Extreme®
Connect Beyond the Network

WiNG™ 5.9.0 Access Point

System Reference Guide

Published June 2017
9035122

Copyright © 2017 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

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 about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

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

Contents

About this guide 1

Document Convention 1
Notational Conventions 2
End-User Software License Agreement 2

Chapter 1: Overview 9

About the WiNG Software 10
Distributed Intelligence 11
High Availability Networks 11
Gap Free Security 11
Outdoor Wireless and Mesh Networking 12
Network Services, Routing and Switching 12
Management, Deployment and Troubleshooting 12

Chapter 2: Web User Interface Features 13

Accessing the Web UI 13
Browser and System Requirements 13
Connecting to the Web UI 13
Glossary of Icons Used 15
Global Icons 15
Dialog Box Icons 16
Table Icons 17
Status Icons 17
Configurable Objects 18
Configuration Objects 21
Configuration Operation Icons 21
Access Type Icons 21
Administrative Role Icons 22
Device Icons 23

Chapter 3: Quick Start 25

Using the Initial Setup Wizard 25
Typical Setup Wizard 28
Virtual Controller AP Mode 30
Standalone Mode 31
Network Topology Selection 31
LAN Configuration 33
WAN Configuration 34
Wireless LAN Setup 36
Summary And Commit Screen 39
Adopt to a controller 40
Advanced Setup Wizard 41
Network Topology Selection 43
LAN Configuration 45
WAN Configuration 46
Radio Configuration 48
Wireless LAN Setup 49
System Information 51
Summary And Commit Screen 53

Adopt to a controller 54

Chapter 4: Dashboard 57

Dashboard 57
Dashboard Conventions 58
Health 58
Inventory 62
Network View 66
Network View Display Options 67
Device Specific Information 68

Chapter 5: Device Configuration 71

RF Domain Configuration 71
RF Domain Sensor Configuration 73
RF Client Name Configuration 76
RF Domain Alias Configuration 77
Basic Alias 78
Network Group Alias 81
Network Service Alias 84
System Profile Configuration 86
General Profile Configuration 87
Profile Radio Power 88
Profile Adoption (Auto Provisioning) Configuration 90
Profile Wired 802.1X Configuration 92
Profile Interface Configuration 93
Ethernet Port Configuration 94
Virtual Interface Configuration 105
Port Channel Configuration 116
Access Point Radio Configuration 124
WAN Backhaul Configuration 138
PPPoE Configuration 141
Bluetooth Configuration 144
Profile Network Configuration 147
DNS Configuration 148
ARP 150
L2TPv3 Profile Configuration 151
IGMP Snooping 161
MLD Snooping 163
Quality of Service (QoS) 165
Spanning Tree Configuration 170
Routing 173
Dynamic Routing (OSPF) 177
Forwarding Database 193
Bridge VLAN 195
Cisco Discovery Protocol Configuration 204
Link Layer Discovery Protocol Configuration 205
Miscellaneous Network Configuration 206
Alias 207
IPv6 Neighbor Configuration 216
Profile Network Configuration and Deployment Considerations 217
Profile Security Configuration 217
Defining Profile VPN Settings 218
Defining Profile Auto IPSec Tunnel 234
Defining Profile Security Settings 236
Setting the Certificate Revocation List (CRL) Configuration 237

Setting the Profile's RADIUS Trustpoint Configuration 238
Setting the Profile's NAT Configuration 239
Setting the Profile's Bridge NAT Configuration 247
Setting a Profile's Application Visibility Settings 250
Profile Security Configuration and Deployment Considerations 252
Virtual Router Redundancy Protocol (VRRP) Configuration 252
Profile Critical Resources 257
Profile Services Configuration 260
Profile Services Configuration and Deployment Considerations 261
Profile Management Configuration 261
Upgrading AP6532 Firmware from 5.1 266
Profile Management Configuration and Deployment Considerations 267
Mesh Point Configuration 267
Vehicle Mounted Modem (VMM) Deployment Consideration 277
Advanced Profile Configuration 278
Advanced Profile Client Load Balancing 278
Configuring MINT Protocol 283
Advanced Profile Miscellaneous Configuration 291
Environmental Sensor Configuration 293
Managing Virtual Controllers 295
Overriding a Device Configuration 297
Basic Configuration 297
Certificate Management 299
Manage Certificates 301
Wired 802.1X Overrides 315
RF Domain Overrides 316
Device Overrides 319
Radio Power Overrides 322
Adoption Overrides 324
Profile Interface Override Configuration 327
Overriding the Network Configuration 380
Overriding Security Configuration 455
Overriding the Virtual Router Redundancy Protocol (VRRP) Configuration 483
Profile Critical Resources 488
Overriding a Services Configuration 492
Overriding Management Configuration 493
Overriding Mesh Point Configuration 497
Overriding Environmental Sensor Configuration 508
Overriding an Advanced Configuration 510
Managing an Event Policy 525

Chapter 6: Wireless Configuration 527

Wireless LANs 527
Configuring WLAN Basic Configuration.... 529
WLAN Basic Configuration Deployment Considerations 532
Configuring WLAN Security Settings 532
802.1x EAP, EAP-PSK and EAP MAC 535
EAP, EAP-PSK and EAP MAC Deployment Considerations 536
MAC Authentication 536
PSK / None 538
Captive Portal 538
Passpoint Policy 539
MAC Registration 539
External Controller 540

TKIP-CCMP 541
WPA2-CCMP 544
WEP 64 547
WEP 128 549
Keyguard 551
Configuring WLAN Firewall Settings 553
Configuring WLAN Client Settings 564
Configuring WLAN Accounting Settings 568
Configuring WLAN Service Monitoring Settings 570
Configuring WLAN Client Load Balancing Settings 572
Configuring WLAN Advanced Settings 574
Configuring Auto Shutdown Settings 579
WLAN QoS Policy 581
Configuring QoS WMM Settings 584
Configuring a WLAN's QoS Rate Limit Settings 588
Configuring Multimedia Optimizations 593
WLAN QoS Deployment Considerations 595
Radio QoS Policy 596
Configuring a Radio's QoS Policy 597
Association ACL 607
Association ACL Deployment Considerations 609
SMART RF 610
Smart RF Configuration and Deployment Considerations 621
MeshConnex Policy 622
Mesh QoS Policy 629
Passpoint Policy 637
Sensor Policy 646

Chapter 7: Network Configuration 651

Policy Based Routing (PBR) 651
L2TP V3 Configuration 657
Crypto CMP Policy 660
AAA Policy 663
AAA TACACS Policy 676
Alias 683
Network Basic Alias 684
Network Group Alias 687
Network Service Alias 689
URL Filtering 692
Web Filtering 695
IPv6 Router Advertisement Policy 697
Application Policy 700
Application 704
Schedule Policy 706
Network Deployment Considerations 708

Chapter 8: Security Configuration 709

Wireless Firewall 709
Defining a Firewall Configuration 710
Configuring IP Firewall Rules 724
Setting an IPv4 or IPv6 Firewall Policy 725
Setting an IP SNMP ACL Policy 729
Setting a Network Group Alias 731
Setting a Network Service Alias 733
Device Fingerprinting 735
Configuring MAC Firewall Rules 743
Wireless IPS (WIPS) 745
Device Categorization 755
Security Deployment Considerations 757

Chapter 9: Services Configuration 759

Configuring Captive Portal Policies 759
Configuring a Captive Portal Policy 759
Setting the DNS Whitelist Configuration 773
Setting the DHCP Server Configuration 774
Defining DHCP Pools 776
Defining DHCP Server Global Settings 786
DHCP Class Policy Configuration 788
DHCP Deployment Considerations 789
Setting the Bonjour Gateway Configuration 790
Configuring the Bonjour Discovery Policy 790
Configuring the Bonjour Forwarding Policy 792
Setting the DHCPv6 Server Policy 794
Defining DHCPv6 Options 796
DHCPv6 Pool Configuration 798
Setting the RADIUS Configuration 800
Creating RADIUS Groups 801
Creating RADIUS Groups 803
Defining User Pools 806
Configuring the RADIUS Server 811
Setting the URL List 822
Services Deployment Considerations 824

Chapter 10: Management Access 825

Creating Administrators and Roles 825
Setting the Access Control Configuration 828
Setting the Authentication Configuration 832
Setting the SNMP Configuration 834
SNMP Trap Configuration 836
Management Access Deployment Considerations 838

Chapter 11: Diagnostics 839

Fault Management 839
Crash Files 844
Advanced 845
UI Debugging 846
View UI Logs 847
View Sessions 848

Chapter 12: Operations 851

Devices 851
Managing Firmware and Configuration Files 852
Managing Running Configuration 853
Managing Startup Configuration 856
Rebooting the Device 858
Managing Crypto CMP Certificates 860
Upgrading Device Firmware 861
Troubleshooting the Device 864
Managing Crash Dump Files 864
Copy Crash Info 866
Copy Tech Support Dump 868
Locating a Device 870
Debugging Wireless Clients 872
Debug Captive Portal Clients 874
Packet Capture 876
Viewing Device Summary Information 879
Adopted Device Upgrades 881
File Management 889
Adopted Device Restart 895
Captive Portal Pages 897
Managing Crypto CMP Certificates 902
Re-elect Controller 903
Certificates 904
Certificate Management 905
RSA Key Management 910
Certificate Creation 916
Generating a Certificate Signing Request (CSR) 918
Smart RF 921
Managing Smart RF for a RF Domain 922
Operations Deployment Considerations 925

Chapter 13: Statistics 927

System Statistics 927
Health 927
Inventory 929
Adopted Devices 930
Pending Adoptions 932
Offline Devices 933
Device Upgrade 934
WIPS Summary 936

RF Domain Statistics 938
Health 939
Inventory 941
Devices 943
AP Detection 944
Wireless Clients 946
Device Upgrade 948
Wireless LANs 949
Radios 950
Status 951
RF Statistics 952
Traffic Statistics 953
Bluetooth 955
Mesh 957
Mesh Point 958
SMART RF 973
WIPS 978
WIPS Client Blacklist 978
WIPS Events 979
Captive Portal 980
Coverage Hole Detection 982
Coverage Hole Summary 982
Coverage Hole Detail 983
Access Point Statistics 985
Health 986
Device 988
Web-Filtering 992
Device Upgrade 994
Adoption 995
Adopted APs 996
AP Adoption History 997
AP Self Adoption History 997
Pending Adoptions 998
AP Detection 999
Guest User 1001
Wireless Clients 1002
Wireless LANs 1004
Policy Based Routing 1005
Radios 1006
Status 1007
RF Statistics 1008
Traffic Statistics 1010
Mesh 1011
Interfaces 1012
General Interface Details 1013
IPv6 Address 1016
Multicast Groups Joined 1020
Network Graph 1021
RTLS 1022
PPPoE 1024
Bluetooth 1025
OSPF 1027
OSPF Summary 1027
OSPF Neighbors 1029
OSPF Area Details 1031

OSPF Route Statistics 1032
OSPF Interface 1035
OSPF State 1036
L2TPv3 Tunnels 1038
VRRP 1040
Critical Resources 1041
LDAP Agent Status 1042
Mint Links 1044
Guest Users 1046
GRE Tunnels 1047
Dot1x 1048
Network 1050
ARP Entries 1051
Route Entries 1052
Default Routes 1054
Bridge 1056
IGMP 1057
MLD 1059
Traffic Shaping 1061
DHCP Options 1063
Cisco Discovery Protocol 1064
Link Layer Discovery Protocol 1065
IPv6 Neighbor 1066
MSTP 1068
DHCPv6 Relay & Client 1069
DHCP Server 1071
DHCP Server General Information 1071
DHCP Server Bindings 1073
DHCP Server Networks 1074
Firewall 1075
Packet Flows 1075
Denial of Service 1076
IP Firewall Rules 1077
IPv6 Firewall Rules 1078
MAC Firewall Rules 1080
NAT Translations 1081
DHCP Snooping 1082
IPv6 Neighbor Snooping 1084
VPN 1085
IKESA 1086
IPSec 1087
Certificates 1088
Trustpoints 1088
RSA Keys 1090
WIPS 1091
WIPS Client Blacklist 1092
WIPS Events 1092
Sensor Servers 1093
Bonjour Services 1094
Captive Portal 1095
Network Time 1097
NTP Status 1097
NTP Association 1098
Load Balancing 1100
Environmental Sensors (AP8132 Models Only) 1101
Wireless Client Statistics 1106

Health 1106
Details 1109
Traffic 1112
WMM TSPEC 1114
Association History 1116
Graph 1117

Chapter 14: WiNG Events 1119

Event History Messages 1119

Appendix A: Publicly Available Software 1

General Information 1
Open Source Software Used 1
OSS Licenses 12
Apache License, Version 2.0 12
The BSD License 14
GNU General Public License, version 2 23
GNU Lesser General Public License 2.1 29
CCO 1.0 Universal 36
GNU Lesser General Public License, version 3.0 48
GNU General Public License 2.0 51
GNU Lesser General Public License, version 2.0 58
GNU Lesser General Public License, version 2.1 65
MIT License 72
Mozilla Public License, version 2 72
The Open LDAP Public License 77

About this guide

This manual supports the following access points:

- Access Points – AP650, AP6521, AP6522, AP6522M, AP6532, AP6562, AP7161, AP7181, AP7502, AP7522, AP7532, AP7562, AP8122, AP8132, AP8163, AP8232, AP8432, and AP8533.



NOTE

In this guide:

- AP6521, AP6522, AP6522M, AP6532 and AP6562 are collectively represented as AP65XX.
- AP7161 and AP7181 are collectively represented as AP71XX.
- AP7502, AP7522, AP7532 and AP7562 are collectively represented as AP75XX.
- AP8122, AP8132 and AP8163 are collectively represented as AP81XX.

This section is organized into the following:

- "Document Convention"
- "Notational Conventions"
- "End-User Software License Agreement"

Document Convention

The following conventions are used in this document to draw your attention to important information:



NOTE

Indicates tips or special requirements.



CAUTION

Indicates conditions that can cause equipment damage or data loss.



WARNING

Indicates a condition or procedure that could result in personal injury or equipment damage.



SWITCH NOTE

Indicates caveats unique to a RFS4000/RFS6000/RFS7000/NX4500/NX4524/NX6500/NX6524/NX7500/NX7510/NX7520/NX7530/NX9000/NX9500/NX9510/NX9600/VX9000 model controllers or service platforms.

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

End-User Software License Agreement

This document is an agreement (“Agreement”) between You, the end user, and Extreme Networks, Inc., on behalf of itself and its Affiliates (“Extreme”) that sets forth your rights and obligations with respect to the “Licensed Materials”. BY INSTALLING SOFTWARE AND/OR THE LICENSE KEY FOR THE SOFTWARE (“License Key”) (collectively, “Licensed Software”), IF APPLICABLE, COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE AND/OR ANY OF THE LICENSED MATERIALS UNDER THIS AGREEMENT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE(S) AND THE LIMITATION(S) OF WARRANTY AND DISCLAIMER(S)/LIMITATION(S) OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY (IF APPLICABLE) TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND/OR LICENSED MATERIALS AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT TO ARRANGE FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1 DEFINITIONS. “Affiliates” means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. “Server Application” means the software application associated to software authorized for installation (per License Key, if applicable) on one or more of Your servers as further defined in the Ordering Documentation. “Client Application” shall refer to the application to access the Server Application. “Network Device” for purposes of this Agreement shall mean a physical computer device, appliance, appliance component, controller, wireless access point, or virtual appliance as further described within the applicable product documentation, which includes the Order Documentation. “Licensed Materials” means the Licensed Software (including the Server Application and Client

Application), Network Device (if applicable), Firmware, media embodying software, and the accompanying documentation. “Concurrent User” shall refer to any of Your individual employees who You provide access to the Server Application at any one time. “Firmware” refers to any software program or code embedded in chips or other media. “Standalone” software is software licensed for use independent of any hardware purchase as identified in the Ordering Documentation. “Licensed Software” collectively refers to the software, including Standalone software, Firmware, Server Application, Client Application or other application licensed with conditional use parameters as defined in the Ordering Documentation. “Ordering Documentation” shall mean the applicable price quotation, corresponding purchase order, relevant invoice, order acknowledgment, and accompanying documentation or specifications for the products and services purchased, acquired or licensed hereunder from Extreme either directly or indirectly.

2 TERM. This Agreement is effective from the date on which You accept the terms and conditions of this Agreement via click-through, commence using the products and services or upon delivery of the License Key if applicable, and shall be effective until terminated. In the case of Licensed Materials offered on a subscription basis, the term of “licensed use” shall be as defined within Your Ordering Documentation.

3 GRANT OF LICENSE. Extreme will grant You a non-transferable, non-sublicensable, non-exclusive license to use the Licensed Materials and the accompanying documentation for Your own business purposes subject to the terms and conditions of this Agreement, applicable licensing restrictions, and any term, user server networking device, field of use, or other restrictions as set forth in Your Ordering Documentation. If the Licensed Materials are being licensed on a subscription and/or capacity basis, the applicable term and/or capacity limit of the license shall be specified in Your Ordering Documentation. You may install and use the Licensed Materials as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4 LICENSE TYPES.

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

- *Subscription*. Licensed Materials, and inclusive Software, Network Device or related appliance updates and maintenance services, licensed to You for use during a subscription period as defined in Your applicable Ordering Documentation.
- *Capacity*. Under the terms of this license, the license granted to You by Extreme authorizes You to use the Licensed Materials up to the amount of capacity or usage as defined in the Ordering Documentation.

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

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

7 TITLE AND PROPRIETARY RIGHTS.

a The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

b You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

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

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

9 MAINTENANCE AND UPDATES. Except as otherwise defined below, updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide updates, modifications, or enhancements, or maintenance and support services for the Licensed Materials to You. If you have purchased Licensed Materials on a subscription basis then the applicable service terms for Your Licensed Materials are as provided in Your Ordering Documentation. Extreme will perform the maintenance and updates in a timely and professional manner, during the Term of Your subscription, using qualified and experienced personnel. You will cooperate in good faith with Extreme in the performance of the support services including, but not limited to, providing Extreme with: (a) access to the Extreme Licensed Materials (and related systems); and (b) reasonably requested assistance and information. Further information about the applicable maintenance and updates terms can be found on Extreme's website at http://www.extremenetworks.com/company/legal/terms-of-support

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

it may have under law, terminate the License and any other agreements between Extreme and You.

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

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

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

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

13 LIMITED WARRANTY AND LIMITATION OF LIABILITY. Extreme warrants to You that (a) the initially-shipped version of the Licensed Materials will materially conform to the Documentation; and (b) the media on which the Licensed Software is recorded will be free from material defects for a period of ninety (90) days from the date of delivery to You or such other minimum period required under applicable law. Extreme does not warrant that Your use of the Licensed Materials will be error-free or uninterrupted.

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

EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

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

14 JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15 FREE AND OPEN SOURCE SOFTWARE. Portions of the Software (Open Source Software) provided to you may be subject to a license that permits you to modify these portions and redistribute the modifications (an Open Source License). Your use, modification and redistribution of the Open Source Software are governed by the terms and conditions of the applicable Open Source License. More details regarding the Open Source Software and the applicable Open Source Licenses are available at www.extremenetworks.com/services/SoftwareLicensing.aspx. Some of the Open Source software may be subject to the GNU General Public License v.x (GPL) or the Lesser General Public Library (LGPL), copies of which are provided with the Licensed Materials and are further available for review at www.extremenetworks.com/services/SoftwareLicensing.aspx, or upon request as directed herein. In accordance with the terms of the GPL and LGPL, you may request a copy of the relevant source code. See the Software Licensing web site for additional details. This offer is valid for up to three years from the date of original download of the software.

16 GENERAL.

a This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

b This Agreement may not be changed or amended except in writing signed by both parties hereto.

c You represent that You have full right and/or authorization to enter into this Agreement.

d This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme' assignees, licensors, and licensees.

e Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

f The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

g Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.6480 Via Del Oro

San Jose, California 95119

USA

ATTN: Legal Department

1 Overview

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

AP7522, AP7532, AP7562, AP8432, and AP8533 access points can now use WiNG software as its onboard operating system. The unique WiNG software enables the access point to function as a Standalone “thick” access point, or a Virtual Controller AP capable of adopting and managing up to 64 access points of the same model.

AP71XX, AP7502, AP81XX and AP82XX access points can now use WiNG software as its onboard operating system. The unique WiNG software enables the access point to function as a Standalone “thick” access point, or a Virtual Controller AP capable of adopting and managing up to 24 access points of the same model.



NOTE

AP6521, AP6522, AP6532, AP6562 are not currently equipped to adopt to managing up to 64 access points of the same model. Only access points on WAVE-1 and WAVE-2 platforms can adopt and manage 64 APs.

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

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



NOTE

The recommended way to administer a network populated by numerous access points is to configure them directly from the Virtual Controller AP. If a single access point configuration requires an update from the Virtual Controller AP’s assigned profile configuration, the administrator should apply a Device Override to change just that access point’s configuration. For more information on applying an override to an access point’s Virtual Controller AP assigned configuration and profile, see “Device Overrides” on page 319.

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

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



NOTE

This guide describes the installation and use of the WiNG software designed specifically for AP6521, AP6522, AP6532, AP6562, AP8432, AP8533, AP71XX, AP7502, AP7522, AP7532, AP81XX and AP82XX access points. It does not describe the version of the WiNG software designed for use with the RFS4000, RFS6000, RFS7000, NX4500, NX4524, NX6500, NX6524, NX7500, NX7510,NX7520, NX7530, NX9000, NX9500 and NX9510. For information on using WiNG in a controller managed network, go to *www.extremenetworks.com/support*.

About the WiNG Software

Extreme Networks' WiNG 5 operating system is the next generation in the evolution of WLAN architectures. WiNG 5 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 point or adaptive access point 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.

The power of 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 point, 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 — period — ensuring compliance with PCI, HIPAA and other government and industry security regulations.

Connectivity for the largest 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.

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. Access points 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 access points lose communication with the controller, they continue to function, able to bridge traffic while still enforcing QoS and security policies, including stateful inspection of Layer2 (locally bridged) or Layer 3 traffic.

Gap Free Security

When it comes to wireless security, one size does not fit all. A variety of solutions are required to meet the varying needs and demands of different types of organizations. Regardless of the size of your WLAN or your security requirements, our tiered approach to security allows you to deploy the features you need to achieve the right level of security for your networks and your data. And where a hub-and-spoke architecture can't stop threats until they reach the controller inside your network, WiNG 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 can provide coverage to enterprise workers in vast campus-style environments as well as public safety personnel in patrol cars.

Network Services, Routing and Switching

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.

2 Web User Interface Features

The access point's on board user interface contains a set of features specifically designed to enable either Virtual Controller AP, Standalone AP or Adopt to Controller functionality. In Virtual Controller AP mode, an access point can manage up to 64 other access points of the same model and share data amongst managed access points. In Standalone mode, an access point functions as an autonomous, non adopted, access point servicing wireless clients. If adopted to controller, an access point is reliant on its connected controller for its configuration and management.

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

- "Accessing the Web UI"
- "Glossary of Icons Used"

Accessing the Web UI

"Web User Interface Features"

The access point uses a *Graphical User Interface* (GUI) which 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. The Web UI is based on Flex, and does not use Java as the underlying UI framework. It is recommended to use a resolution of 1280 x 1024 pixels when using the GUI.

The following browsers have been validated with the Web UI:

- Firefox 3.0 or higher
- Internet Explorer 7 or higher
- Google Chrome 2.0 or higher
- Safari 3 and higher
- Opera 9.5 and higher

Connecting to the Web UI

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

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

NOTE

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

For example:

MAC address - 00:C0:23:00:F0:0A
Zero-config IP address - 169.254.240.10

3 To derive the access point's IP address using its MAC address:

4 Open the Windows calculator be selecting **Start** > **All Programs** > **Accessories** > **Calculator**. This menu path may vary slightly depending on your version of Windows.

