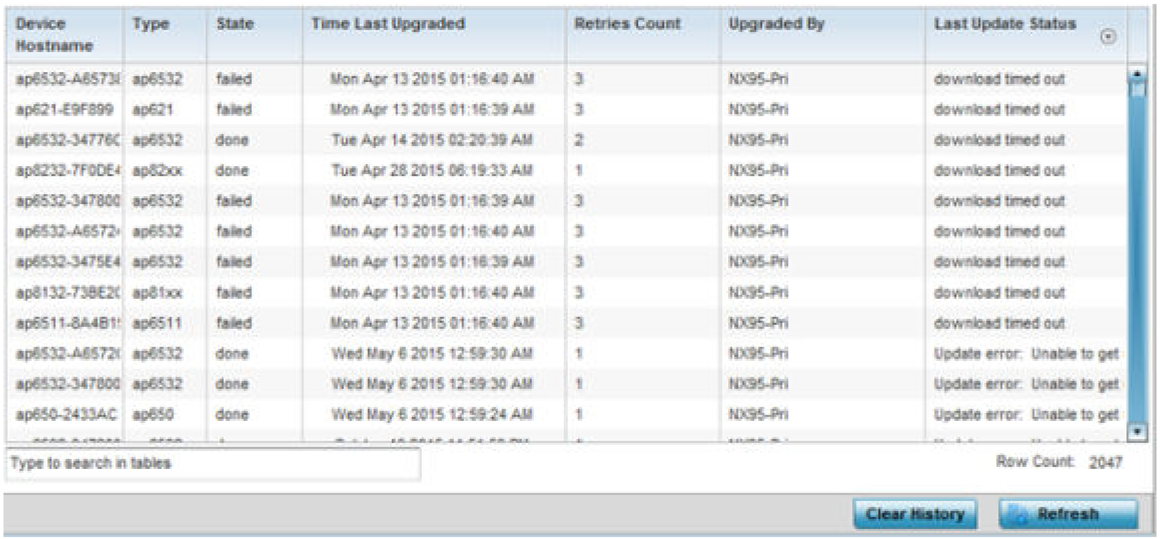
AP Device Upgrade

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, select a **controller or service platform**, and select one of its 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.



Device Hostname	Type	State	Time Last Upgraded	Retries Count	Upgraded By	Last Update Status
ap6532-A6573	ap6532	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap621-E9F899	ap621	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap6532-34776C	ap6532	done	Tue Apr 14 2015 02:20:39 AM	2	NX95-Pri	download timed out
ap8232-7F0DE	ap82xx	done	Tue Apr 28 2015 06:19:33 AM	1	NX95-Pri	download timed out
ap6532-347800	ap6532	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap6532-A6572	ap6532	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6532-3475E4	ap6532	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap8132-73BE2	ap81xx	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6511-8A4B1	ap6511	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6532-A6572	ap6532	done	Wed May 6 2015 12:59:30 AM	1	NX95-Pri	Update error: Unable to get
ap6532-347800	ap6532	done	Wed May 6 2015 12:59:30 AM	1	NX95-Pri	Update error: Unable to get
ap650-2433AC	ap650	done	Wed May 6 2015 12:59:24 AM	1	NX95-Pri	Update error: Unable to get

Row Count: 2047

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

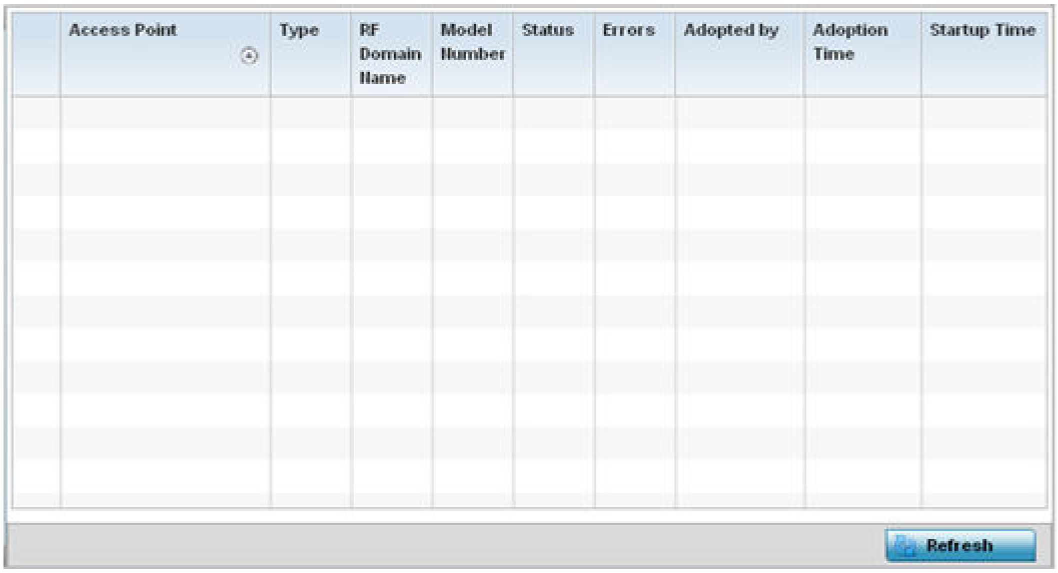
Adopted APs

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, select a **controller or service platform**, and select one of its 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.



	Access Point	Type	RF Domain Name	Model Number	Status	Errors	Adopted by	Adoption Time	Startup Time

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.

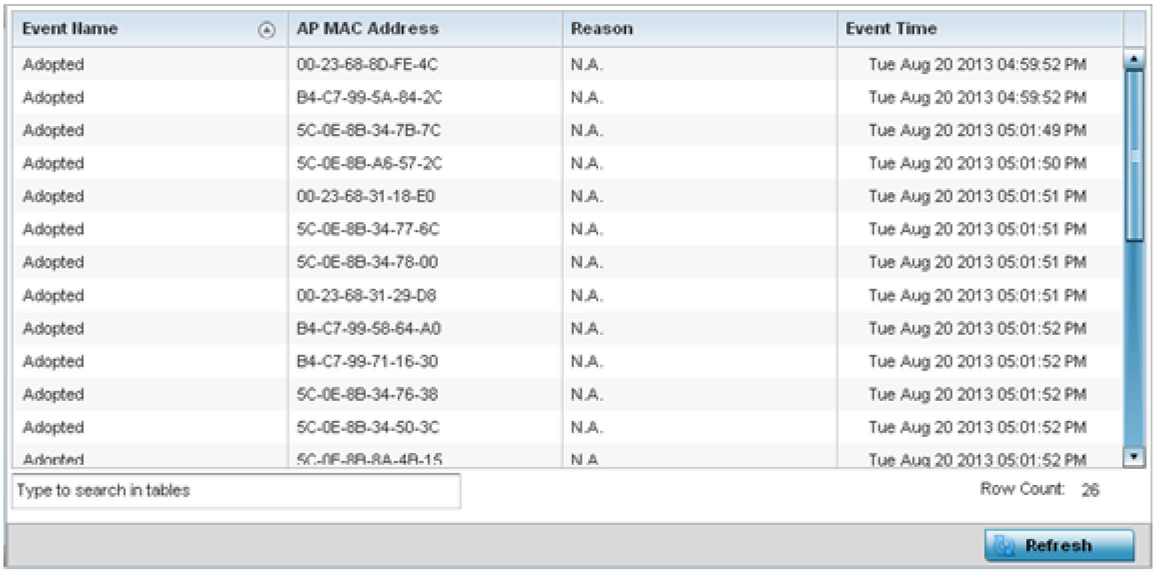
2 Expand the **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Event Name	AP MAC Address	Reason	Event Time
Adopted	00-23-68-8D-FE-4C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	B4-C7-99-5A-84-2C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	5C-0E-8B-34-7B-7C	N.A.	Tue Aug 20 2013 05:01:49 PM
Adopted	5C-0E-8B-A6-57-2C	N.A.	Tue Aug 20 2013 05:01:50 PM
Adopted	00-23-68-31-18-E0	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-77-6C	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-78-00	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	00-23-68-31-29-D8	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	B4-C7-99-58-64-A0	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	B4-C7-99-71-16-30	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-76-38	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-50-3C	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-8A-4B-15	N.A.	Tue Aug 20 2013 05:01:52 PM

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.

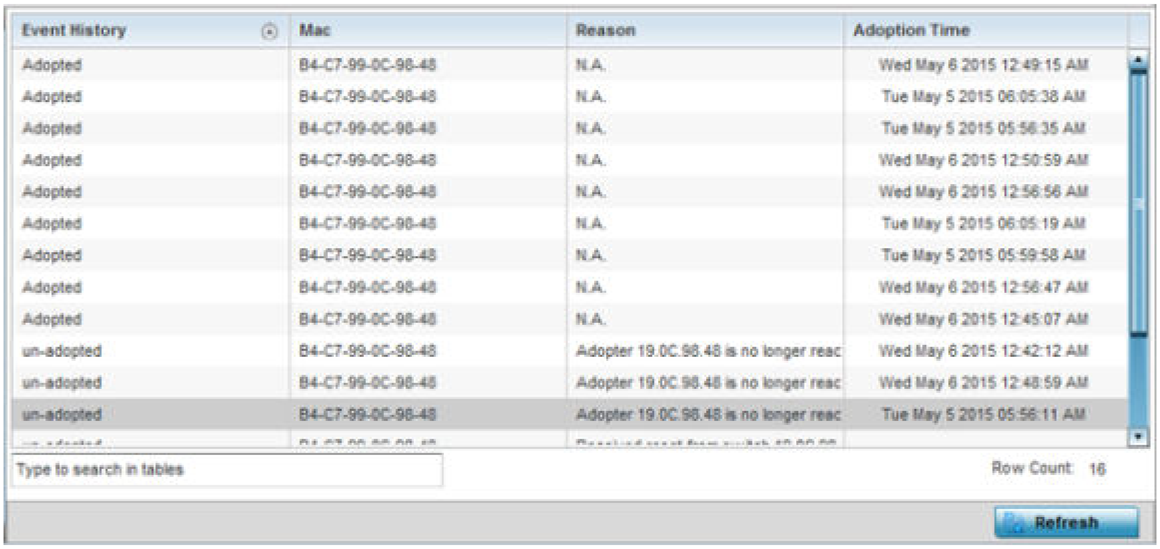
6 Select **Refresh** to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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.



Event History	Mac	Reason	Adoption Time
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:49:15 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 06:05:38 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 05:56:35 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:50:59 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:56:56 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 06:05:19 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 05:59:58 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:56:47 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:45:07 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Wed May 6 2015 12:42:12 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Wed May 6 2015 12:48:59 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Tue May 5 2015 05:56:11 AM

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.

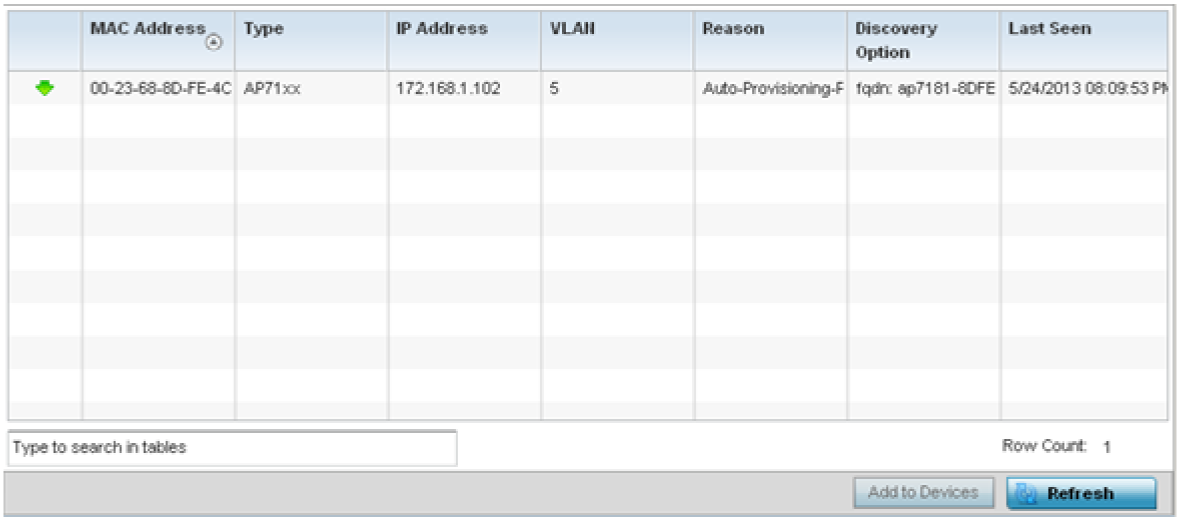
6 Select **Refresh** to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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**.



	MAC Address	Type	IP Address	VLAN	Reason	Discovery Option	Last Seen
▼	00-23-68-8D-FE-4C	AP71xx	172.168.1.102	5	Auto-Provisioning-F	fqdn: ap7181-8DFE	5/24/2013 08:09:53 P

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.

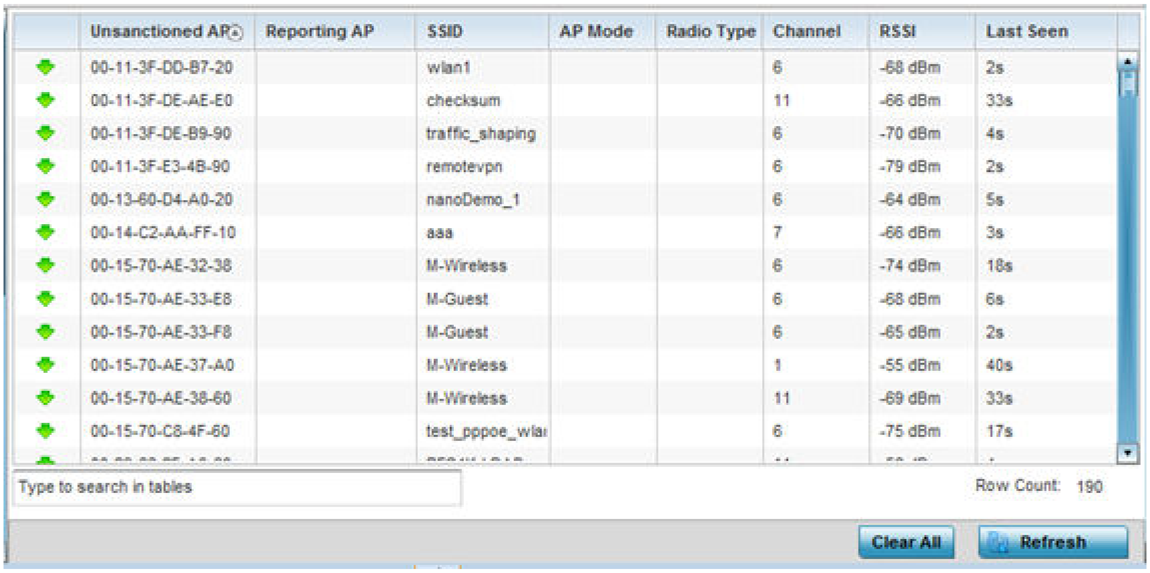
AP Detection

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, select a **controller or service platform**, and select one of its 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.



	Unsanctioned AP	Reporting AP	SSID	AP Mode	Radio Type	Channel	RSSI	Last Seen
◆	00-11-3F-DD-B7-20		wlan1			6	-68 dBm	2s
◆	00-11-3F-DE-AE-E0		checksum			11	-66 dBm	33s
◆	00-11-3F-DE-B9-90		traffic_shaping			6	-70 dBm	4s
◆	00-11-3F-E3-4B-90		remotevpn			6	-79 dBm	2s
◆	00-13-60-D4-A0-20		nanoDemo_1			6	-64 dBm	5s
◆	00-14-C2-AA-FF-10		aaa			7	-66 dBm	3s
◆	00-15-70-AE-32-38		M-Wireless			6	-74 dBm	18s
◆	00-15-70-AE-33-E8		M-Guest			6	-68 dBm	6s
◆	00-15-70-AE-33-F8		M-Guest			6	-65 dBm	2s
◆	00-15-70-AE-37-A0		M-Wireless			1	-55 dBm	40s
◆	00-15-70-AE-38-60		M-Wireless			11	-69 dBm	33s
◆	00-15-70-C8-4F-60		test_pppoe_wla			6	-75 dBm	17s

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.

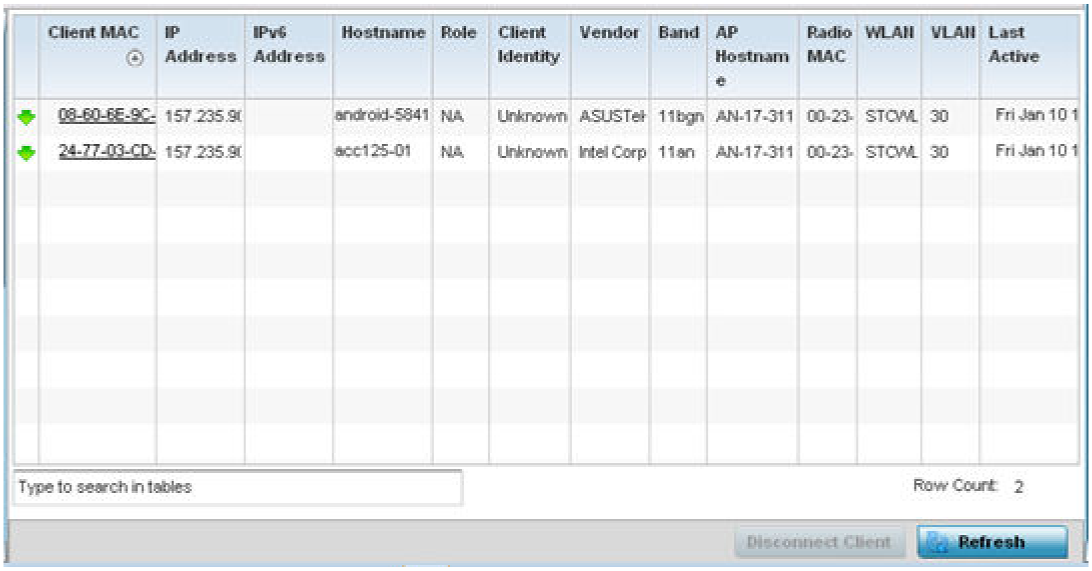
AP Wireless Clients

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, select a **controller or service platform**, and select one of its 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.



Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
08-60-6E-9C-	157.235.9		android-5841	NA	Unknown	ASUSTel	11bgn	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1
24-77-03-CD-	157.235.9		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1

Row Count: 2

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:

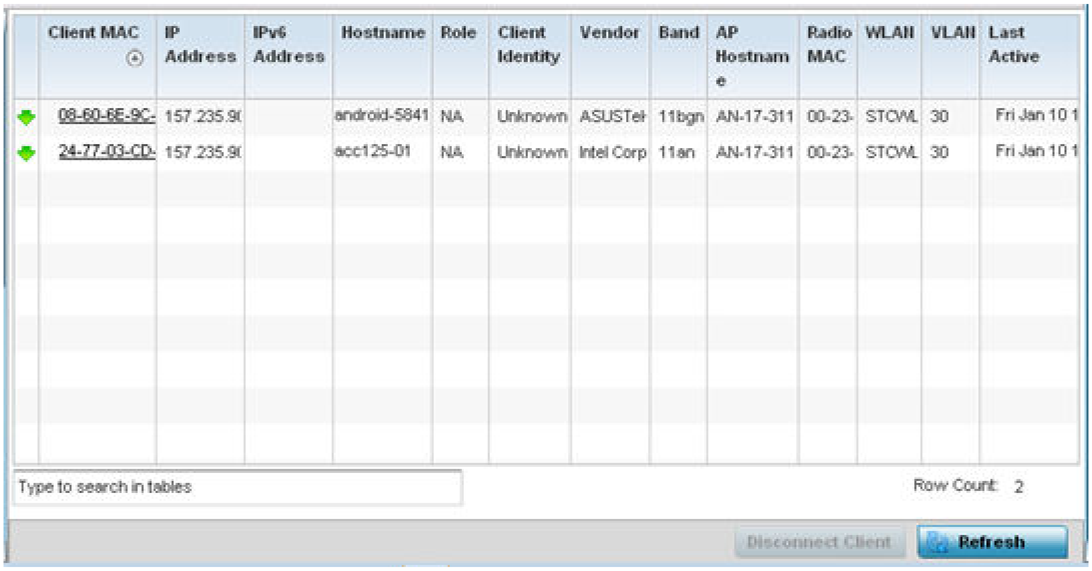
AP Wireless LANs

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, select a **controller or service platform**, and select one of its 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.



	Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
	08-60-6E-9C-	157.235.9		android-5841	NA	Unknown	ASUSTel	11bgn	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1
	24-77-03-CD-	157.235.9		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1

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. Traffic indices are: • *0 – 20* (very low utilization) • *20 – 40* (low utilization) • *40 – 60* (moderate utilization) • *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.

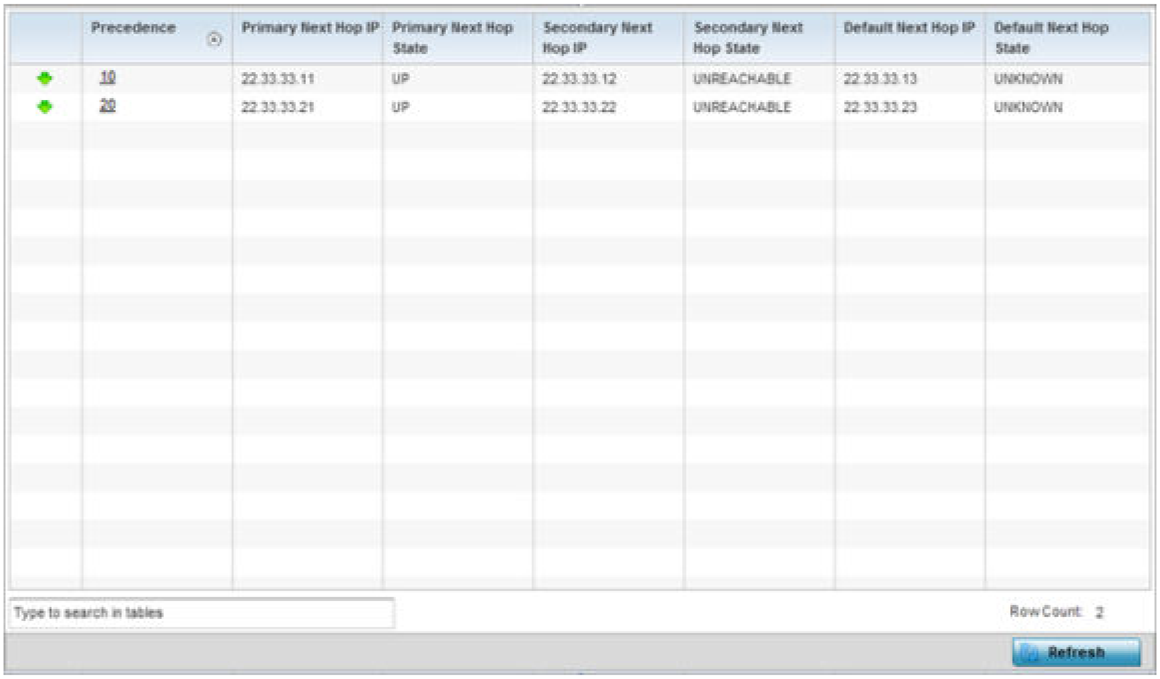
6 Select **Refresh** to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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.**



	Precedence	Primary Next Hop IP	Primary Next Hop State	Secondary Next Hop IP	Secondary Next Hop State	Default Next Hop IP	Default Next Hop State
●	10	22.33.33.11	UP	22.33.33.12	UNREACHABLE	22.33.33.13	UNKNOWN
●	20	22.33.33.21	UP	22.33.33.22	UNREACHABLE	22.33.33.23	UNKNOWN

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 1235
- AP Radio RF Statistics on page 1236
- AP Radio Traffic Statistics on page 1238

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

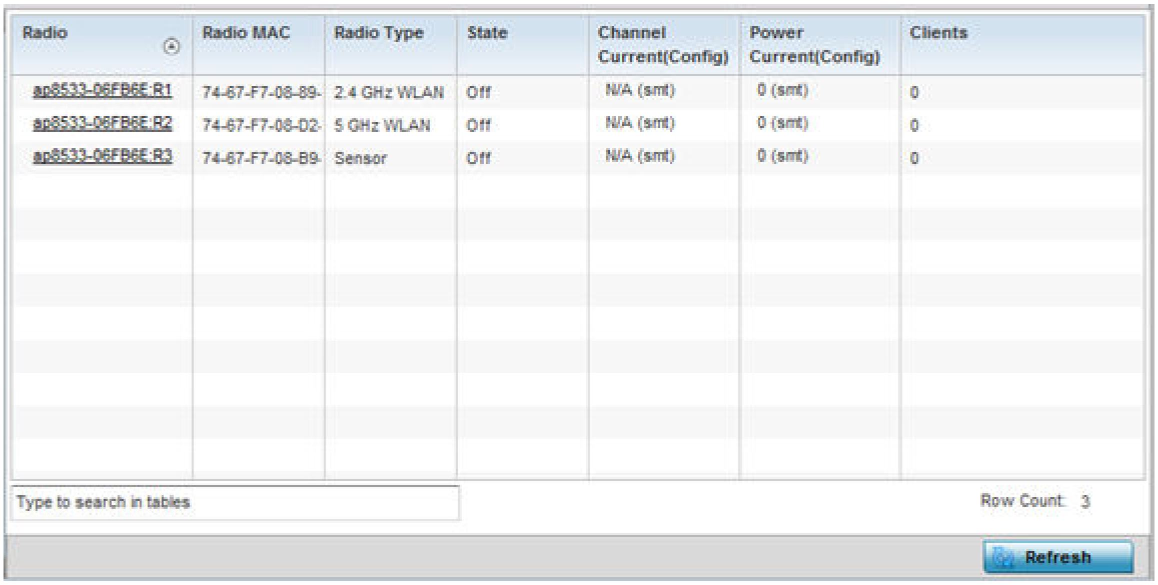
Use the **Status** screen to review access point radio stats in detail. Optionally select individual and access points and launch sub screens with granular performance data. Review radios, operational states, channel utilization and power consumption to assess whether a radio is optimally configured 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, select a **controller or service platform**, and select one of its 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.



Radio	Radio MAC	Radio Type	State	Channel Current(Config)	Power Current(Config)	Clients
ap8533-06FB6E:R1	74-67-F7-08-89-	2.4 GHz WLAN	Off	N/A (smt)	0 (smt)	0
ap8533-06FB6E:R2	74-67-F7-08-D2-	5 GHz WLAN	Off	N/A (smt)	0 (smt)	0
ap8533-06FB6E:R3	74-67-F7-08-B9-	Sensor	Off	N/A (smt)	0 (smt)	0

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.

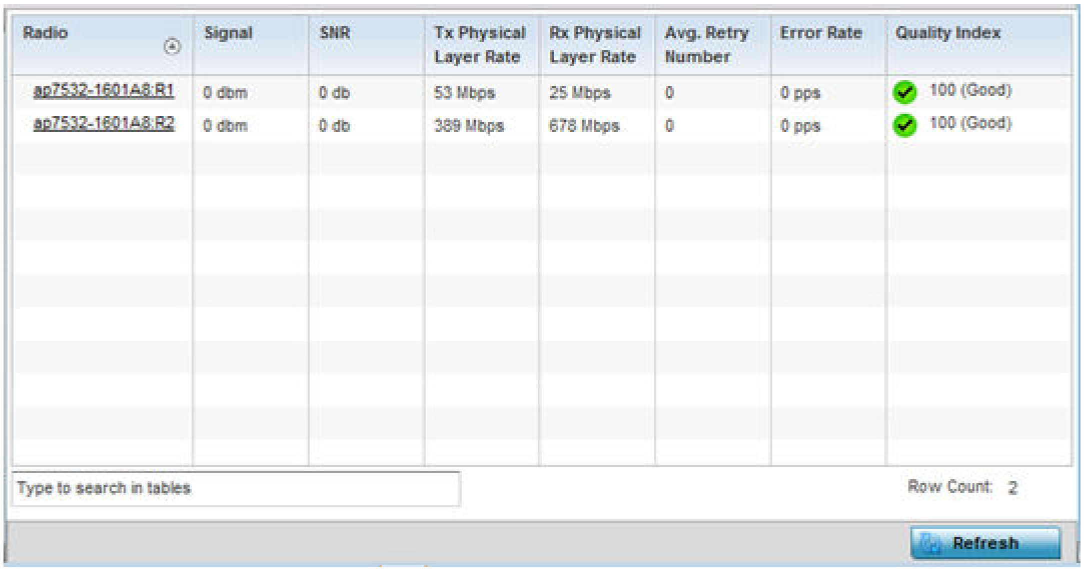
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Radio	Signal	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Avg. Retry Number	Error Rate	Quality Index
ap7532-1601A8:R1	0 dbm	0 db	53 Mbps	25 Mbps	0	0 pps	✓ 100 (Good)
ap7532-1601A8:R2	0 dbm	0 db	389 Mbps	678 Mbps	0	0 pps	✓ 100 (Good)

Row Count: 2

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: • *0 – 50* (poor) • *50 – 75* (medium) • *75 – 100* (good)

6 Select **Refresh** to update the screen's statistics counters to their latest values.

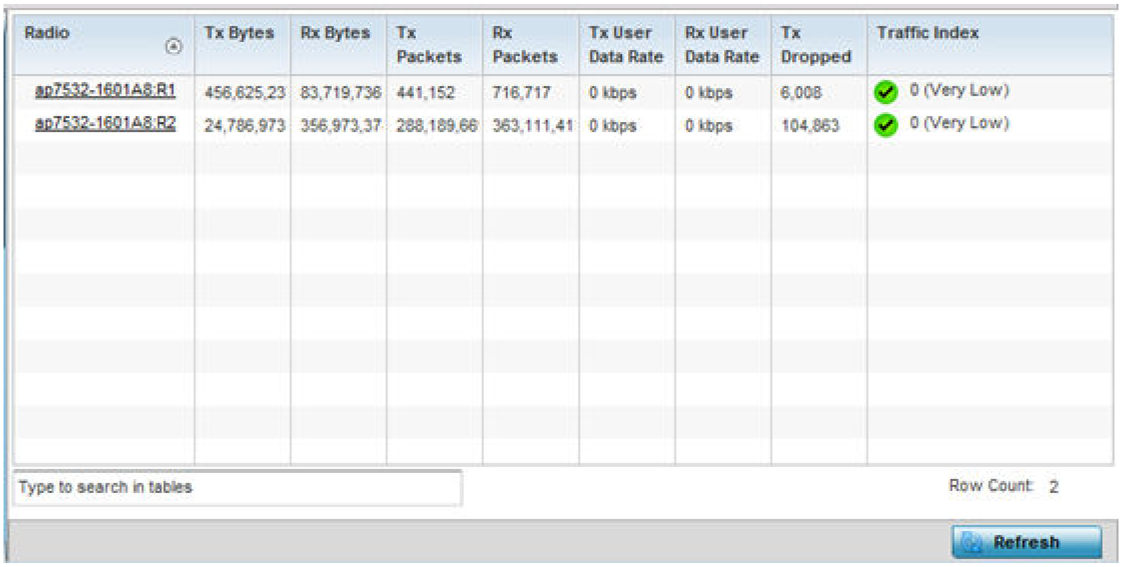
AP Radio Traffic Statistics

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, select a **controller or service platform**, and select one of its 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.



Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Traffic Index
ap7532-1601A8:R1	456,625,23	83,719,736	441,152	716,717	0 kbps	0 kbps	6,008	✓ 0 (Very Low)
ap7532-1601A8:R2	24,786,973	356,973,37	288,189,66	363,111,41	0 kbps	0 kbps	104,863	✓ 0 (Very Low)

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.