5 With the Calculator displayed, select **View** > **Scientific**. Select the **Hex** radio button.

6 Enter a hex byte of the access point's MAC address. For example, *F0*.

7 Select the **Dec** radio button. The calculator converts *F0* into *240*. Repeat this process for the last access point MAC address octet.

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

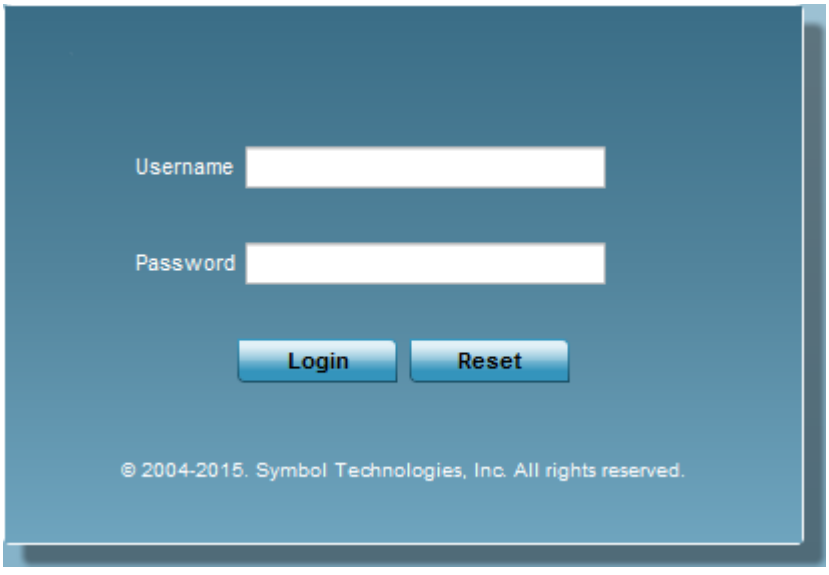


Figure 1: Access Point Web UI Login screen

1 Enter the default username *admin* in the **Username** field.

2 Enter the default password *admin123* in the **Password** field.

3 Select the **Login** button to load the management interface.

If this is the first time the management interface has been accessed, the first screen to display will prompt for a change of the default access point password. Then, a dialogue displays to start the initial setup wizard. For more information on using the initial setup wizard see "Using the Initial Setup Wizard" on page 25.

Glossary of Icons Used

"Web User Interface Features"

The access point interface utilizes a number of icons designed to interact with the system, gather information from managed devices and obtain status. This chapter is a compendium of the icons used, and 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

"Glossary of Icons Used"

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-hand corner of the UI.
	*Add* – Select this icon to add a row in a table. When this icon is selected, a new row is created in the table, or a dialog box opens where you can enter values for that particular list.
	Delete – Select this icon to remove a row from a table. When this icon is clicked, the selected row is immediately 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 this icon is clicked, the selected 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 device configurations, and device profiles.
	*Edit policy* – Select this icon to edit an existing configuration item or policy. To edit a policy, select the policy and this icon.

Dialog Box Icons

"Glossary of Icons Used"

These icons indicate the current state of various controls in a dialog. These icons enables you to gather, at a glance, 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's profile configuration.
	*Mandatory Field* – Indicates the control's value is a mandatory configuration item. You will not be allowed to proceed further without providing all mandatory values in the dialog or the screen.
	*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

"Glossary of Icons Used"

The following two override icons are status indicators for transactions that need to be committed.

	*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 will not be implemented until saved. This icon represents a change from this device's profile assigned configuration.

Status Icons

"Glossary of Icons Used"

These icons define device status, operations on the wireless controller, or any other action that requires a status being 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 some errors were detected that did not stop 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 may just be a message from the system.

Configurable Objects

"Glossary of Icons Used"

These icons define configurable items within the UI.

	*Device Configuration* – Represents a configuration file applicable to a device category.
	*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.
	*Wireless LANs* – States an action impacting a WLAN has occurred.
	*WLAN QoS Policy* – States a *Quality of Service* (QoS) policy configuration has been impacted.
	*Radio QoS Policy* – Indicates a QoS policy 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 Association *Access Control List* (ACL) configuration has been impacted. An ACL is a set of configuration parameters used to set access to managed resources. The association ACL configures the parameters for controlling device associations.
	*Smart RF Policy* – States a Smart RF policy has been impacted. Smart RF enables neighboring APs to take over for an AP that suddenly becomes unavailable. This is accomplished by increasing the power of radios on nearby APs to cover the hole created by the non-functioning AP.
	*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. RF Domain implement location based security restrictions applicable to all VLANs in a particular physical location.
	*Firewall Policy* – Indicates a Firewall policy has been impacted. Firewalls provide a barrier that prevent unauthorized access to secure resources while allowing authorized access to external and internal resources.
	*IP Firewall Rules* – Indicates an IP Firewall rule has been applied. An IP based firewall rule implements firewall restrictions based on the IP address in a received packet.
	*MAC Firewall Rules* – States a MAC based Firewall Rule has been applied. A MAC based firewall rule implements firewall restrictions based on the MAC address in a received 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 APs and wireless clients.

	*Device Categorization* – Indicates a device categorization policy is being applied. This is used by the intrusion prevention system to categorize APs or wireless clients as either neighbors or sanctioned devices. This enables these devices to bypass the intrusion prevention system.
	*Captive Portal* – 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 captive portal services to 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 these IP addresses.
	*RADIUS Group* – Indicates the configuration of RADIUS Group is being 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 is being 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 is being applied. RADIUS server policy is a set of configuration attributes used when a RADIUS server is configured for AAA.
	*Smart Caching Policy* – Smart Caching enables NX4500 and NX6500 series service platforms to temporarily store frequently accessed Web content on network infrastructure devices.
	*Management Policy* – Indicates a management policy is being applied. Management policies are used to configure access control, authentication, traps and administrator permissions.
	*MeshConnex Policy* – Indicates a mesh connex policy is being applied. MeshConnex is a hybrid proactive/on-demand path selection protocol to form efficient mesh paths.
	*Mesh QoS Policy* – Indicates a mesh quality of service policy is being applied. This policy ensures that each mesh point in the network receives a fair share of overall bandwidth for its use.
	*Virtual Controller APs* – Indicates an AP is configured as a Virtual Controller access point. A Virtual Controller access point can manage up to 64 access points of similar type deployed in a network.

Configuration Objects

"Glossary of Icons Used"

Configuration icons are used to define the following:

	*Configuration* – Indicates an item capable of being configured by the access point's interface.
	*View Events / Event History* – Defines a list of events. Select 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 the status of all the processes and memory when a process fails.
	*Panic Snapshots* – Indicates a panic snapshot has been generated. A panic snapshot is a file that records the status of all the processes and memory when a failure occurs.
	*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 user interface, FLEX and the error logs.

Configuration Operation Icons

"Glossary of Icons Used"

The following icons are used to define configuration operations:

	*Revert* – When selected, any unsaved changes are reverted back to their last saved configuration.
	*Commit* – When selected, all changes made to the configuration are written to the access point. Once committed, changes cannot be reverted.
	*Commit and Save* – When selected, changes are saved to the access point's configuration.

Access Type Icons

"Glossary of Icons Used"

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 access point using TELNET.
	*SSH* – Indicates a SSH access permission. A user with this permission is permitted to access an access point using SSH.
	*Console* – Indicates a console access permission. A user with this permission is permitted to access the access point using the device's serial console.

Administrative Role Icons

"Glossary of Icons Used"

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 access point to which they are connected.
	*System* – Indicates system user privileges. A system user is allowed to configure some general settings like boot parameters, licenses, auto install, image upgrades etc.

	*Network* – Indicates network user privileges. A network user is allowed to configure all wired and wireless parameters, like IP configuration, VLANs, L2/L3 security, WLANs, radios etc.
	*Security* – Indicates security user privileges. A security level user is allowed to configure all security related parameters.
	*Monitor* – Indicates a monitor role. This role provides no configuration privileges. A user with this role can view all system configuration but cannot modify them.
	*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 and reboot an access point.
	*Web User* – Indicates a Web user privilege. A Web user is allowed accessing the access point's Web user interface.

Device Icons

- "Glossary of Icons Used"

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

	*System* – This icon indicates the entire WiNG supported system and all of its members including wireless controller, service platforms, and access points that may be interacting at any one time.

	*Cluster* – This icon indicates a cluster. A cluster is a set of access points that work collectively to provide redundancy and load sharing amongst its members.
	*Service Platform* – This icon indicates an NX45xx, NX65xx or NX9000 series service platform that's part of the managed network
	*RF Domain* - This icon indicates a RF Domain. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, a building or a site. Each RF Domain also contains policies that can determine a Smart RF or WIPS configuration.
	*Access Point* – This icon indicates any access point that is a part of the network.
	*Wireless Client* – This icon indicates any wireless client connected within the access point managed network.

3 Quick Start

Access points can utilize an initial setup wizard to streamline the process of initially accessing the wireless network. The wizard defines the access point's operational mode, deployment location, basic security, network and WLAN settings. For instructions on how to use the initial setup wizard, see "Using the Initial Setup Wizard" on page 25.

Using the Initial Setup Wizard

- "Quick Start"

Once the access point is installed and powered on, complete the following steps to get the access point up and running and access management functions:

1 Point the Web browser to the access point's IP address. The following login screen displays:

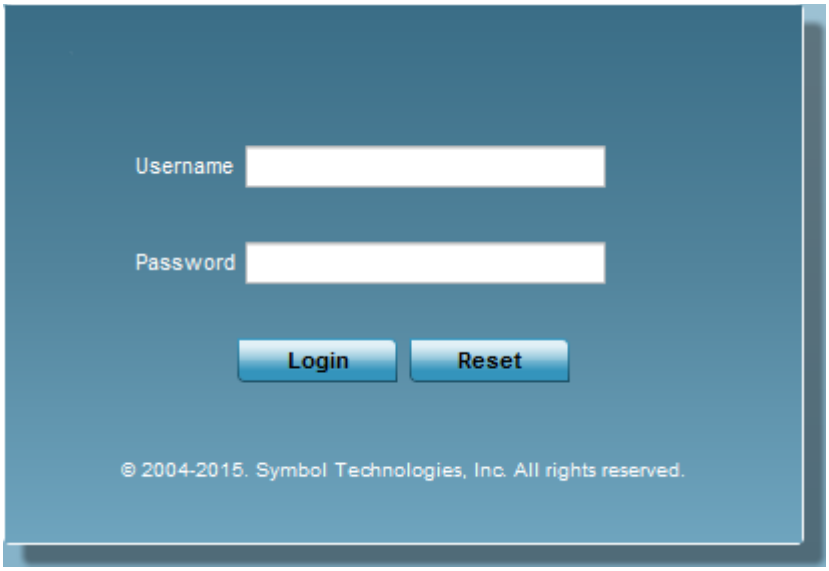


Figure 1: Web UI Login screen

2 Enter the default username *admin* in the **Username** field.

3 Enter the default password *admin123* in the **Password** field.

4 Select the **Login** button to load the management interface.

NOTE

When logging in for the first time, you are prompted to change the password to enhance device security in subsequent logins.

NOTE

If you get disconnected when running the wizard, you can connect again with the access point's actual IP address (once obtained) and resume the wizard.

5 If this is the first time the access point's management interface has been accessed, the **Initial Setup Wizard** automatically displays.

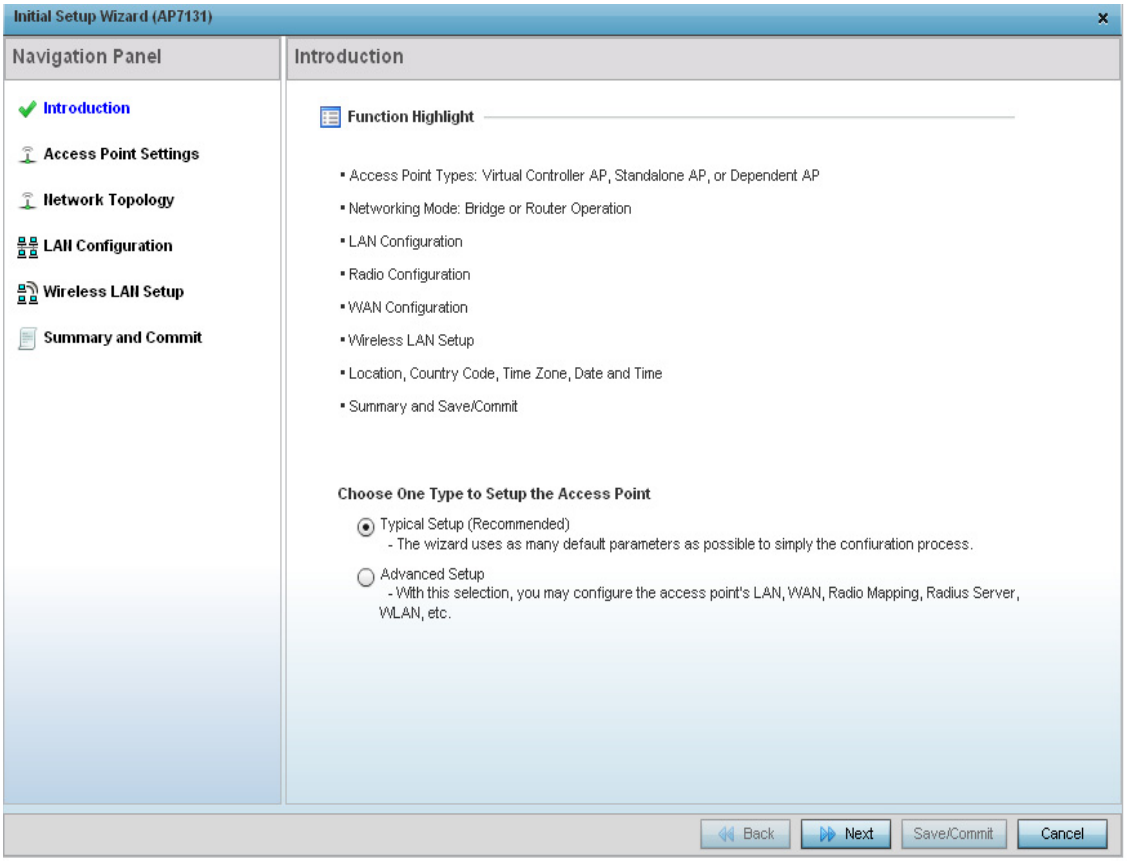


Figure 2: Initial Setup Wizard



NOTE

The Initial Setup Wizard displays the same pages and content for each access point model supported. The only difference being the number of radios configurable by model, as an AP7131 model can support up to three radios, AP6522, AP6532, AP6562, AP81XX, AP82XX, AP7502, AP7522, AP7532 and AP71XX models support two radios and AP6511 and AP6521 models support a single radio.

The **Introduction** screen displays the various actions that can be performed using the wizard under the **Function Highlight** field.

Use the **Choose One type to Setup the** access point field options to select the type of wizard to run. The **Typical Setup** is the recommended wizard. This wizard uses the default parameters for most of the configuration parameters and sets up a working network with the least amount of manual configuration.

The **Advanced Setup** wizard is for administrators who prefer more control over the different configuration parameters. A few more configuration screens are available for customization when the **Advanced Setup** wizard is used.

The first page of the *Initial Setup Wizard* displays the **Navigation Panel** and **Function Highlights** for the configuration activities comprising the access point's initial setup. This page also displays options to select the typical or advanced mode for the wizard.



Figure 3: Initial Setup Wizard - Navigation Panel - Typical Setup Wizard

A green check mark to the left of an item in the **Navigation Panel** defines the listed task as having its minimum required configuration parameters set correctly. A red X defines the task as still requiring at least one parameter be defined correctly. Figure 3 displays the navigation panel for the **Typical Setup Wizard.**

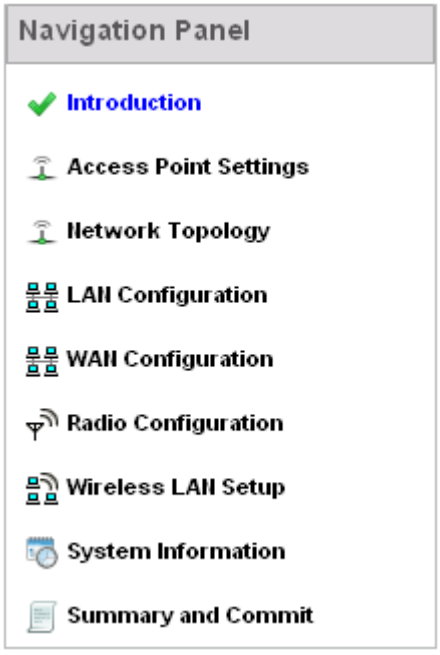


Figure 4: Initial Setup Wizard - Navigation Panel - Advanced Setup Wizard

Figure 4 displays the navigation panel for the **Advanced Setup Wizard.**

NOTE

Note the difference in the number of steps between the Typical Setup and Advanced Setup Wizards.

6 Select **Save/Commit** within each page to save the updates made to that page's configuration. Select **Next** to proceed to the next page listed in the **Navigation Panel**. Select **Back** to revert to the previous screen without saving your updates.

NOTE

While you can navigate to any page in the navigation panel, you cannot complete the *Initial Setup Wizard* until each task in the *Navigation Panel* has a green check mark.

The following sections describe the two different wizards and their parameters. The available wizards are:

- "Typical Setup Wizard"
- "Advanced Setup Wizard"

Typical Setup Wizard

- "Using the Initial Setup Wizard"

The **Typical Setup** is the recommended wizard. This wizard uses default parameters for most of the configuration parameters and creates a working network with the fewest steps.

The **Typical Setup** wizard consists of the following:

- "Network Topology Selection"
- "LAN Configuration"
- "WAN Configuration"
- "Wireless LAN Setup"
- "Summary And Commit Screen"

To configure the access point using the **Typical Setup Wizard**:

1 Select **Typical Setup** from the **Choose One type to Setup the Access Point** field.

2 Select **Next**.

The *Initial Setup Wizard* displays the *Access Point Settings* screen to define the access point's Standalone versus Virtual Controller AP functionality. This screen also enables selection of the country of operation for the access point.

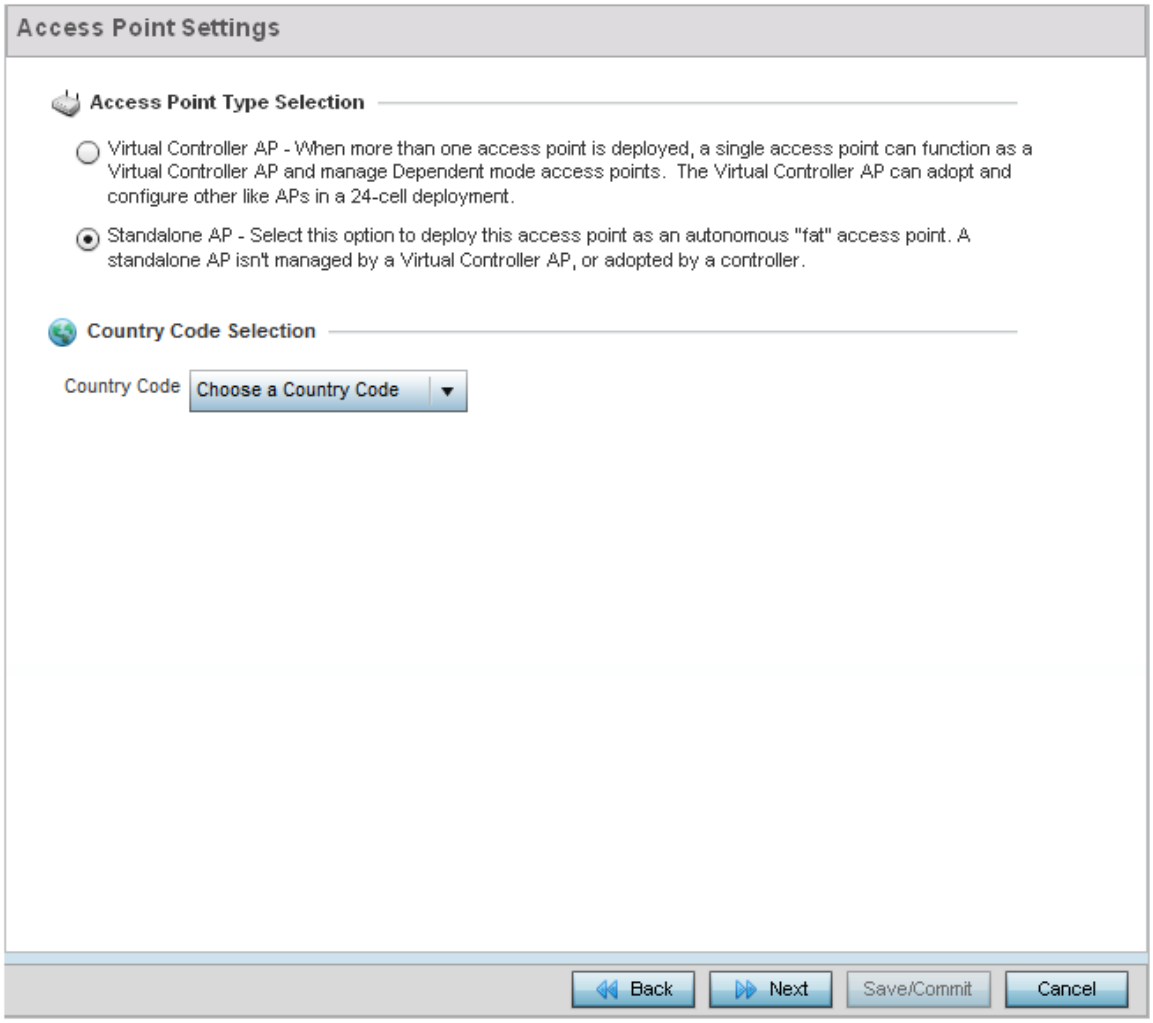


Figure 5: Initial Setup Wizard - Access Point Settings screen for Typical Setup Wizard

3 Select an **Access Point Type** from the following options:

- *Virtual Controller AP* - When more than one access points are deployed, a single access point can function as a Virtual Controller AP. Up to 64 access points can be connected to, and managed by a single Virtual Controller AP. These connected access points must be the same model as the Virtual Controller AP. For more information, see "Virtual Controller AP Mode" on page 30.
- *Standalone AP* - Select this option to deploy this access point as an autonomous access point. A standalone AP is not managed by a Virtual Controller AP, or adopted

by a RFS series wireless controller. For more information, see “Standalone Mode” on page 31.



NOTE

If designating the access point as a Standalone AP, it is recommended that the access point’s UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

- *Adopted to Controller* - Select this option when deploying the access point as a controller managed (Dependent mode) access point. Selecting this option closes the Initial AP Setup Wizard. An adopted access point obtains its configuration from a profile stored on its managing controller. Any manual configuration changes are overwritten by the controller upon reboot. For more information on configuring the access point in the *Adopted to Controller* mode, see “Adopt to a controller” on page 54.



NOTE

The option Adopted to Controller is only available for the *Advanced Setup Wizard*.

4 Select the **Country Code** where the access point is deployed. Selecting a proper country of operation is a very critical task while configuring the access point as it defines the correct channels of operations and ensures compliance to the regulations for the selected country. This field is only available for the *Typical Setup Wizard*.