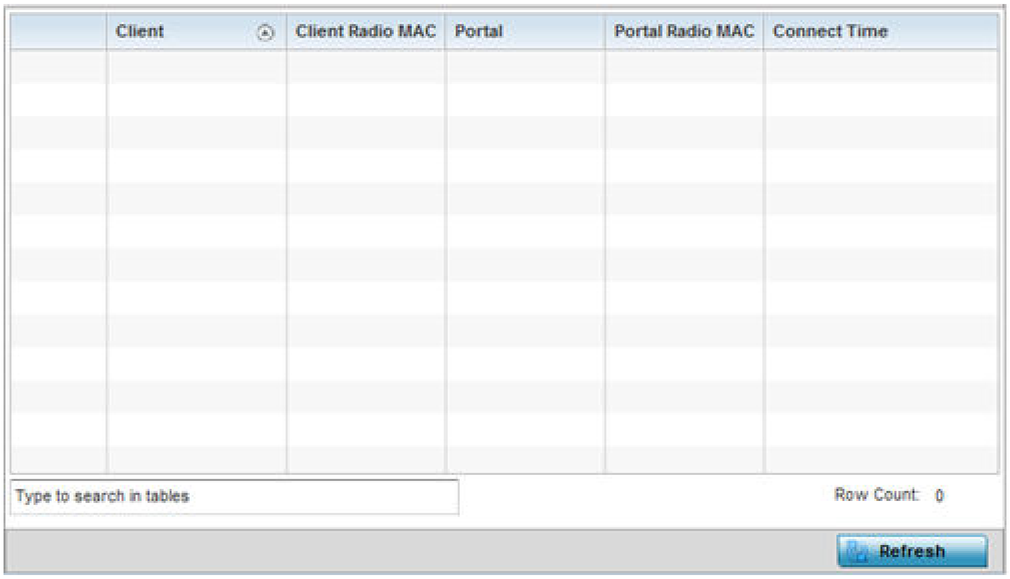
AP Mesh

The Mesh screen provides detailed statistics on each Mesh capable client available within the selected access point's radio coverage area.

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, select a **controller or service platform**, and select one of its 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 1240
- AP Interface IPv6 Address on page 1244
- AP Interface Multicast Groups Joined on page 1247
- AP Interface Network Graph on page 1248

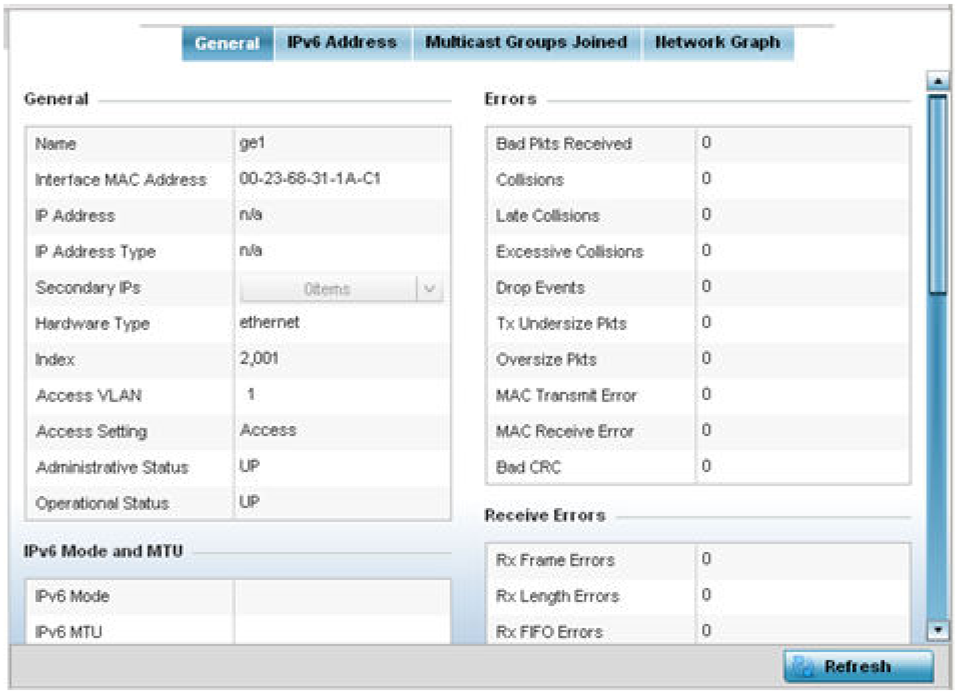
AP Interface General Statistics

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, select a **controller or service platform**, and select one of its 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.



General

Name	ge1
Interface MAC Address	00-23-68-31-1A-C1
IP Address	n/a
IP Address Type	n/a
Secondary IPs	0items
Hardware Type	ethernet
Index	2,001
Access VLAN	1
Access Setting	Access
Administrative Status	UP
Operational Status	UP

IPv6 Mode and MTU

IPv6 Mode	
IPv6 MTU	

Errors

Bad Pkts Received	0
Collisions	0
Late Collisions	0
Excessive Collisions	0
Drop Events	0
Tx Undersize Pkts	0
Oversize Pkts	0
MAC Transmit Error	0
MAC Receive Error	0
Bad CRC	0

Receive Errors

Rx Frame Errors	0
Rx Length Errors	0
Rx FIFO Errors	0

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. Medium types include: **`Copper`** - Used on RJ-45 Ethernet ports **`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: • **`Access`** – This Ethernet interface accepts packets only from the native VLANs. • **`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.

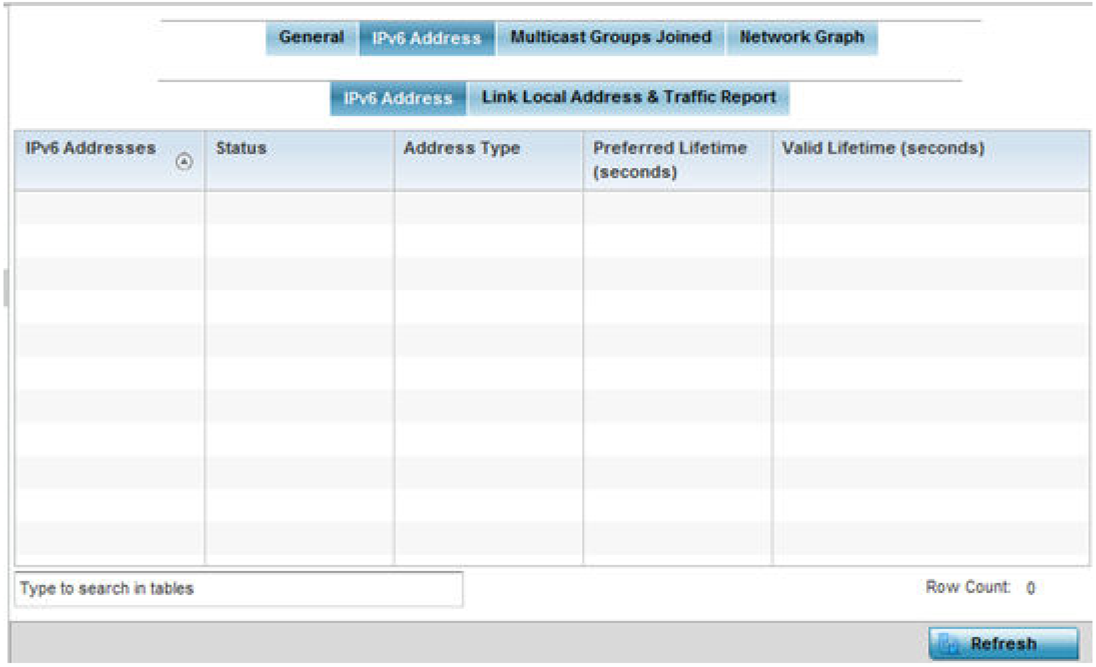
To review IPv6 Address interface statistics:

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, select a **controller or service platform**, and select one of its 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.



IPv6 Addresses	Status	Address Type	Preferred Lifetime (seconds)	Valid Lifetime (seconds)

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.

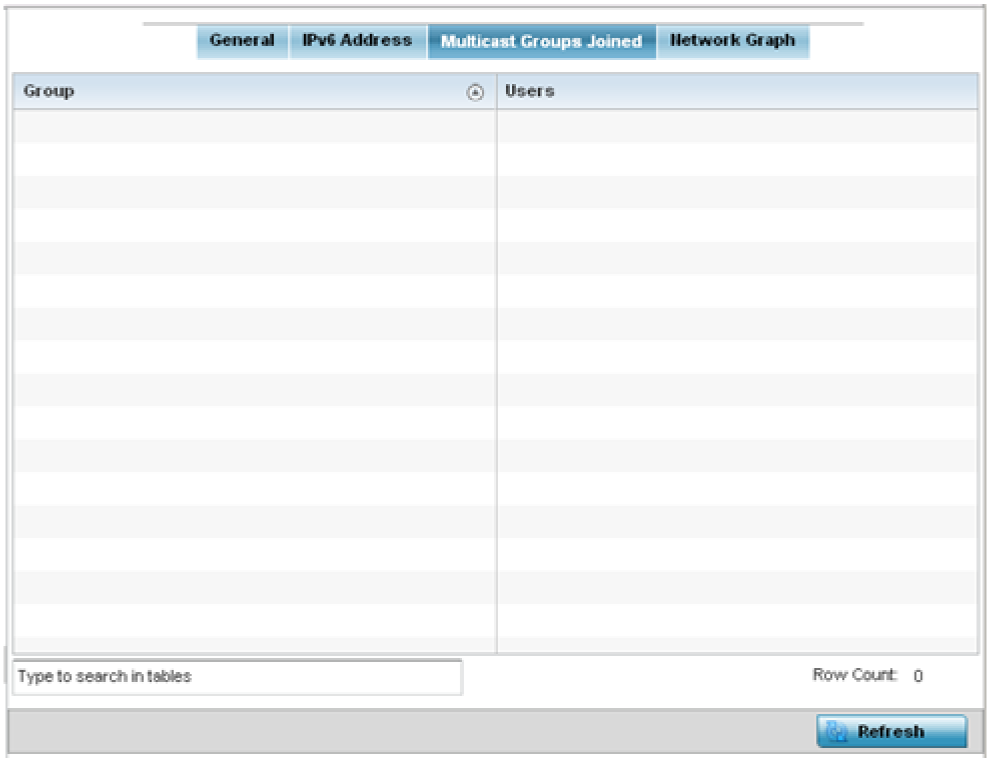
To view the Access Point’s multicast group memberships on the selected interface:

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, select a **controller or service platform**, and select one of its 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).

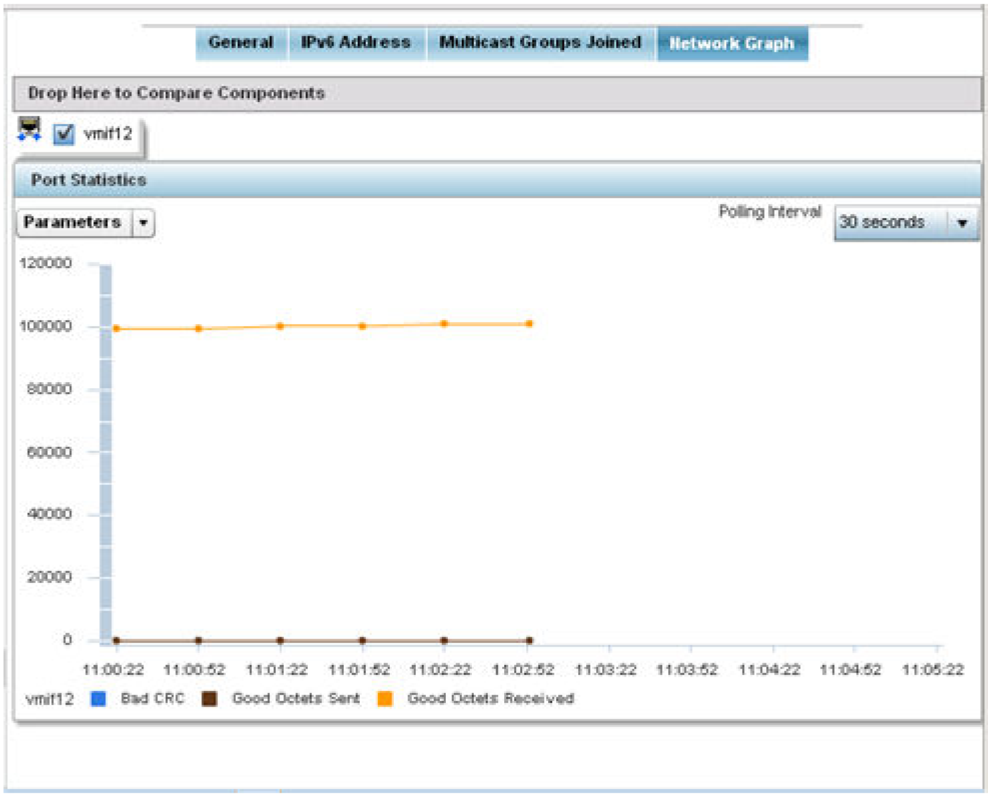
   The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Polling Interval 30 seconds

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:

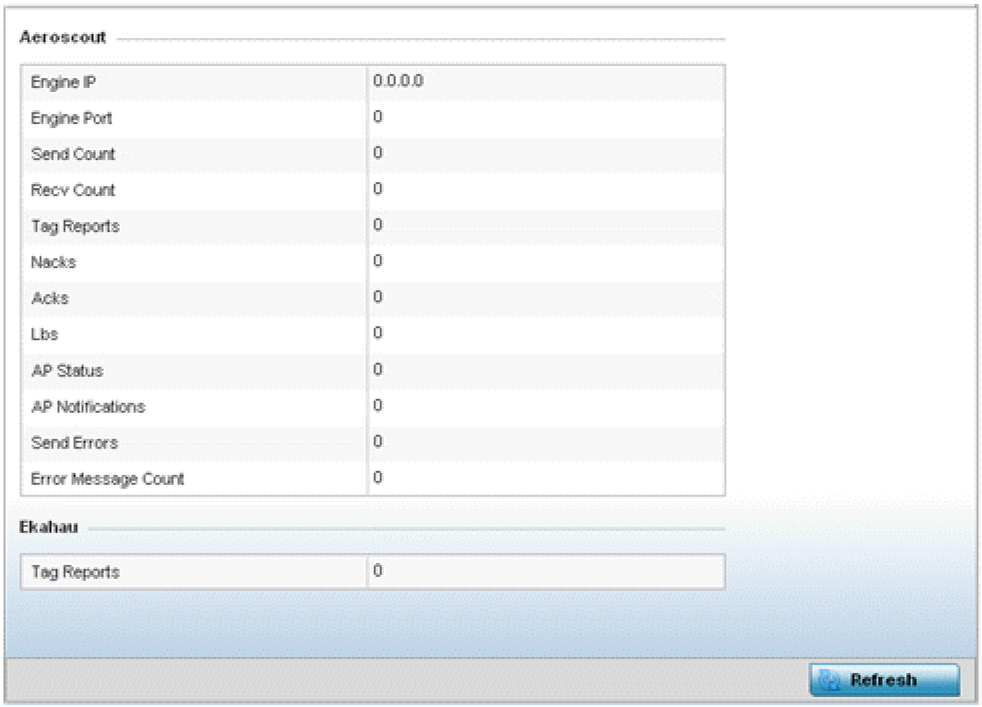
1 Select the Statistics menu from the Web UI.

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, select a **controller or service platform**, and select one of its 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.



Aeroscout

Engine IP	0.0.0.0
Engine Port	0
Send Count	0
Recv Count	0
Tag Reports	0
Nacks	0
Acks	0
Lbs	0
AP Status	0
AP Notifications	0
Send Errors	0
Error Message Count	0

Ekahau

Tag Reports	0

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.

To review a selected access point's PPPoE statistics:

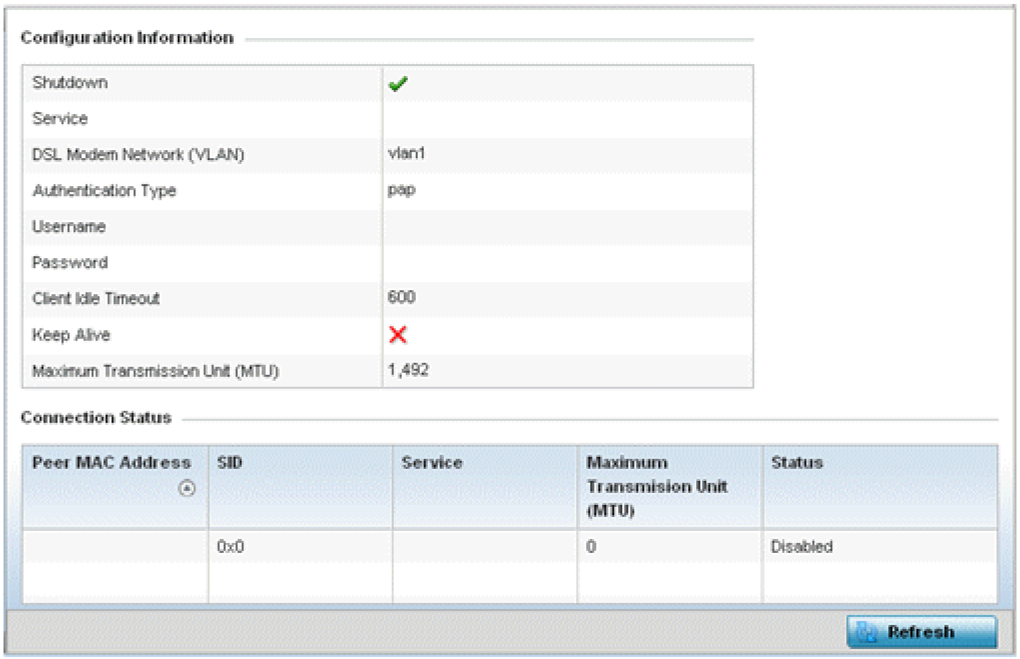
1 Select the Statistics menu from the Web UI.

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, select a **controller or service platform**, and select one of its 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.



Configuration Information

Shutdown	✓
Service	
DSL Modem Network (VLAN)	vlan1
Authentication Type	pap
Username	
Password	
Client Idle Timeout	600
Keep Alive	✗
Maximum Transmission Unit (MTU)	1,492

Connection Status

Peer MAC Address	SID	Service	Maximum Transmision Unit (MTU)	Status
	0x0		0	Disabled

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 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.

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.

5 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:

- AP OSPF Summary on page 1253
- AP OSPF Neighbors on page 1254
- AP OSPF Area Details on page 1256
- AP OSPF Route Statistics on page 1257
- AP OSPF Interface on page 1261
- AP OSPF State on page 1262

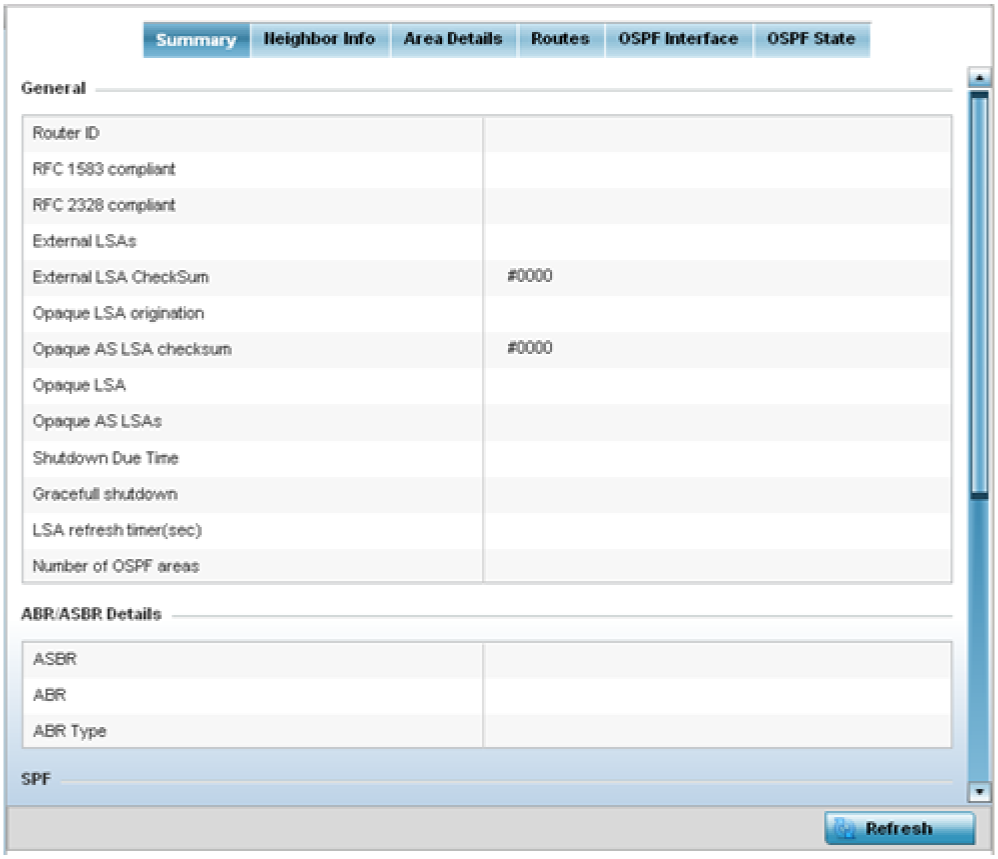
AP OSPF Summary

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, select a **controller or service platform**, and select one of its 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.



General

Router ID	
RFC 1583 compliant	
RFC 2328 compliant	
External LSAs	
External LSA CheckSum	#0000
Opaque LSA origination	
Opaque AS LSA checksum	#0000
Opaque LSA	
Opaque AS LSAs	
Shutdown Due Time	
Gracefull shutdown	
LSA refresh timer(sec)	
Number of OSPF areas	

ABR/ASBR Details

ASBR	
ABR	
ABR Type	

SPF

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.

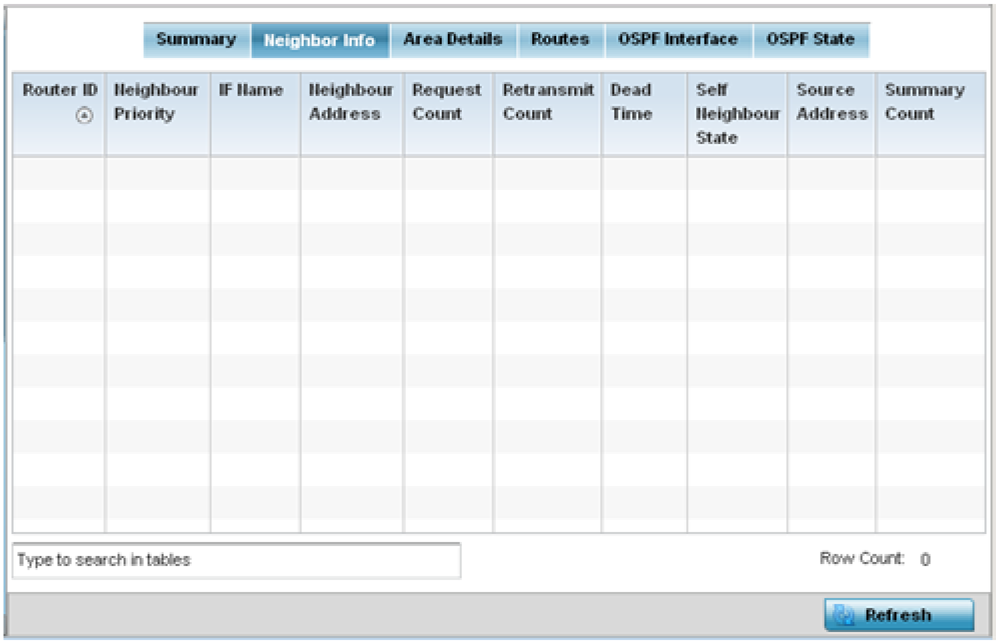
AP OSPF Neighbors

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, select a **controller or service platform**, and select one of its 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.



Summary | Neighbor Info | Area Details | Routes | OSPF Interface | OSPF State

Router ID	Neighbour Priority	IF Name	Neighbour Address	Request Count	Retransmit Count	Dead Time	Self Neighbour State	Source Address	Summary Count

Row Count: 0

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.

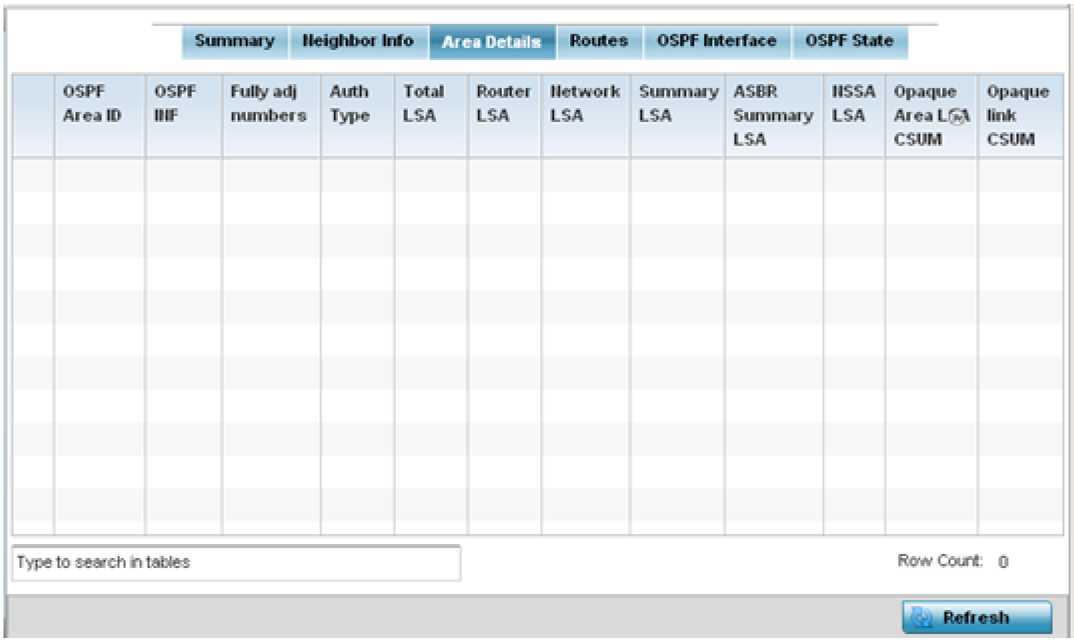
AP OSPF Area Details

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, select a **controller or service platform**, and select one of its 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.



	OSPF Area ID	OSPF INF	Fully adj numbers	Auth Type	Total LSA	Router LSA	Network LSA	Summary LSA	ASBR Summary LSA	NSSA LSA	Opaque Area LSA CSUM	Opaque link CSUM

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. 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 1257.
- AP OSPF External Routes on page 1258.
- AP OSPF Network Routes on page 1259.
- AP OSPF Router Routes on page 1260.

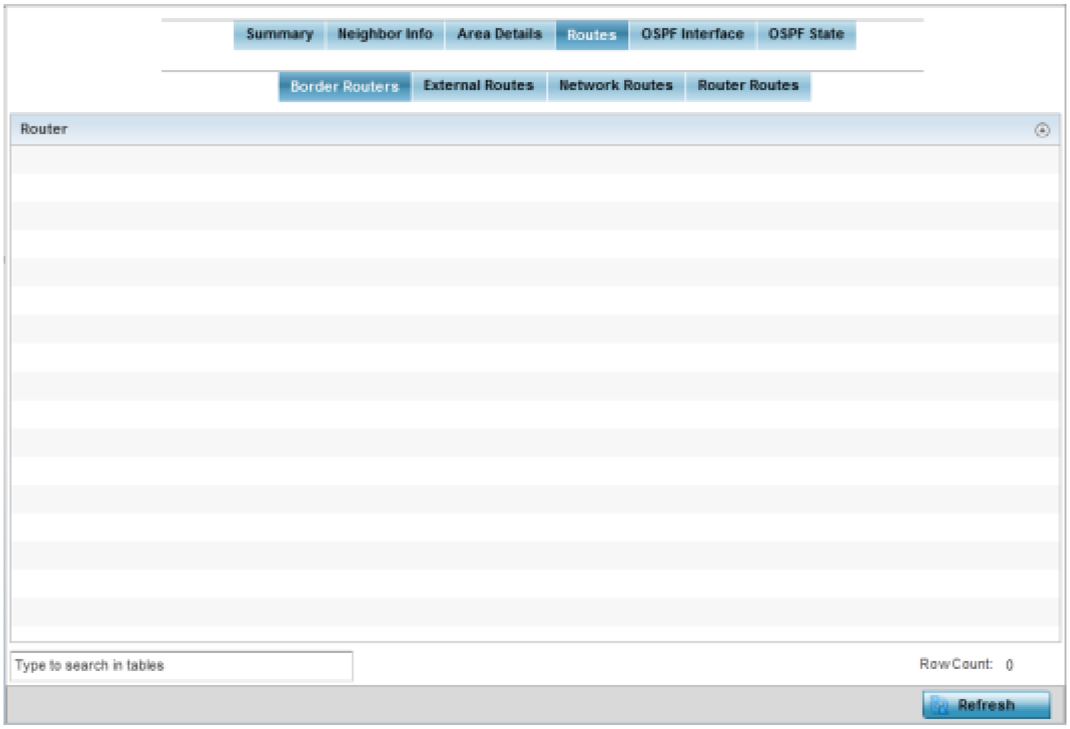
.

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, select a **controller or service platform**, and select one of its 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.

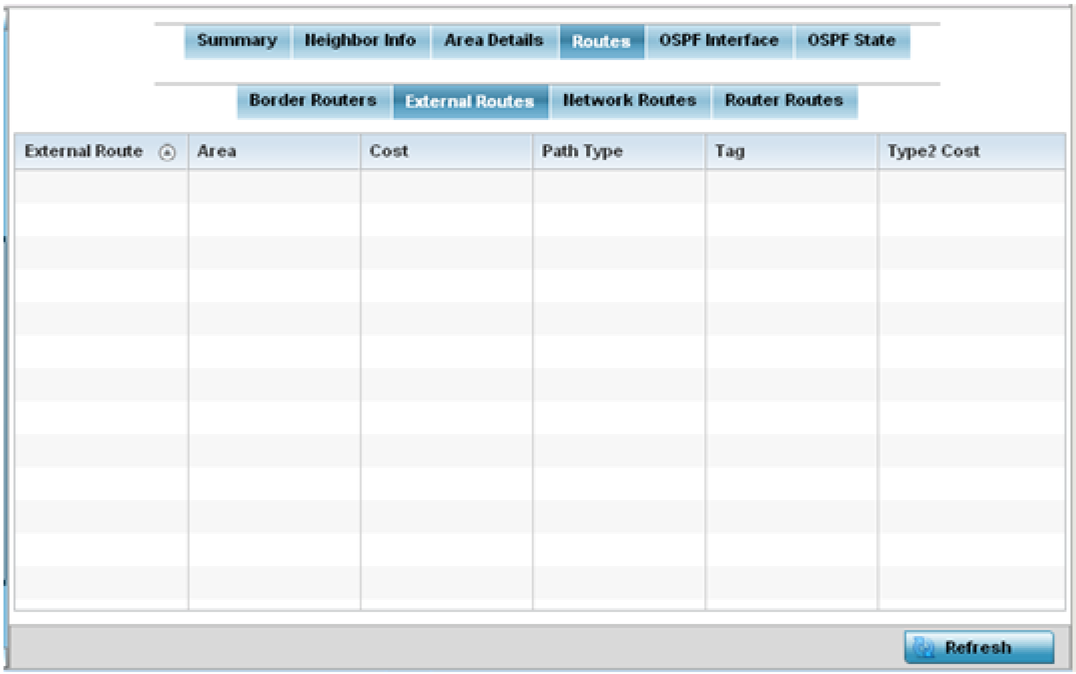
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller** or **service platform**, and select one of its connected **access points**. The selected device'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 Route	Area	Cost	Path Type	Tag	Type2 Cost

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.

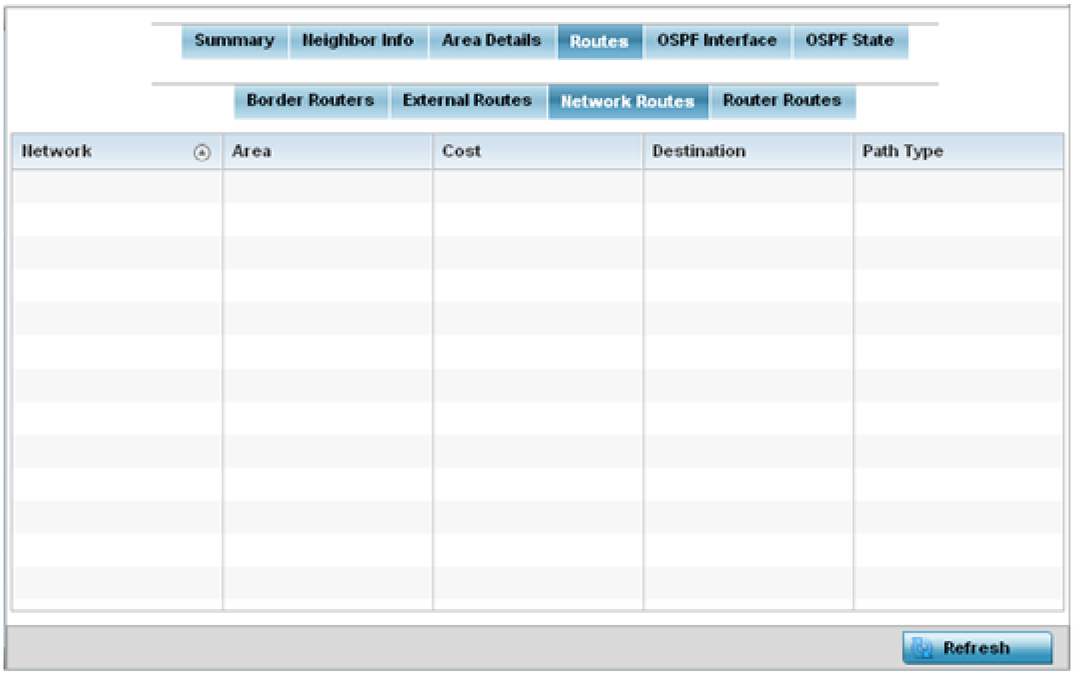
6 Select **Refresh** to update the statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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	Area	Cost	Destination	Path Type

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*.

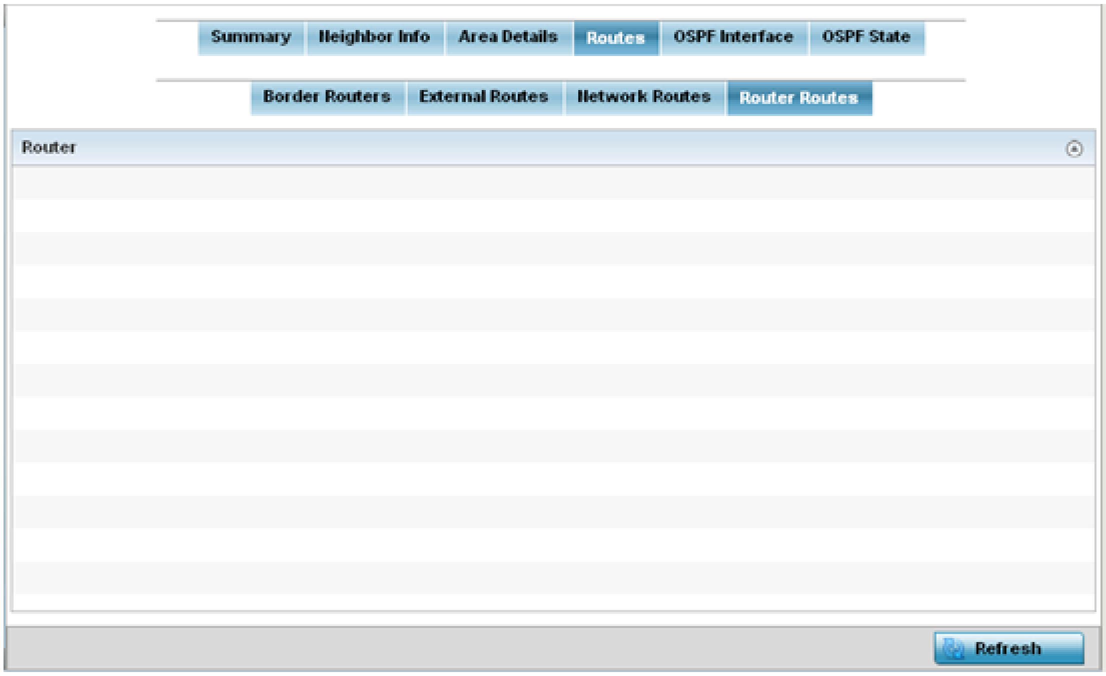
7 Select **Refresh** to update the statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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.

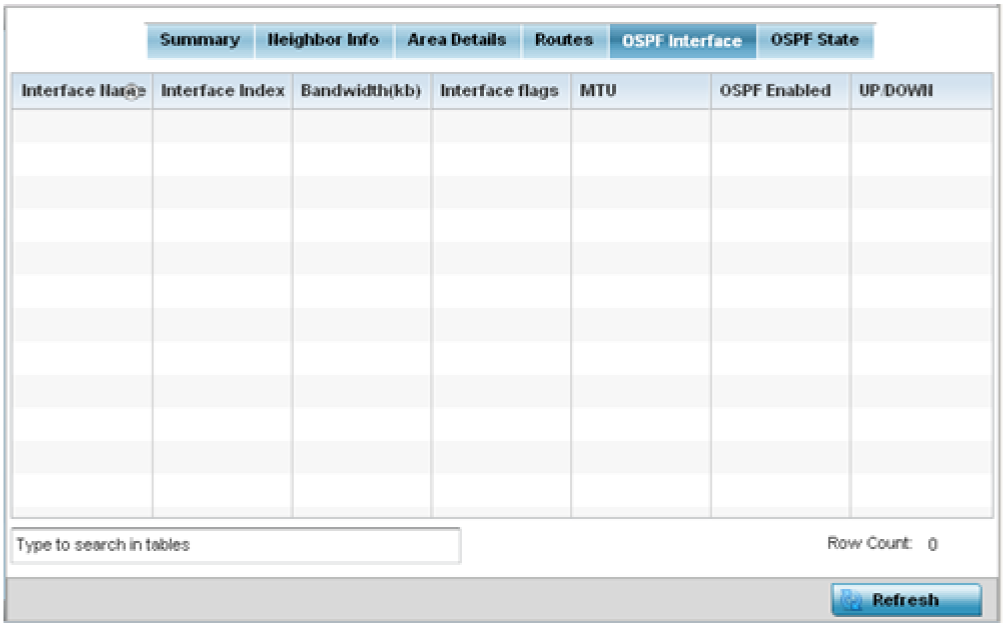
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.

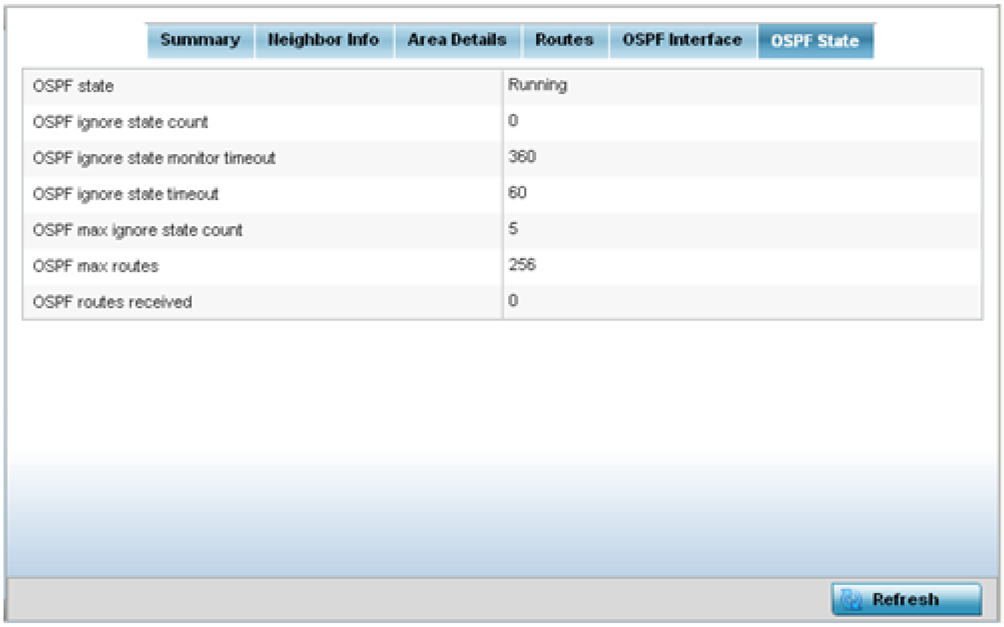
To view OSPF state statistics:

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, select a **controller or service platform**, and select one of its 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



OSPF state	Running
OSPF ignore state count	0
OSPF ignore state monitor timeout	360
OSPF ignore state timeout	60
OSPF max ignore state count	5
OSPF max routes	256
OSPF routes received	0

The OSPF Statetab 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

AP-8432 and AP-8533 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-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 raises an alarm.

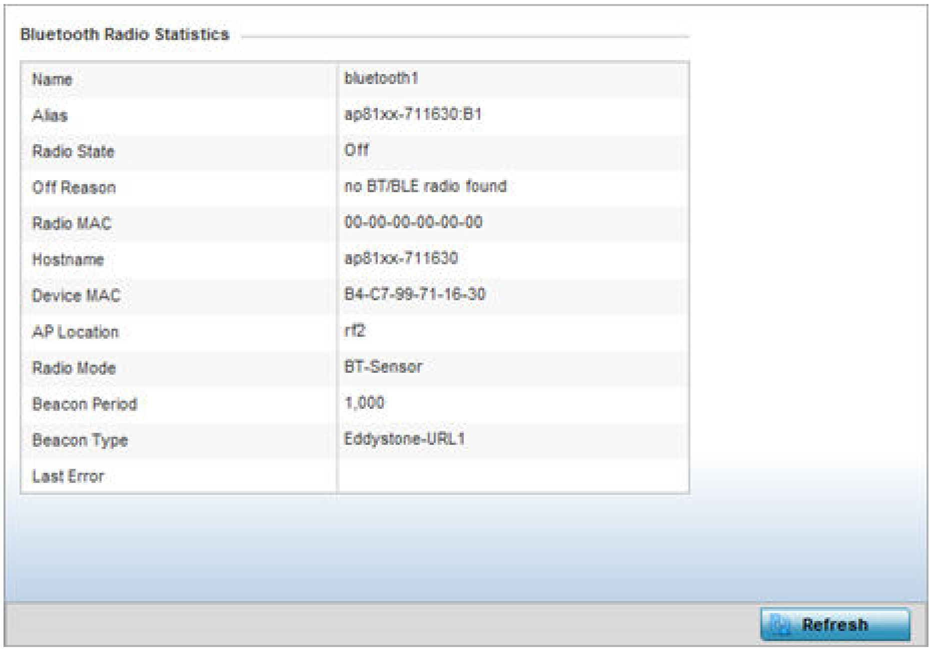
AP-8432 and AP-8533 model access points emit either iBeacon or Eddystone-URL beacons. The AP's Bluetooth radio periodically sends non-connectable, undirected LE *(low-energy)* advertisement packets. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are still customizable.

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, select a **controller or service platform**, and select one of its 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 **Buletooth**.

   The **Statistics** → **AP** → **Bluetooth** screen is displayed.



Bluetooth Radio Statistics

Name	bluetooth1
Alias	ap81xx-711630:B1
Radio State	Off
Off Reason	no BT/BLE radio found
Radio MAC	00-00-00-00-00-00
Hostname	ap81xx-711630
Device MAC	B4-C7-99-71-16-30
AP Location	rf2
Radio Mode	BT-Sensor
Beacon Period	1,000
Beacon Type	Eddystone-URL1
Last Error	

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.

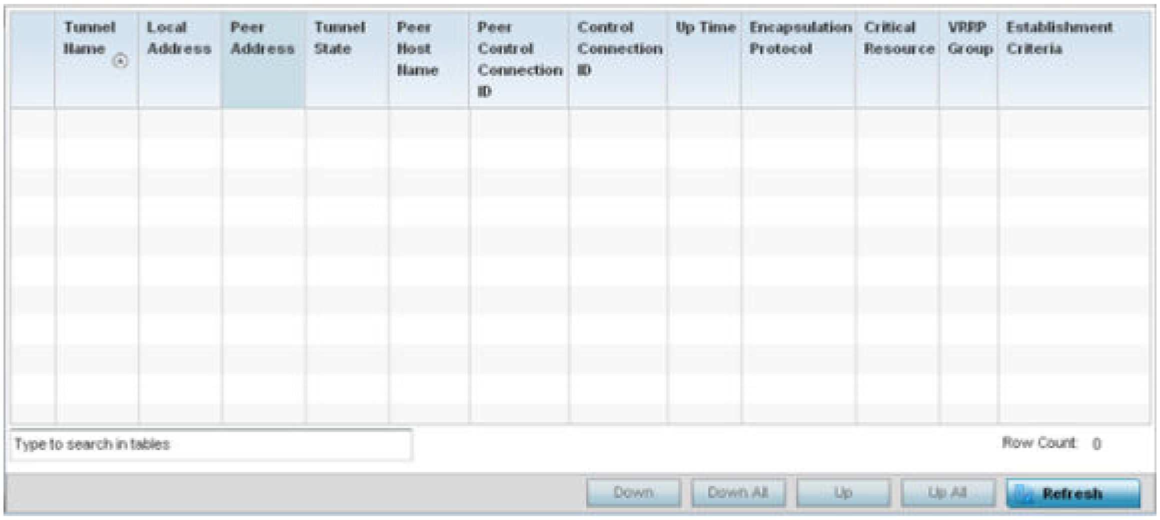
AP L2TPv3 Tunnels

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, select a **controller or service platform**, and select one of its 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:

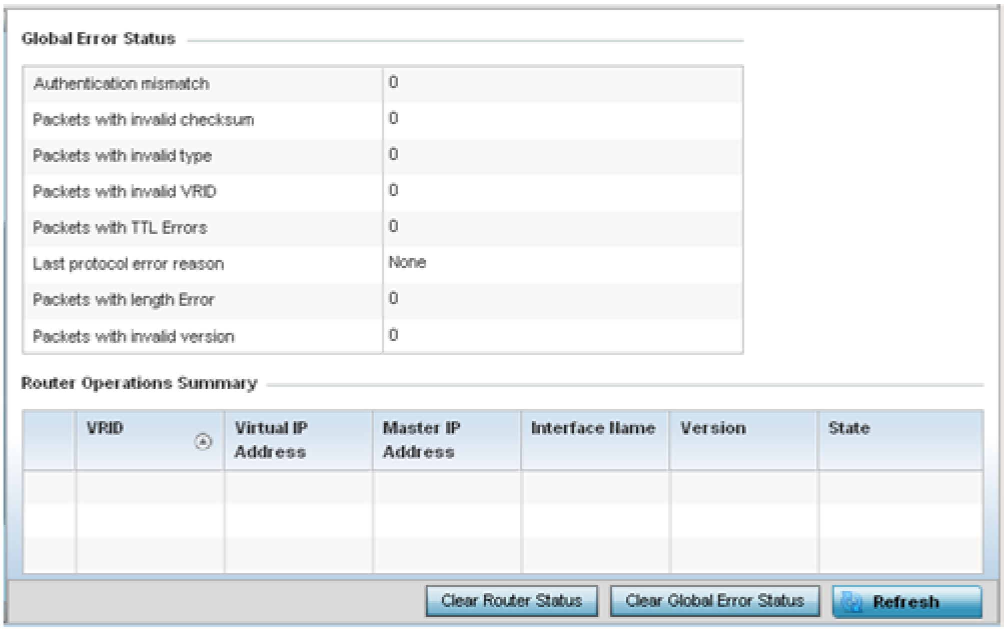
1 Select the **Statistics** menu from the Web UI.

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, select a **controller or service platform**, and select one of its 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.



Global Error Status

Authentication mismatch	0
Packets with invalid checksum	0
Packets with invalid type	0
Packets with invalid VRID	0
Packets with TTL Errors	0
Last protocol error reason	None
Packets with length Error	0
Packets with invalid version	0

Router Operations Summary

	VRID	Virtual IP Address	Master IP Address	Interface Name	Version	State

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:

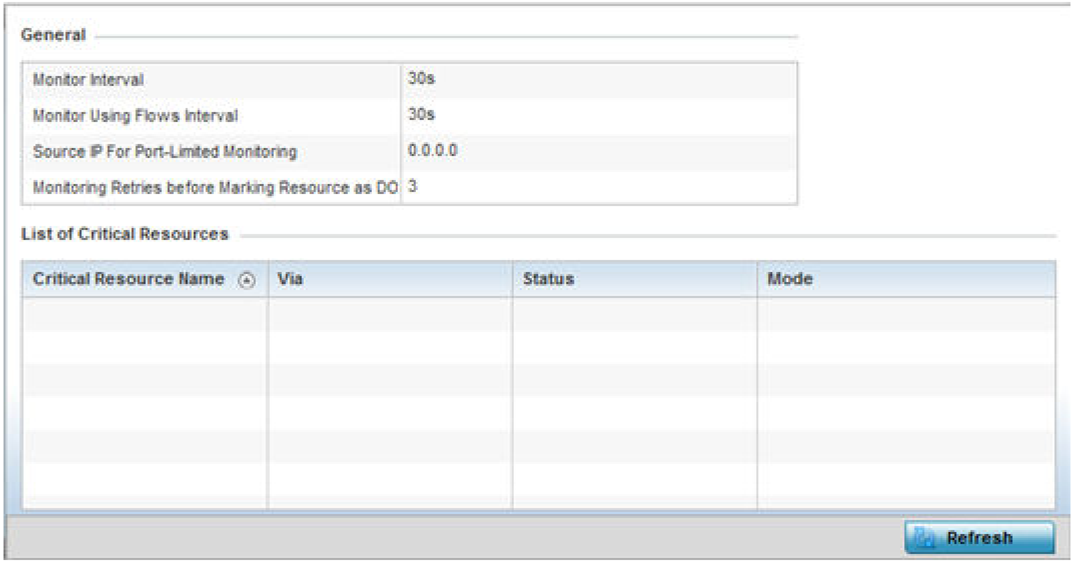
1 Select the Statistics menu from the Web UI.

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, select a **controller or service platform**, and select one of its 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.



General

Monitor Interval	30s
Monitor Using Flows Interval	30s
Source IP For Port-Limited Monitoring	0.0.0.0
Monitoring Retries before Marking Resource as DO	3

List of Critical Resources

Critical Resource Name	Via	Status	Mode

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

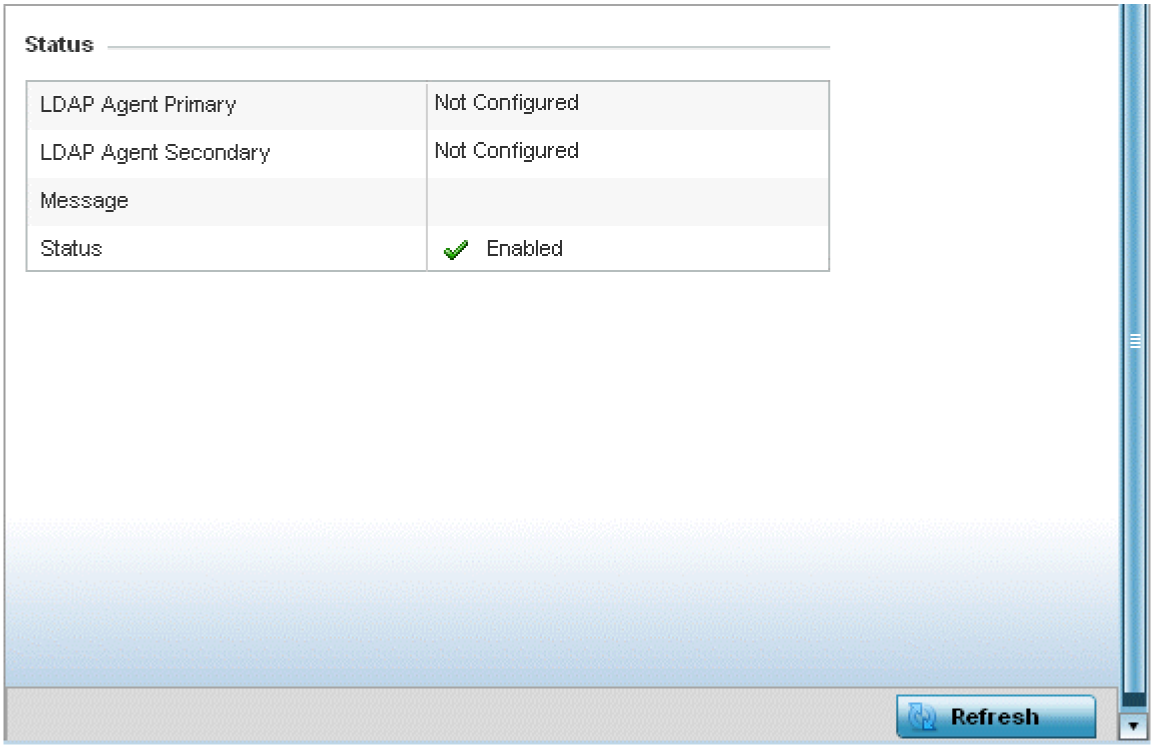
When LDAP has been specified as an external resource (as opposed to local access point RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP 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.

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, select a **controller or service platform**, and select one of its 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.



Status

LDAP Agent Primary	Not Configured
LDAP Agent Secondary	Not Configured
Message	
Status	✓ Enabled

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:

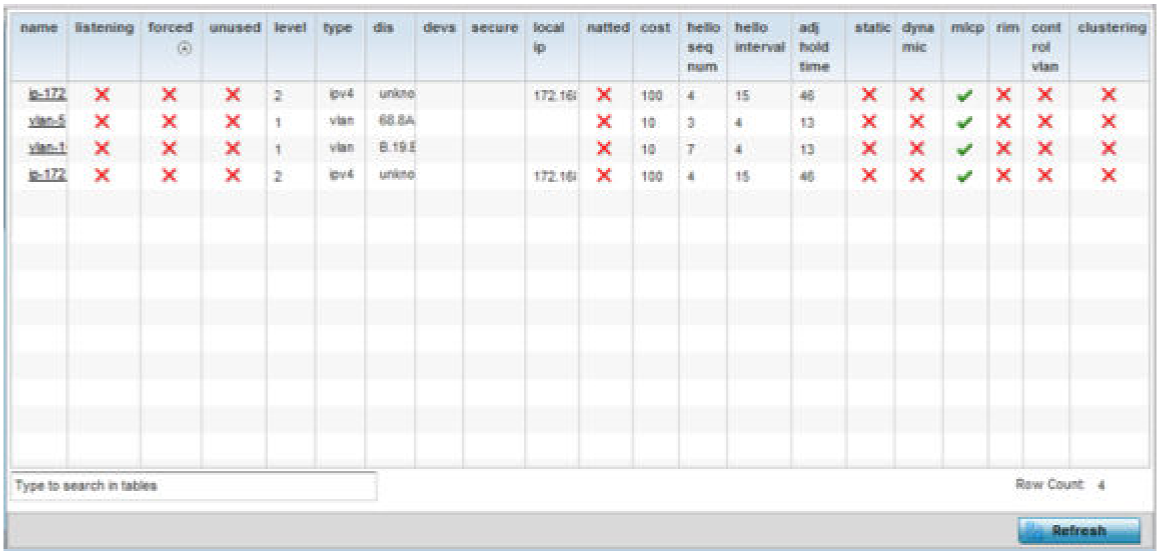
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node from the navigation pane (on the left-hand side of the screen).

   The System node expands to display the RF Domains created within the managed network.
3. Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



name	listening	forced	unused	level	type	dis	devs	secure	local ip	natted	cost	hello seq num	hello interval	adj hold time	static	dynamic	mlcp	rim	control vlan	clustering
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗
vlan-5	✗	✗	✗	1	vlan	68.8A				✗	10	3	4	13	✗	✗	✓	✗	✗	✗
vlan-1	✗	✗	✗	1	vlan	B.19.E				✗	10	7	4	13	✗	✗	✓	✗	✗	✗
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗

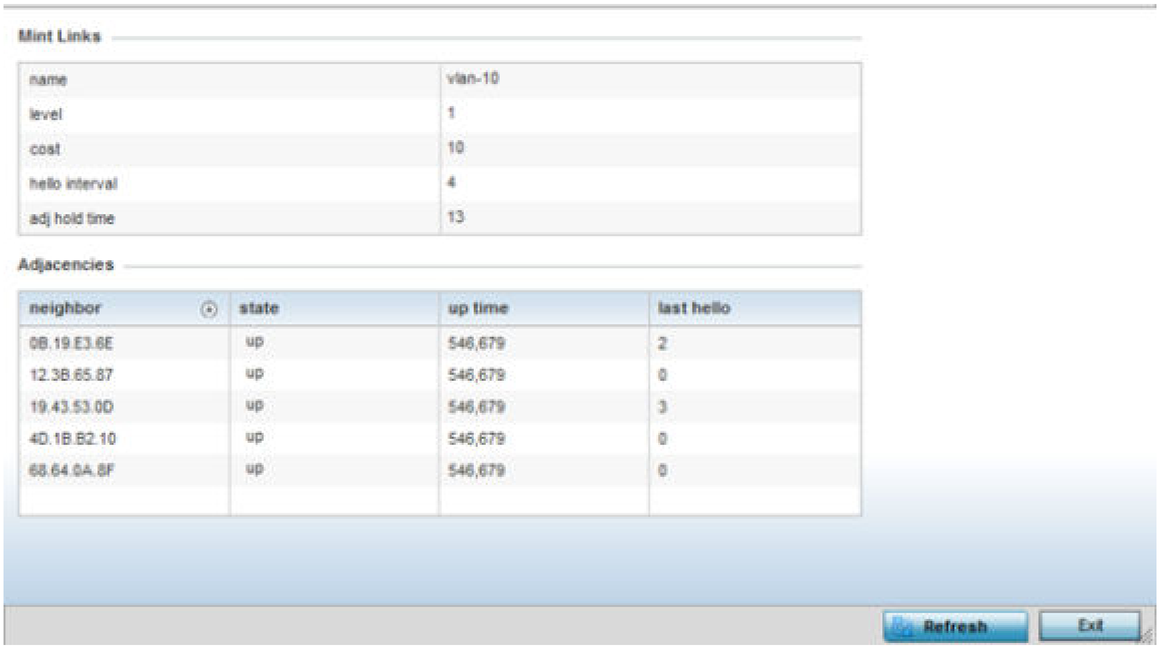
The Mint Links screen lists the name of the impacted VLAN or link in the form of a link that can be selected to display more granular information about that VLAN. A green check mark or a red X defines whether the listed VLAN is listening to traffic, forced to stay up or unused with the Mint link. The 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.



Mint Links

name	vlan-10
level	1
cost	10
hello interval	4
adj hold time	13

Adjacencies

neighbor	state	up time	last hello
0B.19.E3.6E	up	546,679	2
12.3B.65.87	up	546,679	0
19.43.53.0D	up	546,679	3
4D.1B.B2.10	up	546,679	0
68.64.0A.8F	up	546,679	0

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 834.

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).

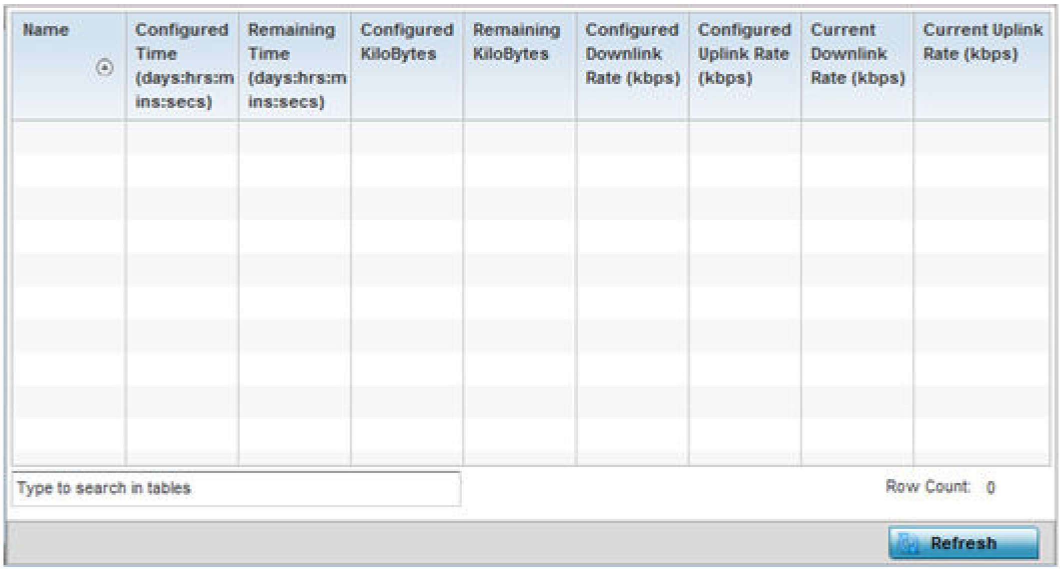
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Name	Configured Time (days:hrs:mins:secs)	Remaining Time (days:hrs:mins:secs)	Configured KiloBytes	Remaining KiloBytes	Configured Downlink Rate (kbps)	Configured Uplink Rate (kbps)	Current Downlink Rate (kbps)	Current Uplink Rate (kbps)

Type to search in tables

Row Count: 0

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 888.
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 888.

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 888.
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 888 .

5. Click **Refresh** to update the statistics counters to their latest values.

AP GRE Tunnel

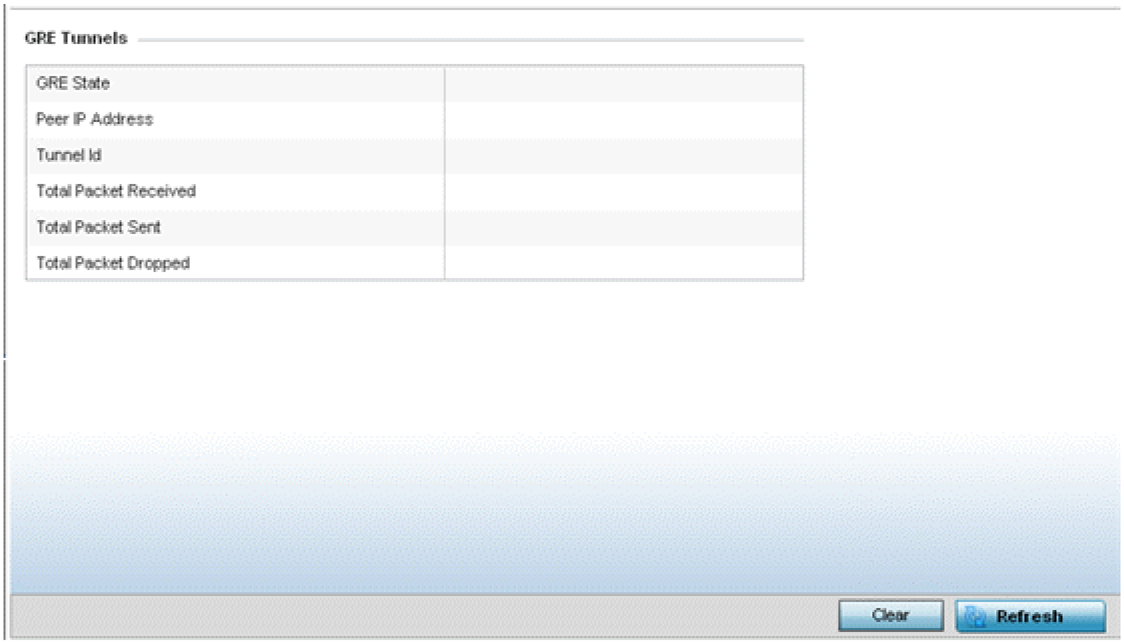
Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel 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, select a **controller or service platform**, and select one of its 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

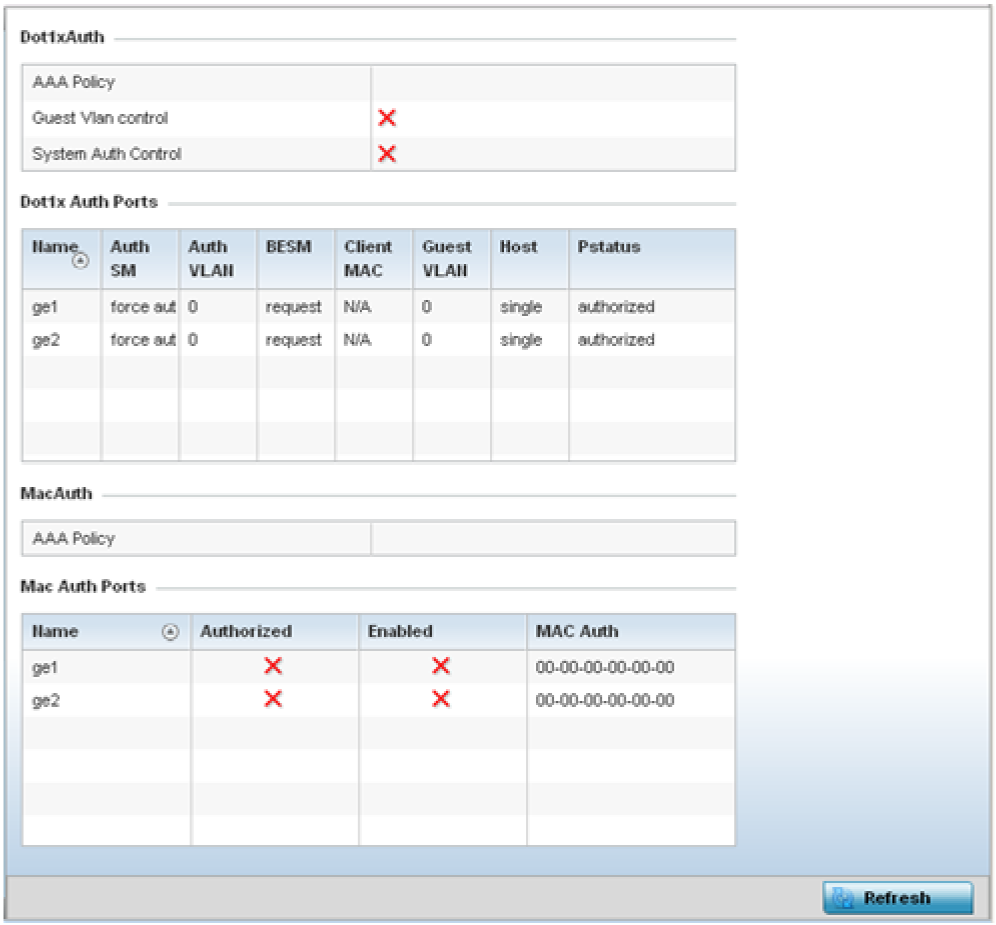
Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing 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, select a **controller or service platform**, and select one of its 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.