5 Select the **Next** button to start configuring the access point in the selected mode.

Virtual Controller AP Mode

“Using the Initial Setup Wizard”

When more than one access point is deployed, a single access point can function as a Virtual Controller AP. Up to 64 access points can be connected to, and managed by a single Virtual Controller AP of the same access point model. These connected access points must be of the same model as the Virtual Controller AP.

To designate an access point as a Virtual Controller AP:

1 From the **Access Point Settings** screen, select **Virtual Controller AP**.

2 Select **Next.**

The remainder of a Virtual Controller AP configuration is the same as a Standalone access point.

Standalone Mode

"Using the Initial Setup Wizard"

In the *Standalone* mode, the access point is not adopted to a wireless controller. Select this option to deploy this access point as an autonomous fat access point.



CAUTION

This is caution text.If designating the access point as a Standalone AP, it is recommended that the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

To configure the access point to work in the *Standalone* mode:

1 From the **Access Point Settings** screen, select **Standalone AP**.

2 Select **Next**.

The remainder of a Standalone AP configuration is the same as a Virtual Controller access point.

Network Topology Selection

"Typical Setup Wizard"

Use the *Network Topology* screen to define how the access point manages network traffic. The available modes are:

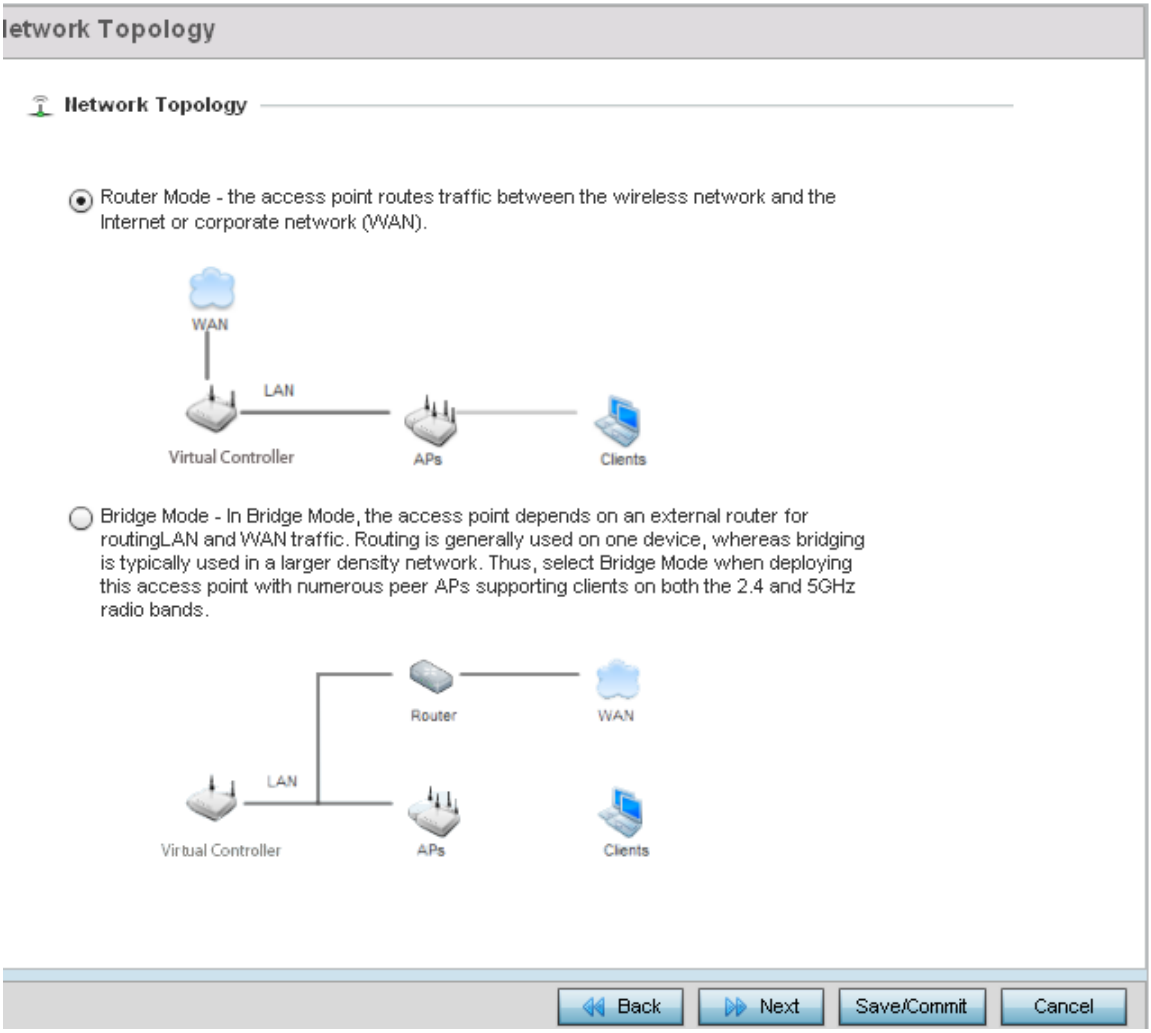


Figure 6: Initial Setup Wizard - Network Topology screen for Typical Setup Wizard

- **Router Mode** - In Router Mode, the access point routes traffic between the *local network* (LAN) and the Internet or *external network* (WAN). Router mode is recommended in a deployment supported by just a single access point.
- **Bridge Mode** - In Bridge Mode, the access point depends on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger density network. Select *Bridge Mode* when deploying this access point with numerous peer access points supporting clients on both the 2.4 GHz and 5.0 GHz radio bands.



NOTE

When *Bridge Mode* is selected, WAN configuration cannot be performed and the *Initial Setup Wizard* does not display the WAN configuration screen.

1 Select **Next**. The *Typical Setup Wizard* displays the **LAN Configuration** screen to set the access point's LAN interface configuration. For more information, see "LAN Configuration" on page 33.

LAN Configuration

"Typical Setup Wizard"

Use the *LAN Configuration* screen to set the access point's DHCP and LAN network address configuration.

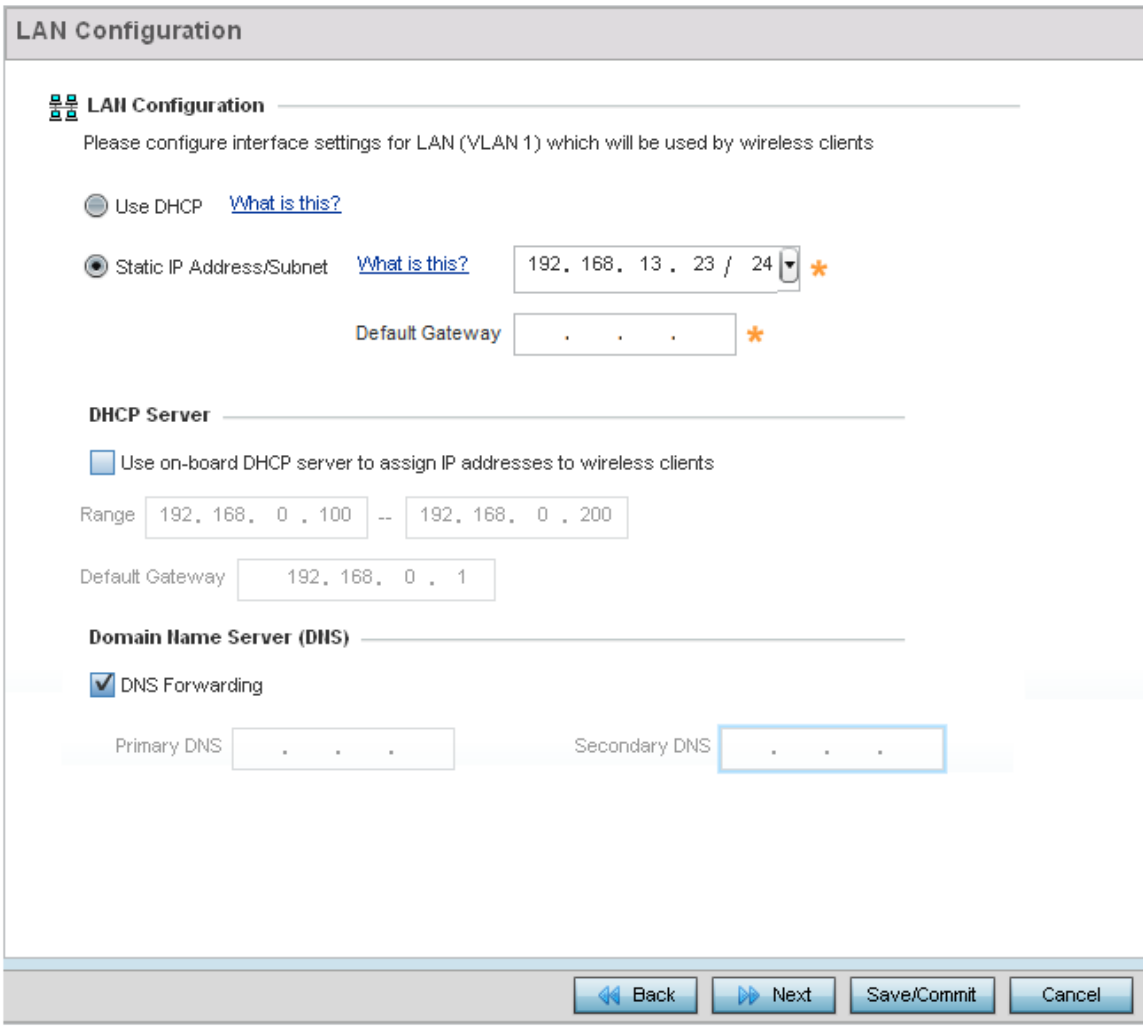


Figure 7: Initial Setup Wizard - LAN Configuration screen for Typical Setup Wizard

1 Set the following DHCP and Static IP Address/Subnet information:

- **Use DHCP** - Select this option to enable an automatic network address configuration using DHCP server.
- **Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's LAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **DHCP Server** and **Domain Name Server (DNS)** resources, as those fields will become enabled on the bottom portion of the screen.

- **Use on-board DHCP server to assign IP addresses to wireless clients** - Select the check box to enable the access point's DHCP server to provide IP and DNS information to clients on the LAN interface.
- **Range** - Enter a starting and ending IP Address range for client assignments on the access point's LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.
- **Default Gateway** - Define a default gateway address for use with the default gateway. This is a required parameter.
- **DNS Forwarding** - Select this option to allow a DNS server to translate domain names into IP addresses. If this option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.
- **Primary DNS** - Enter an IP Address for the main Domain Name Server providing DNS services for the access point's LAN interface.
- **Secondary DNS** - Enter an IP Address for the backup Domain Name Server providing DNS services for the access point's LAN interface

2 Select **Next**. The *Typical Setup Wizard* displays the *Wireless LAN Setup* screen to set the access point's Wireless LAN interface configuration. For more information see "Wireless LAN Setup" on page 36.

If *Router Mode* is selected as the **Network Topology**, the *Typical Setup Wizard* displays the WAN configuration screen. For more information, see "WAN Configuration" on page 34.

WAN Configuration

"Typical Setup Wizard"



NOTE

This option is only available when *Router Mode* is selected in the Network Topology screen.

Use the **WAN Setting** screen to define network address settings for the WAN interface. The WAN interface connects the access point to a wired local area network or backhaul.

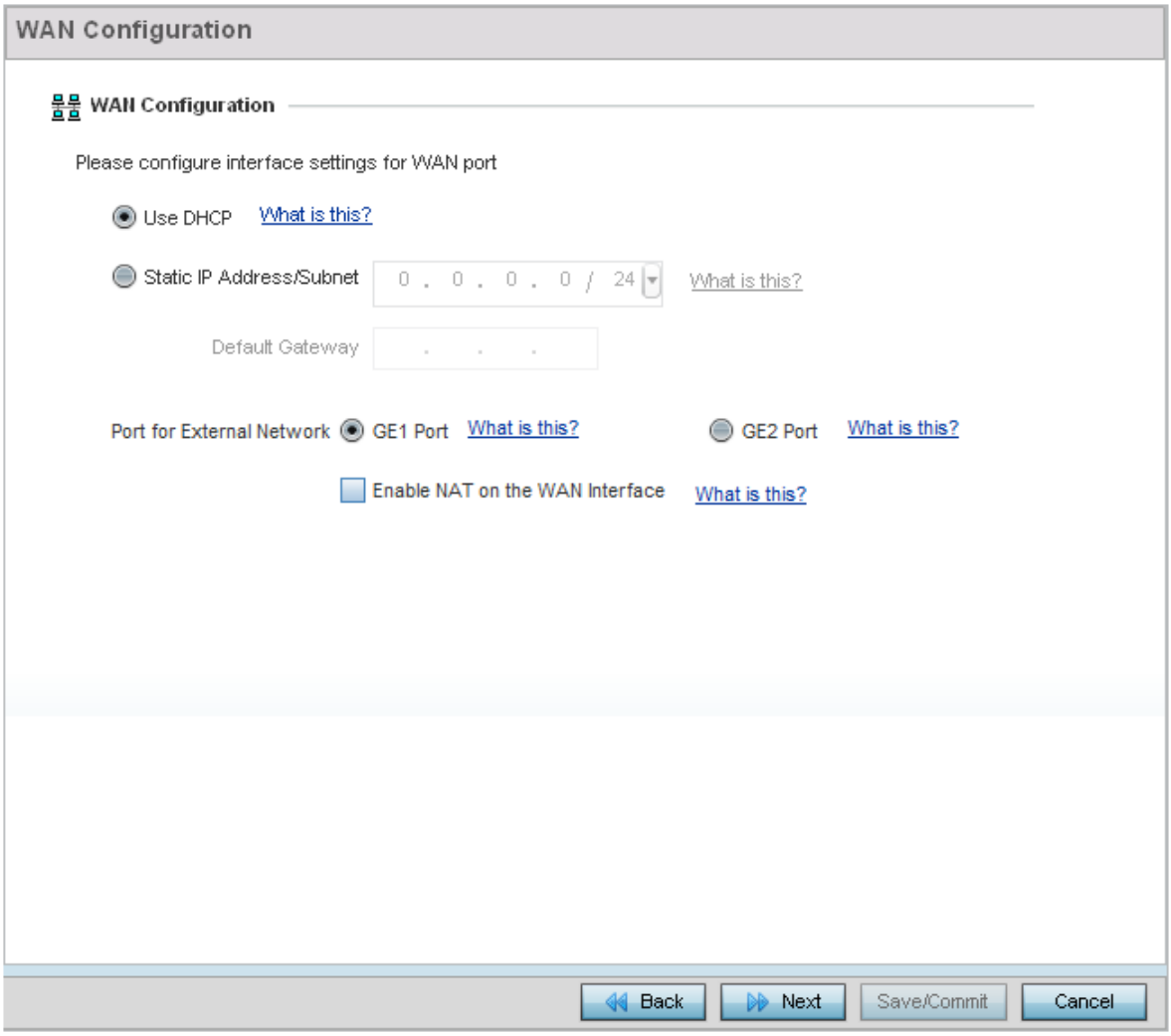


Figure 8: Initial Setup Wizard - WAN Configuration screen of the Typical Setup Wizard

1 Set the following WAN parameters:

- **Use DHCP** - Select the radio control to enable an automatic network address configuration using external DHCP servers. An automatic IP address is configured to the access point's WAN port using DHCP servers located on the WAN side of the network.
- **Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's WAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define **Default Gateway** information, as the field will become enabled on the bottom portion of the screen. The provided IP address is assigned to the WAN interface of the access point. The **Default Gateway** is a router that serves as a access to other networks.
- **Port for External Network** – Select the port connected to an external network.
- **Enable NAT on the WAN Interface** – Select this option to enable *Network Address Translation* on the selected GE interface.

2 Select **Next**. The *Typical Setup Wizard* displays the **Wireless LAN Setup** screen to set the access point's wireless LAN configuration. For more information, see "Wireless LAN Setup" on page 36.

Wireless LAN Setup

"Typical Setup Wizard"

A *Wireless Local Area Network* (WLAN) is a data-communications system and local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one 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.

Up to two (2) WLANs can be configured for the access point using the wizard.

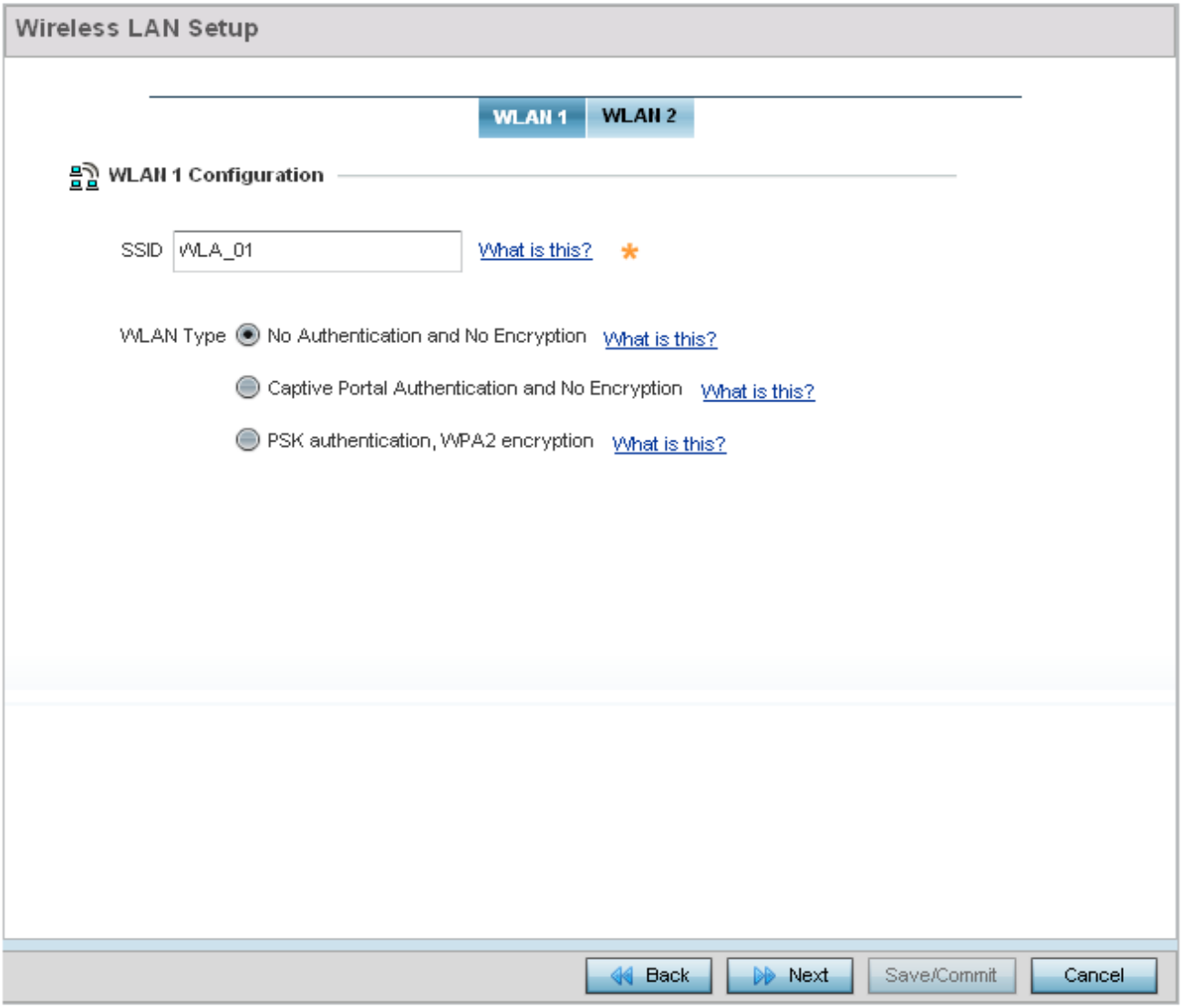


Figure 9: Initial Setup Wizard - Wireless LAN Setup screen for Typical Setup Wizard

1 Set the following WLAN1 configuration parameters:

- **SSID –** Configure the SSID for the WLAN.
- **WLAN Type** – Configure the encryption and authentication to use with this WLAN.
- **No Authentication and No Encryption** – Configures a network without any authentication. This means any device can access the network. This option also configures the network without encryption. This means any data transmitted through the network is in plain text.
- **Captive Portal Authentication and No Encryption** – Configures a network that uses a RADIUS server to authenticate users before allowing them on to the network. Once on the network, no encryption is used for the data being transmitted through the network. Select this option to use a Web page (either internally or externally hosted) to authenticate users before access is granted to the network
  - **External RADIUS Server** – When this option is selected, provide the IP address of the external RADIUS server used for user authentication. Also provide the shared secret in the **RADIUS Shared Secret** field.
  - **Onboard RADIUS Server** – When this option is selected, a new screen is displayed where additional updates can be made. For more information on configuring the onboard RADIUS server, see "RADIUS Server Configuration" on page 37.
- **PSK authentication, WPA2 encryption** – Configures a network that uses PSK authentication and WPA2 encryption. Select this option to implement a pre-shared key that must be correctly shared between the access point and requesting clients using this WLAN
  - **WPA Key** – Provide a 64 character HEX key or 8-63 character ASCII key. Use the drop-down to specify the type of key being provided. Select *ASCII* or *HEX* to specify the key type being provided in the **WPA Key** field.

2 Select **Next**. The *Typical Setup Wizard* displays the **RADIUS Server Configuration** screen if required. For more information, see "RADIUS Server Configuration" on page 37

Otherwise, the *Typical Setup Wizard* displays the **Summary and Commit** screen. For more information, see "Summary And Commit Screen" on page 39.

RADIUS Server Configuration

"Wireless LAN Setup"

Use the RADIUS Server Configuration screen to configure the users for the onboard RADIUS server. Use the screen to add, modify and remove RADIUS users.