Dot1xAuth

AAA Policy	
Guest Vlan control	✗
System Auth Control	✗

Dot1x Auth Ports

Name	Auth SM	Auth VLAN	BESM	Client MAC	Guest VLAN	Host	Pstatus
ge1	force aut	0	request	N/A	0	single	authorized
ge2	force aut	0	request	N/A	0	single	authorized

MacAuth

AAA Policy	

Mac Auth Ports

Name	Authorized	Enabled	MAC Auth
ge1	✗	✗	00-00-00-00-00-00
ge2	✗	✗	00-00-00-00-00-00

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 1278
- AP Network Route Entries on page 1279
- AP Network Default Routes on page 1281
- AP Network Bridge on page 1283
- AP Network IGMP on page 1285
- AP Network MLD on page 1286
- AP Network Traffic Shaping on page 1288
- AP Network DHCP Options on page 1289
- AP Network Cisco Discovery Protocol on page 1290
- AP Network Link Layer Discovery Protocol on page 1291
- AP Network IPv6 Neighbor on page 1293
- AP Network MSTP on page 1294

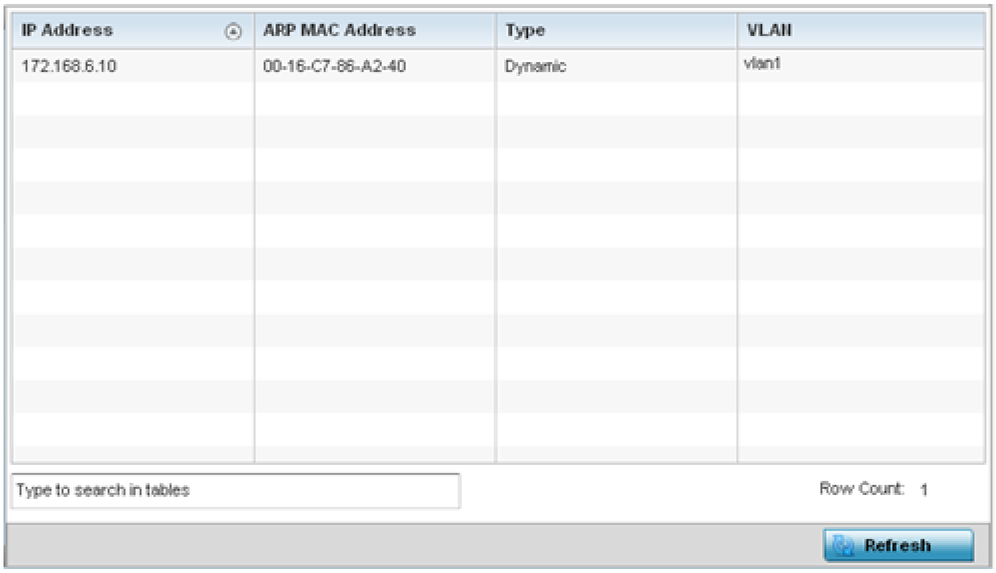
AP Network ARP Entries

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, select a **controller or service platform**, and select one of its 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 Entrie**s screen is displayed.



IP Address	ARP MAC Address	Type	VLAN
172.168.6.10	00-16-C7-86-A2-40	Dynamic	vlan1

Type to search in tables

Row Count: 1

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.

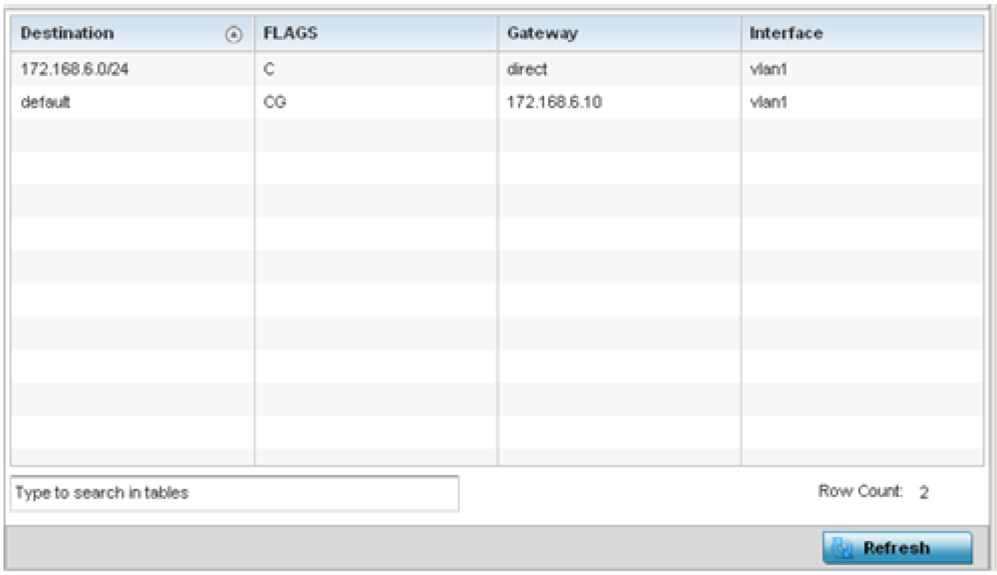
AP Network Route Entries

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, select a **controller or service platform**, and select one of its 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.



Destination	FLAGS	Gateway	Interface
172.168.6.0/24	C	direct	vlan1
default	CG	172.168.6.10	vlan1

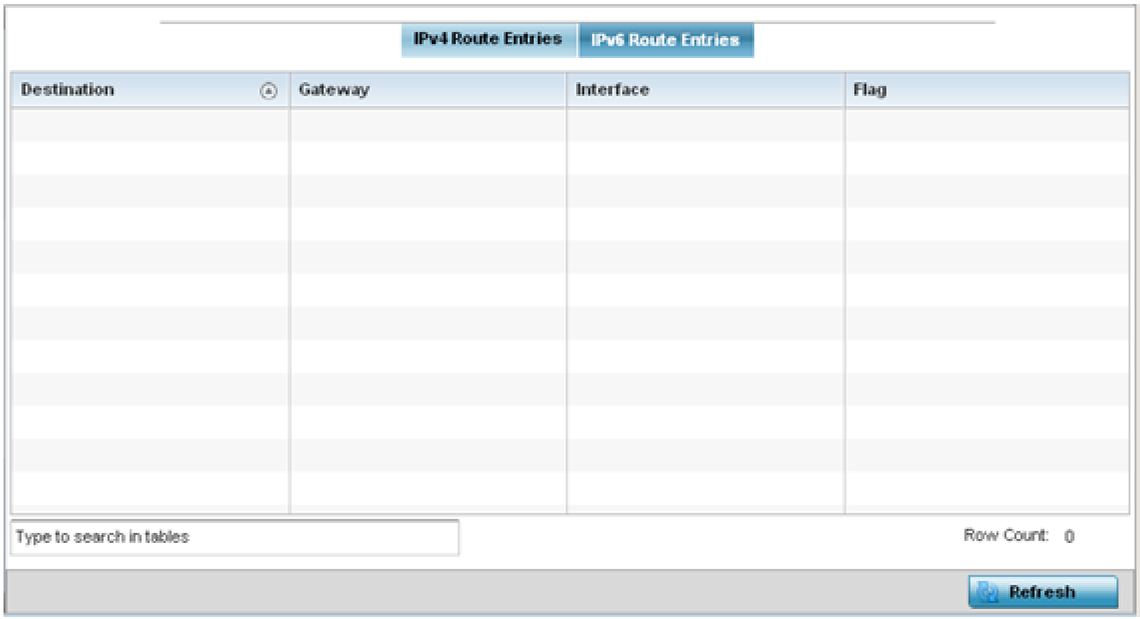
Row Count: 2

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.

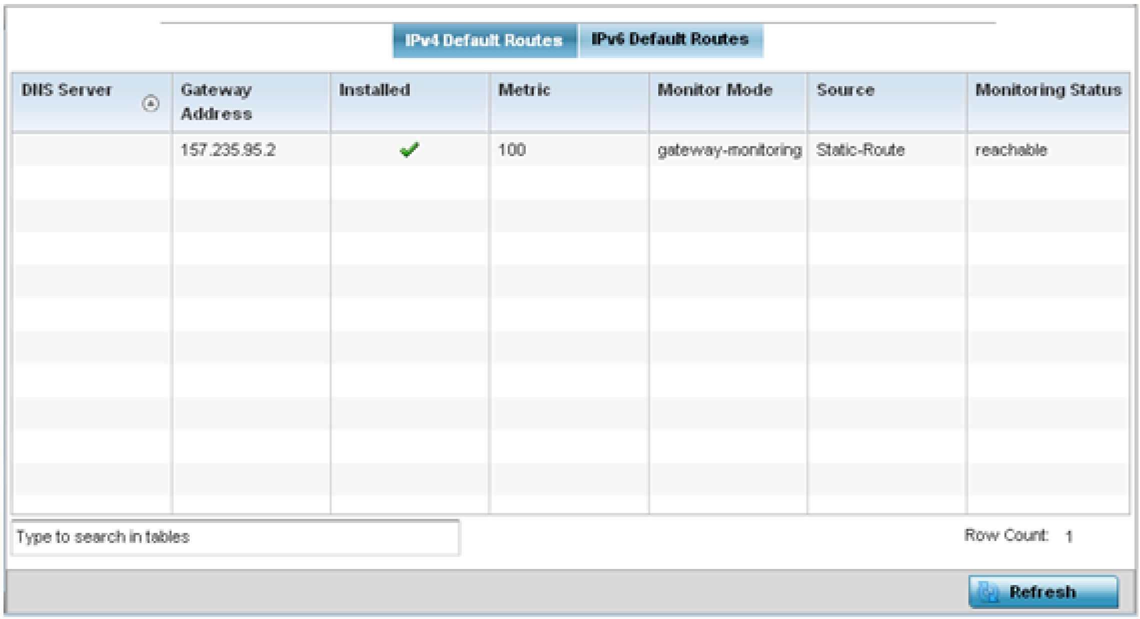
3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

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.



DNS Server	Gateway Address	Installed	Metric	Monitor Mode	Source	Monitoring Status
	157.235.95.2	✓	100	gateway-monitoring	Static-Route	reachable

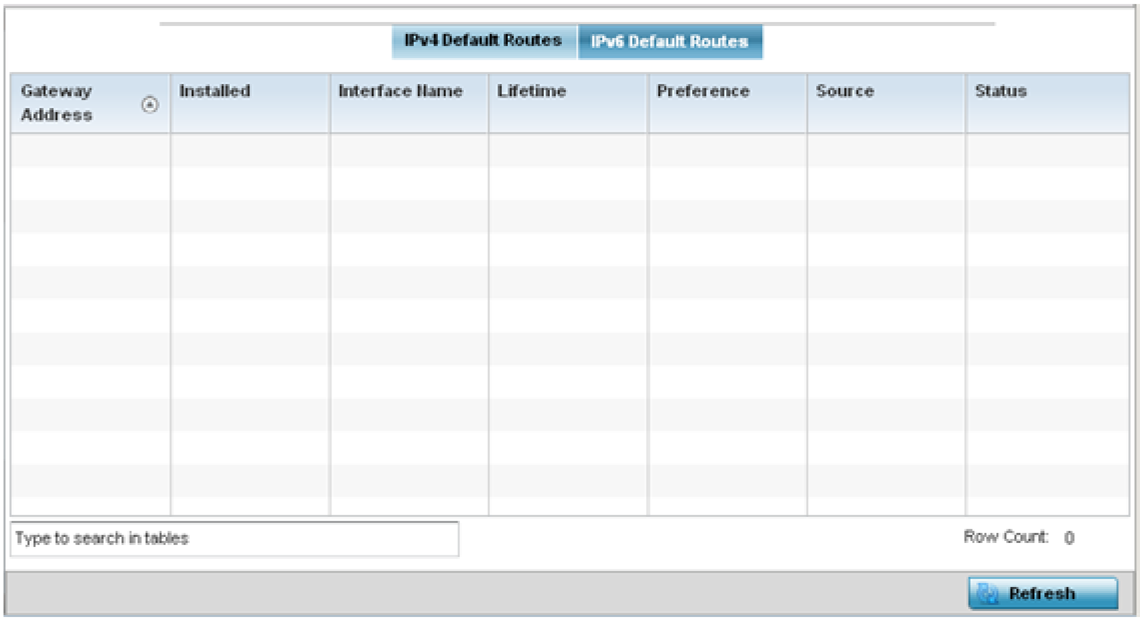
Row Count: 1

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*

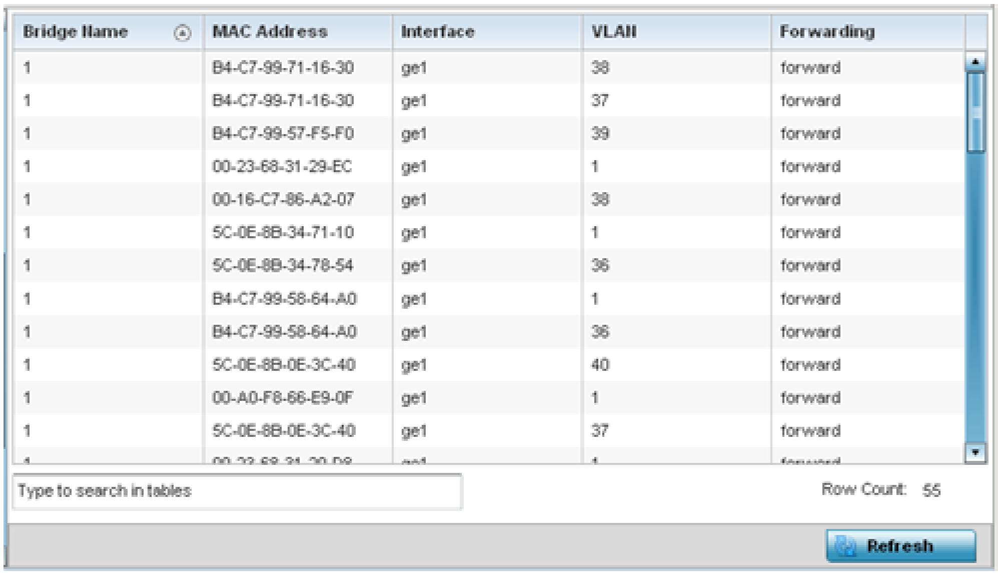
- *Permits access to other networks*
- *Times out old logins*

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, select a **controller or service platform**, and select one of its 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.



Bridge Name	MAC Address	Interface	VLAN	Forwarding
1	B4-C7-99-71-16-30	ge1	38	forward
1	B4-C7-99-71-16-30	ge1	37	forward
1	B4-C7-99-57-F5-F0	ge1	39	forward
1	00-23-68-31-29-EC	ge1	1	forward
1	00-16-C7-86-A2-07	ge1	38	forward
1	5C-0E-8B-34-71-10	ge1	1	forward
1	5C-0E-8B-34-78-54	ge1	36	forward
1	B4-C7-99-58-64-A0	ge1	1	forward
1	B4-C7-99-58-64-A0	ge1	36	forward
1	5C-0E-8B-0E-3C-40	ge1	40	forward
1	00-A0-F8-66-E9-0F	ge1	1	forward
1	5C-0E-8B-0E-3C-40	ge1	37	forward

   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.

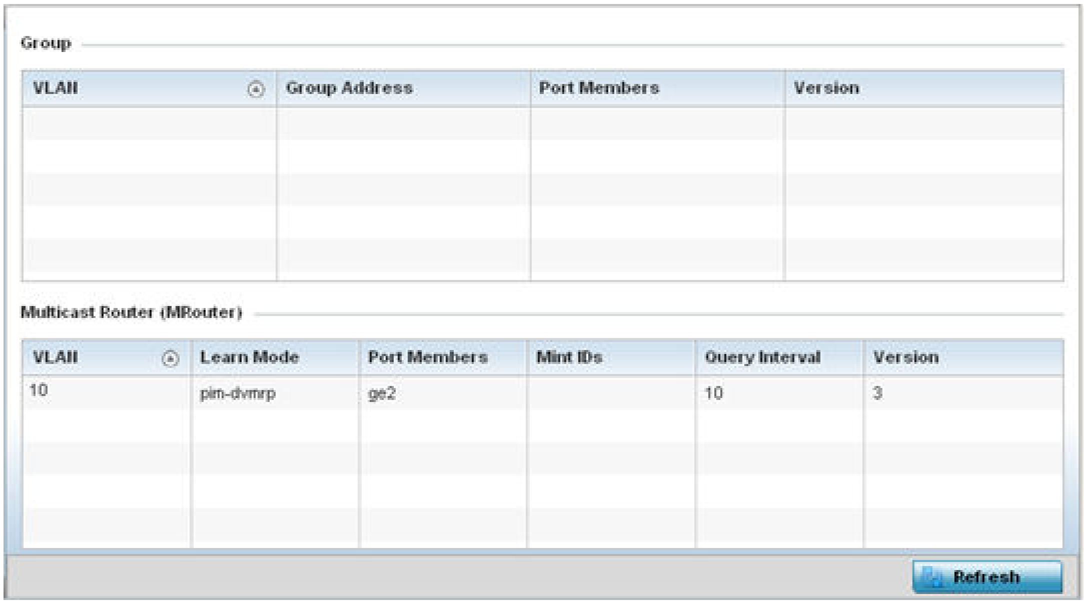
6. Select **Refresh** to update the counters to their latest values.

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, select a **controller or service platform**, and select one of its 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**.



Group

VLAN	Group Address	Port Members	Version

Multicast Router (MRouter)

VLAN	Learn Mode	Port Members	Mint IDs	Query Interval	Version
10	pim-dvmrp	ge2		10	3

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.

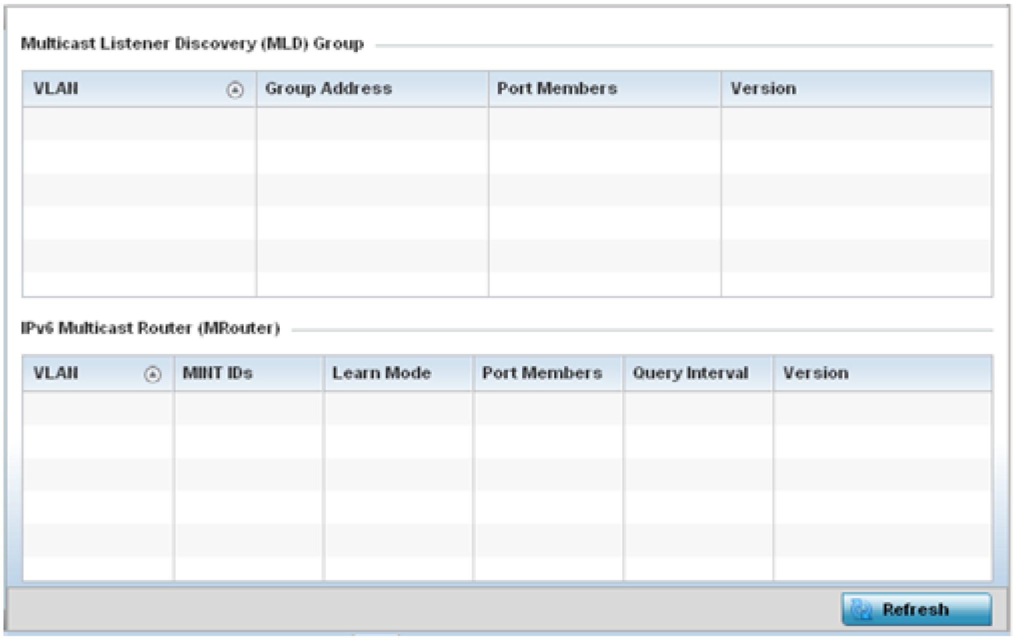
3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

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 1288
- Traffic Shaping - Statistics on page 1288

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, select a **controller or service platform**, and select one of its 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

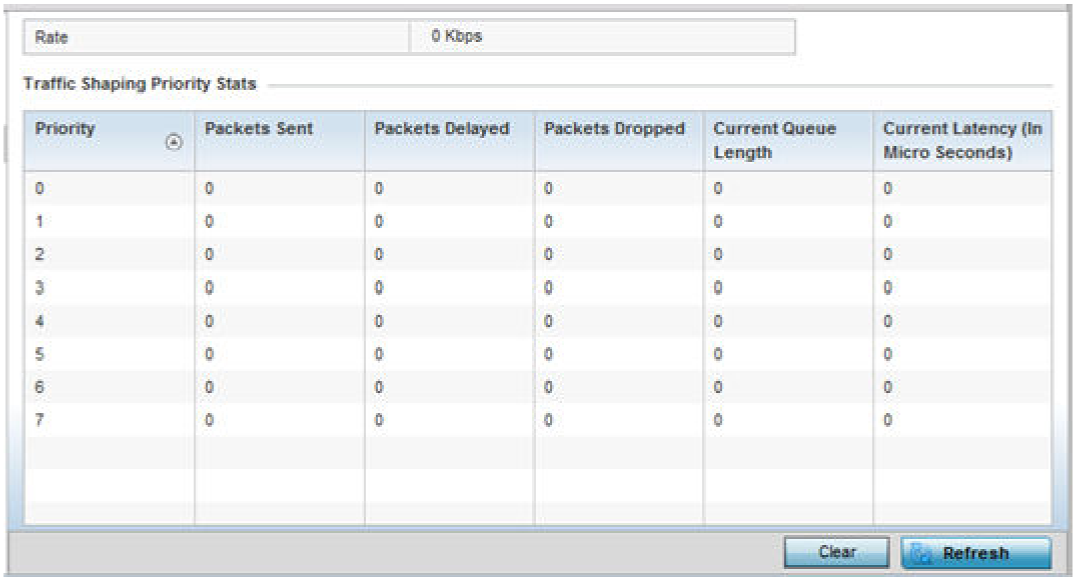
To view network Access Point traffic shaping statistics:

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, select a **controller or service platform**, and select one of its 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.



Rate	0 Kbps

Traffic Shaping Priority Stats

Priority	Packets Sent	Packets Delayed	Packets Dropped	Current Queue Length	Current Latency (In Micro Seconds)
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0

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

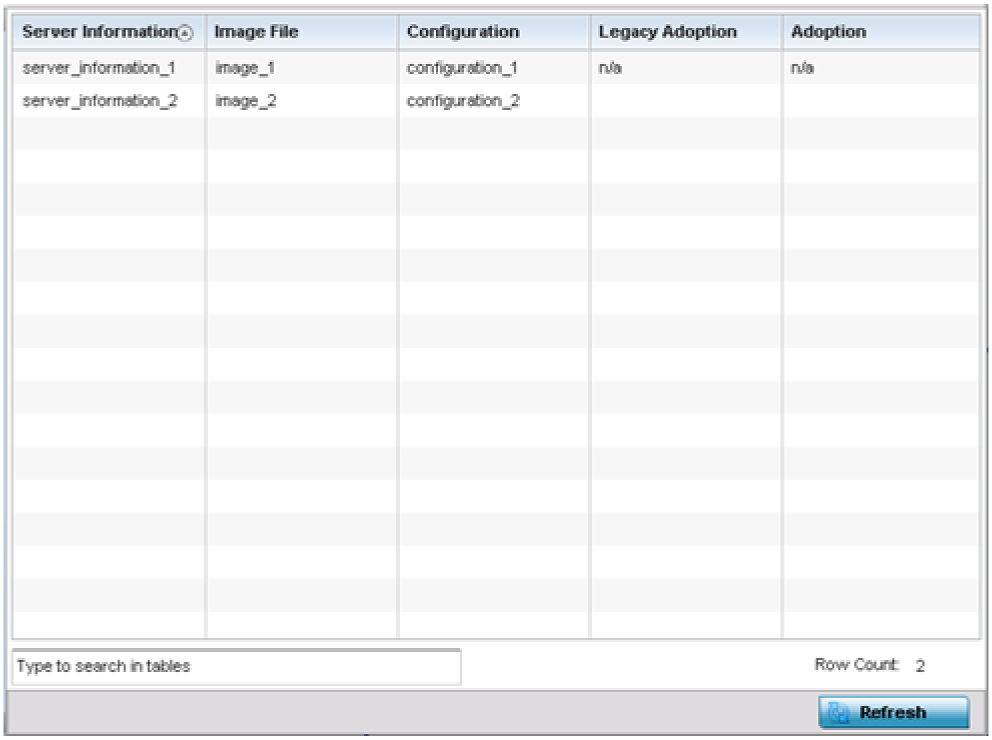
Supported access points can use internal or external DHCP server resources to provide the dynamic assignment of IP addresses to requesting clients. DHCP is a protocol that includes IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these 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, select a **controller or service platform**, and select one of its 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.

Server Information	Image File	Configuration	Legacy Adoption	Adoption
server_information_1	image_1	configuration_1	n/a	n/a
server_information_2	image_2	configuration_2		

   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.

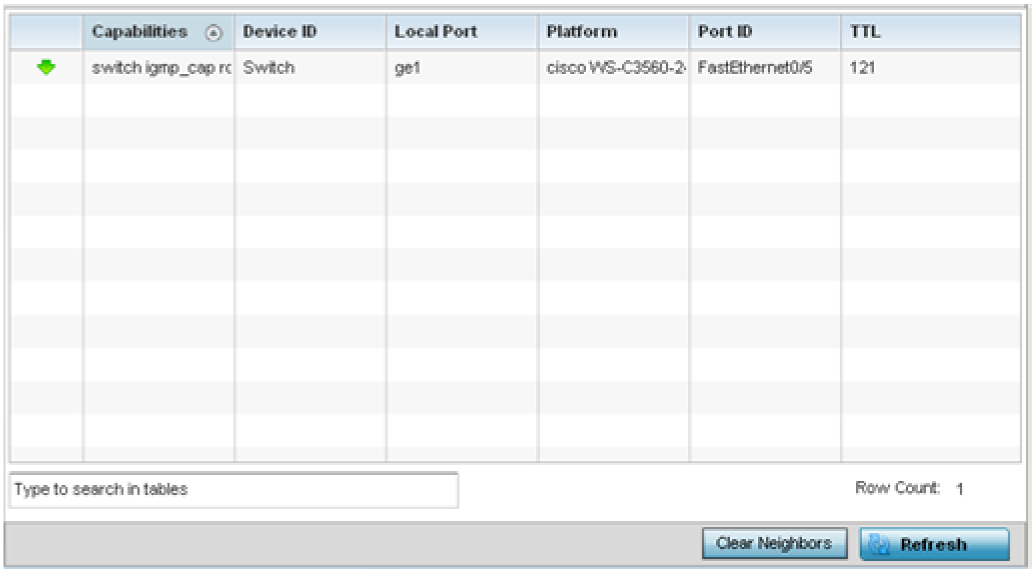
AP Network Cisco Discovery Protocol

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, select a **controller or service platform**, and select one of its 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.



	Capabilities	Device ID	Local Port	Platform	Port ID	TTL
	switch igmp_cap rc	Switch	ge1	cisco WS-C3560-2	FastEthernet0/5	121

Row Count: 1

   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.

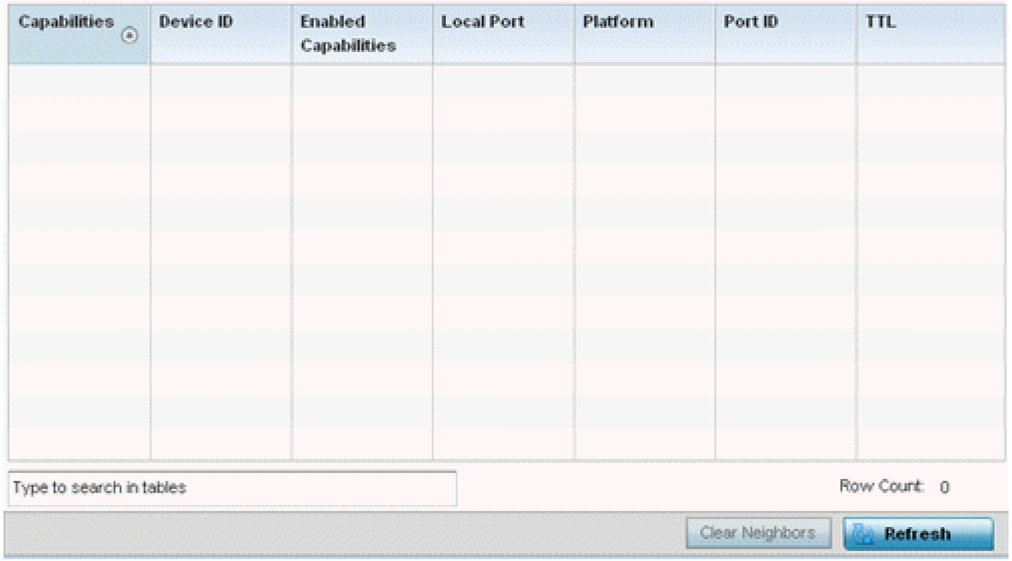
AP Network Link Layer Discovery Protocol

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, select a **controller or service platform**, and select one of its 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.