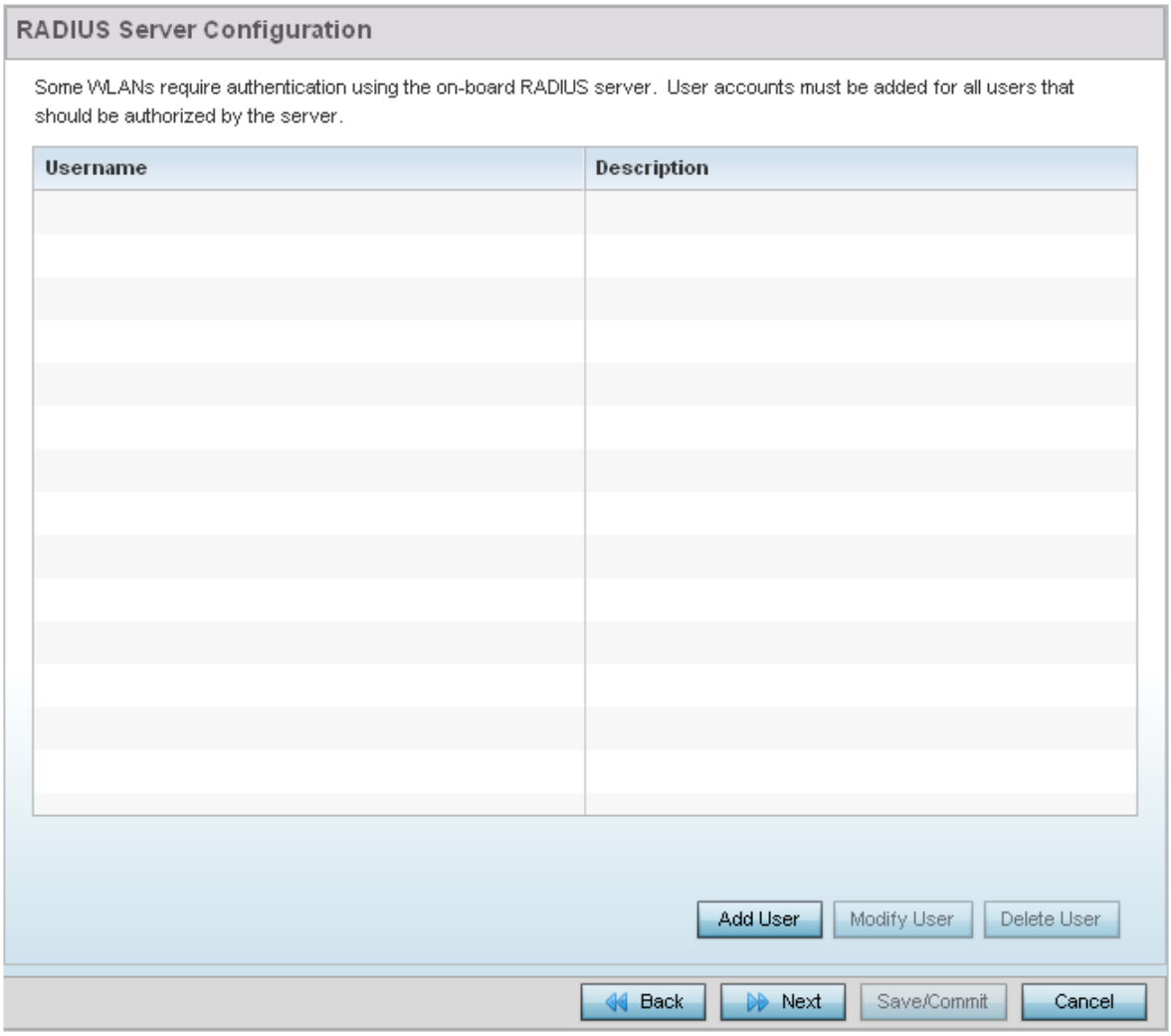


Figure 10: Initial Setup Wizard - RADIUS Server Configuration screen for Typical Setup Wizard

Use the **Add User** button to add a new RADIUS user. A dialog displays where details about the user is entered.

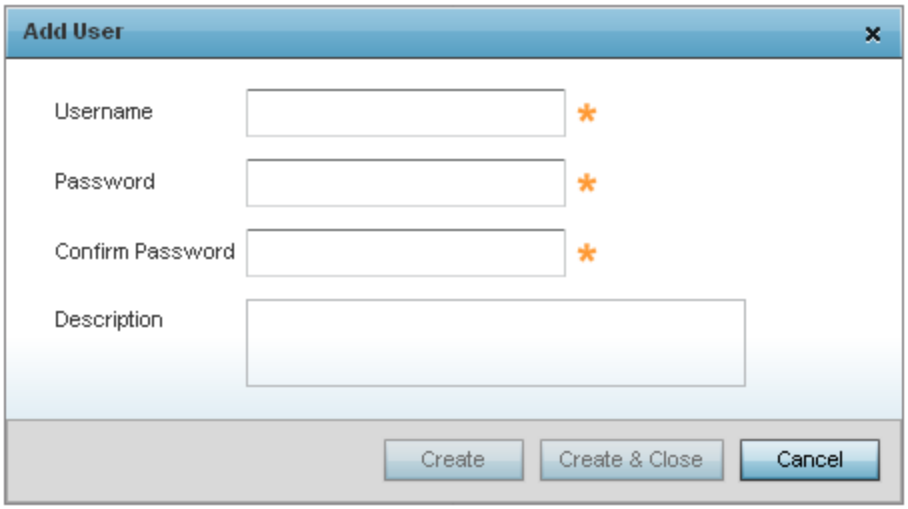


Figure 11: Initial Setup Wizard - RADIUS Server Configuration - Add User screen for Typical Setup Wizard

1 Use the **Add User** dialog to provide user information to add to the RADIUS server user database.

- **Username** – Provide a user name to authenticate the user
- **Password** – Provide a password to authenticate the user
- **Confirm Password** – Confirm the password by entering the same password entered in the **Password** field
- **Description** – Provide a description for the user created in the RADIUS server user database

2 To create the user and continue with creating another user, select **Create**. To create the user and close this dialog, click **Create & Close**. To close the dialog and abandon the operation, select **Cancel**.

Use the **Modify User** button to modify the details for an existing user in the RADIUS user database. Select the user to modify details for and then click **Modify User**. The username for the user cannot be modified using this dialog.

Use the **Delete User** button to remove the details of an existing user from the RADIUS user database. Select the user to remove and then click **Delete User**. A confirmation dialog appears. Once confirmed, the user is removed from the RADIUS user database.

3 Click **Next** The *Typical Setup Wizard* displays the **Summary and Commit** screen. For more information, see "Summary And Commit Screen" on page 39.

Summary And Commit Screen

"Typical Setup Wizard"

The *Summary And Commit* screen displays a complete overview of the configurations made in the previous screens.

There is no user intervention or additional settings required. The *Summary and Commit* screen is an additional means of validating the configuration before it is deployed.

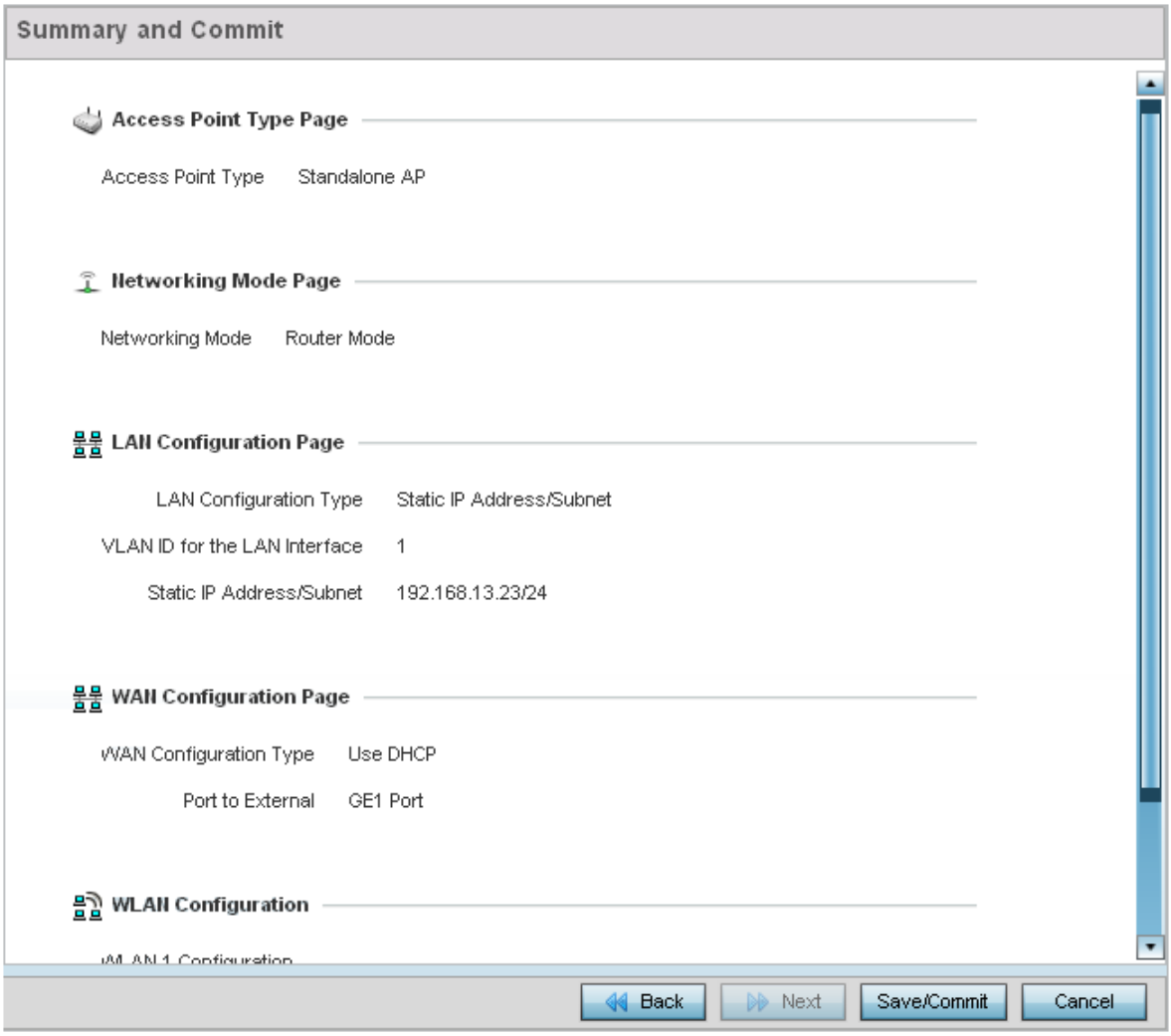


Figure 12: Initial Setup Wizard - Summary And Commit Screen of the Typical Setup Wizard

If the configuration displays as intended, select the **Save/Commit** button to implement these settings to the access point's configuration. If additional changes are warranted based on the summary, either select the target page from the **Navigation Panel**, or use the **Back** button.

Adopt to a controller

"Using the Initial Setup Wizard"

Adopted to Controller is the default behavior of the access point. When the access point is switched on for the first time, it looks for a wireless controller on the default subnet and that runs the same WiNG firmware version and automatically adopts to it. Use the *Initial Setup Wizard* to configure the preferred wireless controller that the access point must adopt to.

When *Adopted to Controller* is selected, further configuration settings are displayed in the same screen. Select the **Automatic controller discovery** option to enable the access point to be discovered and adopted using layer 2 settings.

If preferring layer 3 adoption, select the **Static Controller Configuration** option, and define the addresses of the preferred controllers. When using the static method, you will also need to define whether the access point receives an IP address using DHCP or if IP resources are provided statically. Up to two (2) controllers can be defined. The access point will try to adopt to the controller defined in the Controller 1 field first. Should the controller not be found, then the access point tries to adopt to the controller defined in Controller 2 field.

When preferring layer 3 adoption, configure how an IP will be assigned to this access point. Select **Use DHCP** to use DHCP to assign an IP address to this access point. If this access point requires a static IP to be assigned, select **Static IP Address/Subnet** and provide the appropriate IP address and net mask. For your convenience, the netmask is automatically set to 24. Also assign the **Default Gateway** to forward traffic to.

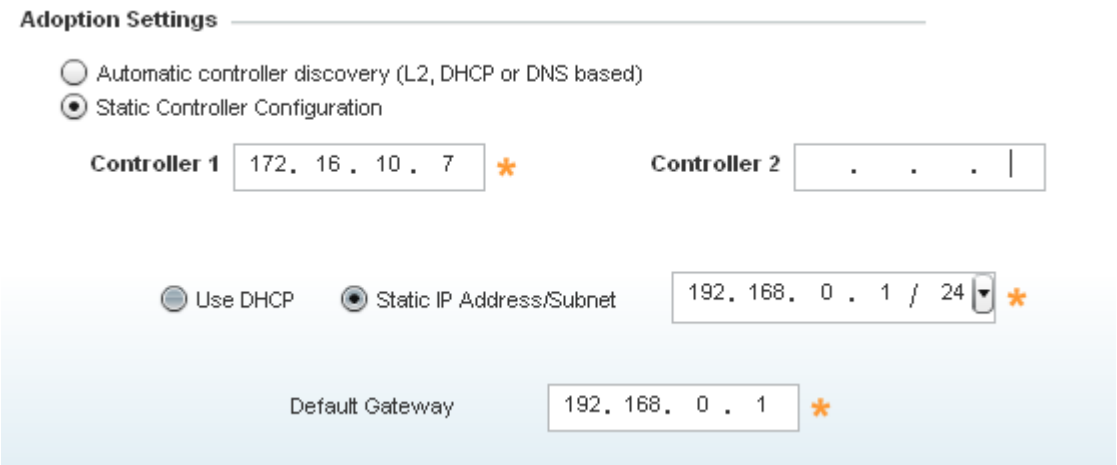


Figure 13: Initial Setup Wizard - Adoption Settings

Select the **Save/Commit** button to save the current configuration. Select the **Cancel** button to exit the **Initial Setup Wizard** without making any changes. Select the **Back** button to go back to the previous screen of the *Initial Setup Wizard*.

Advanced Setup Wizard

"Using the Initial Setup Wizard"

The **Advanced Setup** is the recommended wizard for users who want more control on how the access point is configured beyond minimum default settings. This wizard provides additional radio and system information settings.

The *Advanced Setup* wizard consists of the following:

- "Network Topology Selection"
- "LAN Configuration"
- "WAN Configuration"
- "Radio Configuration"

- "Wireless LAN Setup"
- "System Information"
- "Summary And Commit Screen"

To configure the access point using the *Advanced Setup Wizard*:

1 Select **Advanced Setup** from the **Choose One type to Setup the Access Point** field.

2 Select **Next**.

The *Advanced Setup Wizard* displays the **Access Point Settings** screen to define the access point's Standalone versus Virtual Controller AP versus functionality. This screen also enables selection of the country of operation.

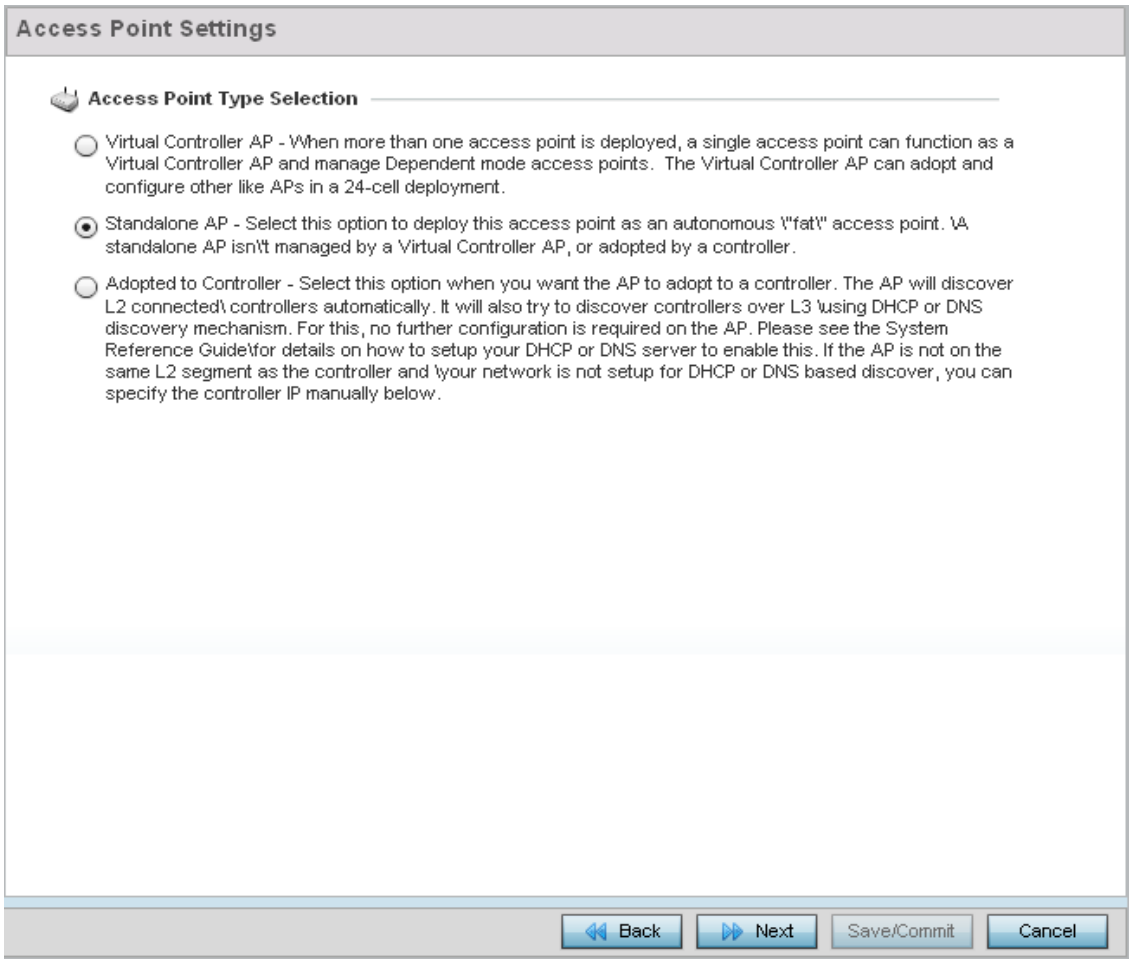


Figure 14: Initial Setup Wizard - Access Point Settings screen for Advanced Setup Wizard

3 Select an **Access Point Type** from the following options:

- *Virtual Controller AP* - When more than one access point is deployed, a single access point can function as a Virtual Controller AP. Up to 64 access points can be connected to, and managed by, a single Virtual Controller AP. These connected access

points must be the same model as the Virtual Controller AP. For more information, see “Virtual Controller AP Mode” on page 30.

- *Standalone AP* - Select this option to deploy this access point as an autonomous fat access point. A standalone AP is not managed by a Virtual Controller AP, or adopted by a RFS series wireless controller. For more information see “Standalone Mode” on page 31.



NOTE

If designating the access point as a Standalone AP, it is recommended that the access point’s UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile and the UI does not. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.

- *Adopted to Controller* - Select this option when deploying the access point as a controller managed (Dependent mode) access point. Selecting this option closes the Initial AP Setup Wizard. An adopted access point obtains its configuration from a profile stored on its managing controller. Any manual configuration changes are overwritten by the controller upon reboot. For more information on configuring the access point in the *Adopted to Controller* mode, see “Adopt to a controller” on page 54.

4 Select the **Next** button to start configuring the access point in the selected mode. If the **Access Point Type** is *Virtual Controller AP* or *Standard AP,* see “Network Topology Selection” on page 43.

If the **Access Point Type** is *Adopted to Controller,* see “Adopt to a controller” on page 54.

Network Topology Selection

“Advanced Setup Wizard”

Use the *Network Topology* screen to define how the access point manages network traffic. The available modes are:

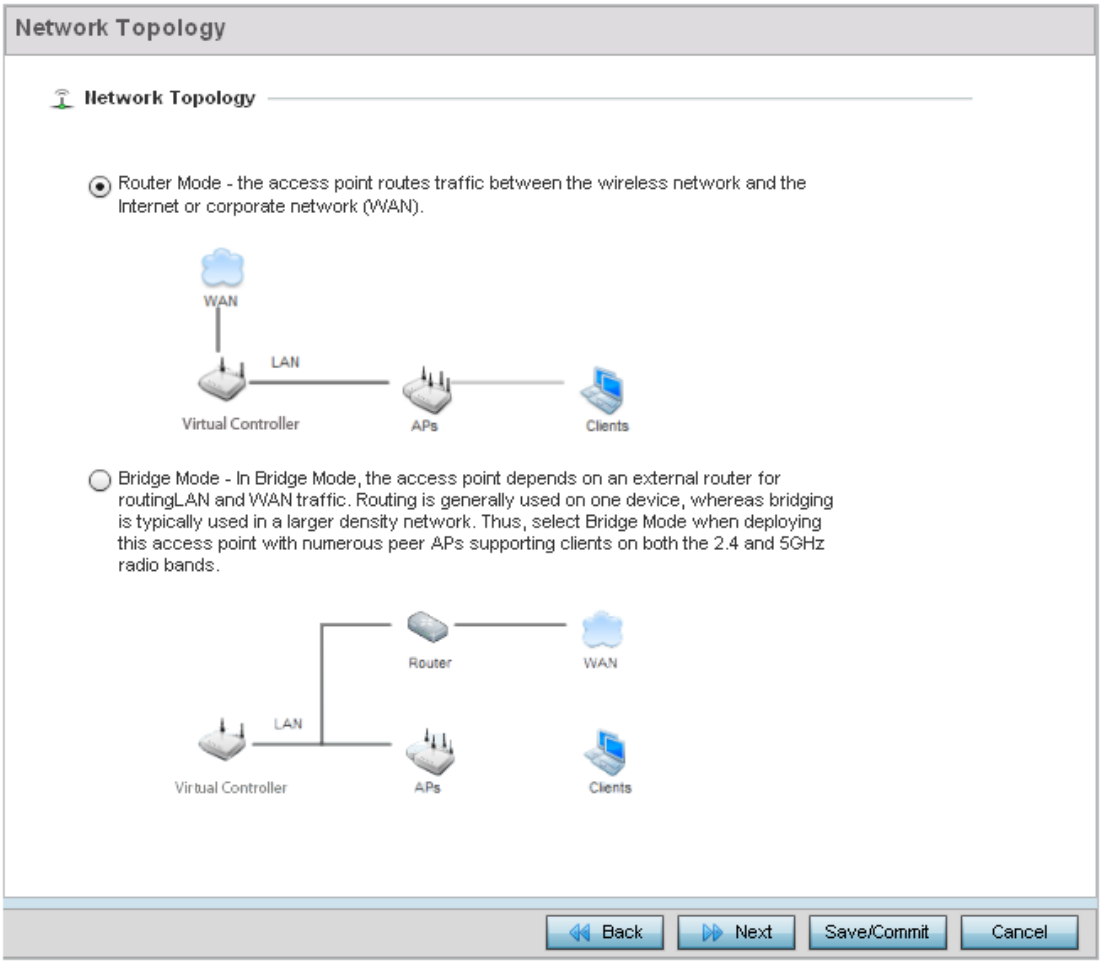


Figure 15: Initial Setup Wizard - Access Point Mode screen for Advanced Setup Wizard

- **Router Mode** - In Router Mode, the access point routes traffic between the local network (LAN) and the Internet or external network (WAN). Router mode is recommended in a deployment supported by just a single access point.
- **Bridge Mode** - In Bridge Mode, the access point depends on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger density network. Select *Bridge Mode* when deploying this access point with numerous peer access points supporting clients on both the 2.4 GHz and 5.0 GHz radio bands.



NOTE

When *Bridge Mode* is selected, WAN configuration cannot be performed and the Initial Setup Wizard does not display the WAN configuration screen.

1 Select **Next**. The *Advanced Setup Wizard* displays the **LAN Configuration** screen to set the access point's LAN interface. For more information, see "LAN Configuration" on page 45.

LAN Configuration

"Advanced Setup Wizard"

Use the *LAN Configuration* screen to configure the parameters required for setting a *Local Area Network* (LAN) on the access point.

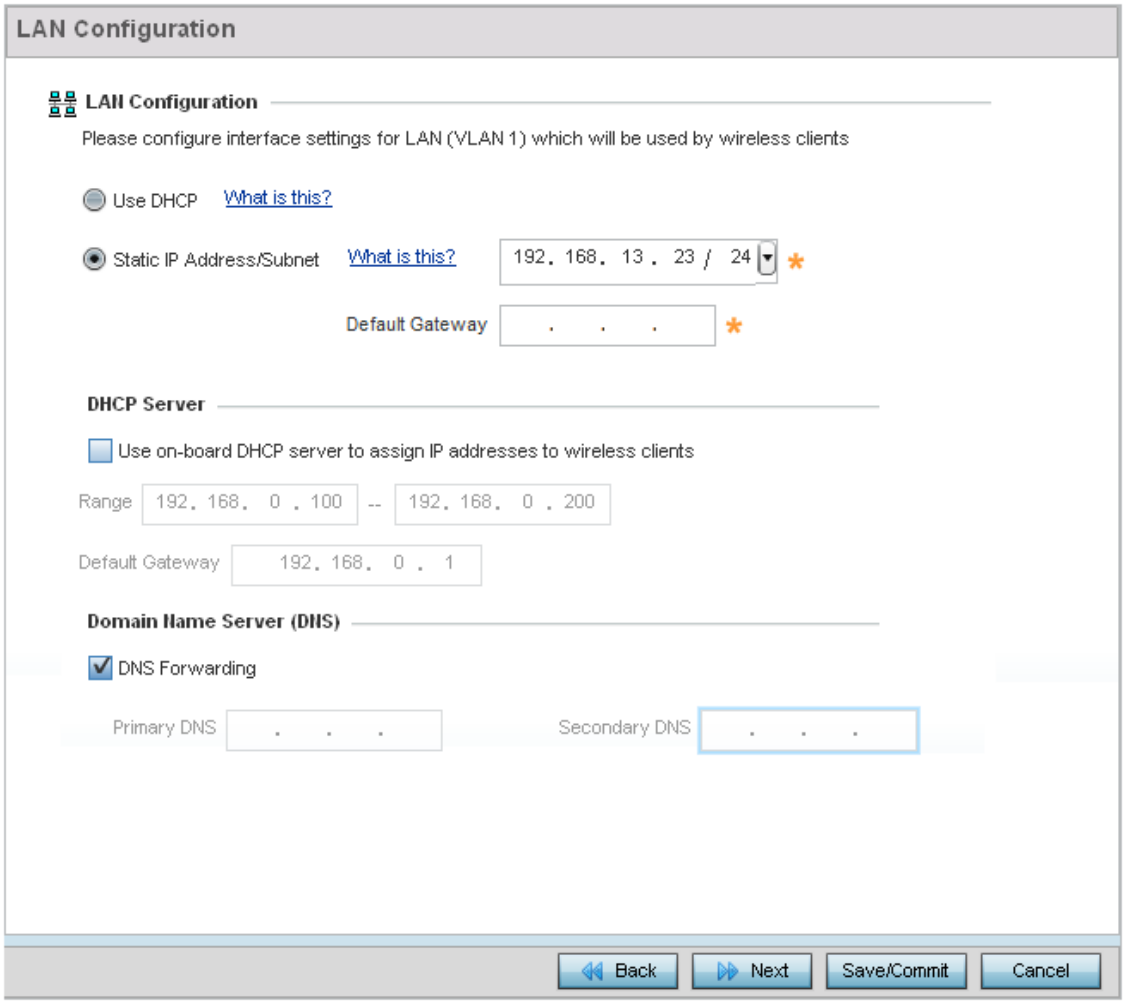


Figure 16: Initial Setup Wizard - LAN Configuration screen for Advanced Setup Wizard

1 Set the following DHCP and Static IP Address/Subnet information for the LAN interface:

- **Use DHCP** - Select this option to enable an automatic network address configuration using DHCP server.
- **Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's LAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **DHCP Server** and **Domain Name Server (DNS)** resources, as those fields will become enabled on the bottom portion of the screen.

- **Default Gateway** - Define a default gateway address for use with the static IP address configuration. This is a required parameter.
- **Use on-board DHCP server to assign IP addresses to wireless clients** - Select the check box to enable the access point's DHCP server to provide IP and DNS information to clients on the LAN interface.
- **Range** - Enter a starting and ending IP Address range for client assignments on the access point's LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.
- **Default Gateway** - Define a default gateway address for use with the DHCP server configuration. This is a required parameter.
- **DNS Forwarding** - Select this option to allow a DNS server to translate domain names into IP addresses. If this option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.
- **Primary DNS** - Enter an IP Address for the main Domain Name Server providing DNS services for the access point's LAN interface.
- **Secondary DNS** - Enter an IP Address for the backup Domain Name Server providing DNS services for the access point's LAN interface

2 Select **Next**. The *Advanced Setup Wizard* displays the *Radio Configuration* screen to set the access point's radios. For more information, see "Radio Configuration" on page 48.

If *Router Mode* is selected as the **Network Topology**, then the *Advanced Setup Wizard* displays the WAN configuration screen. For more information, see "WAN Configuration" on page 34.

WAN Configuration

"Advanced Setup Wizard"



NOTE

This option is only available when *Router Mode* is selected in the Network Topology screen of the *Advanced Setup Wizard.*

The *Advanced Setup Wizard* displays the **WAN Setting** screen to define DHCP and network address information for the WAN interface. The WAN interface is used to connect the access point to a wired local area network or backhaul.

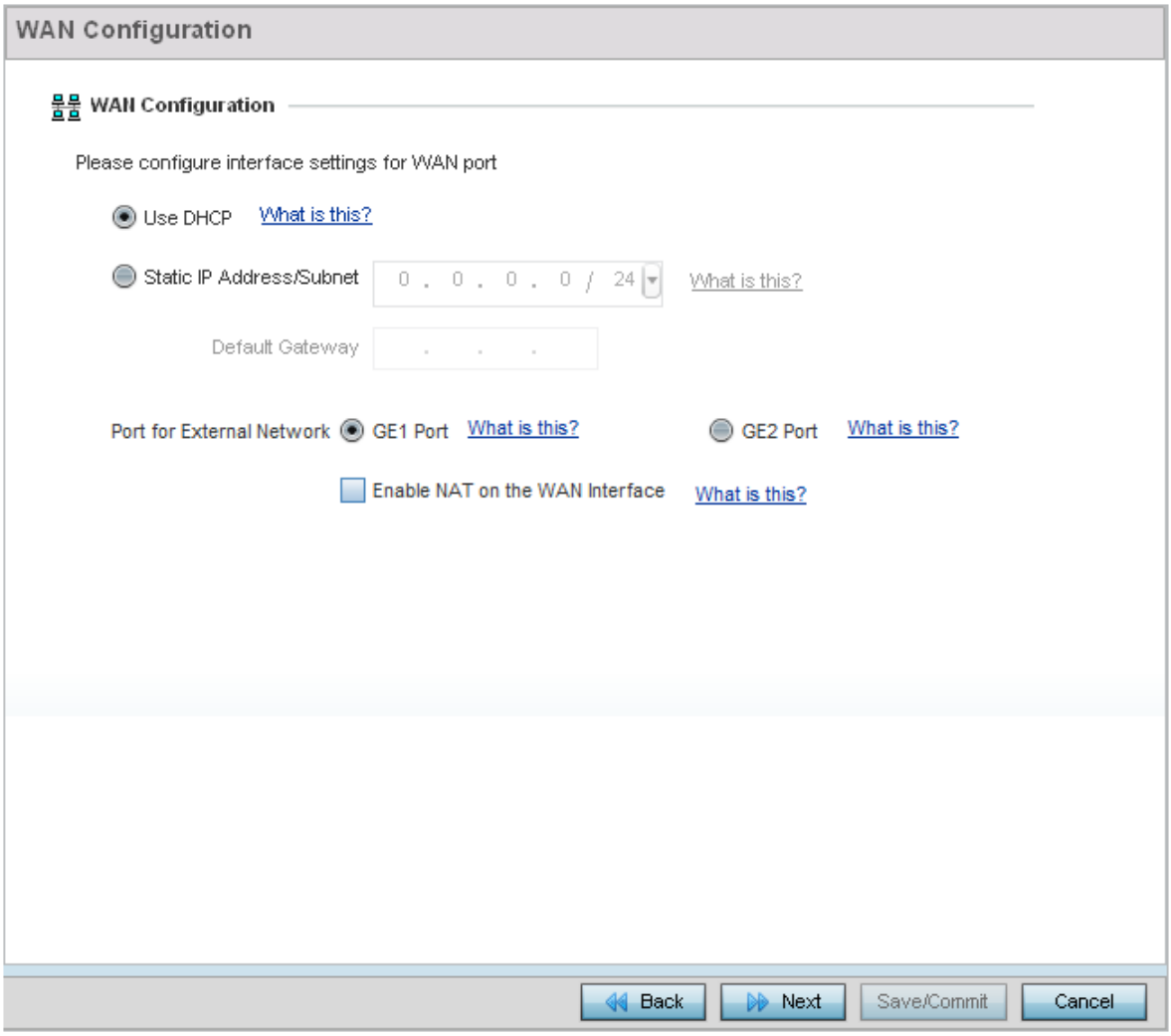


Figure 17: Initial Setup Wizard - WAN Configuration screen of the Advanced Setup Wizard

1 Set the following WAN parameters:

- **Use DHCP** - Select the radio control to enable an automatic network address configuration using external DHCP servers. An automatic IP address is configured to the access point's WAN port using DHCP servers located on the WAN side of the network.
- **Static IP Address/Subnet** - Enter an IP Address and a subnet for the access point's WAN interface. If **Use DHCP** is selected, this field is not available. When selecting this option, define the following **Default Gateway** information as the field will become enabled on the bottom portion of the screen. The IP address defined in this field is assigned to the WAN interface. The **Default Gateway** is a router that serves as a access to other networks.
- **Select the port that's connected to the WAN** – Select the port that is connected to the WAN.
- **Enable NAT on the WAN Interface** – Select this option to enable *Network Address Translation* on the selected GE interface.

2 Select **Next**. The *Advanced Setup Wizard* displays the **Radio Configuration** screen to set the access point's radios. For more information, see "Radio Configuration" on page 48.

Radio Configuration

"Advanced Setup Wizard"

Use the **Radio Configuration** screen to define radio support for the 2.4 GHz radio band, 5.0 GHz radio band or set the radio as a dedicated sensor.



NOTE

The *Radio Configuration* screen displays separate configurable fields for each access point radio. Supported access point models can have from one to three radios. The ADSP Sensor Server field displays at the bottom of the screen only if one of the radios has been dedicated as a sensor.

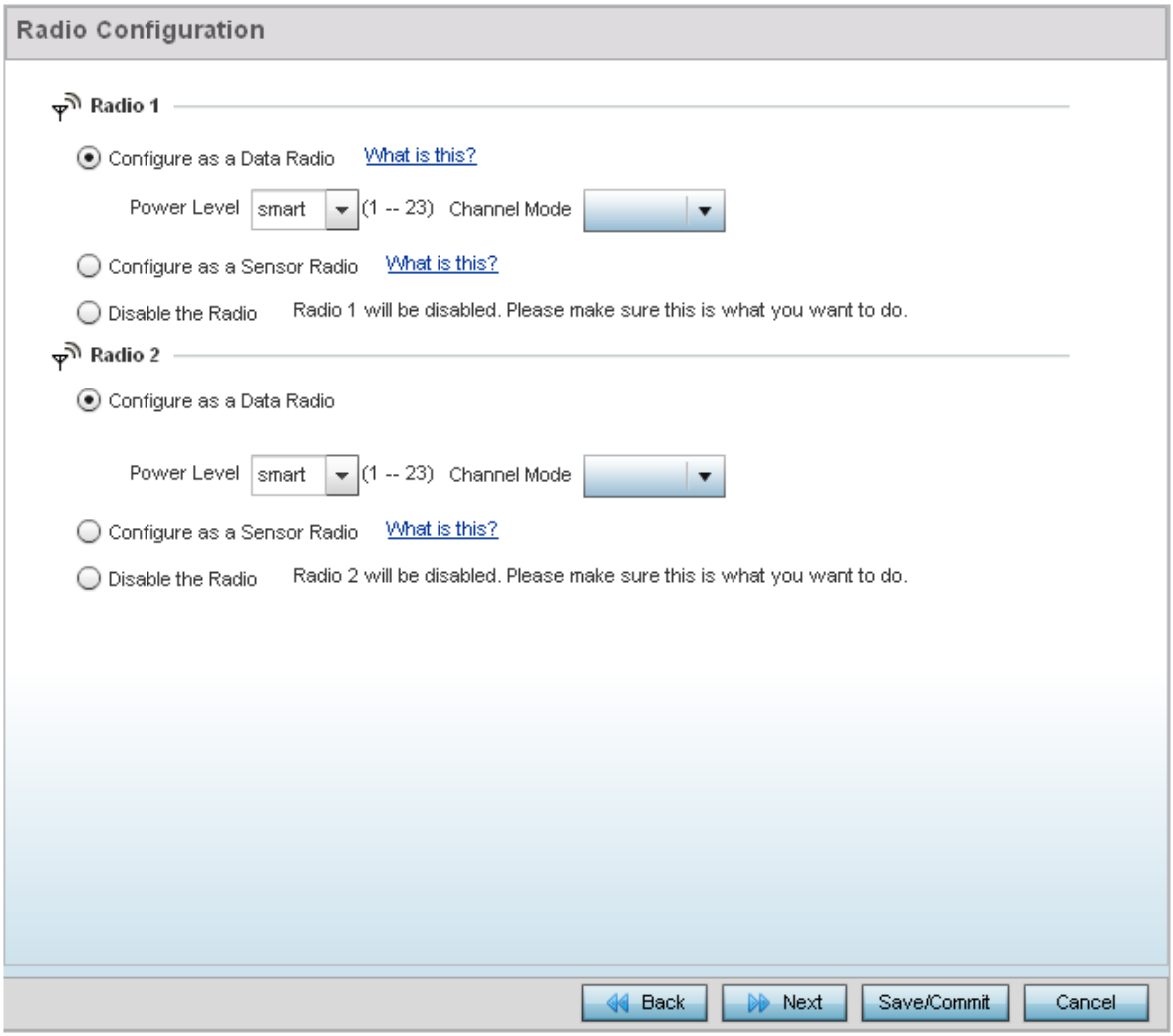


Figure 18: Initial Setup Wizard - Radio Configuration screen of the Advanced Setup Wizard

1 Set the following for each radio:

- **Configure as a Data Radio** - Select this option to dedicate this radio to WLAN client support in the selected 2.4 GHz or 5.0 GHz radio band.
- **Radio Frequency Band** - Select the 2.4 GHz or 5.0 GHz radio band to use with the radio when selected as a Data Radio. The selected band is used for WLAN client support. Consider selecting one radio for 2.4 GHz and another for 5.0 GHz support (if using a dual or three radio model) when supporting clients in the 802.11bg, 802.11n and 802.11ac bands.
- **Power Level** - Use the spinner control to select a 1 - 23 dBm minimum power level to assign to this radio in selected 2.4 GHz or 5.0 GHz band. 1 dBm is the default setting.
- **Channel Mode** - Select either *Random*, *Best* or *Static*. Select *Random* for use with a 802.11a/n radio. To comply with *Dynamic Frequency Selection* (DFS) requirements in the European Union, the 802.11a/n radio uses a randomly selected channel each time the access point is powered on. Select *Best* to enable the access point to scan non-overlapping channels and listen for beacons from other access points. After the channels are scanned, it will select the channel with the fewest access points. In the case of multiple access points on the same channel, it will select the channel with the lowest average power level. When *Constantly Monitor* is selected, the access point will continuously scan the network for excessive noise and sources of interference. Select *Static* to assign the access point a permanent channel and scan for noise and interference only when initialized.
- **Configure as a Sensor Radio** - Select this option to dedicate the radio to sensor support exclusively. When functioning as a sensor, the radio scans in sensor mode across all channels within the 2.4 and 5.0 GHz bands to identify potential threats. If dedicating a radio as a sensor resource, a primary and secondary ADSP server must be specified as an ADSP management resource.



NOTE

If configuring an AP6521 model access point as a sensor, the access point will require a reboot before its sensor functionality is invoked. The reboot can take place at the completion of the Initial Setup Wizard.

- **Disable the Radio** - Select this option to disable this radio, thus prohibiting it from either providing WLAN or sensor support. Verify this course action with your network administrator before rendering the radio offline.

2 Select **Next**. The *Advanced Setup Wizard* displays the *Wireless LAN Setup* screen to set the access point's Wireless LAN interface configuration. For more information, see "Wireless LAN Setup" on page 49.

Wireless LAN Setup

"Advanced Setup Wizard"

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one 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.

Use the *Wireless LAN Setup* screen to configure the WLAN parameters. Up to two (2) WLANs can be configured for the access point.

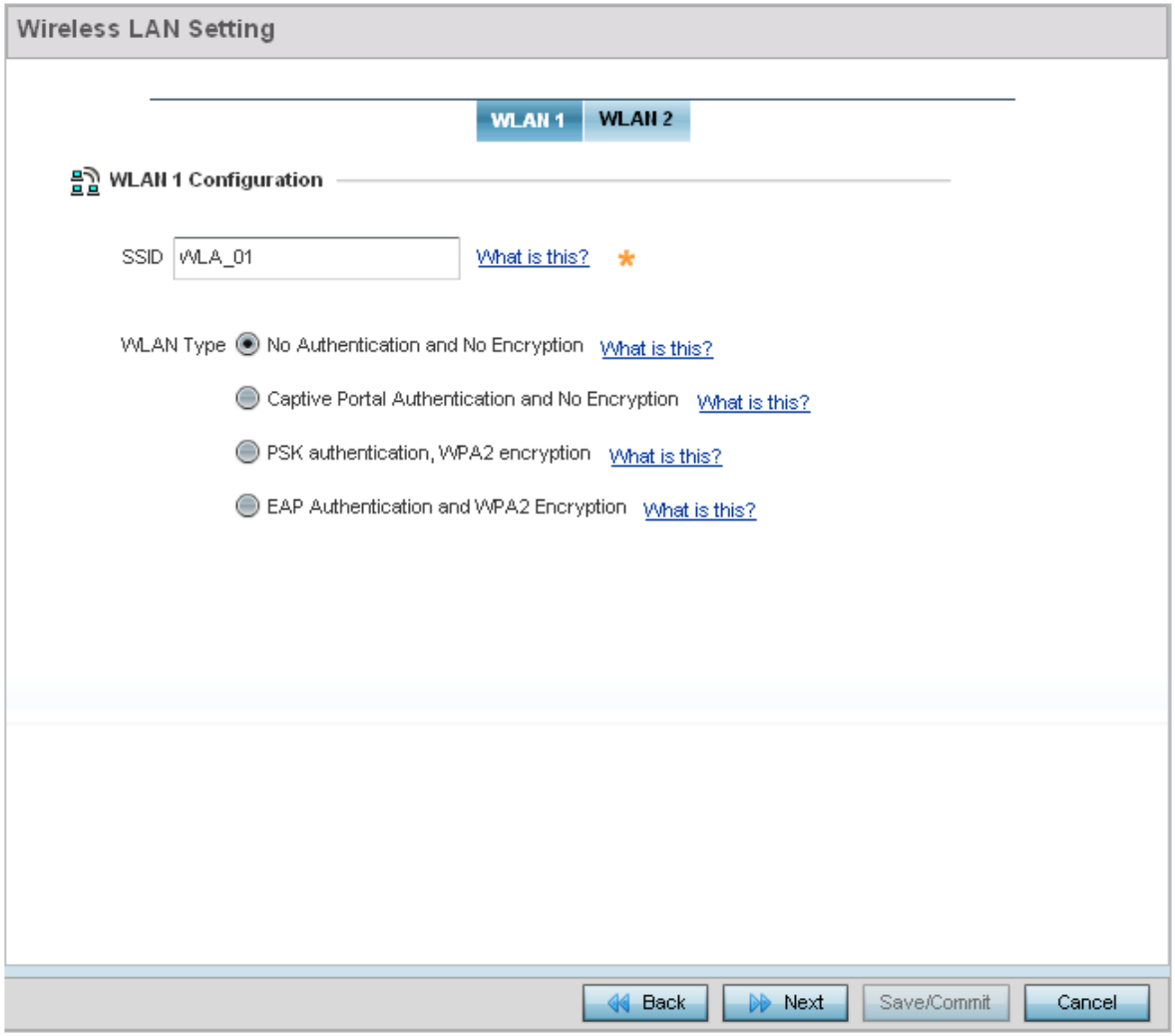


Figure 19: Initial Setup Wizard - WAN Configuration screen for Advanced Setup Wizard

1 Set the following WLAN1 Configuration parameters:

- **SSID** – Configure the SSID for the WLAN.
- **WLAN Type** – Configure the encryption and authentication to use with this WLAN.

- **No Authentication and No Encryption** – Configures a network without any authentication. This means any device can access the network. This option also configures the network without encryption. This means any data transmitted through the network is in plain text.
- **Captive Portal Authentication and No Encryption** – Configures a network using a RADIUS server to authenticate users before allowing them on to the network. Once on the network, no encryption is used for the data transmitted through the network.

Select this option to use a Web page (either internally or externally hosted) to authenticate users before access is granted to the network.

- **External RADIUS Server** – When selected, provide the IP address of the external RADIUS server used for user authentication. Also enter the shared secret in the **RADIUS Shared Secret** field.
- **Onboard RADIUS Server** – When selected, a new screen displays where further configuration can be performed. For more information, see "RADIUS Server Configuration" on page 37.

- **PSK authentication, WPA2 encryption** – Configures a network that uses PSK authentication and WPA2 encryption. Select this option to implement a pre-shared key that must be correctly shared between the access point and requesting clients on the WLAN.
  - **WPA Key** – Provide a 64 character HEX key or 8-63 character ASCII key. Use the drop-down to specify the type of key provided. Select ASCII or HEX to specify the key type provided in the **WPA Key** field.
- **EAP Authentication and WPA2 Encryption** – Configures a network that uses EAP authentication and WPA2 encryption.Select this option to authenticate clients within this WLAN through the exchange and verification of certificates.
  - **External RADIUS Server** – When selected, provide the IP address of the external RADIUS server used for user authentication. Also provide the shared secret in the **RADIUS Shared Secret** field.
  - **Onboard RADIUS Server** – When selected, a new screen is displayed where further configuration can be performed. For more information, see "RADIUS Server Configuration" on page 37.

2 Select **Next**. The *Advanced Setup Wizard* displays the *RADIUS Server Configuration* screen if required. This screen is only displayed when **Onboard RADIUS Server** is selected for either **Captive Portal Authentication And No Encryption** or for **EAP Authentication and WPA2 Encryption** fields. For more information, see "RADIUS Server Configuration" on page 37.

Otherwise, the *Advanced Setup Wizard* displays the *System Information* screen. For more information, see "System Information" on page 51.

System Information

"Advanced Setup Wizard"

Use the *System Information* screen to define the device's location, contact information for an administrator, and the country where this access point is deployed.