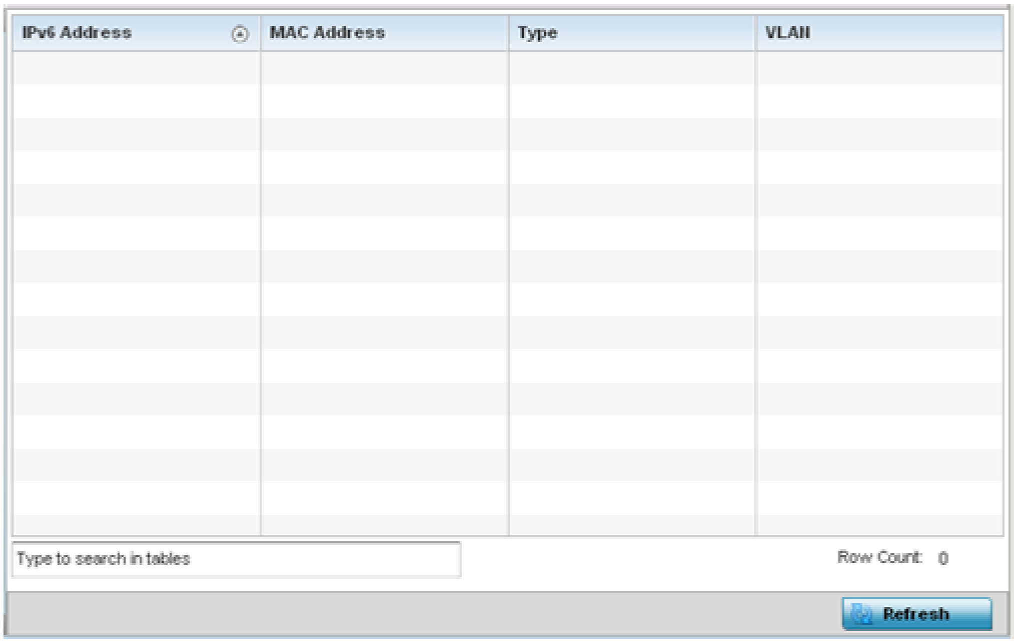
To view an access point's IPv6 neighbor statistics:

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, select a **controller or service platform**, and select one of its 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:

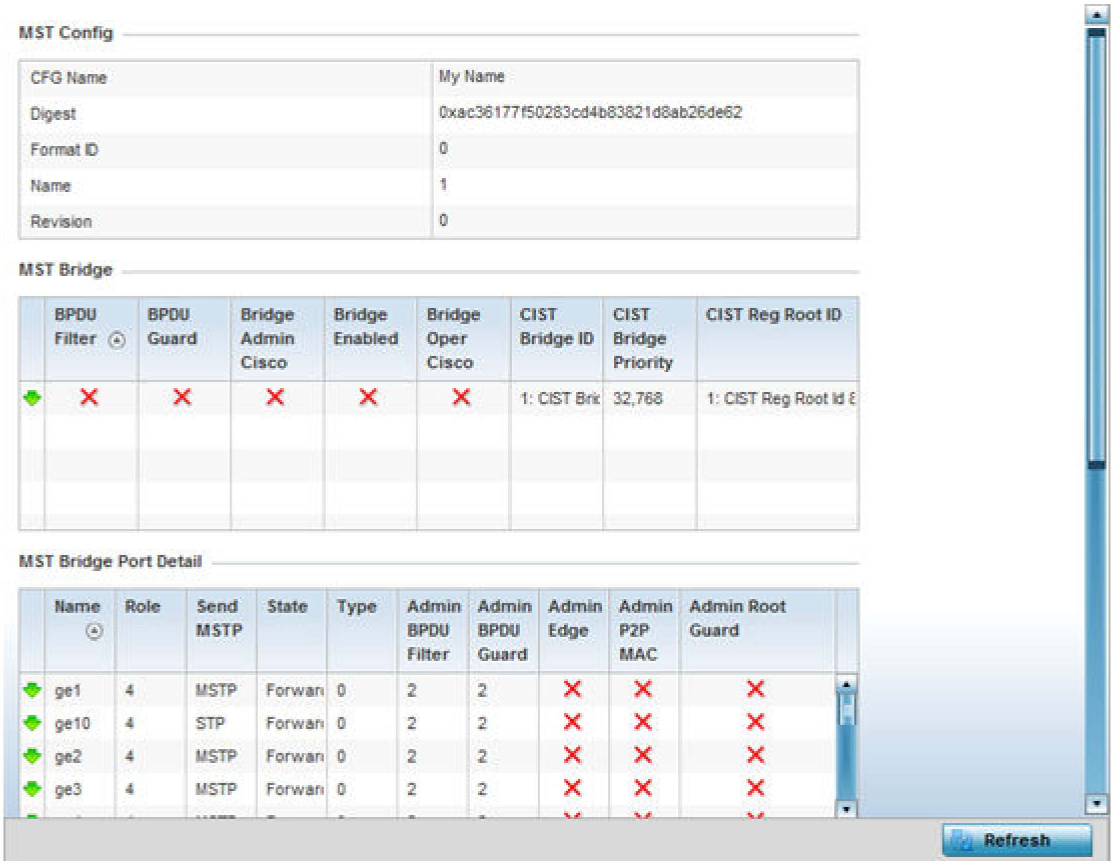
1. Select the **Statistics** menu from the Web UI.
2. Expand the **System** node from the navigation pane (on the left-hand side of the screen).

   The System node expands to display the RF Domains created within the managed network.
3. Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



MST Config

CFG Name	My Name
Digest	0xac36177f50283cd4b83821d8ab26de62
Format ID	0
Name	1
Revision	0

MST Bridge

BPDU Filter	BPDU Guard	Bridge Admin Cisco	Bridge Enabled	Bridge Oper Cisco	CIST Bridge ID	CIST Bridge Priority	CIST Reg Root ID
✗	✗	✗	✗	✗	1: CIST Bri	32,768	1: CIST Reg Root Id

MST Bridge Port Detail

Name	Role	Send MSTP	State	Type	Admin BPDU Filter	Admin BPDU Guard	Admin Edge	Admin P2P MAC	Admin Root Guard
ge1	4	MSTP	Forwar	0	2	2	✗	✗	✗
ge10	4	STP	Forwar	0	2	2	✗	✗	✗
ge2	4	MSTP	Forwar	0	2	2	✗	✗	✗
ge3	4	MSTP	Forwar	0	2	2	✗	✗	✗

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).

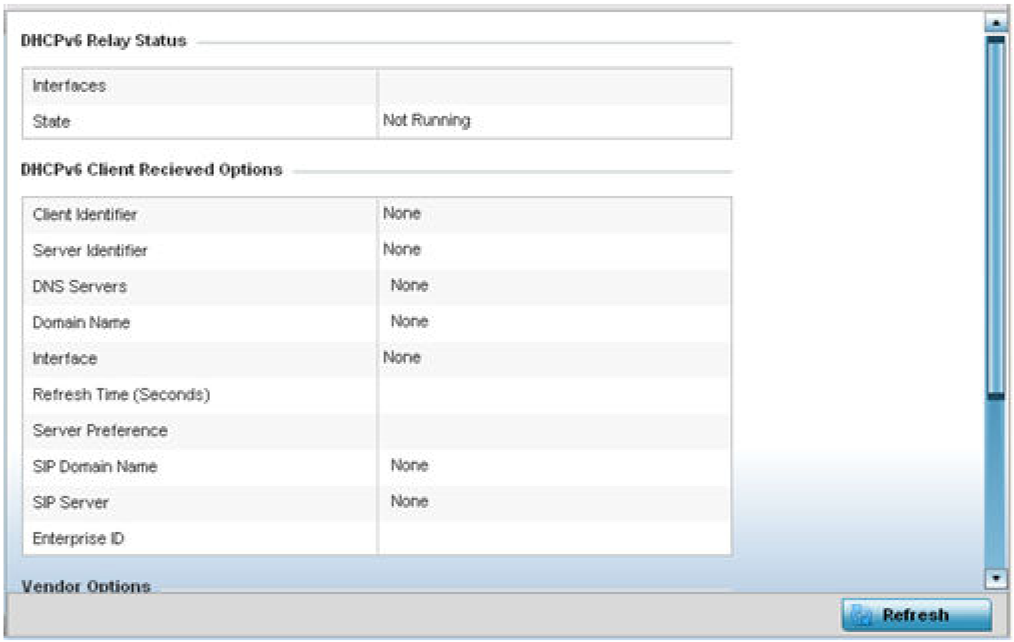
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



DHCPv6 Relay Status

Interfaces	
State	Not Running

DHCPv6 Client Recieved Options

Client Identifier	None
Server Identifier	None
DNS Servers	None
Domain Name	None
Interface	None
Refresh Time (Seconds)	
Server Preference	
SIP Domain Name	None
SIP Server	None
Enterprise ID	

Vendor Options

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 1298
- AP DHCP - Bindings on page 1299
- AP DHCP - Networks on page 1300

AP DHCP - General

To view General DHCP status and binding information:

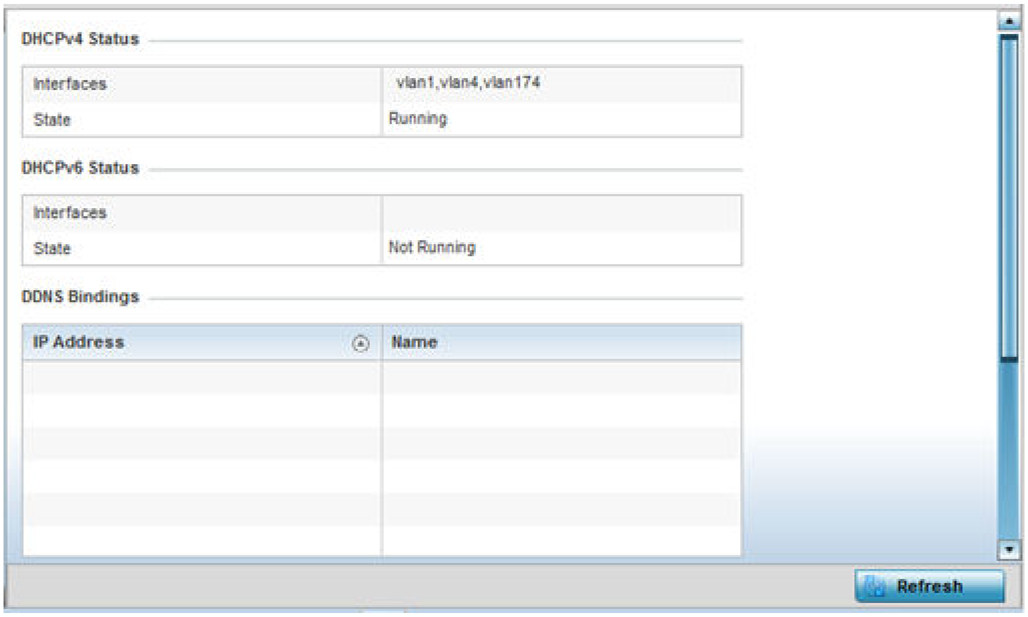
1 Select the Statistics menu from the Web UI.

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, select a **controller or service platform**, and select one of its 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.



DHCPv4 Status

Interfaces	vlan1,vlan4,vlan174
State	Running

DHCPv6 Status

Interfaces	
State	Not Running

DDNS Bindings

IP Address	Name

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

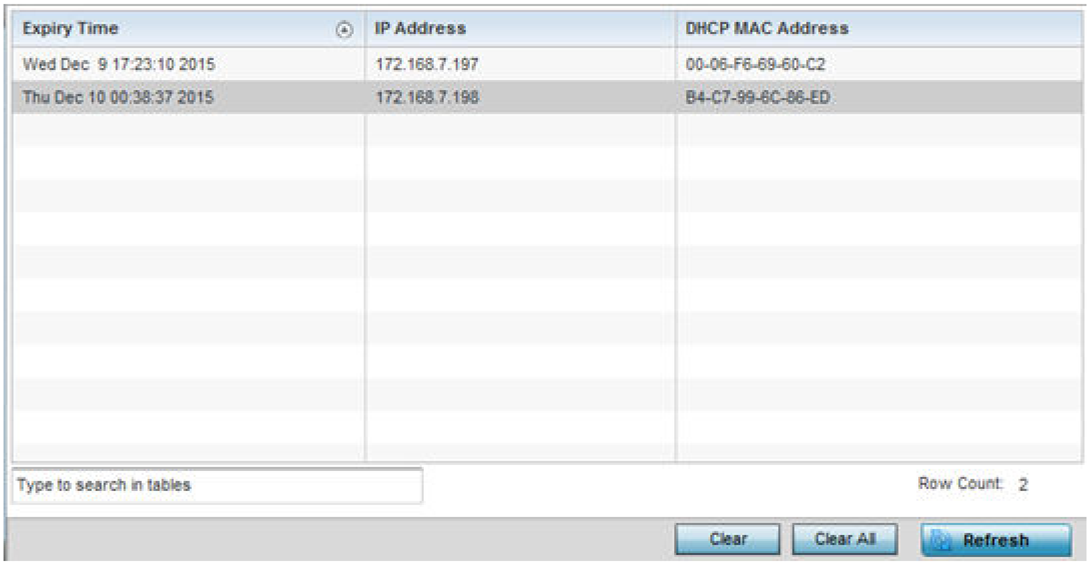
The DHCP Binding displays DHCP binding information such as expiry time, client IP addresses and their MAC address.

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, select a **controller or service platform**, and select one of its 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.



Expiry Time	IP Address	DHCP MAC Address
Wed Dec 9 17:23:10 2015	172.168.7.197	00-06-F6-69-60-C2
Thu Dec 10 00:38:37 2015	172.168.7.198	B4-C7-99-6C-86-ED

   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

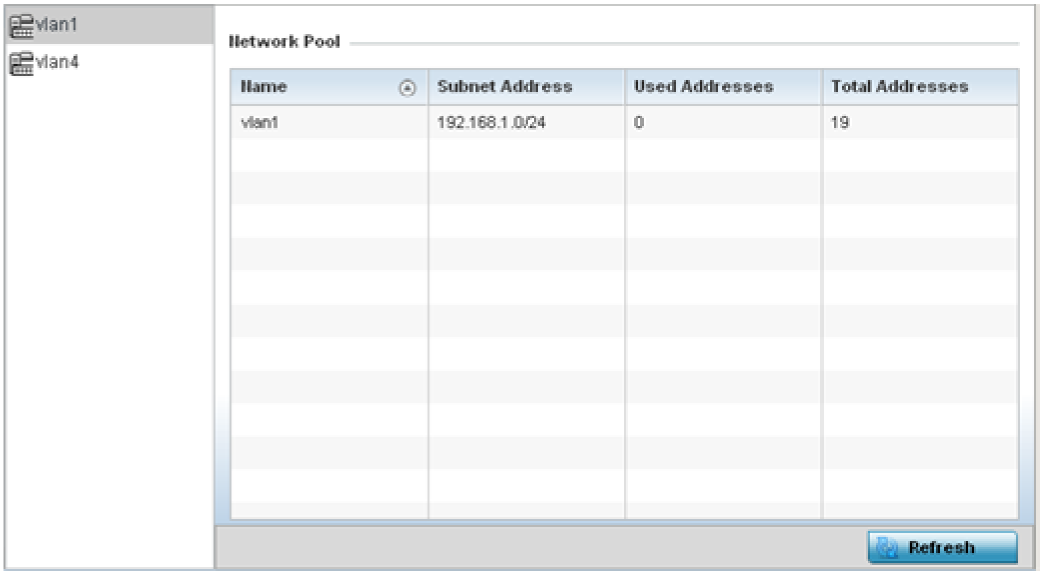
A controller, service platform or access point's DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers, etc). On receiving a valid client request, the DHCP server assigns an IP address, a lease (the validity of time), and other IP 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, select a **controller or service platform**, and select one of its 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.



Network Pool

Name	Subnet Address	Used Addresses	Total Addresses
vlan1	192.168.1.0/24	0	19

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

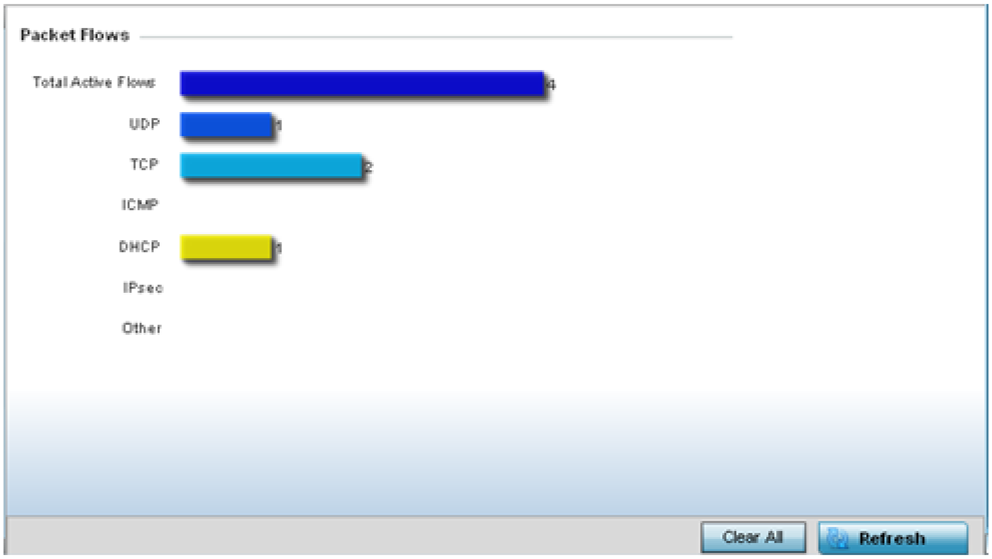
The Packet Flows screen displays data traffic packet flow utilization. The chart represents the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized.

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, select a **controller or service platform**, and select one of its 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.

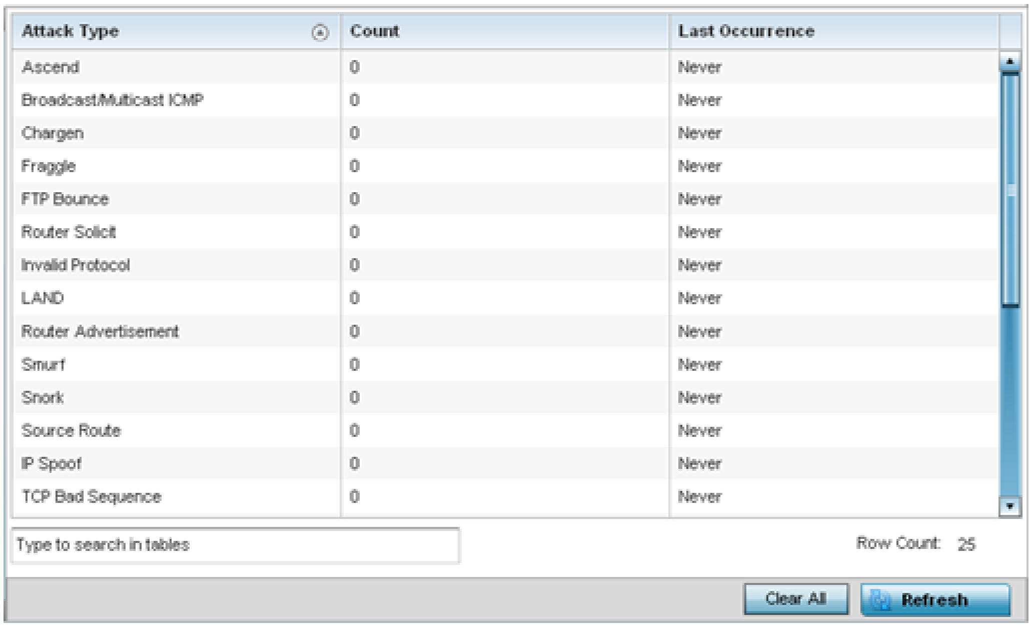
One common method involves saturating the target's machine with external communications requests, so it cannot respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable. DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its 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, select a **controller or service platform**, and select one of its 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.



Attack Type	Count	Last Occurrence
Ascend	0	Never
Broadcast/Multicast ICMP	0	Never
Chargen	0	Never
Fraggle	0	Never
FTP Bounce	0	Never
Router Solicit	0	Never
Invalid Protocol	0	Never
LAND	0	Never
Router Advertisement	0	Never
Smurf	0	Never
Snork	0	Never
Source Route	0	Never
IP Spoof	0	Never
TCP Bad Sequence	0	Never

Type to search in tables

Row Count: 25

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:

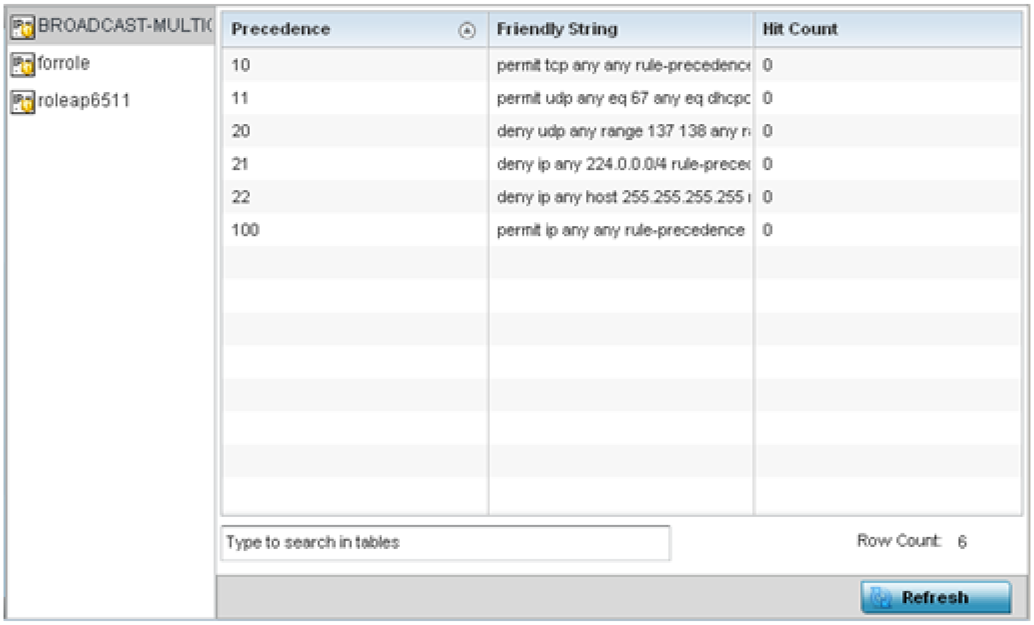
- *Allow a connection*.
- *Allow a connection only if it is secured through the use of Internet Protocol security*.
- *Block a connection*.

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, select a **controller or service platform**, and select one of its 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.



Precedence	Friendly String	Hit Count
10	permit tcp any any rule-precedenc	0
11	permit udp any eq 67 any eq dhcpc	0
20	deny udp any range 137 138 any r	0
21	deny ip any 224.0.0.0/4 rule-prece	0
22	deny ip any host 255.255.255.255	0
100	permit ip any any rule-precedence	0

Row Count: 6

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.

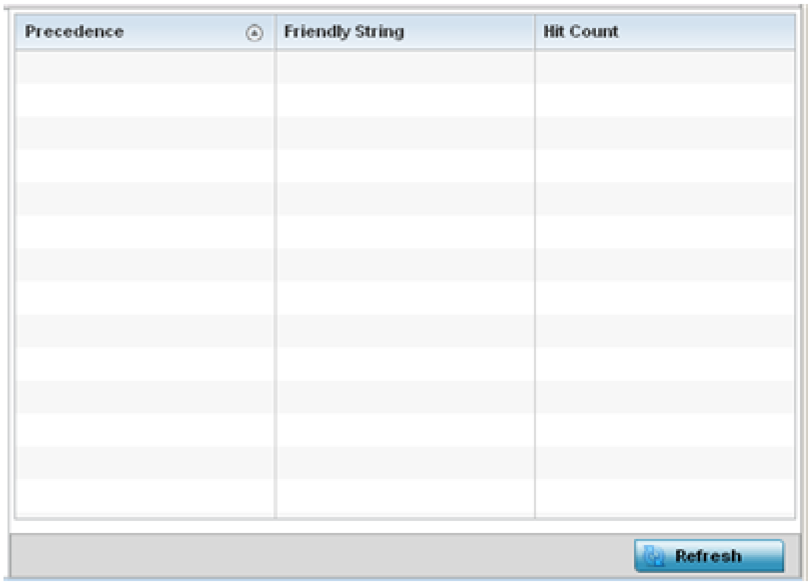
3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

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.



Precedence	Friendly String	Hit Count

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.

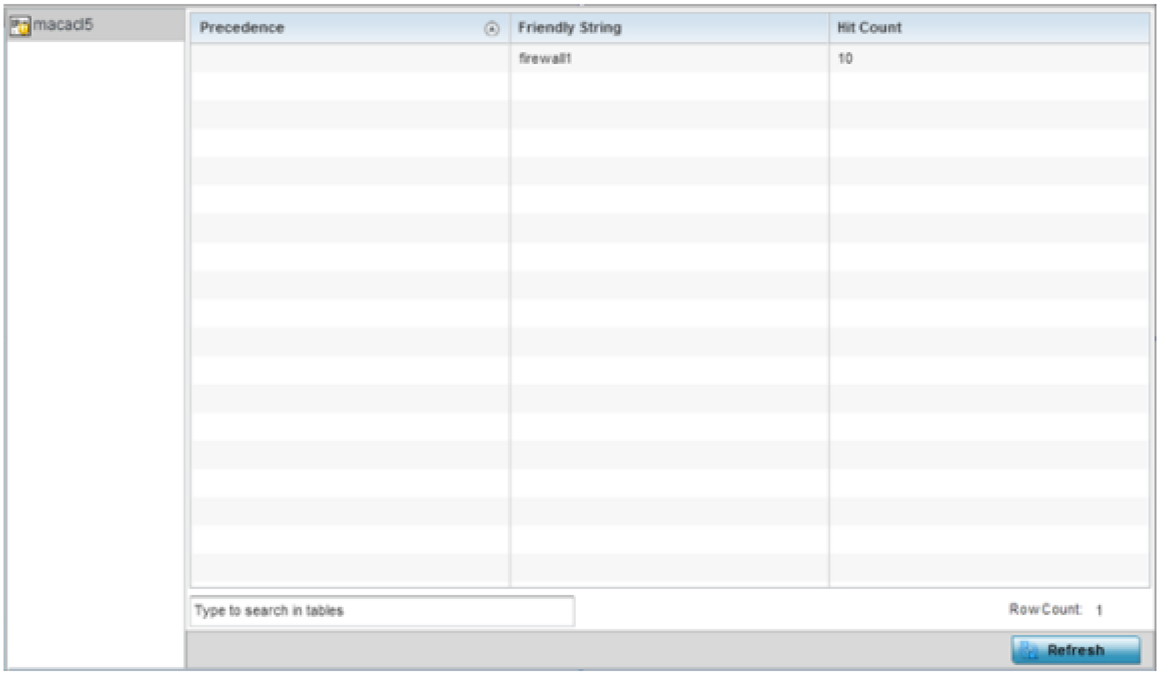
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Precedence	Friendly String	Hit Count
	firewall1	10

Row Count: 1

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

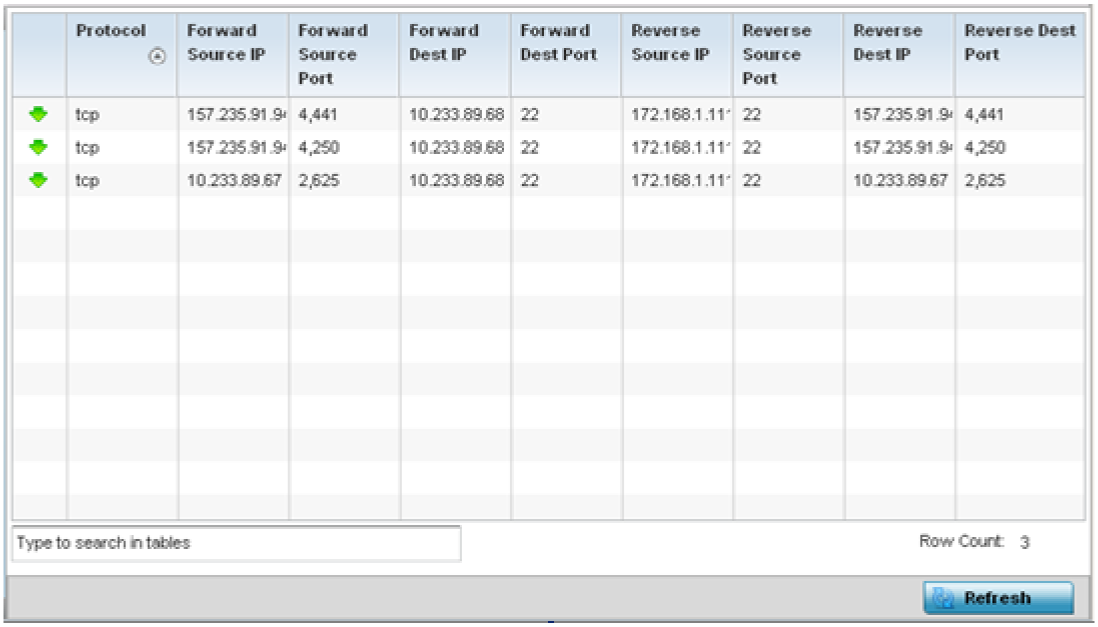
NAT is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses 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, select a **controller or service platform**, and select one of its 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.



	Protocol	Forward Source IP	Forward Source Port	Forward Dest IP	Forward Dest Port	Reverse Source IP	Reverse Source Port	Reverse Dest IP	Reverse Dest Port
◆	tcp	157.235.91.9	4,441	10.233.89.68	22	172.168.1.11	22	157.235.91.9	4,441
◆	tcp	157.235.91.9	4,250	10.233.89.68	22	172.168.1.11	22	157.235.91.9	4,250
◆	tcp	10.233.89.67	2,625	10.233.89.68	22	172.168.1.11	22	10.233.89.67	2,625

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.

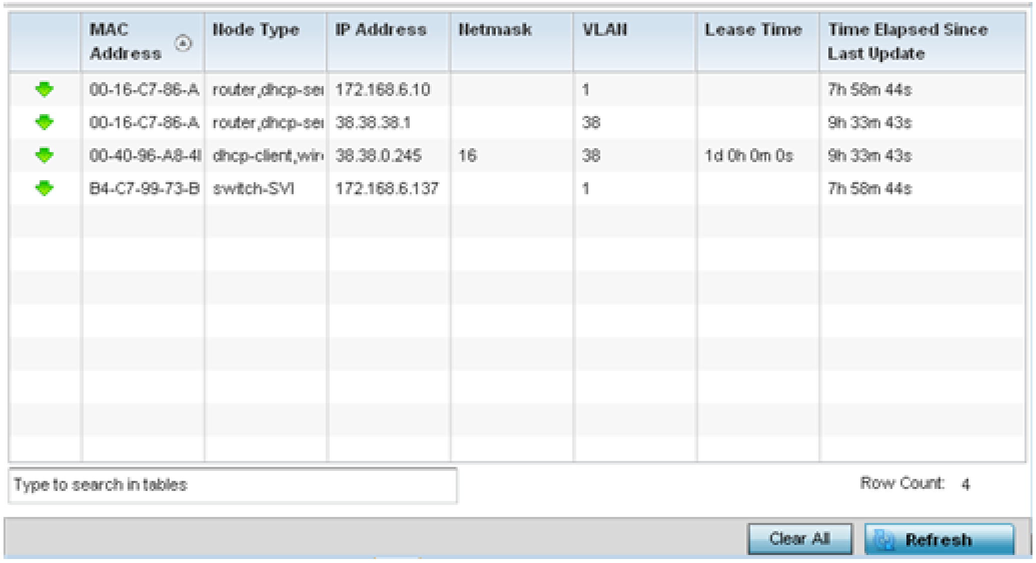
6. Select **Refresh** to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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.



	MAC Address	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since Last Update
	00-16-C7-86-A	router,dhcp-se	172.168.6.10		1		7h 58m 44s
	00-16-C7-86-A	router,dhcp-se	38.38.38.1		38		9h 33m 43s
	00-40-96-A8-4	dhcp-client,wir	38.38.0.245	16	38	1d 0h 0m 0s	9h 33m 43s
	B4-C7-99-73-B	switch-SVI	172.168.6.137		1		7h 58m 44s

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).