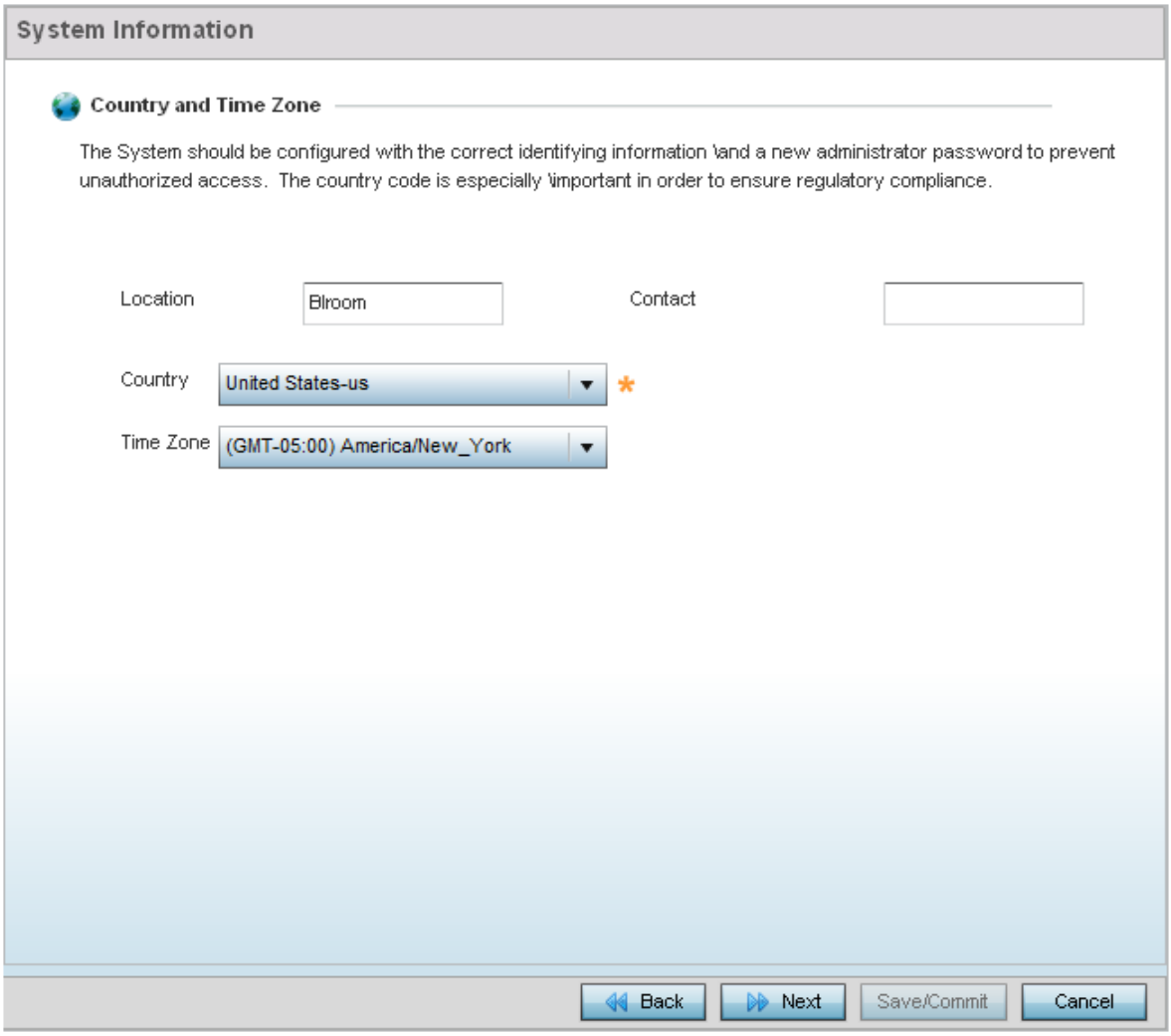


Figure 20: Initial Setup Wizard - System Information screen for the Advanced Setup Wizard

- **Location** - Provide the location of the access point.
- **Contact** - Specify the contact information for the administrator. The credentials provided should accurately reflect the individual responding to service queries.
- **Country** - Select the country where the access point is deployed. The access point prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. 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. This is a required parameter.
- **Time Zone** - Set the time zone where the access point is deployed. This is a required parameter. The setting should be complimentary with the selected deployment country.

1 Select **Next**. The *Advanced Setup Wizard* displays the *Summary and Commit* screen to summarize the screens (pages) and settings updated using the Initial AP Setup Wizard. For more information, see "Summary And Commit Screen" on page 53.

Summary And Commit Screen

"Advanced Setup Wizard"

The *Summary And Commit* screen displays an overview of the updates made using the *Advanced Setup Wizard*.

There is no user intervention or additional settings required. This screen is an additional means of validating the configuration before it is deployed. However, if a screen displays settings not intended as part of the initial configuration, the screen can be selected from within the **Navigation Panel** and its settings modified accordingly.

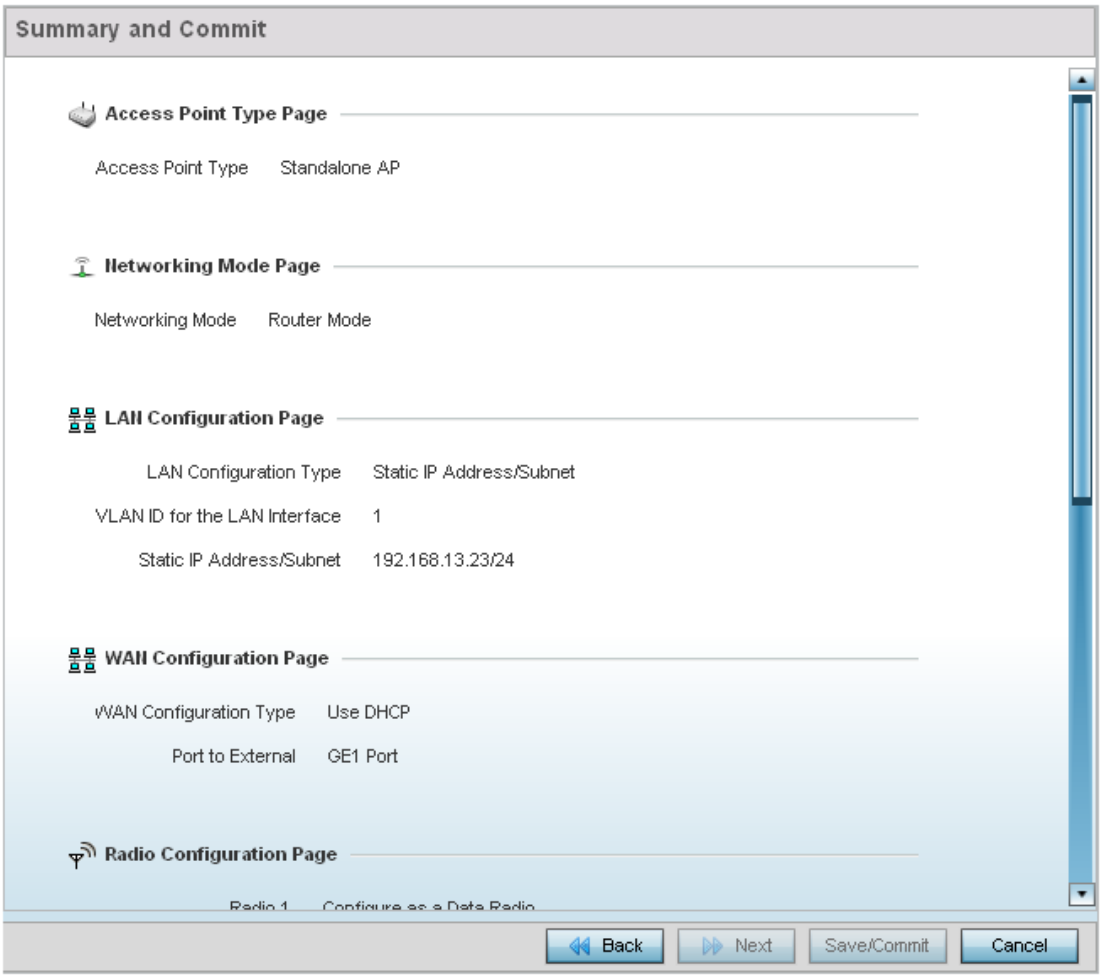


Figure 21: Initial Setup Wizard - Summary and Commit screen for the Advanced Setup Wizard

If the configuration displays as intended, select **Save/Commit** to implement these settings to the access point. If additional changes are warranted, either select the target page from the *Navigational Panel*, or use the **Back** button.

Adopt to a controller

"Advanced Setup Wizard"

When the access point is powered on for the first time, it looks for a wireless controller on the default subnet running the same firmware version and automatically adopts to it.

When *Adopted to Controller* is selected, further configuration settings are displayed in the same screen. Select **Automatic controller discovery** to enable the access point to be discovered and adopted using layer 2 settings.

If preferring layer 3 adoption, select **Static Controller Configuration**, and define the addresses of the preferred controllers. When using the static method, define whether the access point receives an IP address using DHCP or if IP resources are provided statically. Up to two (2) controllers can be defined. The access point will try to adopt to the controller defined in the **Controller 1** field first. Should the controller not be found, the access point tries to adopt to the controller defined in **Controller 2** field.

When preferring layer 3 adoption, configure how an IP is assigned to this access point. Select **Use DHCP** to use DHCP to assign an IP address to this access point. If this access point requires a static IP, select **Static IP Address/Subnet** and provide the appropriate IP address and net mask. For your convenience, the netmask is automatically set to 24. Also assign the **Default Gateway** for forwarding traffic.

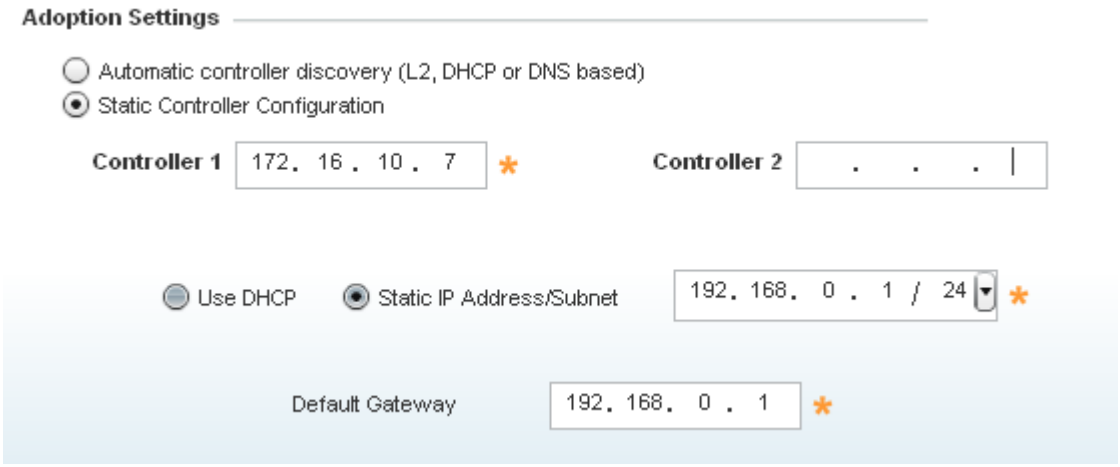


Figure 22: Initial Setup Wizard - Adoption Settings

NOTE

The best way to administer a network populated by numerous access points is to configure them directly from their managing controller or Virtual Controller AP. If an access point's configuration requires an exception from the wireless controller or Virtual Controller AP's assigned profile configuration, the administrator should apply a Device Override to change just that access point's configuration.

Select the **Save/Commit** button to save the current configuration. Select the **Cancel** button to exit the *Initial Setup Wizard* without making any changes. Select the **Back** button to go back to the previous screen of the *Initial Setup Wizard*.

4 Dashboard

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

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

The dashboard provides the following tools and diagnostics:

- "Dashboard"
- "Network View"

Dashboard

"Dashboard"

The *Dashboard* screen displays device information organized by device association and inter-connectivity between an access point and connected wireless clients.

To review dashboard information:

1 Select **Dashboard**. Expand the **System** menu item on the upper, left-hand, side of the UI and select either an access point or connected client.

The *Dashboard* screen displays the **Health** tab by default.

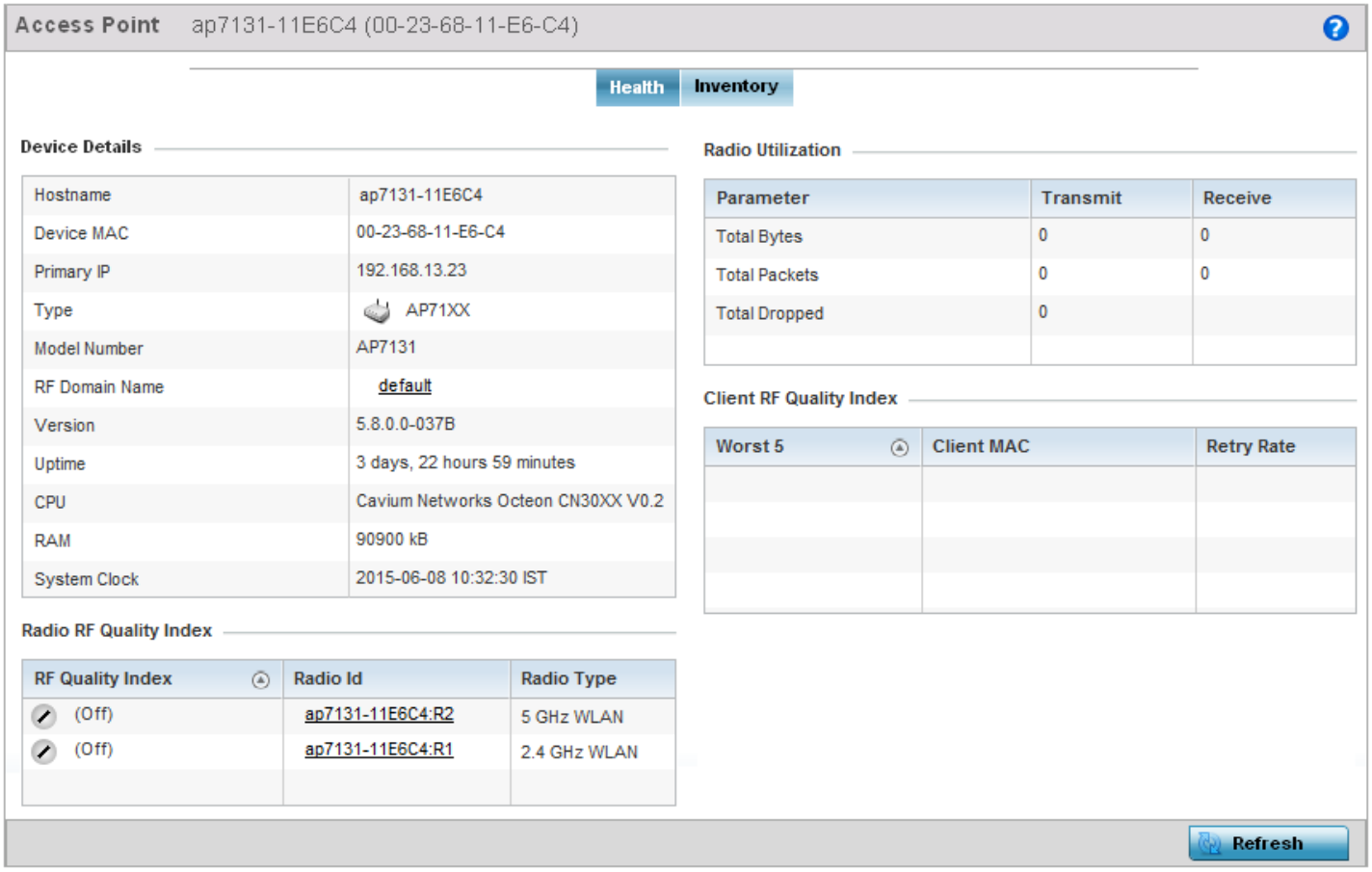


Figure 23: Dashboard - Health tab

Dashboard Conventions

The *Dashboard* screen displays device information using the following conventions:

- "Health" – Displays the state of the access point managed network.
- "Inventory" – Displays the physical devices managed by the access point.

Health

"Dashboard Conventions"

The **Health** tab displays performance and utilization data for the access point managed network.

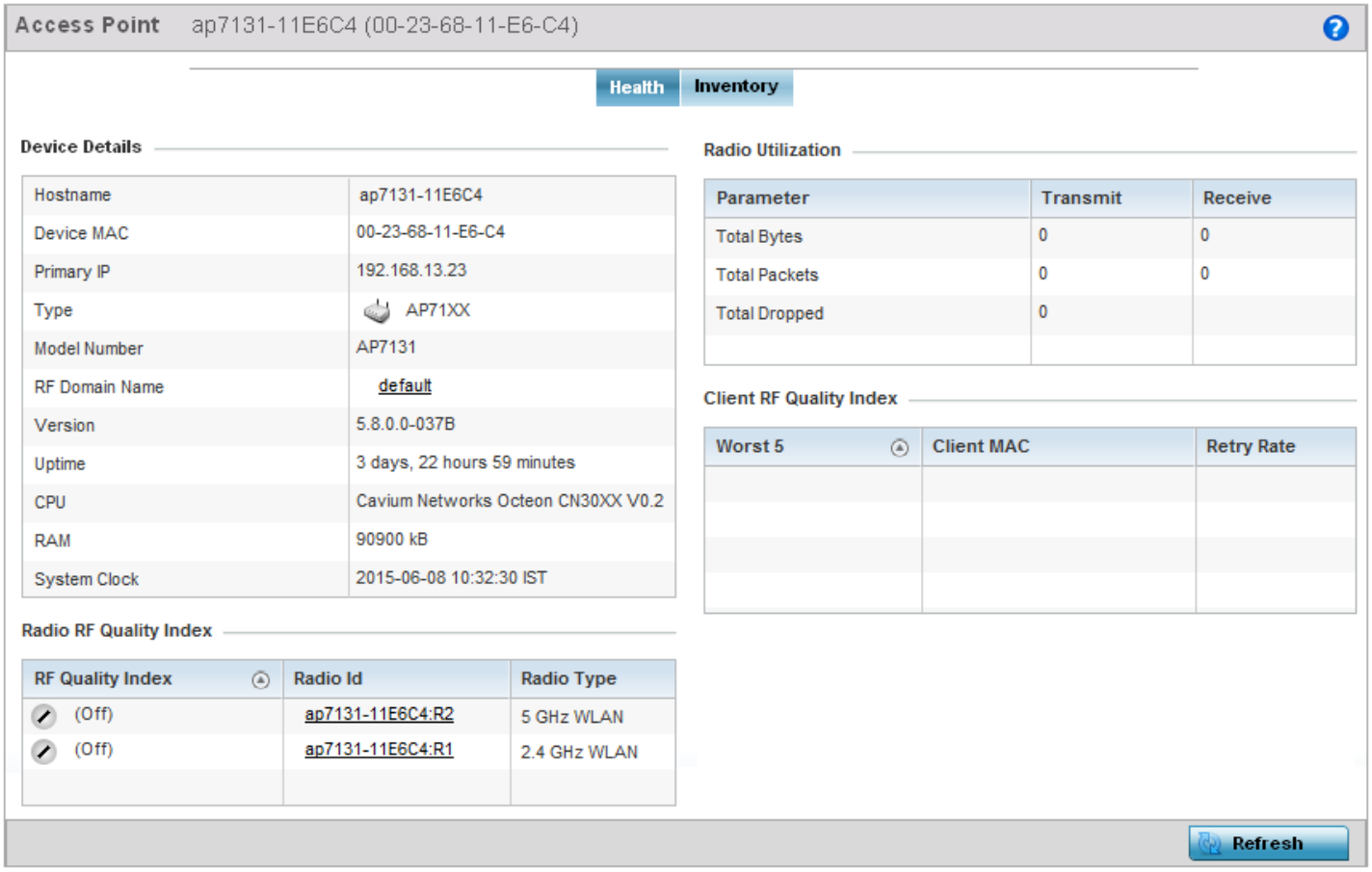


Figure 24: Dashboard - Health tab

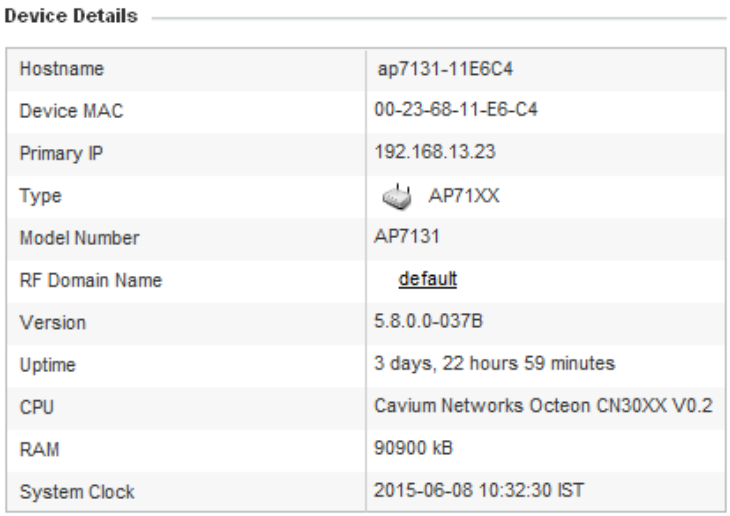
For more information, see:

- "Device Details"
- "Radio RF Quality Index"
- "Radio Utilization Index"
- "Client RF Quality Index"

Device Details

▲ "Health"

The **Device Details** field displays model and version information.



Device Details

Hostname	ap7131-11E6C4
Device MAC	00-23-68-11-E6-C4
Primary IP	192.168.13.23
Type	AP71XX
Model Number	AP7131
RF Domain Name	default
Version	5.8.0.0-037B
Uptime	3 days, 22 hours 59 minutes
CPU	Cavium Networks Octeon CN30XX V0.2
RAM	90900 kB
System Clock	2015-06-08 10:32:30 IST

Figure 25: Dashboard - Health tab - Device Details field

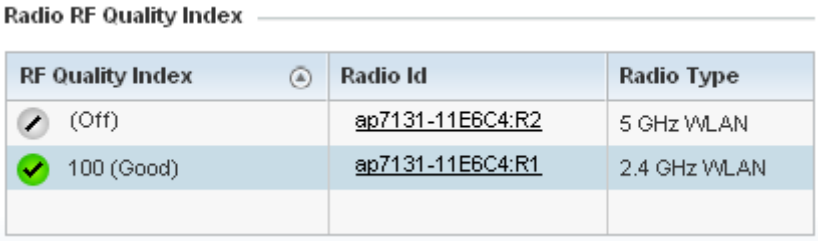
The **Device Details** field displays the name assigned to the selected access point, factory encoded MAC address, primary IP address, model type, RF Domain, software version, uptime, CPU and RAM information and system clock. Use this data to determine whether a software upgrade is warranted, or if the system clock needs adjustment.

Periodically select **Refresh** (at the bottom of the screen) to update the data displayed.

Radio RF Quality Index

"Dashboard Conventions"

The **Radio RF Quality Index** displays a RF quality table for the access point's single default RF Domain. It is a percentage of the overall effectiveness of the RF environment. It is a function of the data rate in both directions, the retry rate and the error rate.



Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type
(Off)	ap7131-11E6C4:R2	5 GHz WLAN
100 (Good)	ap7131-11E6C4:R1	2.4 GHz WLAN

Figure 26: Dashboard - Health tab - Radio RF Quality Index field

RF Quality displays as the average quality index for the single RF Domain utilized by the access point. The table lists the bottom five (5) RF quality values for the RF Domain.

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 Index

"Dashboard Conventions"

The **Radio Utilization Index** displays how efficiently the RF medium is used by the access point. Traffic utilization is defined as the percentage of throughput relative to the maximum possible throughput.

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.

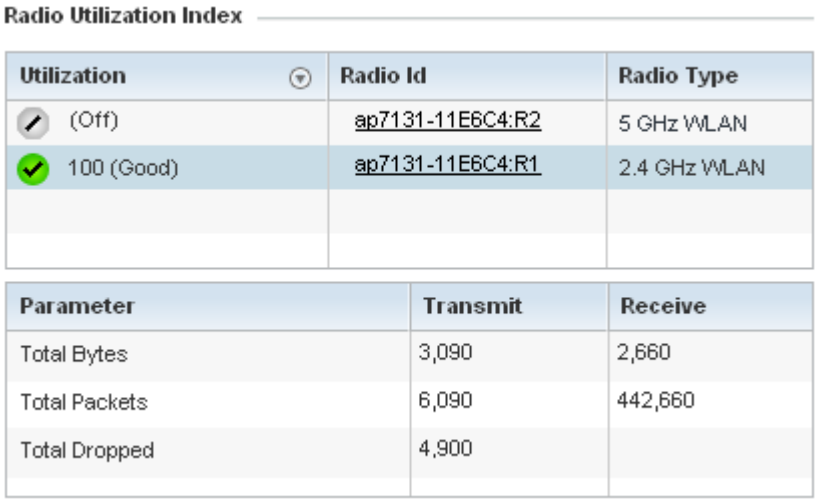


Figure 27: Dashboard - Health tab - Radio Utilization Index field

Client RF Quality Index

"Dashboard Conventions"

The **Client RF Quality Index** displays a list of the worst 5 performing clients managed by the selected access point.