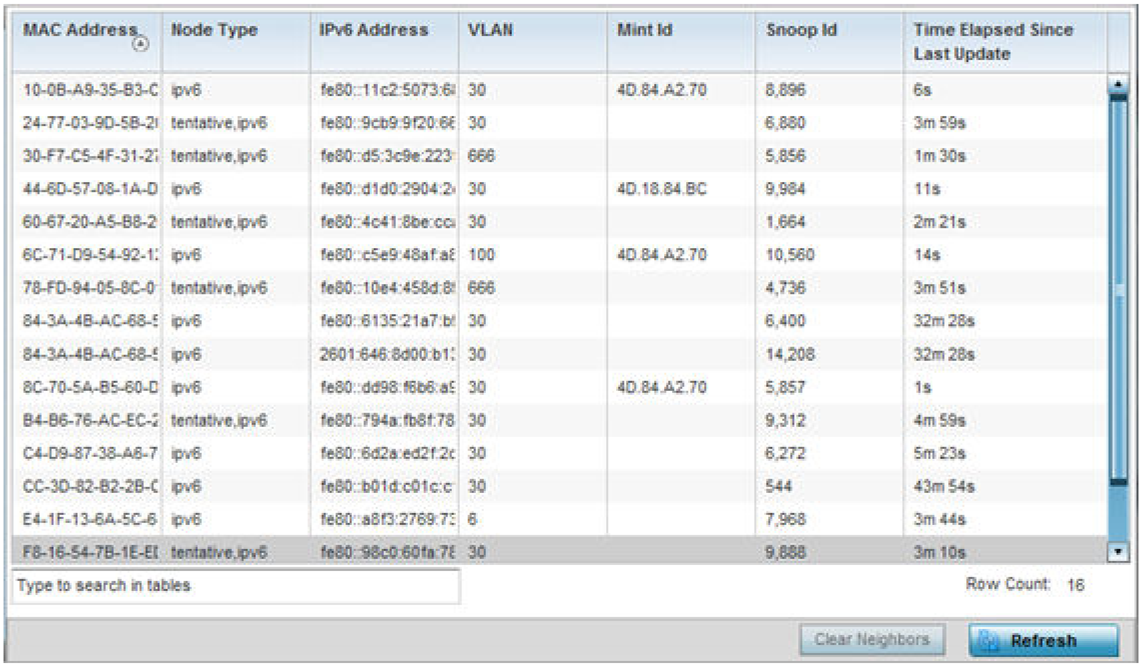
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



MAC Address	Node Type	IPv6 Address	VLAN	Mint Id	Snoop Id	Time Elapsed Since Last Update
10-0B-A9-35-B3-C	ipv6	fe80::11c2:5073:6	30	4D.84.A2.70	8,896	6s
24-77-03-9D-5B-2	tentative,ipv6	fe80::9cb9:9f20:6	30		6,880	3m 59s
30-F7-C5-4F-31-2	tentative,ipv6	fe80::d5:3c9e:223	666		5,856	1m 30s
44-6D-57-08-1A-D	ipv6	fe80::d1d0:2904:2	30	4D.18.84.BC	9,984	11s
60-67-20-A5-B8-2	tentative,ipv6	fe80::4c41:8be:cc	30		1,664	2m 21s
6C-71-D9-54-92-1	ipv6	fe80::c5e9:48af:a	100	4D.84.A2.70	10,560	14s
78-FD-94-05-8C-0	tentative,ipv6	fe80::10e4:458d:8	666		4,736	3m 51s
84-3A-4B-AC-68-5	ipv6	fe80::6135:21a7:b	30		6,400	32m 28s
84-3A-4B-AC-68-5	ipv6	2601:646:8d00:b1	30		14,208	32m 28s
8C-70-5A-B5-60-D	ipv6	fe80::dd98:f6b6:a	30	4D.84.A2.70	5,857	1s
B4-B6-76-AC-EC-2	tentative,ipv6	fe80::794a:fb8f:78	30		9,312	4m 59s
C4-D9-87-38-A6-7	ipv6	fe80::6d2a:ed2f:2	30		6,272	5m 23s
CC-3D-82-B2-2B-C	ipv6	fe80::b01d:c01c:c	30		544	43m 54s
E4-1F-13-6A-5C-6	ipv6	fe80::a8f3:2769:7	6		7,968	3m 44s
F8-16-54-7B-1E-E	tentative,ipv6	fe80::98c0:60fa:7	30		9,888	3m 10s

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.

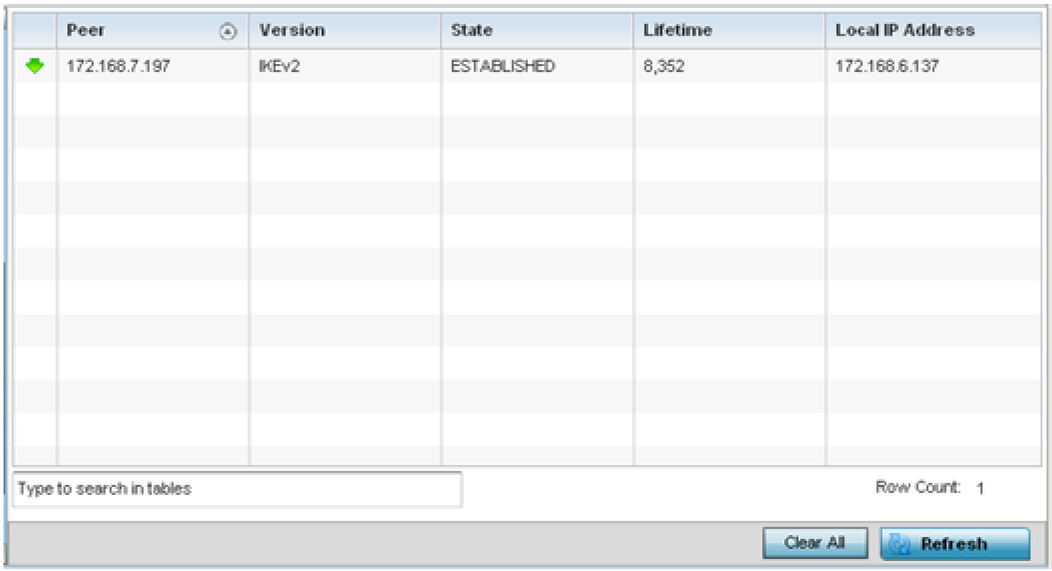
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Peer	Version	State	Lifetime	Local IP Address
172.168.7.197	IKEv2	ESTABLISHED	8,352	172.168.6.137

Row Count: 1

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.

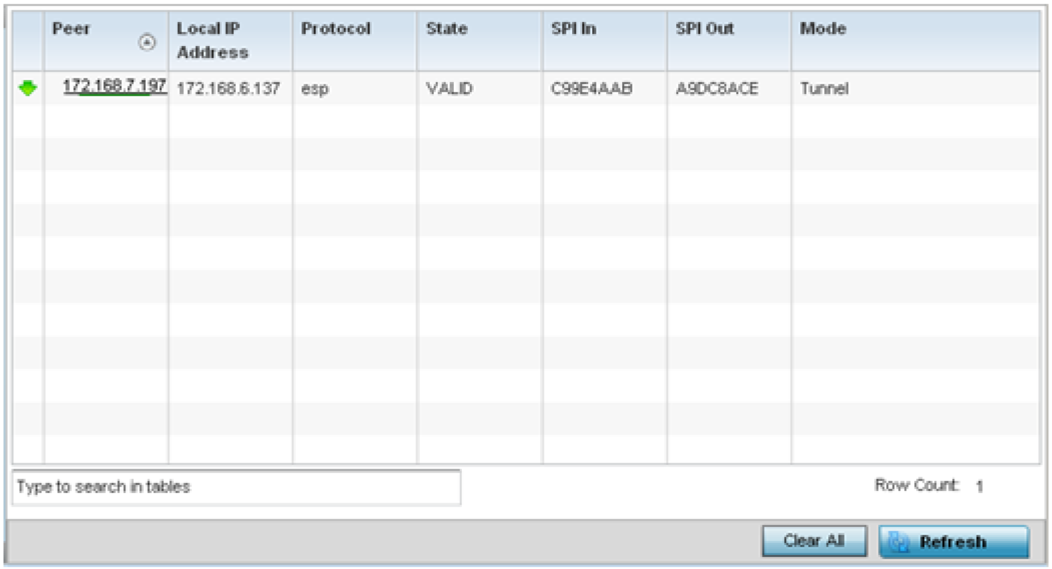
8 Select **Refresh** to update the screen's statistics counters to their latest values.

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, select a **controller or service platform**, and select one of its 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.



	Peer	Local IP Address	Protocol	State	SPI In	SPI Out	Mode
◆	172.168.7.197	172.168.6.137	esp	VALID	C99E4AAB	A9DC8ACE	Tunnel

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:

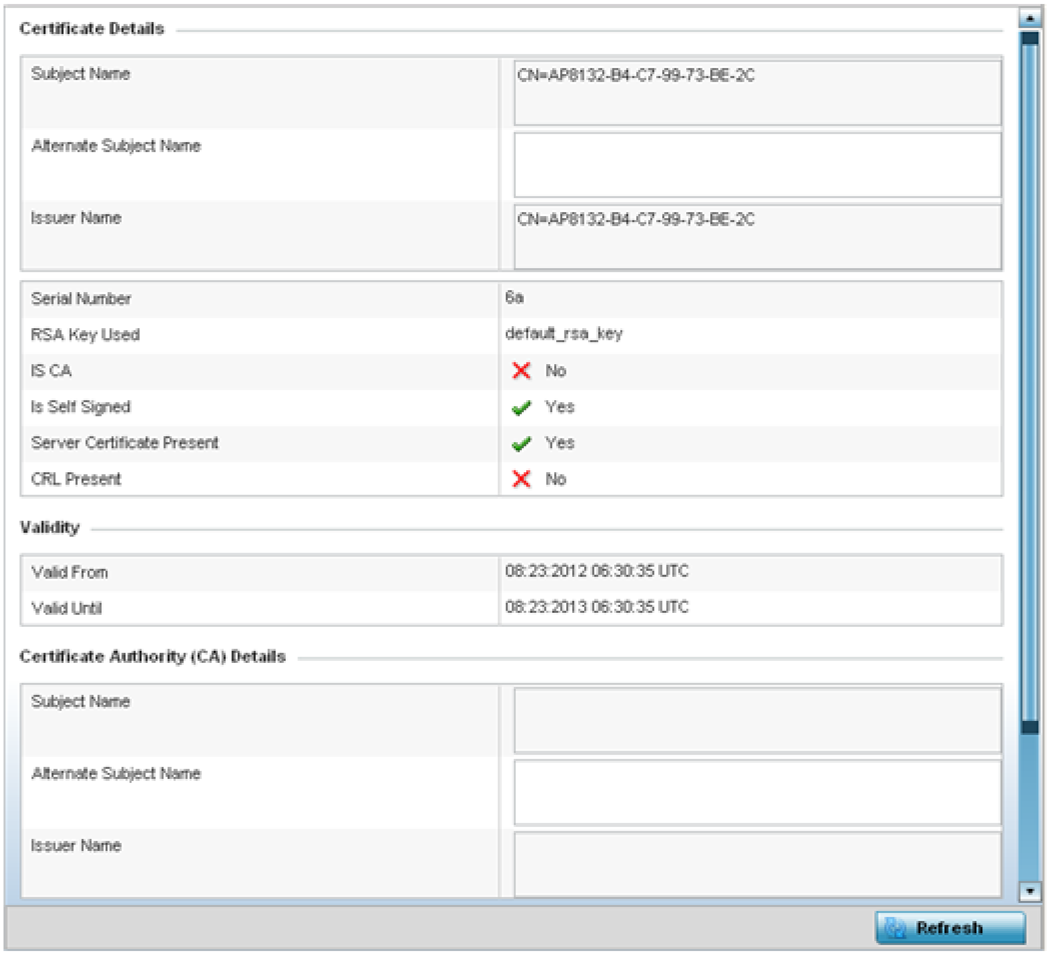
- AP Certificates Trustpoints on page 1314
- AP Certificates RSA Keys on page 1316

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, select a **controller or service platform**, and select one of its 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.



Certificate Details

Subject Name	CN=AP8132-B4-C7-99-73-BE-2C
Alternate Subject Name	
Issuer Name	CN=AP8132-B4-C7-99-73-BE-2C

Serial Number	6a
RSA Key Used	default_rsa_key
IS CA	✗ No
Is Self Signed	✓ Yes
Server Certificate Present	✓ Yes
CRL Present	✗ No

Validity

Valid From	08:23:2012 06:30:35 UTC
Valid Until	08:23:2013 06:30:35 UTC

Certificate Authority (CA) Details

Subject Name	
Alternate Subject Name	
Issuer Name	

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

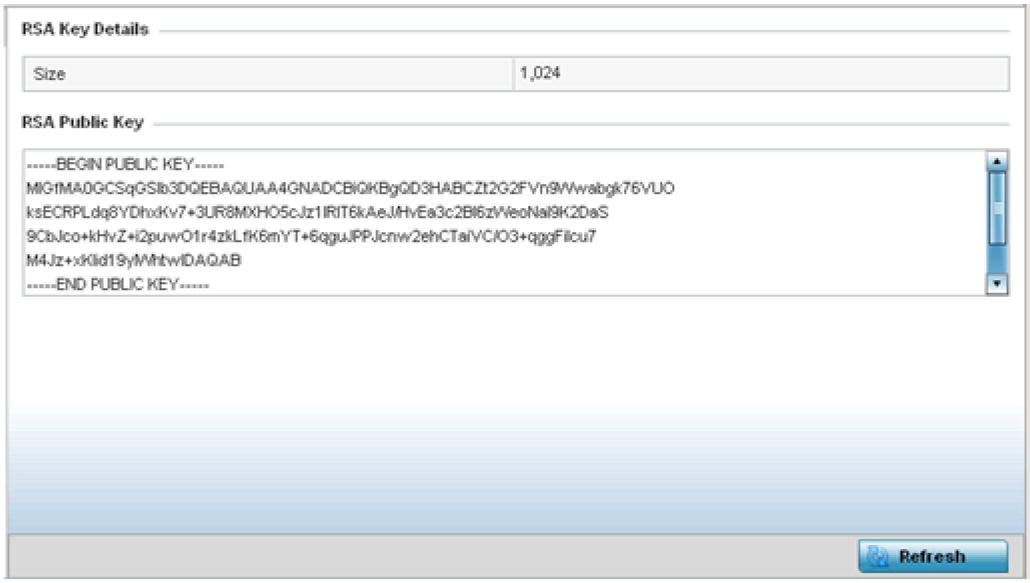
RSA is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption.

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, select a **controller or service platform**, and select one of its 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.