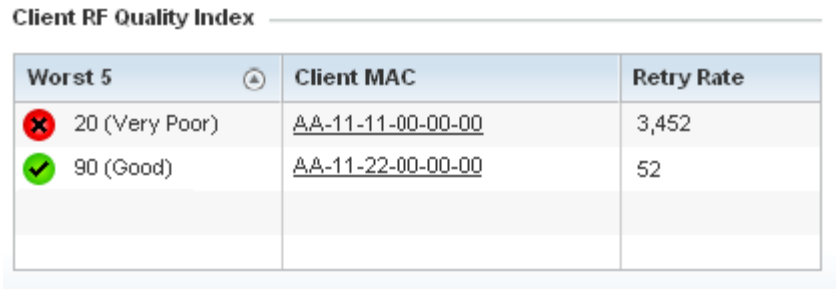


Figure 28: Dashboard - Health tab - Client RF Quality Index field

1 The **Client RF Quality Index** displays the following:

Worst 5	Lists the worst 5 performing client radios connected to the access point. The RF Quality Index measures the overall effectiveness of the RF environment as a percentage. It is a function of the connect rate in both directions, as well as 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*
Client MAC	Displays the factory encoded MAC address assigned to each connected radio listed. Use this information to assist in the identification of poorly performing radios.
Retry Rate	Lists the number of retries attempted to re-connect with the listed radio.

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

Inventory

"Dashboard Conventions"

The **Inventory** tab displays information relative to the devices managed by the selected access point. The Inventory screen affords a system administrator an overview of the number and state of managed devices. The screen contains links to display more granular data specific to a radio.

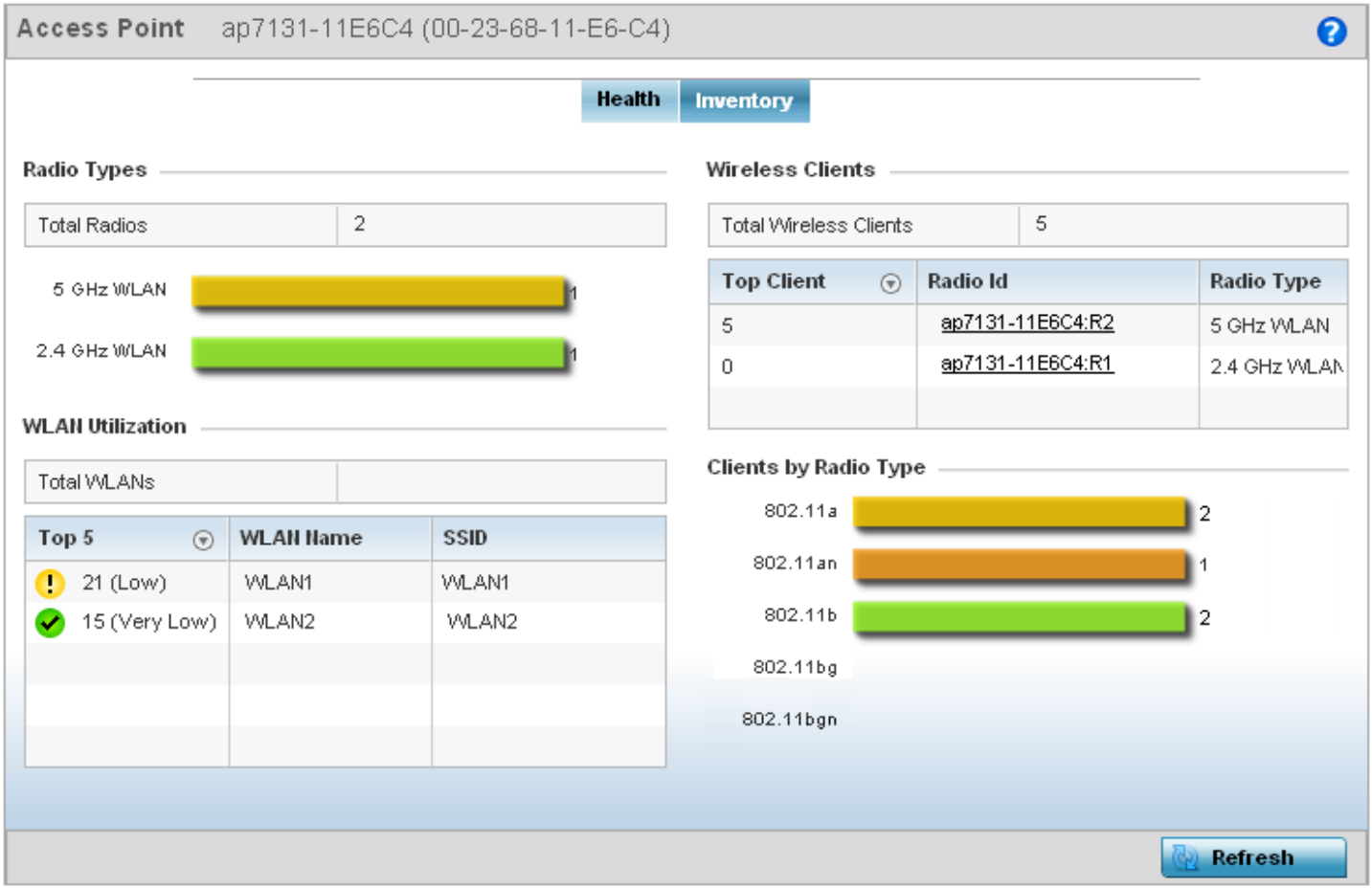


Figure 29: Dashboard - Inventory tab

The Inventory tab is partitioned into the following fields:

- "Radio Types"
- "WLAN Utilization"
- "Wireless Clients"
- "Clients by Radio Type"

Radio Types

"Inventory"

The **Radio Types** field displays the total number and types of radios managed by the selected access point.

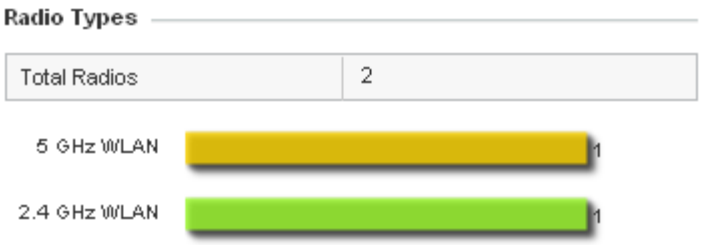


Figure 30: Dashboard - Inventory tab - Radio Types field

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.

WLAN Utilization

"Inventory"

The **WLAN Utilization** field displays the top 5 WLANs utilized by this access point in respect to client support. 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

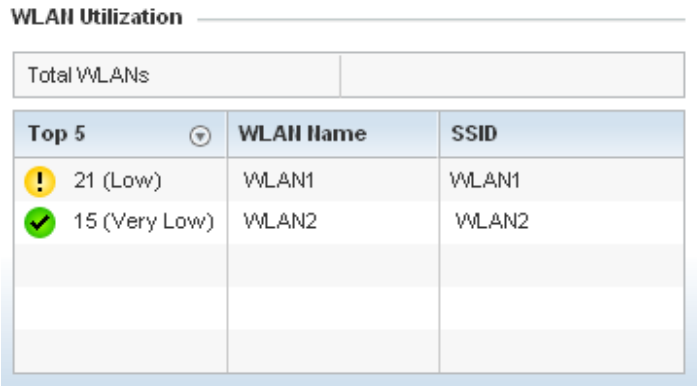


Figure 31: Dashboard - Inventory tab - WLAN Utilization field

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

Wireless Clients

"Inventory"

The **Wireless Clients** field displays information about the wireless clients managed by the selected access point.

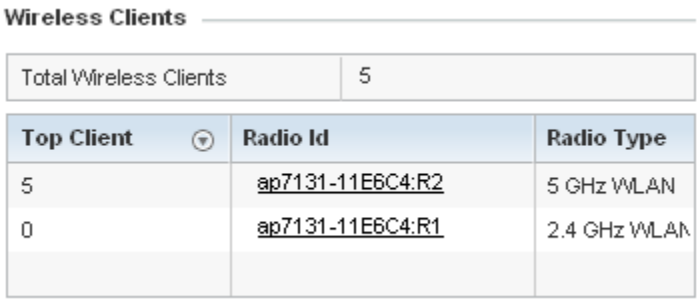


Figure 32: Dashboard - Inventory tab - Wireless Clients field

Information within the **Wireless Clients** field is presented in two tables. The first table lists the total number of wireless clients managed by this access point. The second table lists an ordered ranking of radios based on their supported client count. Use this information to assess if an access point managed radio is optimally deployed in respect to its radio type and intended client support requirements.

NOTE

AP6522, AP6532, AP6562, AP8132, AP8232, AP7161 and AP7181 model access points can support up to 256 client connections to a single access point. AP6521 model access point (single radio model) can support up to 128 client connections per access point.

Clients by Radio Type

"Inventory"

The **Clients by Radio Type** field displays a bar graph illustrating the number of connected clients currently operating on supported radio bands.

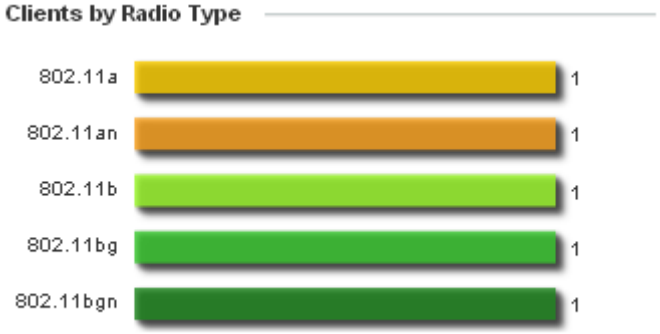


Figure 33: Dashboard - Inventory tab - Clients by Radio Type field

For 5.0 GHz, clients are displayed supporting the *802.11a* and *802.11an* radio bands. For 2.4 GHz, clients are displayed supporting the *802.11b*, *802.11bg*, and *802.11bgn* radio bands. Use this information to determine if all the access point's client radio bands are optimally supported for the access point's radio coverage area.

Network View

"Dashboard"

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

Access points and clients can be selected and viewed using various color schemes in respect to neighboring access points, connected devices and performance criteria. Display options can be utilized to review device performance and utilization, as well as the RF band, channel and vendor. For more information, see "Network View Display Options" on page 67.

To review a device's Network Topology, select **Dashboard > Network View**.

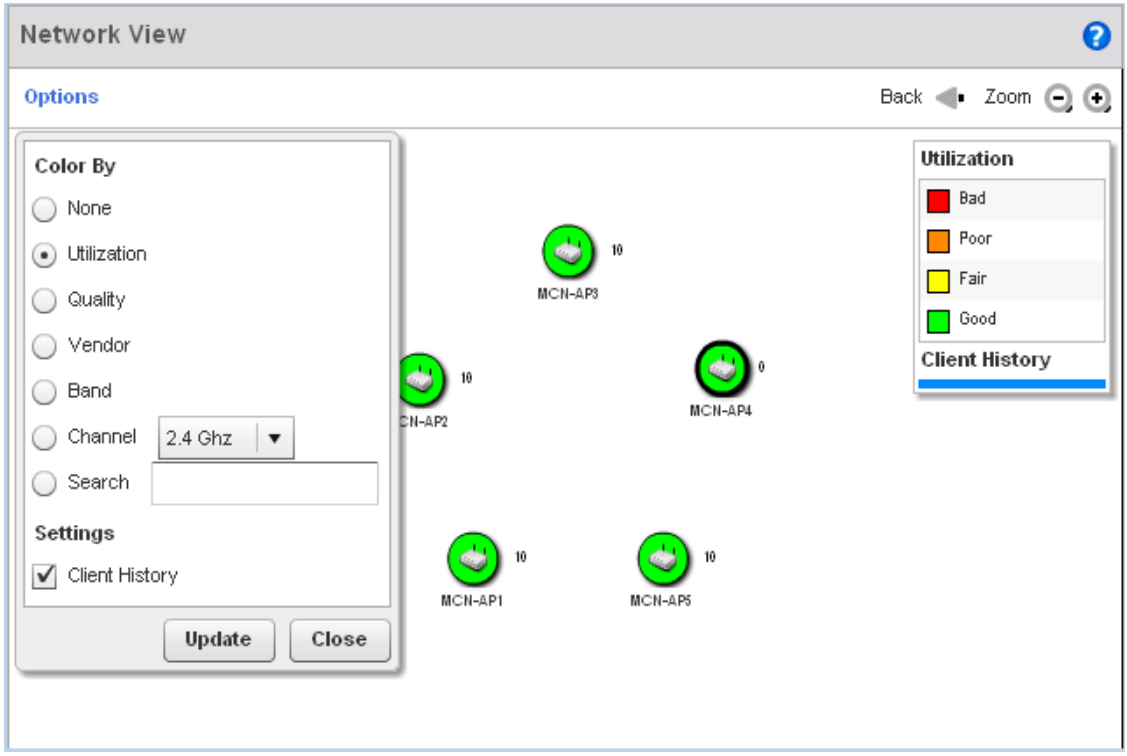


Figure 34: Network View Topology

The left-hand side of the *Network View* screen contains an expandable System Browser where access points can be selected and expanded to display connected clients. Navigate

the System Browser to review device connections within the access point managed network. Many of these peer access points are available for connection to access points in Virtual Controller AP mode.

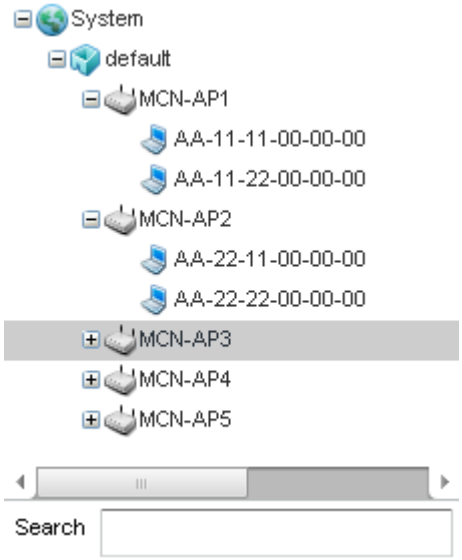


Figure 35: Network View - System Browser

Network View Display Options

"Network View"

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

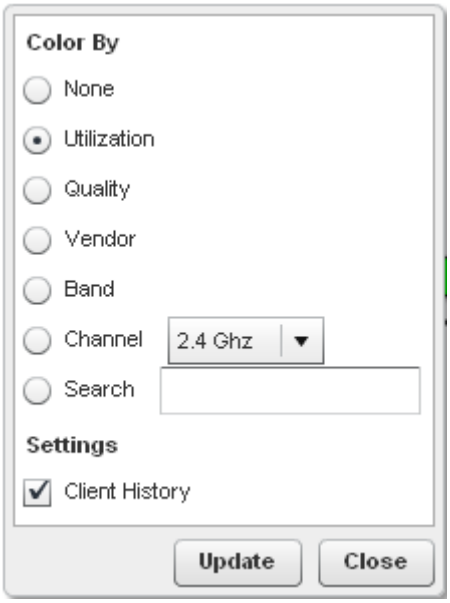


Figure 36: Network View - Display Options

2 The following display filter options are available:

- *None* - Select this option to keep the *Network View* display as it currently appears, without any additional color or device interaction adjustments.
- *Utilization* – Select this option to filter based on the percentage of current throughput relative to maximum throughput. Utilization results include: *Red* (Bad Utilization), *Orange* (Poor Utilization), *Yellow* (Fair Utilization) and *Green* (Good Utilization).
- *Quality* – Select this option to filter based on the overall RF health. RF health is a ratio of connection rate, retry rates, and error rates. Quality results include: *Red* (Bad Quality), *Orange* (Poor Quality), *Yellow* (Fair Quality) and *Green* (Good Quality).
- *Vendor* – Displays the device manufacturer.
- *Band* – Select this option to filter based on the 2.4 or 5.0 GHz radio band of connected clients. Results include: *Yellow* (2.4 GHz radio band) and *Blue* (5.0 GHz radio band). Selecting band is a good way to determine whether 2.4 and 5.0 GHz radios are optimally deployed in respect to the access point client loads on both bands.
- *Channel* - Use the 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.

3 Select the **Update** button to update the display with the changes made to the filter options. Select **Close** to close the options field and remove it from the *Network View*.

Device Specific Information

"Network View"

A device specific information screen is available for individual devices selected from within the Network View (not the System Browser). The screen displays the name assigned to the device, its model, factory encoded MAC address, number of radios within the device, number of connected clients, as well as the highest and lowest reported quality, utilization and *Signal to Noise Ratio* (SNR). This information cannot be modified by the administrator.

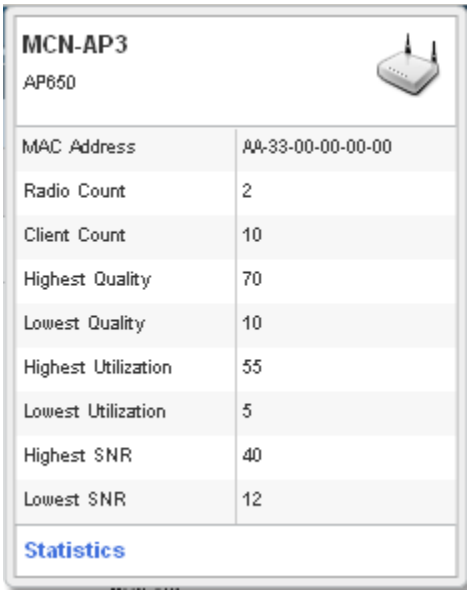


Figure 37: Network View - Device Specific Information

Optionally select the **Statistics** link at the bottom of the display to open a screen where access point device data can be reviewed on a much more granular level. For more information, see "Health" on page 58.

5 Device Configuration

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

Refer to the following to set an access point's sensor functionality, Virtual Controller AP designation, and license and certificate usage configuration:

- "RF Domain Configuration"
- "System Profile Configuration"
- "Managing Virtual Controllers"
- "Overriding a Device Configuration"
- "Managing an Event Policy"

An RF Domain allows an administrator to assign comparable configuration data to multiple access points deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these devices share, as their general client support roles are quite similar. However, access point configurations may need periodic refinement and overrides from their original RF Domain administered design. For more information, see "RF Domain Overrides" on page 316.

Profiles enable administrators to assign a common set of configuration parameters and policies to access points of the same model. Profiles can be used to assign shared network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. To define a configuration profile for a specific access point model, refer to "System Profile Configuration" on page 86.

However, device Profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could be applied an override from a configuration shared amongst numerous peer devices deployed within a particular site. For more information, see "Device Overrides" on page 319.

RF Domain Configuration

- "Device Configuration"

An access point's configuration consists of numerous elements including a RF Domain, WLAN and device specific settings. RF Domains are used to assign regulatory, location and relevant policies to access points of the same model. For example, an AP6532 RF Domain can only be applied to another AP6532 model.

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

However, an access point's RF Domain configuration may need periodic refinement from its original RF Domain designation. Unlike a RFS series wireless controller, an access point supports just a single RF domain. Thus, administrators should be aware that overriding an access point's RF Domain configuration results in a separate configuration that must be managed in addition to the RF Domain configuration. Thus, a configuration should only be overridden when needed. For more information, see "RF Domain Overrides" on page 316.

The access point's RF Domain can have a WIPS sensor configuration applied. For more information on defining a WIPS sensor configuration for use with the access point's RF Domain, see "RF Domain Sensor Configuration" on page 73.

To set a RF Domain configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **RF Domains** from the options on left-hand side of the UI.

The RF Domain **Basic Configuration** tab displays by default with the access point RF Domain activated.

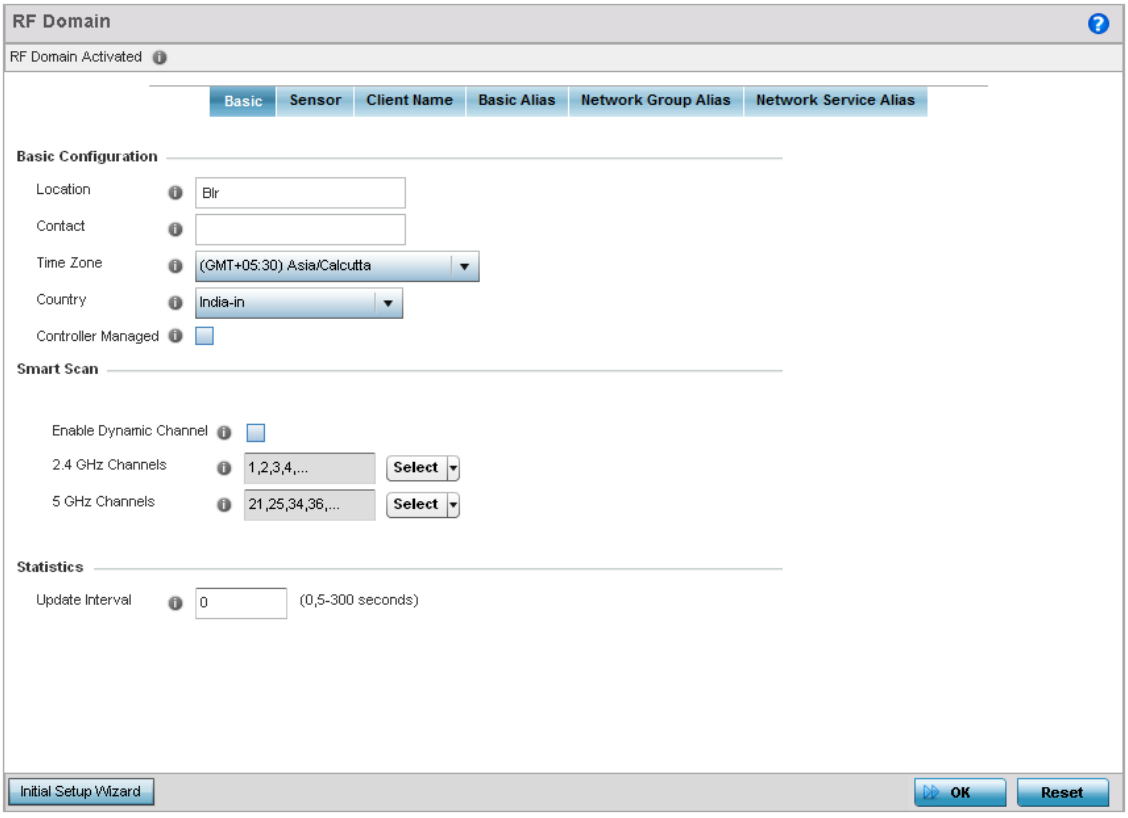


Figure 1: RF Domain - Basic Configuration tab

4 Define the following **Basic Configuration** values for the access point RF Domain:

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

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

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

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

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

7 Use the **Initial Setup Wizard** to configure the device. For more information on using the **Initial Setup Wizard**, see "Using the Initial Setup Wizard" on page 25.

8 Select **OK** to save the changes to the Basic Configuration, or select **Reset** to revert to the last saved configuration.

RF Domain Sensor Configuration

"RF Domain Configuration"

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

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

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

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

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

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **RF Domains** from the options on left-hand side of the UI.