Size	1,024

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD3HABCZt2G2FVn9Wwabgk76VUO
ksECRPLdq8YDhxKv7+3UR8MXHO5cJz1IRIT6kAeJ/HvEa3c2BI6zWeoNal9K2DaS
9CbJco+kHvZ+i2puwO1r4zkLfK6mYT+6qguJPPJcnw2ehCTaIVC/O3+qggFilcu7
M4Jz+xKlid19yMhtwIDAQAB
-----END PUBLIC KEY-----
```

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 on page 1317
- AP WIPS Events on page 1318

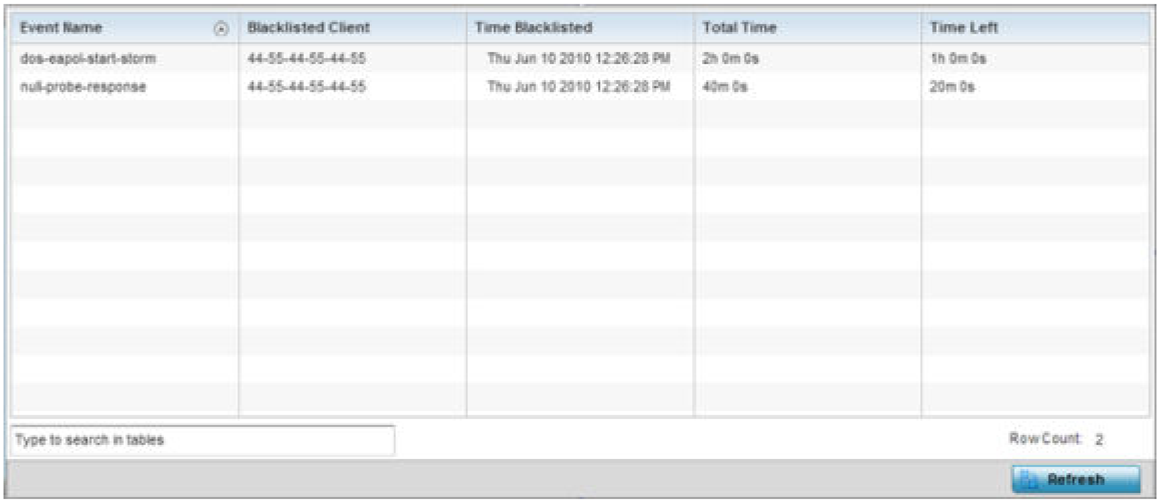
AP WIPS Client Blacklist

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, select a **controller or service platform**, and select one of its 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



Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-eapol-start-storm	44-55-44-55-44-55	Thu Jun 10 2010 12:26:28 PM	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2010 12:26:28 PM	40m 0s	20m 0s

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

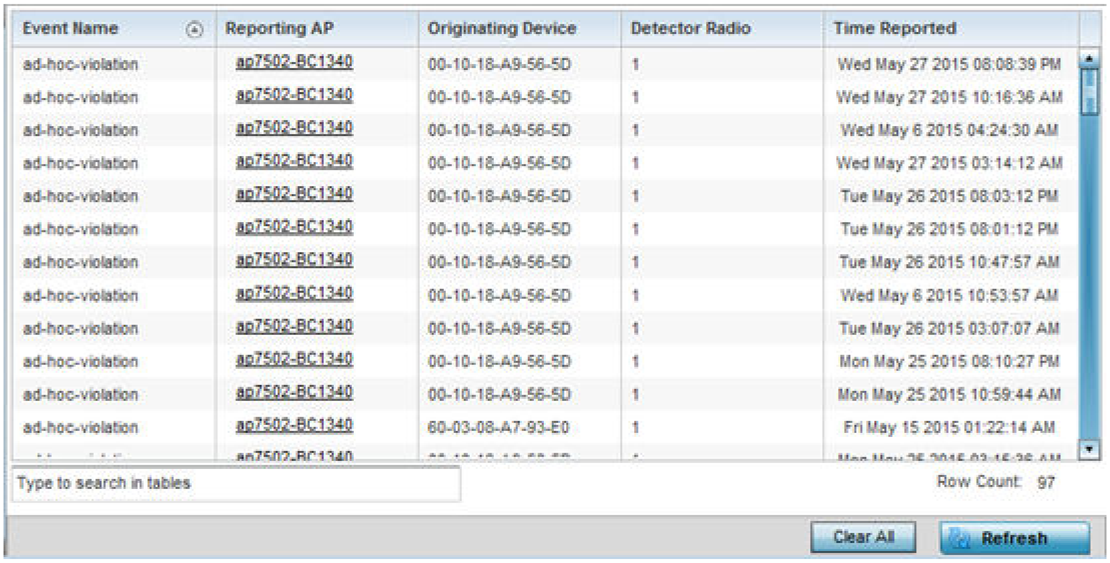
Periodically review the WIPS Events screen to assess whether any new or existing events require additional administration to protect the security of authorized devices. Events are listed by name, detecting AP, originating device, detector radio and time. The reporting AP can be selected to review that 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, select a **controller or service platform**, and select one of its 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.



Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	ap7502-BC1340	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

Row Count: 97

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.

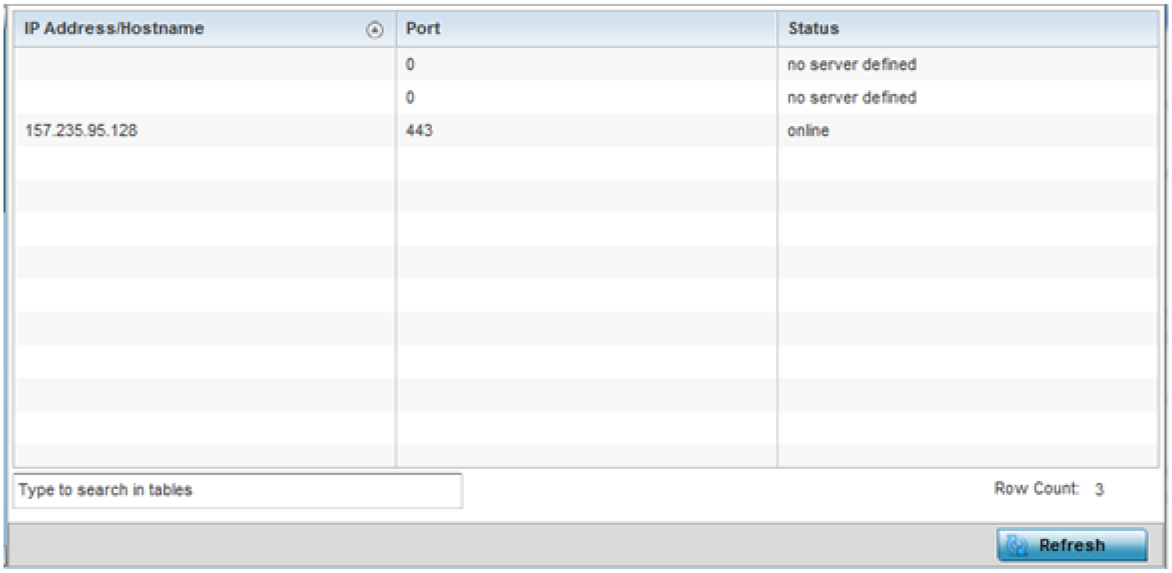
To view the network address and status information of the sensor server resources available to the access point:

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, select a **controller or service platform**, and select one of its 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.



IP Address/Hostname	Port	Status
	0	no server defined
	0	no server defined
157.235.95.128	443	online

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).

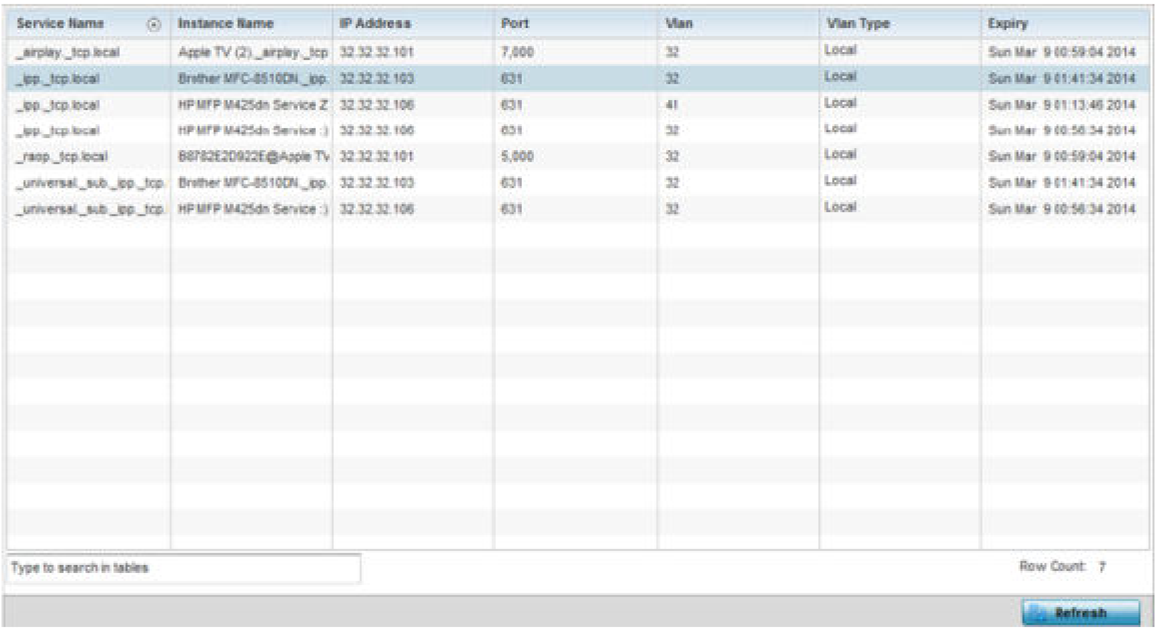
The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Service Name	Instance Name	IP Address	Port	Vlan	Vlan Type	Expiry
_airplay._tcp.local	Apple TV (2)._airplay._tcp	32.32.32.101	7,000	32	Local	Sun Mar 9 00:59:04 2014
_ipp._tcp.local	Brother MFC-8510DN._ipp.	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_ipp._tcp.local	HP MFP M425dn Service Z	32.32.32.106	631	41	Local	Sun Mar 9 01:13:46 2014
_ipp._tcp.local	HP MFP M425dn Service :)	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014
_raop._tcp.local	B8782E2D922E@Apple Tv	32.32.32.101	5,000	32	Local	Sun Mar 9 00:59:04 2014
_universal._sub._ipp._tcp.	Brother MFC-8510DN._ipp.	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_universal._sub._ipp._tcp.	HP MFP M425dn Service :)	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014

Row Count: 7

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.

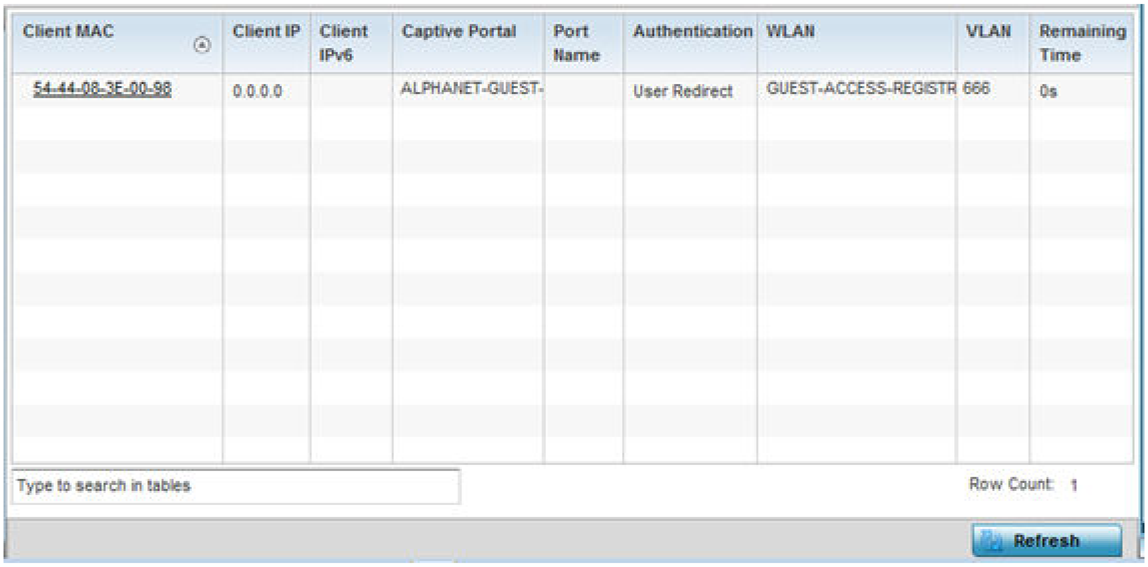
AP Captive Portal

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, select a **controller or service platform**, and select one of its 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.



Client MAC	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
54-44-08-3E-00-98	0.0.0.0		ALPHANET-GUEST-		User Redirect	GUEST-ACCESS-REGISTR	666	0s

Row Count: 1

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:

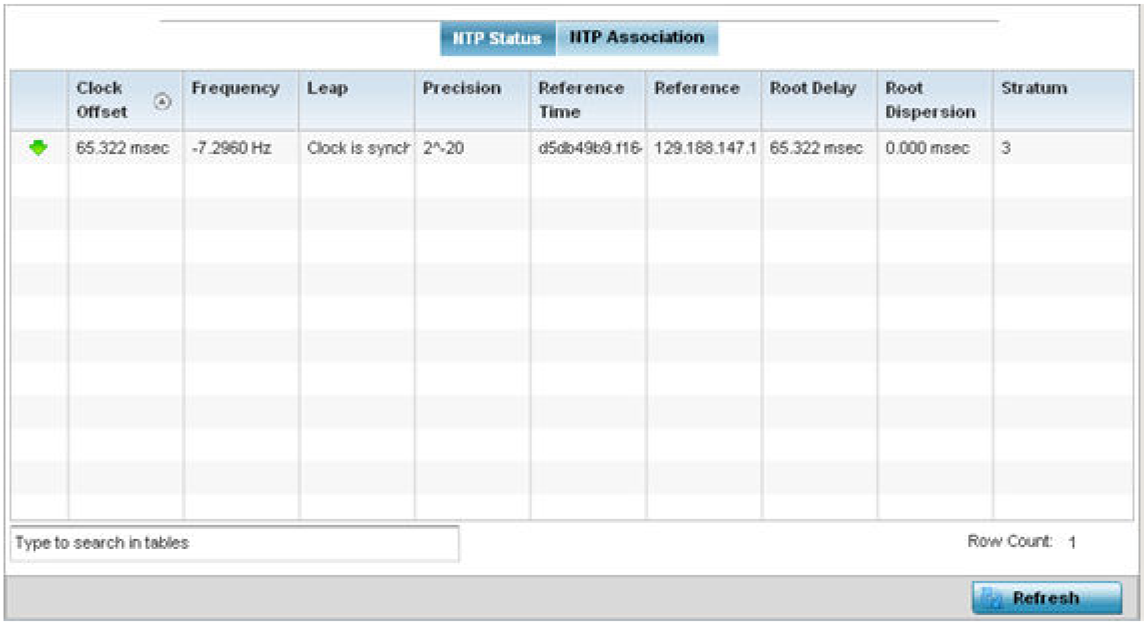
- AP NTP Status on page 1323
- AP NTP Association on page 1324

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, select a **controller or service platform**, and select one of its 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.



	Clock Offset	Frequency	Leap	Precision	Reference Time	Reference	Root Delay	Root Dispersion	Stratum
▼	65.322 msec	-7.2960 Hz	Clock is synch	2^-20	d5db49b9.f16	129.188.147.1	65.322 msec	0.000 msec	3

Row Count: 1

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.

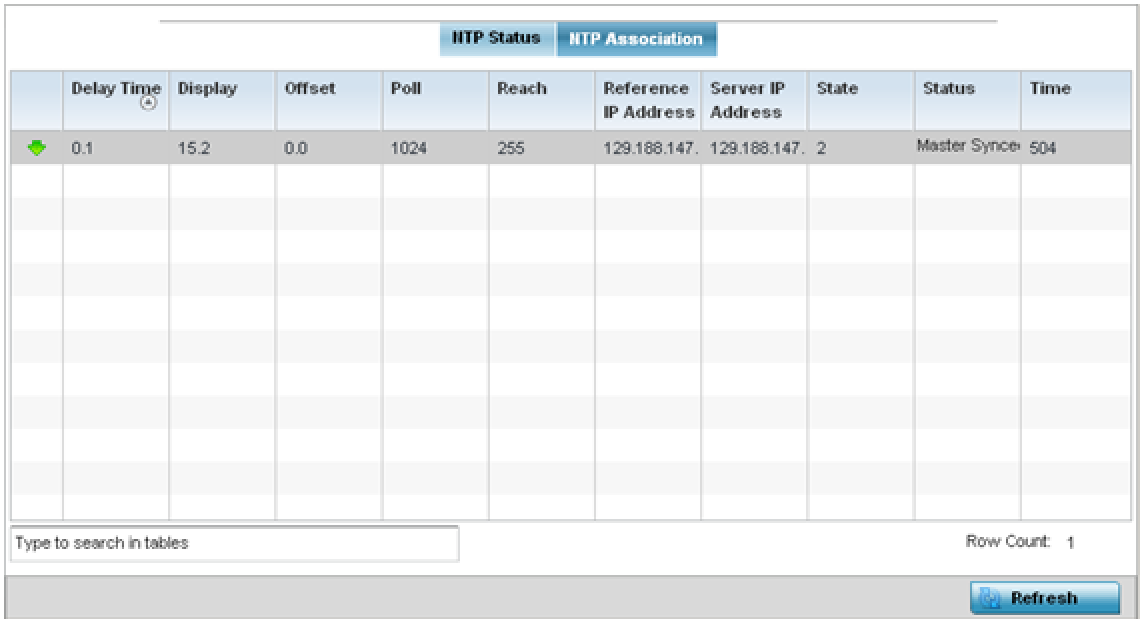
AP NTP Association

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, select a **controller or service platform**, and select one of its 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.



	Delay Time	Display	Offset	Poll	Reach	Reference IP Address	Server IP Address	State	Status	Time
▼	0.1	15.2	0.0	1024	255	129.188.147.	129.188.147.	2	Master Synce	504

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: • **Synced** – Indicates the controller or service platform is synchronized to this NTP server. • **Unsynced** – Indicates the controller or service platform has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC. • **Selected** – Indicates this NTP master server will be considered the next time the controller or service platform chooses a new master to synchronize with. • **Candidate** – Indicates this NTP master server may be considered for selection the next time the controller or service platform chooses a NTP master server. • **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

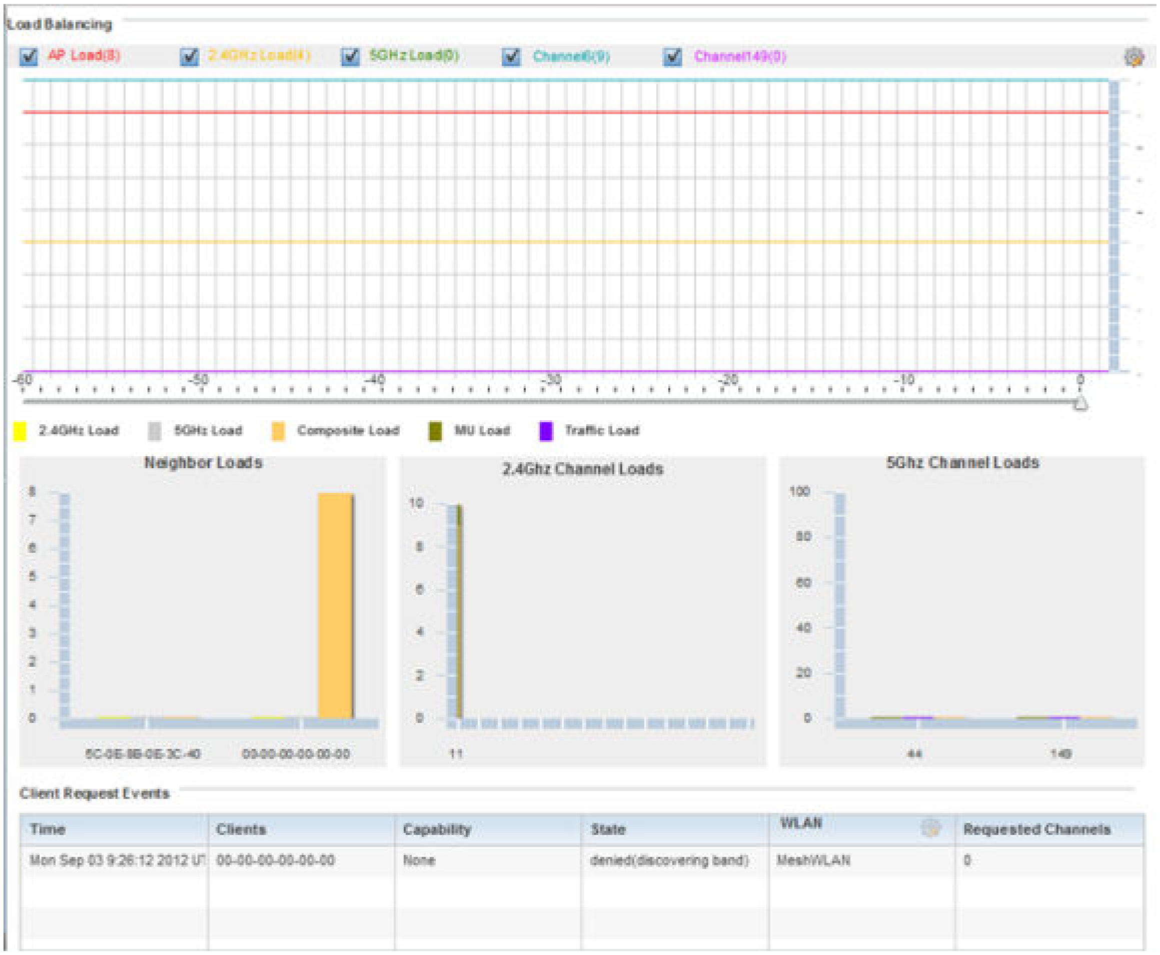
AP Load Balancing

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, select a **controller or service platform**, and select one of its 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.



Load Balancing

☑ AP Load(8) ☑ 2.4GHz Load(4) ☑ 5GHz Load(0) ☑ Channel6(9) ☑ Channel149(0)

Client Request Events

Time	Clients	Capability	State	WLAN	Requested Channels
Mon Sep 03 9:26:12 2012 U	00-00-00-00-00-00	None	denied(discovering band)	MeshWLAN	0

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:

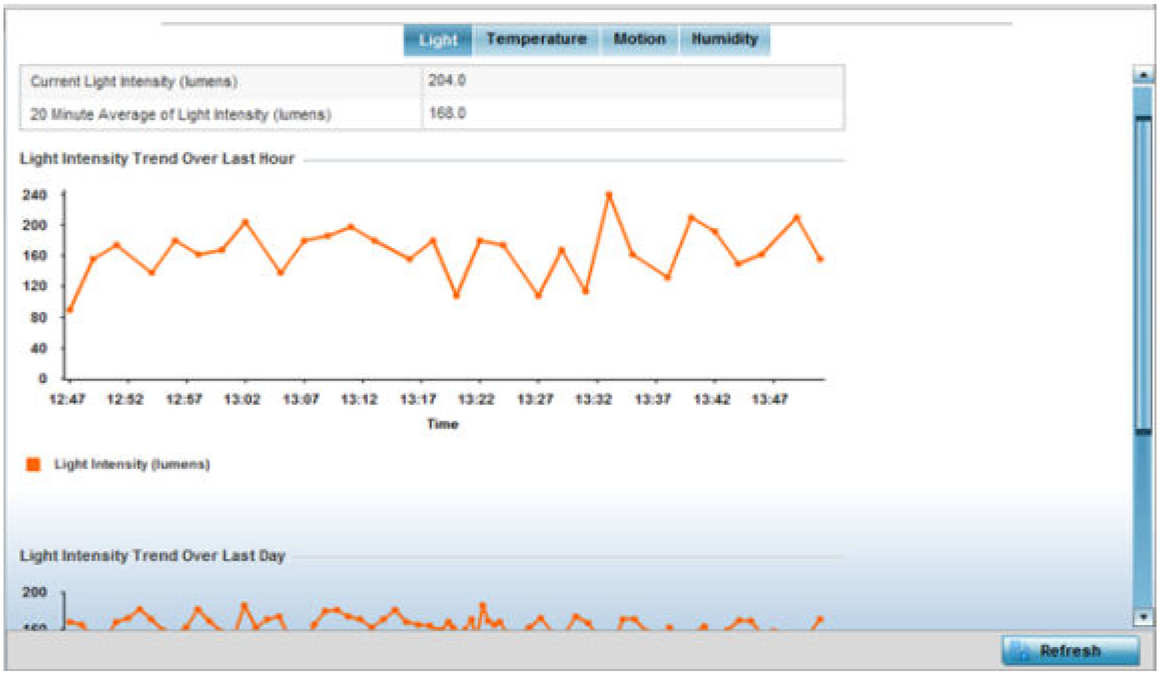
- AP Light Sensor on page 1328.
- AP Temperature Sensor on page 1329.
- AP Motion Sensor on page 1330.
- AP Humidity Sensor on page 1331,

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, select a **controller or service platform**, and select one of its 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.



Current Light Intensity (lumens)	204.0
20 Minute Average of Light Intensity (lumens)	168.0

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.

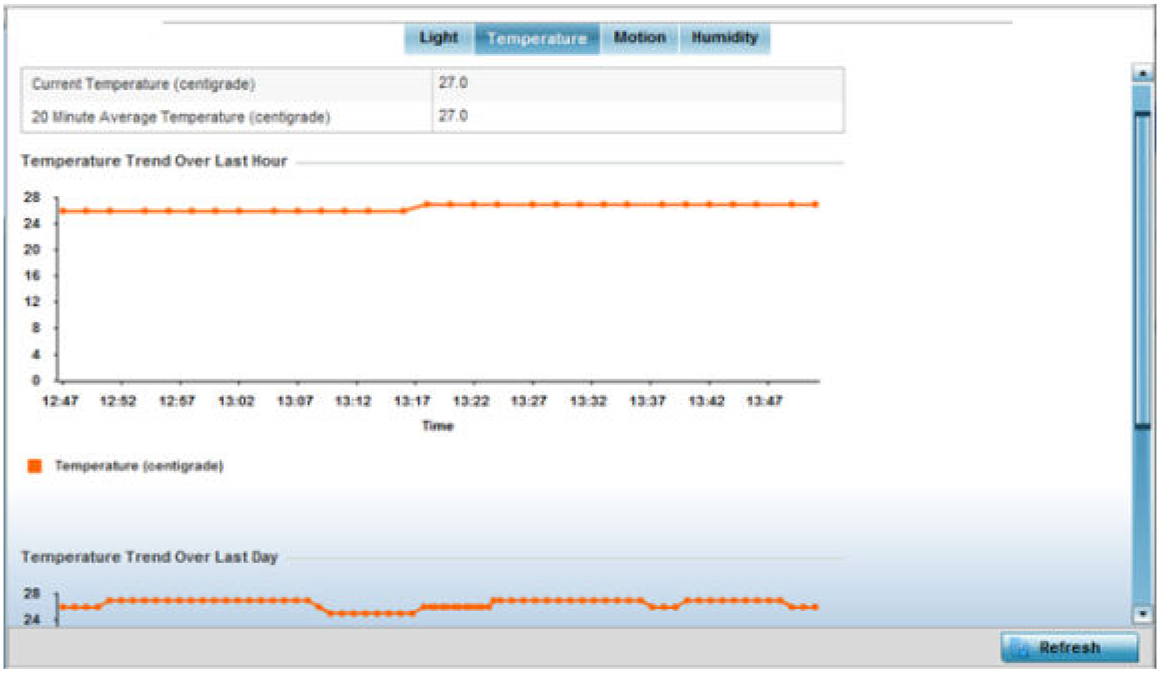
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Current Temperature (centigrade)	27.0
20 Minute Average Temperature (centigrade)	27.0

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.

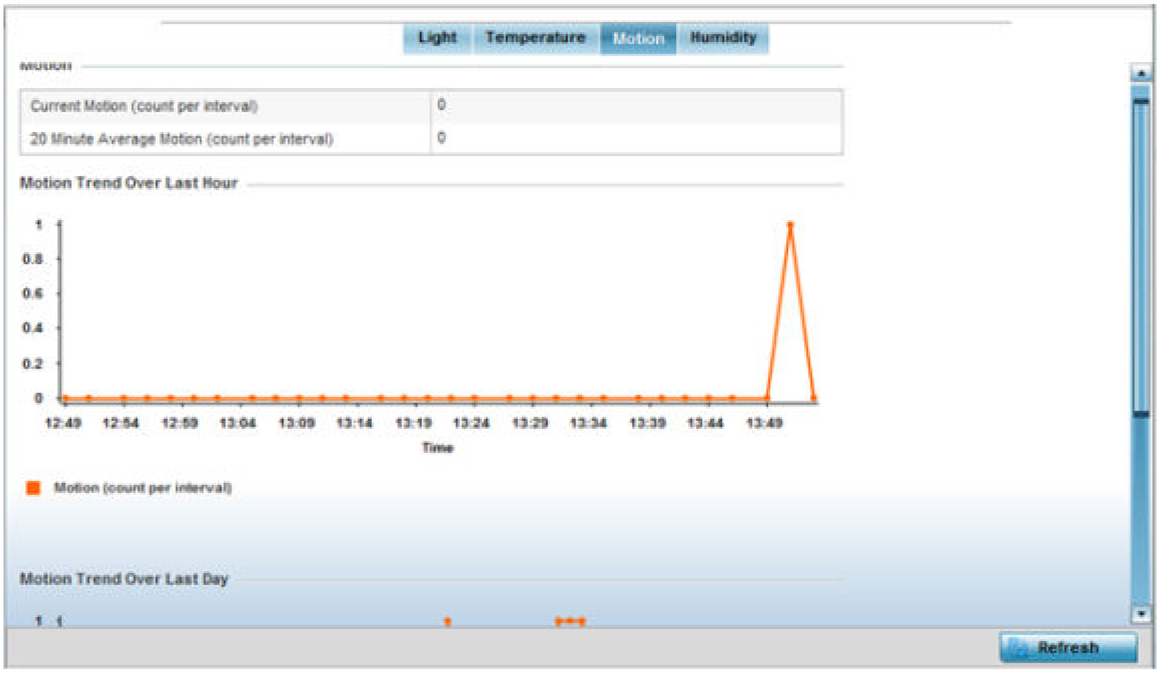
2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its 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.



Current Motion (count per interval)	0
20 Minute Average Motion (count per interval)	0

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.

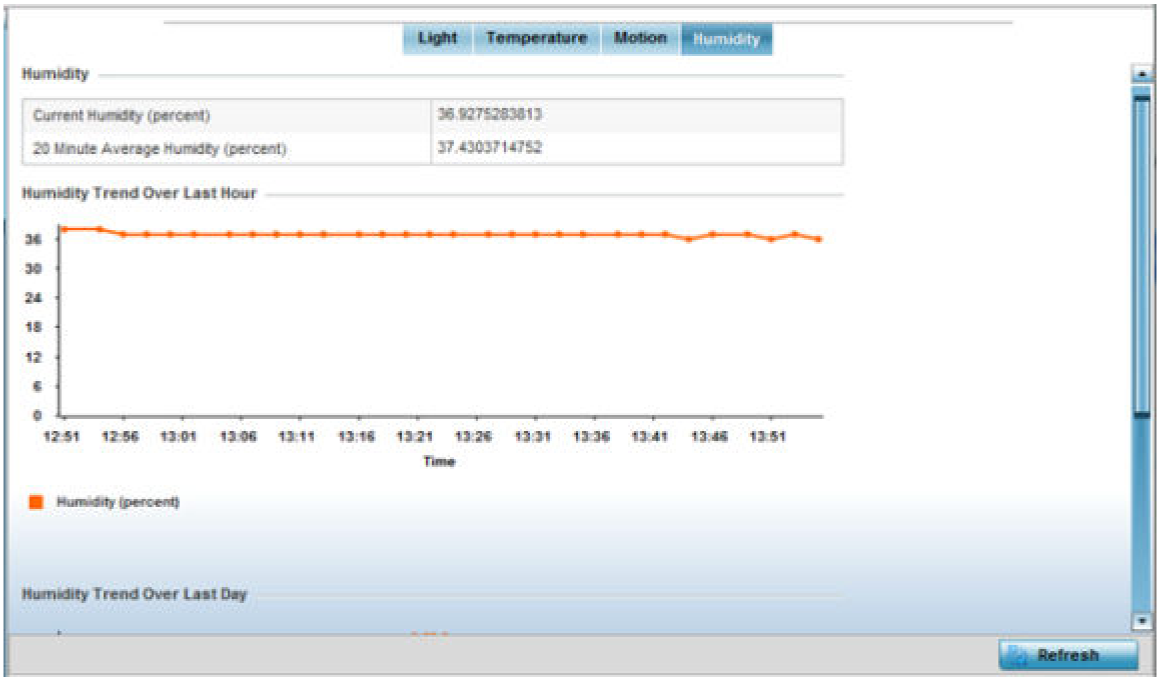
7. Refer to the Motion Trend Over Last Hour graph to assess the fluctuation in user movement over the last hour. Use this graph in combination with the Light and Temperature graphs (in particular) to assess the deployment area's activity level.
8. Refer to the Motion Trend Over Last Day graph to assess 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, select a **controller or service platform**, and select one of its 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.



Humidity

Current Humidity (percent)	36.9275283813
20 Minute Average Humidity (percent)	37.4303714752

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

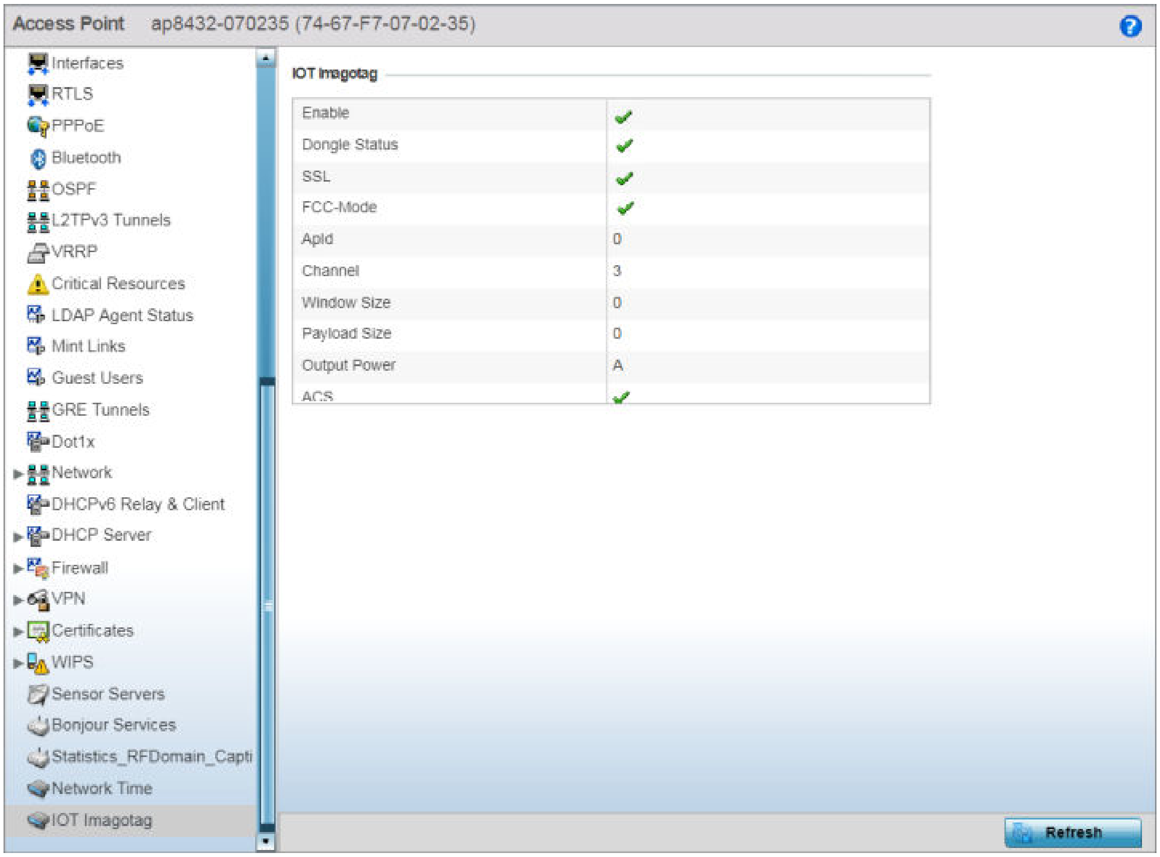
The WiNG AP-8432 model access points support SES-imagotag's ESL tags. An Imagotag-enabled AP recognizes the ESL communicator and facilitates communication between communicator and tags. To enable an AP-8432 as an infrastructure device facilitating communication between the ESL communicator and tags, 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 900

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.



Enable	✓
Dongle Status	✓
SSL	✓
FCC-Mode	✓
ApId	0
Channel	3
Window Size	0
Payload Size	0
Output Power	A
ACS	✓

Figure 405: 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 1334.
- Client Details on page 1337.
- Client Traffic on page 1340.
- Client WMM TSPEC on page 1343.
- Client Association History on page 1344.
- Client Graph on page 1345.

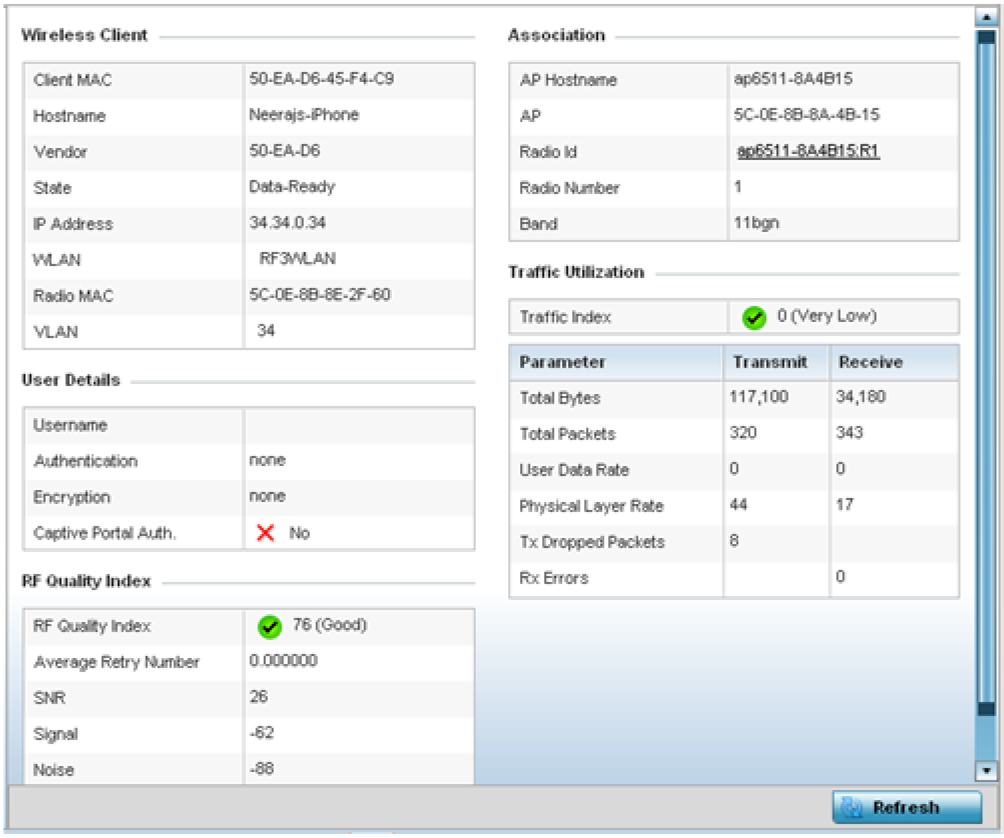
Client Health

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.



Wireless Client

Client MAC	50-EA-D6-45-F4-C9
Hostname	Neerajs-iPhone
Vendor	50-EA-D6
State	Data-Ready
IP Address	34.34.0.34
WLAN	RF3WLAN
Radio MAC	5C-0E-8B-8E-2F-60
VLAN	34

User Details

Username	
Authentication	none
Encryption	none
Captive Portal Auth.	✗ No

RF Quality Index

RF Quality Index	✓ 76 (Good)
Average Retry Number	0.000000
SNR	26
Signal	-62
Noise	-88

Association

AP Hostname	ap6511-8A4B15
AP	5C-0E-8B-8A-4B-15
Radio Id	ap6511-8A4B15:R1
Radio Number	1
Band	11bgn

Traffic Utilization

Traffic Index	✓ 0 (Very Low)

Parameter	Transmit	Receive
Total Bytes	117,100	34,180
Total Packets	320	343
User Data Rate	0	0
Physical Layer Rate	44	17
Tx Dropped Packets	8	
Rx Errors		0

Figure 406: 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: • *0 – 20* (Very poor quality) • *20 – 40* (Poor quality) • *40 – 60* (Average quality) • *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.

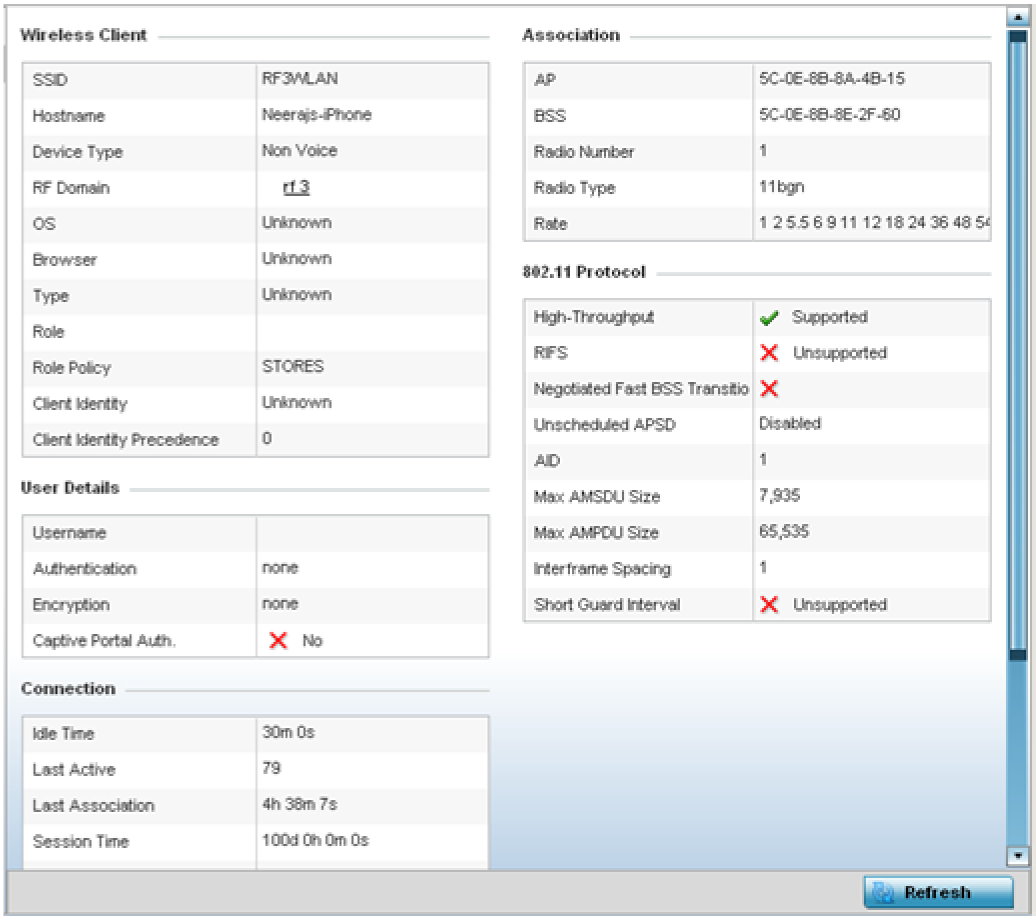
To view the details screen of a connected wireless client:

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.



Wireless Client

SSID	RF3WLAN
Hostname	Neerajs-iPhone
Device Type	Non Voice
RF Domain	rf 3
OS	Unknown
Browser	Unknown
Type	Unknown
Role	
Role Policy	STORES
Client Identity	Unknown
Client Identity Precedence	0

User Details

Username	
Authentication	none
Encryption	none
Captive Portal Auth.	✗ No

Connection

Idle Time	30m 0s
Last Active	79
Last Association	4h 38m 7s
Session Time	100d 0h 0m 0s

Association

AP	5C-0E-8B-8A-4B-15
BSS	5C-0E-8B-8E-2F-60
Radio Number	1
Radio Type	11bgn
Rate	1 2 5.5 6 9 11 12 18 24 36 48 5

802.11 Protocol

High-Throughput	✓ Supported
RIFS	✗ Unsupported
Negotiated Fast BSS Transitio	✗
Unscheduled APSD	Disabled
AID	1
Max AMSDU Size	7,935
Max AMPDU Size	65,535
Interframe Spacing	1
Short Guard Interval	✗ Unsupported

Figure 407: 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.

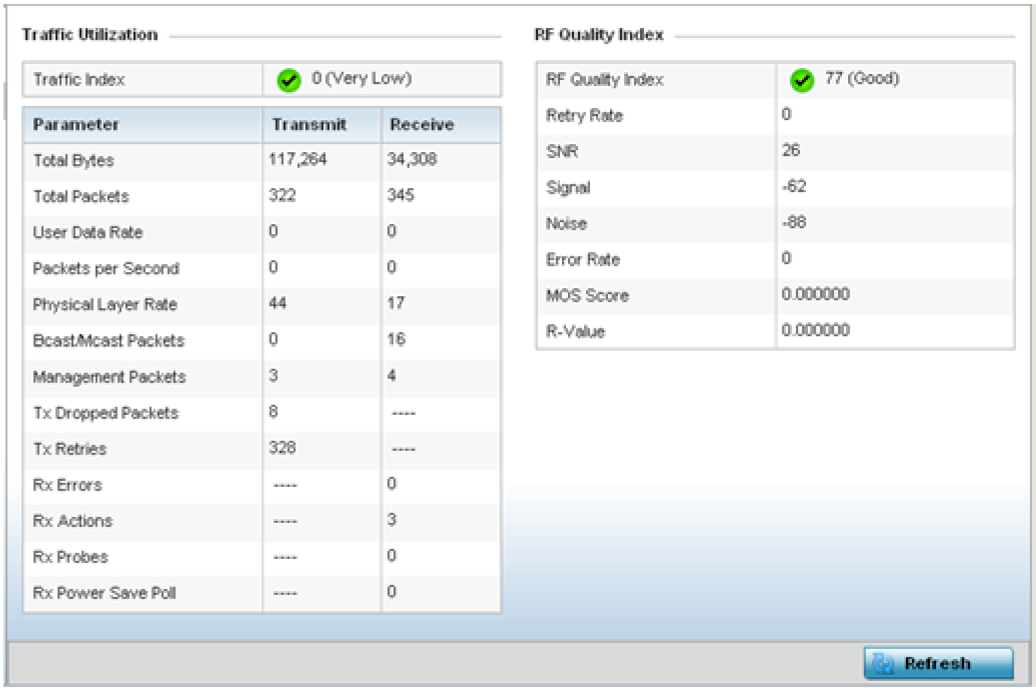
Client Traffic

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.



Traffic Utilization

Traffic Index	✓ 0 (Very Low)	
Parameter	**Transmit**	**Receive**
Total Bytes	117,264	34,308
Total Packets	322	345
User Data Rate	0	0
Packets per Second	0	0
Physical Layer Rate	44	17
Bcast/Mcast Packets	0	16
Management Packets	3	4
Tx Dropped Packets	8	----
Tx Retries	328	----
Rx Errors	----	0
Rx Actions	----	3
Rx Probes	----	0
Rx Power Save Poll	----	0

RF Quality Index

RF Quality Index	✓ 77 (Good)
Retry Rate	0
SNR	26
Signal	-62
Noise	-88
Error Rate	0
MOS Score	0.000000
R-Value	0.000000

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: • *0 – 20* (Very low utilization) • *20 – 40* (Low utilization) • *40 – 60* (Moderate utilization) • *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

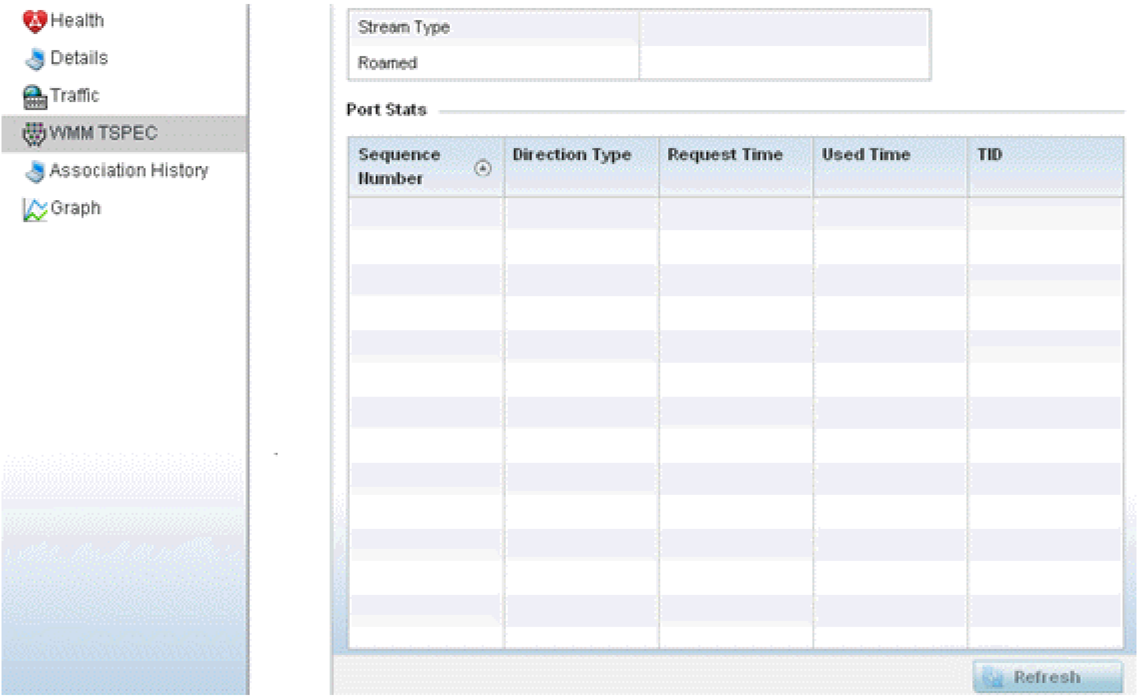
The 802.11e TSPEC *(Traffic Specification)* provides a set of parameters that define the characteristics of the traffic stream, (operating requirement and scheduling etc.). The sender's TSPEC specifies parameters available within packet flows. Both sender and the receiver use TSPEC.

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.

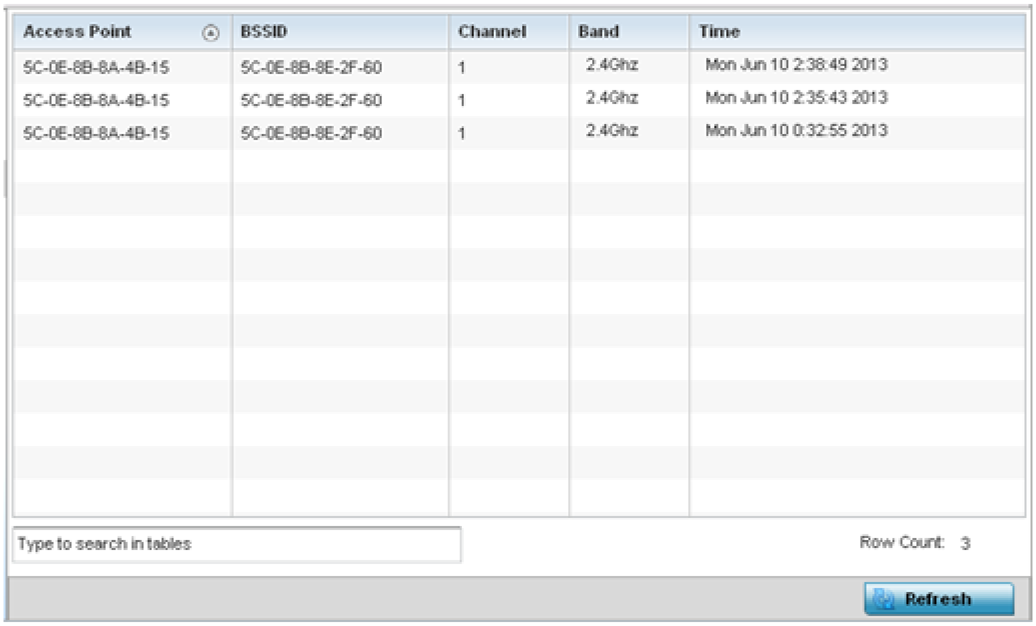
To view a selected client's association history:

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.



Access Point	BSSID	Channel	Band	Time
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:38:49 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:35:43 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 0:32:55 2013

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:

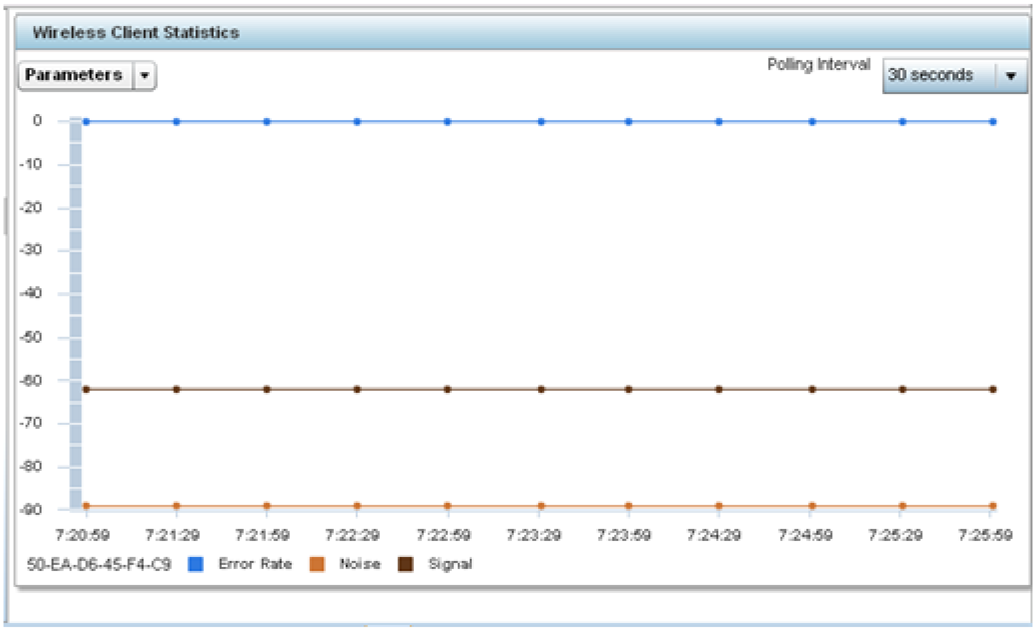
1 Select the **Statistics** menu from the Web UI.

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.

Guest Access Statistics

Guest client statistics are uniquely available for wireless clients requesting the required pass code, authentication and access into the WiNG managed guest client network.

- Guest Access Cumulative Statistics on page 1346
- Guest Access Social Media Statistics on page 1348
- Guest Access Reports on page 1350
- Guest Access Notifications on page 1351
- Guest Access Database on page 1353

Guest Access Cumulative Statistics

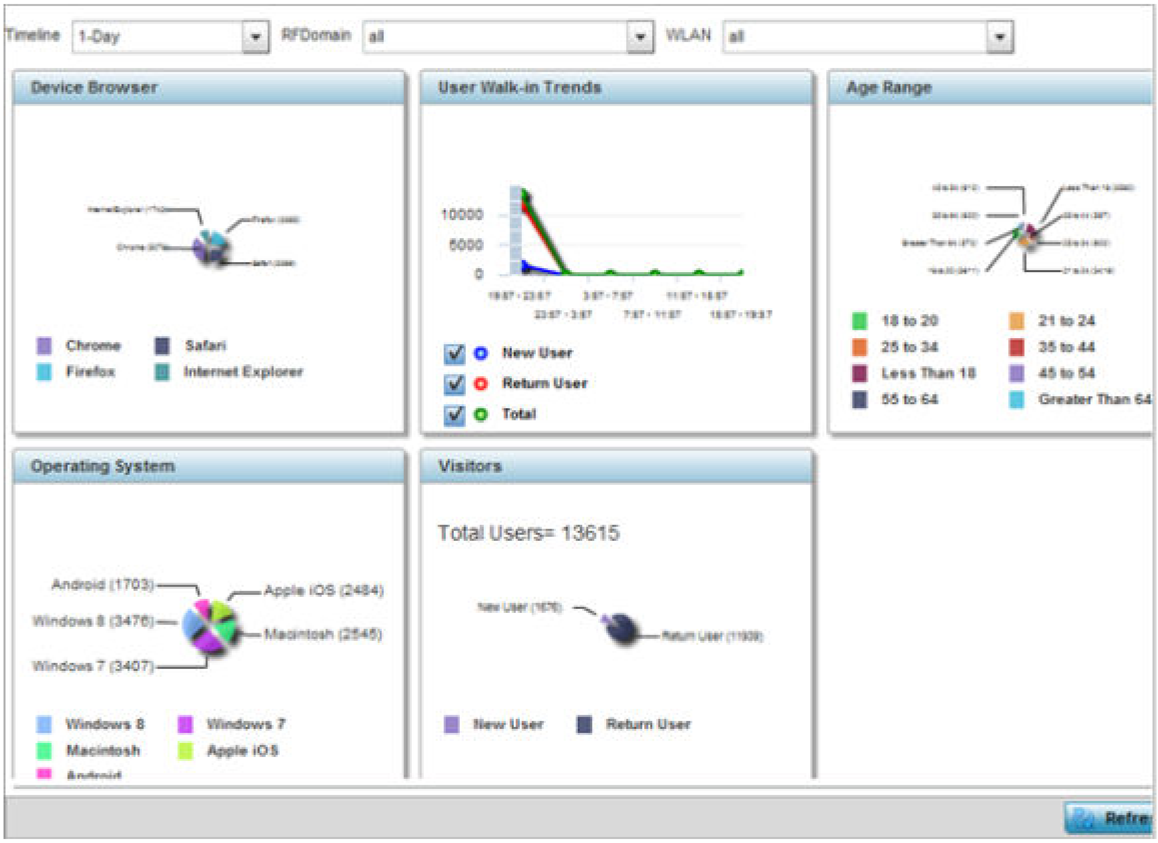
The Statistics screen displays information on the WiNG managed guest client network. Its includes browser utilization, new versus returning user trends, client user age, client operating system, device type proliferation and gender trending.

To view a cumulative set of client guest access statistics:

1. Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

The **Guest Access** → **Statistics** page displays in the right-hand pane, with the Statistics screen selected by default.



Timeline 1-Day RFDomain all WLAN all

Total Users= 13615

Figure 408: Guest Access - Statistics Screen

3 Use the following filters, available at the top of the screen, to filter guest access statistical data.

Timeline	Use the drop-down menu to specify whether statistics are gathered for **`1-Day`**, **`1-Month`**, **`1-Week`**, **`2-Hours`**, **`30-Mins`** or **`5-Hours`**. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
RFDomain	Use the drop-down menu to select a single RF Domain from which to filter guest access statistics. Optionally select **All** to include data from each RF Domain supported.
WLAN	Use the drop down menu to filter guest access statistics to a specific WLAN. Optionally select **All** to include data from all WLANs within the selected RF Domain. Note: A WLAN can belong to more then one RF Domain.

4 Refer to the following to assess guest client browser, operating system, age, gender and new versus returning status to assess whether guest client utilization is in line with WiNG guest access deployment objectives:

Device Browser	Displays guest user browser utilization in pie-chart format. Each client browser type (Chrome, Firefox, Safari and Internet Explorer) detected within the defined trending period displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each browser also displays numerically.
User Walk-in Trends	Walk-in trending enables an administrator to filter new guest access clients versus return guest clients out of the total reported for the trending period and selected RF Domain and WLAN. New guest users (blue), return guests (red) or total guests can either be collectively displayed or individually displayed by selecting one, two or all three of the options.
Age Range	Displays guest user age differentiation in pie-chart format. Age ranges are uniquely color coded as: **`Less Than 18`**, **`18 to 20`**, **`21 to 24`**, **`25 to 34`**, **`35 to 44`**, **`45 to 54`**, **`55 to 64`** and **`Greater Than 64`**. Each age group detected within the trending period displays uniquely in its own color for easy differentiation. Each age range also displays numerically. Periodically assess whether the age ranges meet expectations for guest client access within the WiNG managed guest network.
Operating System	Displays guest client operating system utilization in pie-chart format. Each client operating system type (Android, Windows 7, Windows 8, Apple iOS and Macintosh) displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each operating system also displays numerically.
Visitors	Displays return guest clients versus new guest clients in pie-chart format. Both new and returning clients display uniquely in their own color for easy differentiation. Periodically assess whether the number of returning guest clients is line with the guest network's deployment objectives in respect to the RF Domain(s) and WLAN(s) selected for trending.
Customer Loyalty App	Graphically displays the number of guest clients with loyalty application presence enabled. Loyalty application detection occurs on the Access Point to which the client is associated, allowing 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.
Devices	Displays guest client device type utilization in pie-chart format. Each client device type (Windows PC, Macintosh, Apple iPad, and Android Mobile) displays uniquely in its own color for easy differentiation. The number of each device type detected also displays numerically to help assess their proliferation with WiNG managed guest network.
Gender	Displays guest client gender in pie-chart format. Detected male and female guest users display uniquely in their own color for easy differentiation. Guest clients whose gender is unspecified also displays to help assess the undetermined gender client count out of total. The number of male, female and unspecified guest clients also displays numerically.

Guest Access Social Media Statistics

Device registration using social media login credentials requires user validation through the guest user's social media account. The guest user authenticates with an administrator configured social media server like Facebook or Google. Upon successful authentication, the guest user's social media profile data (collected from the social media server) is registered on the device.

To view guest access social media utilization for guest clients:

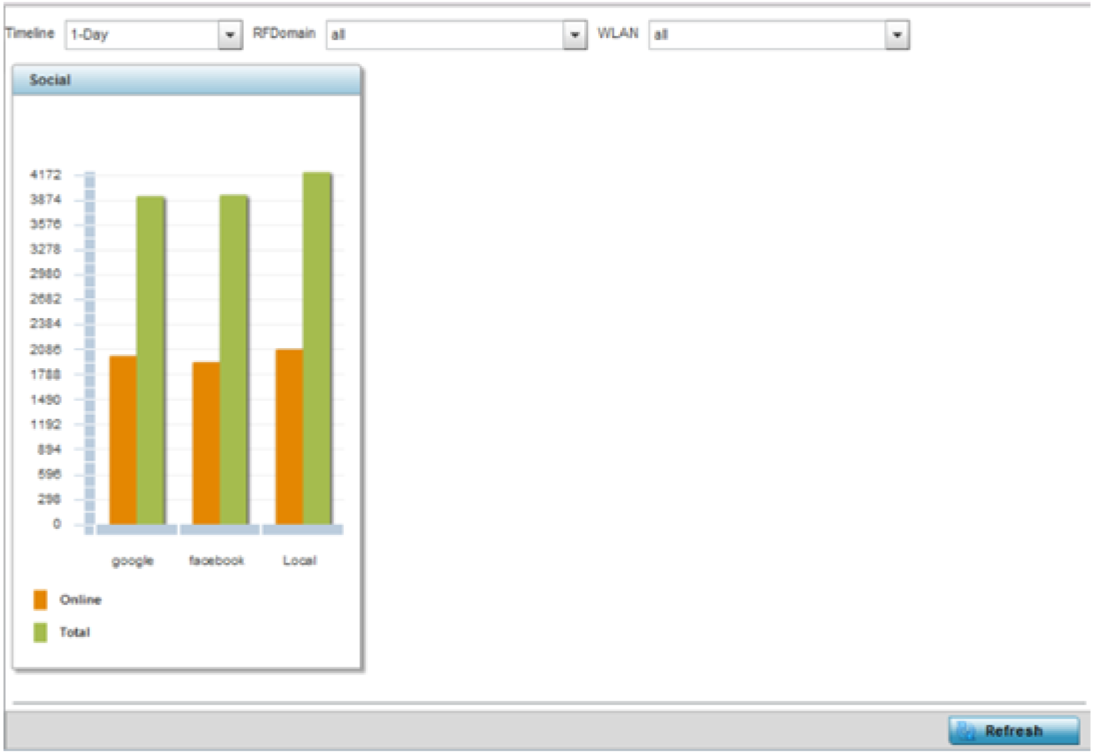
1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

The Guest Access statistics menu is displayed in the right-hand pane, with the Statistics screen selected by default.

3 Select **Social** from the statistics menu.

The **Guest Access > Social** page displays.



Timeline 1-Day RFDomain all WLAN all

Figure 409: Guest Access - Social Media - Statistics Screen

4 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access social media trending:

Timeline	Use the drop-down menu to specify whether statistics are gathered for **`1-Day`**, **`1-Month`**, **`1-Week`**, **`2-Hours`**, **`30-Mins`** or **`5-Hours`**. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
RFDomain	Use the drop-down menu to select a single RF Domain from which to filter social media guest access statistics. Optionally select All to include data from each RF Domain supported.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN. A single WLAN can belong to more then one RF Domain.

The data displays in bar graph format, with the total number of social media authenticating clients listed in *green*, and those currently online displayed in *orange* for both Google and Facebook authenticating clients. Refer to the Local graph to assess those clients requiring captive portal authentication as a fallback mechanism for guest registration through social media authentication.

5 Periodically select **Refresh** to update the statistics counters to their latest values.

Guest Access Reports

Report queries can be filtered and run to obtain information on targeted guest clients within the WiNG guest network.

To generate customized guest client reports:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

The Guest Access statistics menu is displayed in the right-hand pane, with the Statistics screen selected by default.

3 Select **Reports** from the statistics menu.

The **Guest Access** → **Reports** page displays.

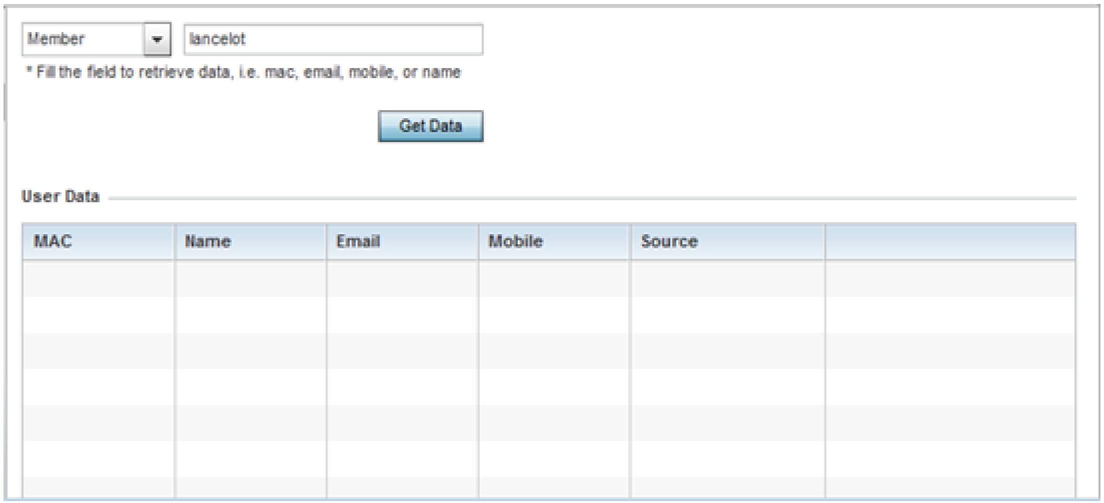

Member
lancelot
* Fill the field to retrieve data, i.e. mac, email, mobile, or name
Get Data
User Data
MAC
Name
Email
Mobile
Source

Figure 410: Guest Access - Reports Screen

4 Use the drop-down menu at the top, left-hand, side of the screen to define whether the guest client's report data is fetched based on the client's `MAC` address, `Name`, `Mobile`, `Email`, `Member` or `Time` (login duration). Once provided, enter an appropriate search string to generate a report for the target guest client.

5 After specifying the data filter criteria, select **Get Data**.

6 Refer to the User Data table to review the following report output:

MAC	Displays the factory encoded hardware MAC address assigned to this guest client at the factory by the manufacturer. This is the guest client's hardware identifier added to the guest user database. If the guest client requests access later, this MAC address is validated against the guest user database, and the client is allowed access to the WiNG managed guest network.
Name	Lists the name used for guest access authentication and pass code generation.

Email	Lists the E-Mail address used for guest access authentication and the receipt of the required passcode.
Mobile	Lists the guest client's registered mobile number used for guest access authentication requests and the receipt of the required passcode.
Source	Lists the source (Facebook, Google) whose username and password were used as the client's social media authenticator.

Guest Access Notifications

For each registered guest user, a passcode is sent by E-mail, SMS *(short message service)*or both. A guest management policy defines E-mail host and SMS gateway commands, along with credentials required for sending a passcode to guest client via E-mail and SMS Users can configure up to 32 different guest management policies. Each policy enables the user to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. There can be only one guest management policy active per device at any one time.

The SMS is the text messaging service component of phone, E-Mail and mobile systems. SMS uses standardized communications protocols to allow fixed or mobile phone devices to exchange text messages.

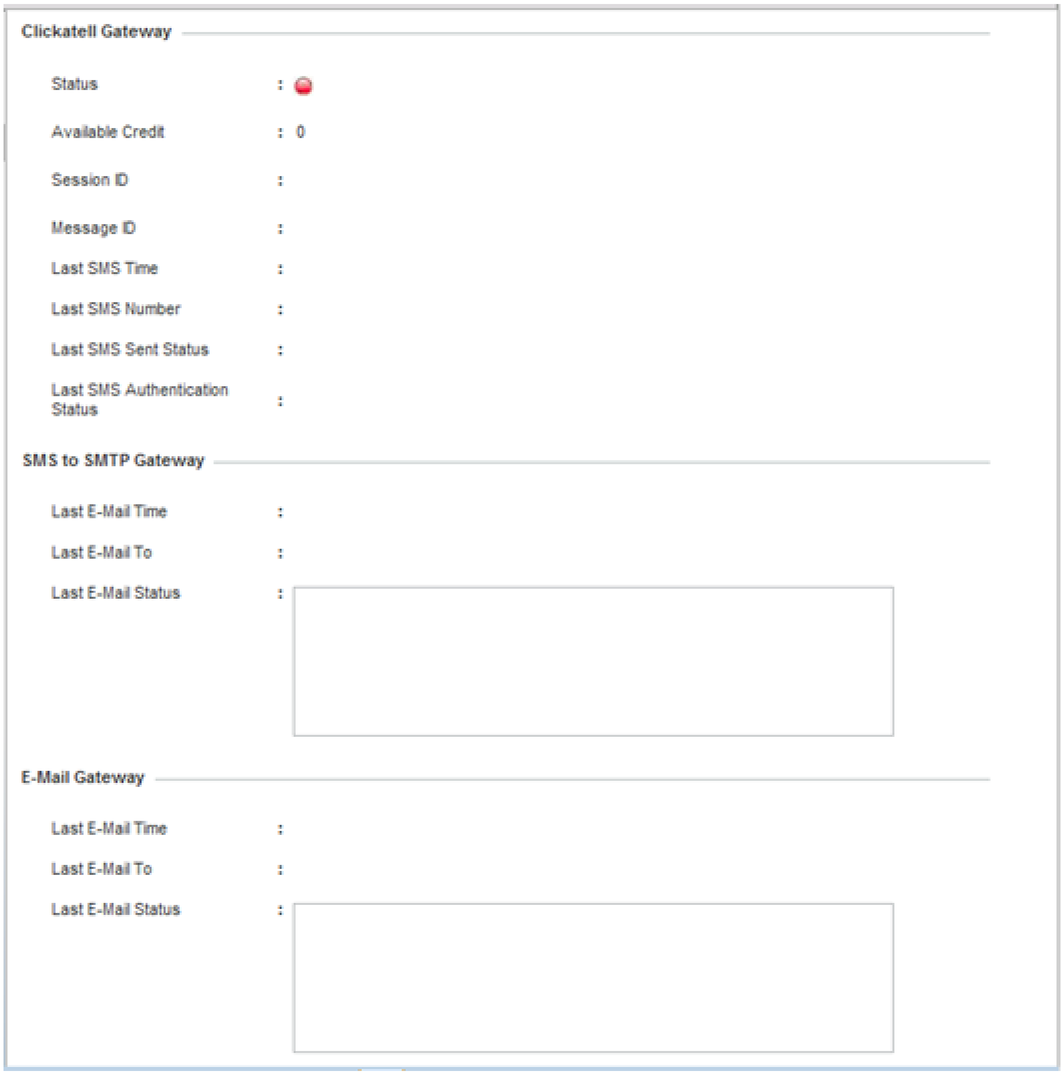
To review guest client notification statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

   The Guest Access statistics menu is displayed in the right-hand pane of the UI. The cumulative statistics screen is displayed by default.

3 Select **Notification** from the statistics menu.

The **Guest Access > Notification** page displays.



Clickatell Gateway

Status : ●

Available Credit : 0

Session ID :

Message ID :

Last SMS Time :

Last SMS Number :

Last SMS Sent Status :

Last SMS Authentication Status :

SMS to SMTP Gateway

Last E-Mail Time :

Last E-Mail To :

Last E-Mail Status :

E-Mail Gateway

Last E-Mail Time :

Last E-Mail To :

Last E-Mail Status :

Figure 411: Guest Access - Notification Screen

4 Review the following Clickatell Gateway information. By default, clickatell is the host SMS gateway server resource for guest access.

Status	Displays an icon as a visual indicator of the gateway status. *Green* defines the gateway as available. *Red* indicates the gateway is down and unavailable.
Available Credit	PENDING
Session ID	Lists an event ID for the clickatell gateway session credential and passcode exchange.
Message ID	Lists the unique SMS message ID created for the successful message exchange with the clickatell host SMS gateway server.
Last SMS Time	Lists the timestamp appended to the sent time of the clickatell SMS gateway message.

Last SMS Number	Lists the numeric status code returned in response to a SMS gateway server guest access request.
Last SMS Sent Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.
Last SMS Authentication Status	Lists the SMS authentication credential and validation message exchange status for the listed clieckatell gateway session ID.

5 Review the following SMS to SMTP Gateway information.

Last E-Mail Time	Displays the most recent E-Mailed passcode to a guest via SMS. SMS enables guest users to register with their E-Mail or mobile device ID as the primary key for authentication.
Last E-Mail To	Lists the recipient of the most recent SMS to SMTP server credential E-mail exchange containing the required passcode for the registered guest.
Last E-Mail Status	Lists the completion status of the most recent server SMS to SMTP gateway credential exchange containing the required passcode for the authenticating guest client.

6 Review the following Email Gateway information.

Last E-Mail Time	Displays the time of the most recent E-Mailed passcode to a guest access requesting client. Guest users can register with their E-mail credentials as the primary means of authentication.
Last E-Mail To	Lists the recipient of this session’s server E-Mail credential exchange containing the required passcode for the authenticating guest client.
Last E-Mail Status	Lists the completion status of the most recent server E-Mail credential exchange containing the required passcode for the authenticating guest client.

Guest Access Database

Guest client statistics are uniquely available for wireless clients requesting the required pass code, authentication and access into the WiNG managed guest client network.

To administrate the guest access database:

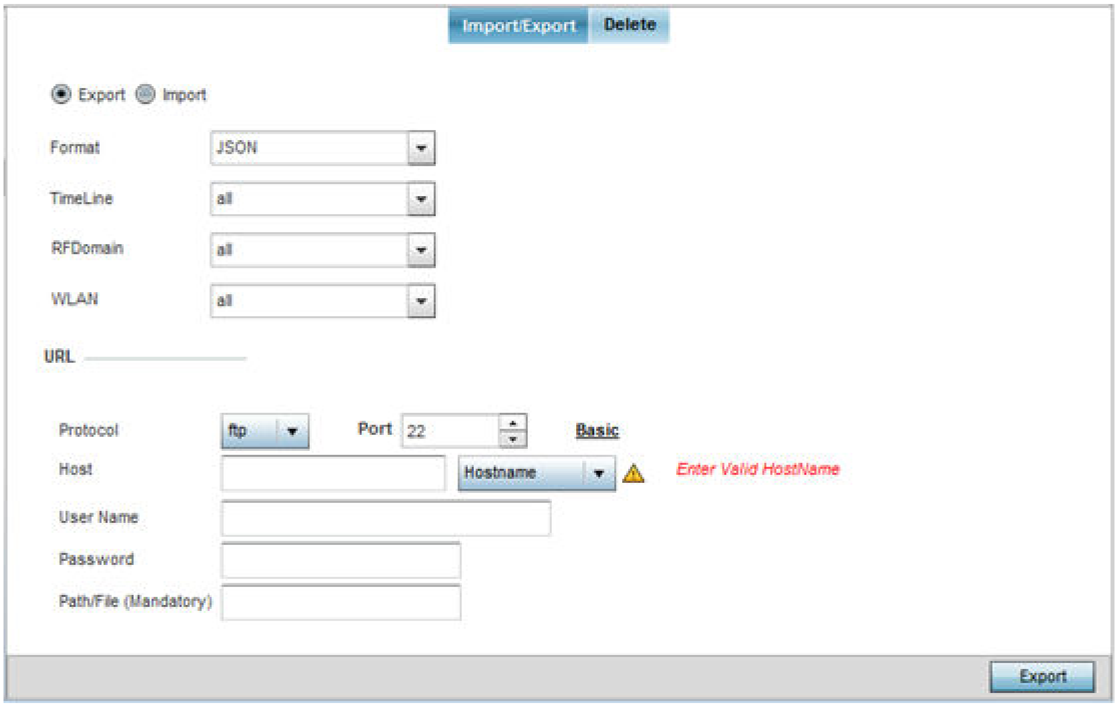
1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

The Guest Access statistics menu is displayed in the right-hand pane, with the Statistics screen selected by default.

3 Select **Database** from the statistics menu.

The **Guest Access** → **Database** page displays.



● Export ○ Import

Format: JSON

TimeLine: all

RFDomain: all

WLAN: all

Protocol: ftp

Port: 22

Host: Hostname

Enter Valid HostName

User Name

Password

Path/File (Mandatory)

Figure 412: Guest Access - Database - Import/Export Screen

4 Select **Export** to archive guest access data (in JSON or CSV format) to a designated remote location, or **Import** to upload guest access utilization data back to the WiNG managed controller, service platform or access point.

5 If conducting an Export operation, provide the following to refine the data exported:

Format	Define whether the guest access data is exported in **`JSON`** or **`CSV`** format. JSON *(JavaScript Object Notation)* is an open standard format using text to export data objects consisting of attribute value pairs. A CSV *(comma-separated values)* file stores tabular data in plain text. Plain text means that the file is interpreted a sequence of characters, so that it is human-readable with a standard text editor. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.
Timeline	Use the drop-down menu to specify whether guest access statistics are exported for the previous **`1-Day`**, **`1-Month`**, **`1-Week`**, **`2-Hours`**, **`30-Mins`** or **`5-Hours`**. Timelines support the latest time period from present. For example, specifying 30-Mins exports statistics trended over the most recent 30 minutes.
RFDomain	Use the drop-down menu to select a single RF Domain from which to filter social media guest access statistics. Optionally select **All** to include data from each RF Domain supported.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN. Optionally select **All** to include data from all WLANs within the selected RF Domain. Note: A WLAN can belong to more then one RF Domain.

6 When exporting or importing guest access data (regardless or format), provide the following URL data to accurately configure the remote host.

Protocol	Select the data transfer protocol used for exporting or importing guest access data. Available options include: • tftp • ftp • sftp
Port	Use the spinner control to set the virtual port for the for the export or import operation.
Host	Provide a textual hostname or numeric IP address of the server used for guest access data transfer operations. Hostnames cannot include an underscore character. 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.
User Name	If using FTP or SFTP as the data transfer protocol, enter the *username* required by the remote FTP or SFTP server resource.
Password	If using FTP or SFTP as the data transfer protocol, enter the *password* required by the remote FTP or SFTP server resource.
Path/File (Mandatory)	Specify the path to the server resource where guest access data is either exported or imported. Enter the complete relative path to the file on the server. If electing to use SFTP as the file transfer protocol, its recommended the path/ file be set using the CLI *(command line interface)*.

7 When the URL data is accurately entered, select the **Export** or **Import** button respectively to initiate the operation.

8 Optionally select the **Delete** tab to purge either all or part of the guest user database.

The **Guest Access** → **Database** → **Delete** Screen displays.

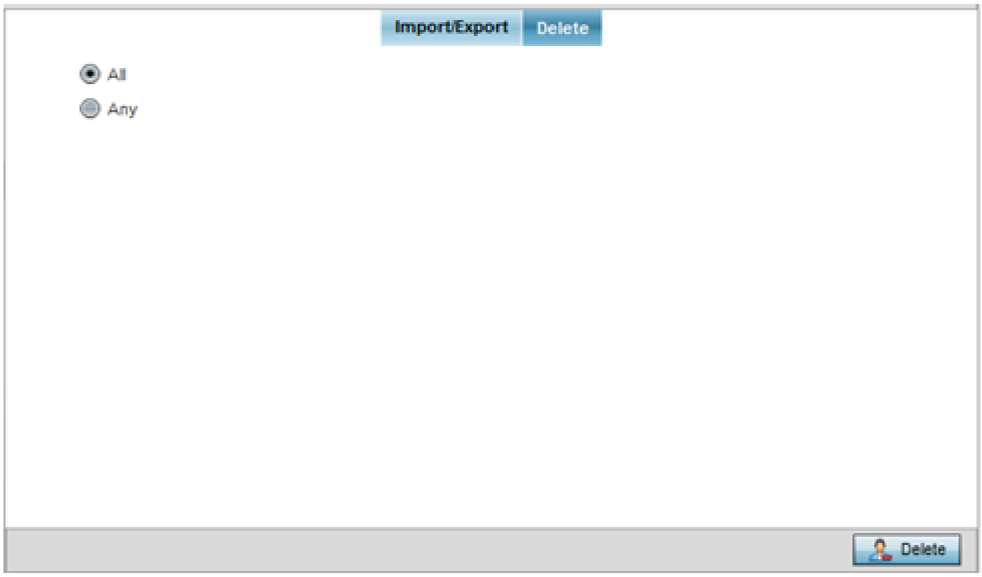


Figure 413: Guest Access - Database - Delete Screen

9 Select **All** to remove the contents of the entire database. Select **Any** to invoke a drop-down menu where **`MAC`**, **`Name`**, **`Mobile`**, **`Email`** or a **`WLAN`** can be selected to refine the database removal to just a selected entity. Enter the name of the MAC address, user, mobile number or WLAN you wish to remove from the database, then select **Delete**.

16 WiNG Events

WiNG Event Messages

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 943.

WiNG Event Messages

Refer to the following (read only) information to assess logged diagnostic events.

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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

Event	Description
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
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

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)