4 Select the **Sensor Configuration** tab.

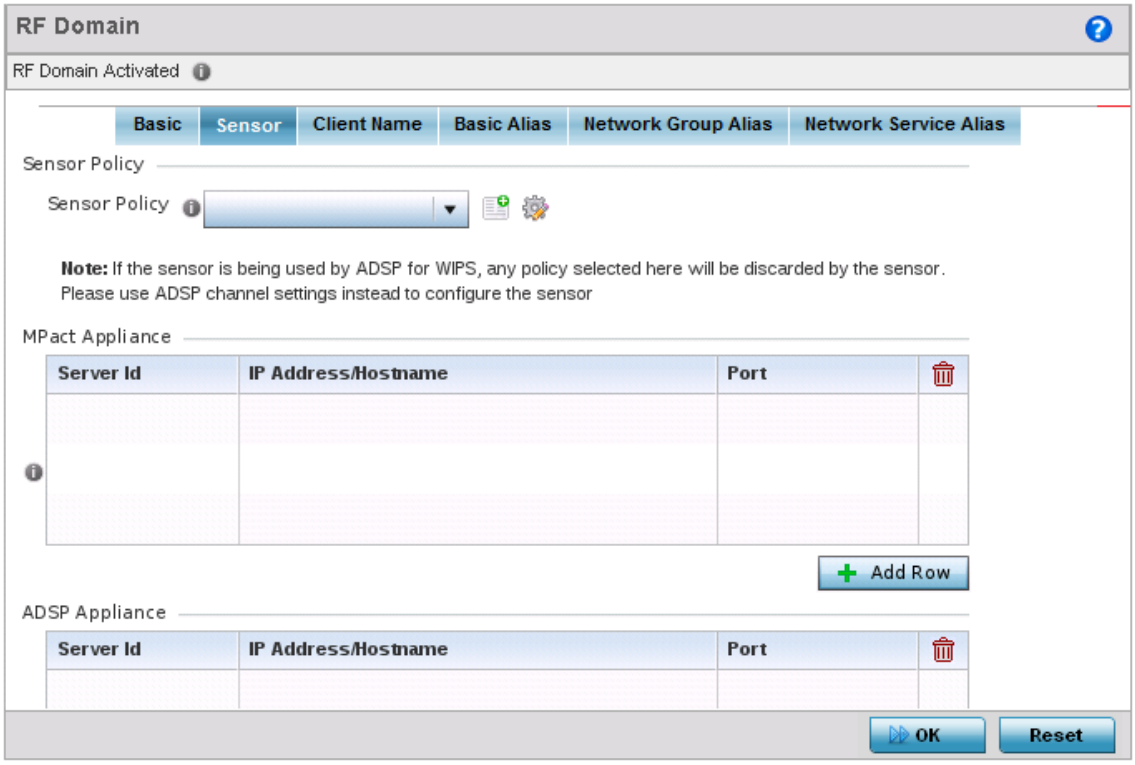


Figure 2: RF Domain - Sensor Configuration tab

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



NOTE

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

Select the **Create** icon to create a new sensor policy or select the **Edit** icon to update the configuration of an existing policy. The Sensor Policy addition screen displays with the Scan Mode set to *Default-Scan*. The user configurable parameters available within the screen differ depending on the Scan Mode option selected. For more information, see "Sensor Policy" on page 646

6 Within a **MPact Appliance** architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated MPact Server resource, as opposed to an ADSP server. Select the **+ Add Row** button to populate the screen with up to three rows for MPact server credentials.

Server Id	Use the spinner control to assign a numeric ID for up to three MPact servers designated to receive RSSI scan data from a WiNG dedicated server. The server with the lowest defined ID is the first reached. The default ID is 1.
IP Address/Hostname	Provide the numeric (non DNS) IP address or hostname of up to three MPact server resources for receiving RSSI scan data. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of the MPact sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443.

7 For an **ADSP Appliance** sensor architecture, select the **+ Add Row** button to populate the screen with up to three rows for ADSP server credentials:

Server Id	Use the spinner control to assign a numeric ID for up to three ADSP servers designated to receive RSSI scan data from a WiNG dedicated server. The server with the lowest defined ID is the first reached. The default ID is 1.
IP Address/Hostname	Provide the numeric (non DNS) IP address or hostname of up to three ADSP server resources for receiving RSSI scan data. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of the ADSP sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443.

8 Either select the **+ Add Row** button to create a new WIPS server configuration or highlight an existing Sensor Server Configuration and select the **Delete** icon to remove it.

9 Use the spinner control to assign a numerical **Server ID** to each WIPS server defined. The server with the lowest defined ID is the first reached by the access point. The default ID is 1.

10 Provide the numerical (non DNS) **IP Address** of each server used as a WIPS sensor server by the RF Domain.

11 Use the spinner control to specify the **Port** of each WIPS server. The default port is 443.

12 Select **OK** to save the changes to the AirDefense WIPS configuration, or select **Reset** to revert to the last saved configuration.

RF Client Name Configuration

"RF Domain 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 RF Domain member devices:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **RF Domains** from the options on left-hand side of the UI.

4 Select the **Client Name** tab.

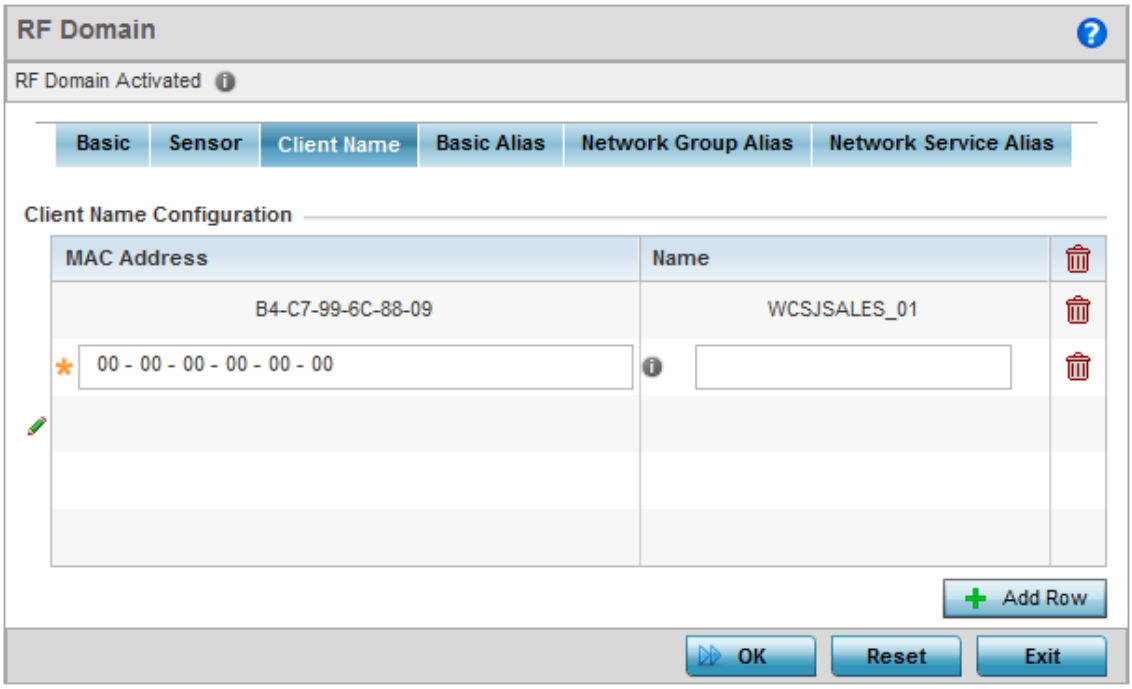


Figure 3: RF Domain Client Configuration screen

5 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.

6 Enter the client's factory coded MAC address.

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

8 Select **OK** to save the changes to the configuration, or select **Reset** to revert to the last saved configuration.

RF Domain Alias Configuration

"RF Domain Configuration"

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

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

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

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

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

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

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an *Network Alias* defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment

location to suit the local requirement. For the remote deployment location, the network alias works with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

Alias can be classified as:

- "Basic Alias"
- "Network Group Alias"
- "Network Service Alias"

Basic Alias

"RF Domain Alias Configuration"

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

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

To edit or delete a basic alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Devices.**

3 Select **RF Domain.**

4 Select the **Basic Alias** tab. The **Basic Alias** screen displays.

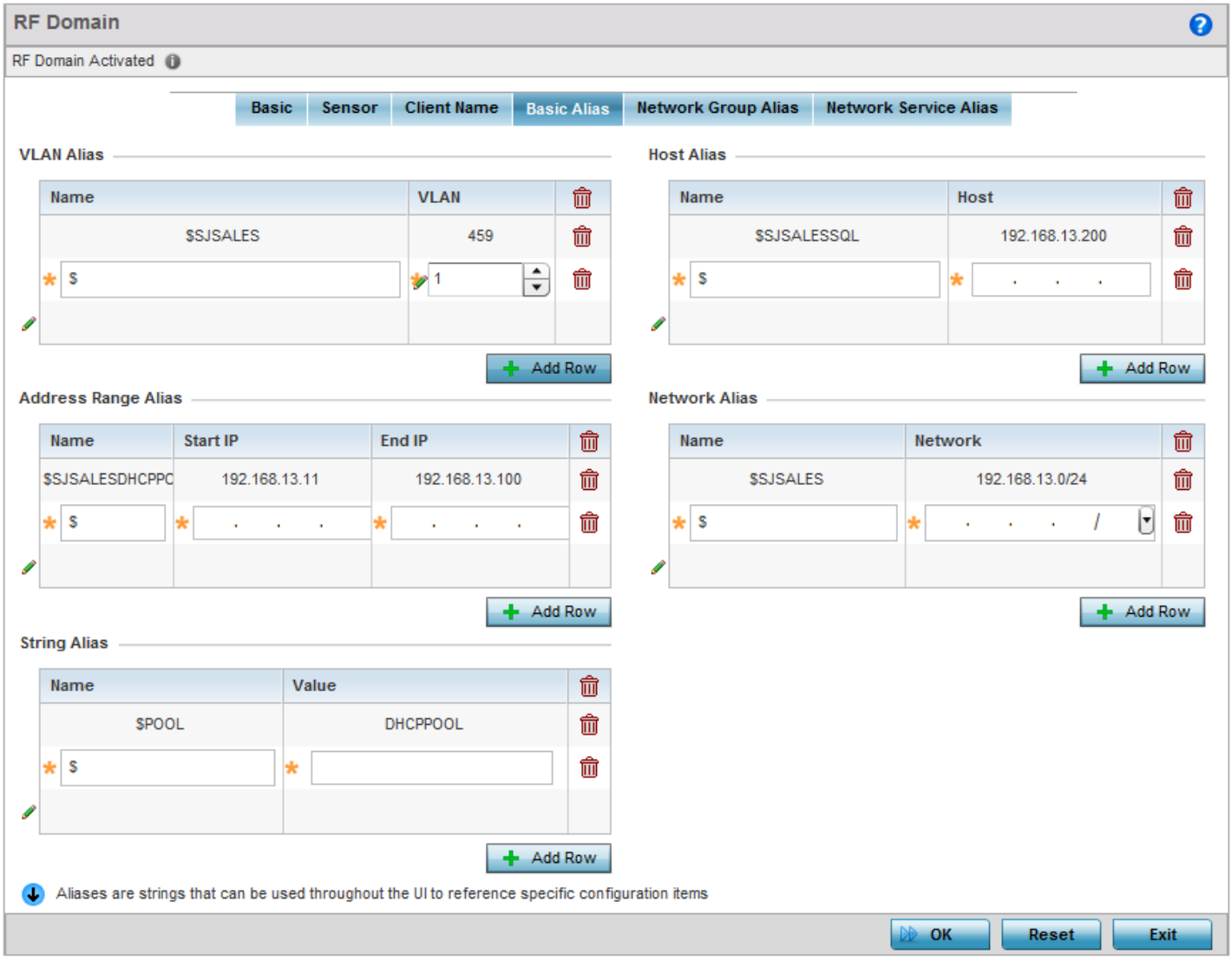


Figure 4: RF Domain - Basic Alias screen

5 Select **+ Add Row** to define **VLAN Alias** settings:

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

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

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

- Bridge VLAN

- IP Firewall Rules
- L2TPv3
- Switchport
- Wireless LANs

6 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 a ending IP address used with a range of addresses utilized with the address range alias.

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

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

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

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

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

- IP Firewall Rules
- DHCP

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

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

- IP Firewall Rules
- DHCP

9 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 string value to use in the alias.

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

10 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

"RF Domain Alias Configuration"

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

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

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

To edit or delete a network alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Devices**.

3 Select **RF Domain.**

4 Select the **Network Group Alias** tab.

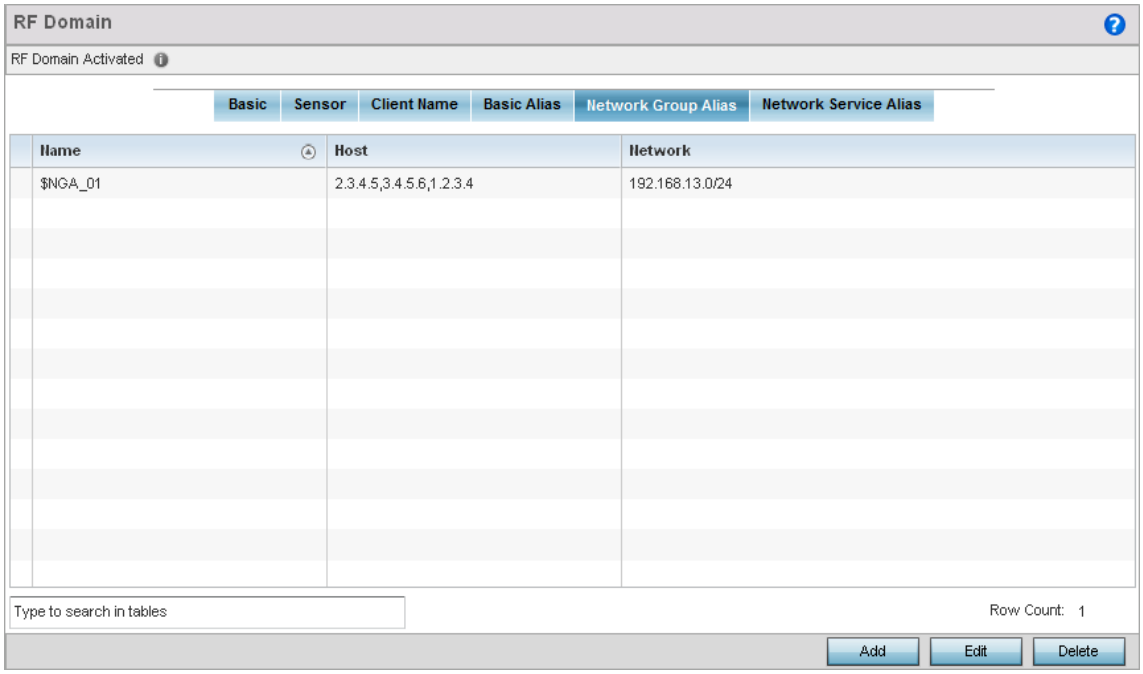


Figure 5: RF Domain - Network Group Alias screen

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

5 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new Network Group Alias. **Copy** to copy an existing policy or **Rename** to rename an existing policy.

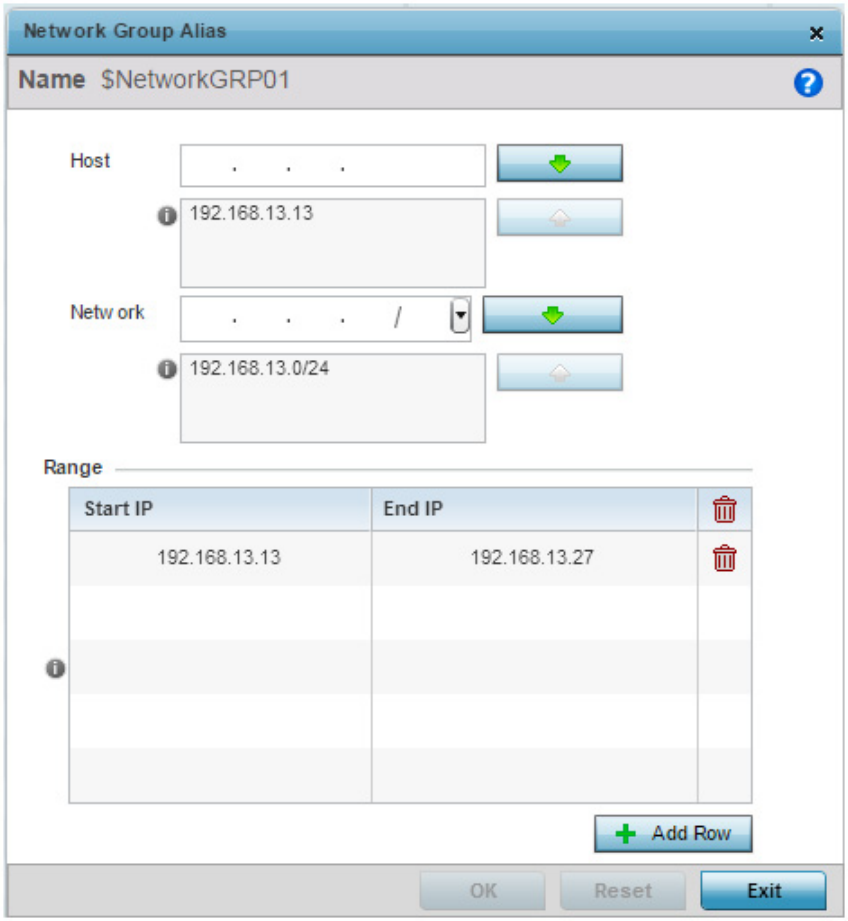


Figure 6: RF Domain - Network Group Alias Add screen

6 If adding a new **Network Group Alias**, provide it a name of up to 32 characters.

NOTE

The **Network Group Alias Name** always starts with a dollar sign ($).

7 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.

8 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 an alias range entry to edit it.

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

Network Service Alias

"RF Domain 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.

Network Service Alias can be used in the following location to substitute protocols and ports:

- IP Firewall Rules

To edit or delete a service alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Devices**.

3 Select **RF Domain.**

4 Select the **Network Service Alias** tab.

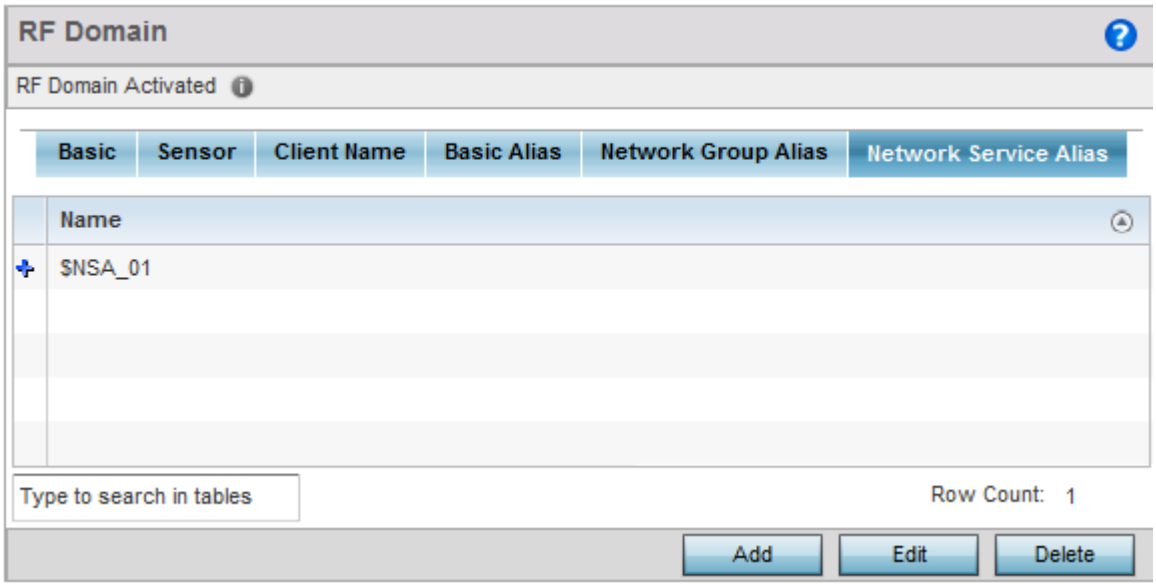


Figure 7: RF Domain - Network Service Alias screen

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

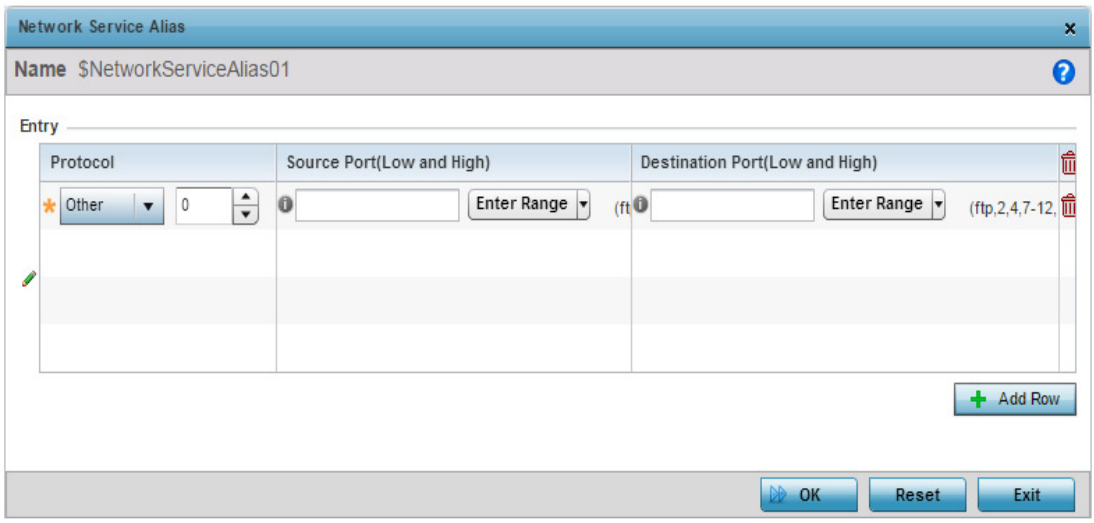


Figure 8: RF Domain - Network Service Alias Add screen

6 If adding a new **Network Service Alias**, provide it a name up to 32 characters.

NOTE

The **Network Service Alias Name** always starts with a dollar sign ($).

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

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

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

System Profile Configuration

"Device Configuration"

An access point profile enables an administrator to assign a common set of configuration parameters and policies to access points of the same model. Profiles can be used to assign common or unique network, wireless and security parameters to across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. All WING 5 supported access point models supported a single profile that is either shared amongst multiple access point or not. The central benefit of a profile is the ability to update access points collectively without having to modify individual configurations.

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

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



NOTE

A central difference compared to the default-radio configurations in previous WiNG 5 releases is default profiles are used as pointers for an access point's configuration, not just templates from which the configuration is copied. Therefore, if a change is made in one of the parameters in a profile, the change is reflected across all access points using that profile.

For more information, refer to the following:

- "General Profile Configuration"
- "Profile Radio Power"
- "Profile Adoption (Auto Provisioning) Configuration"
- "Profile Wired 802.1X Configuration"
- "Profile Interface Configuration"
- "Profile Network Configuration"
- "Profile Security Configuration"
- "Virtual Router Redundancy Protocol (VRRP) Configuration"
- "Profile Critical Resources"

- "Profile Services Configuration"
- "Profile Management Configuration"
- "Mesh Point Configuration"
- "Advanced Profile Configuration"
- "Environmental Sensor Configuration"

General Profile Configuration

- "System Profile Configuration"

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

Network time protocol (NTP) manages time and/or network clock synchronization within the access point managed network. NTP is a client/server implementation. The access point periodically synchronizes its clock with a master clock (an NTP server). For example, the access point resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Use the *General* screen of *System Profile* configuration screen to define whether the access point can act as a RF Domain manager for its RF Domain.

To define a profile's general configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

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

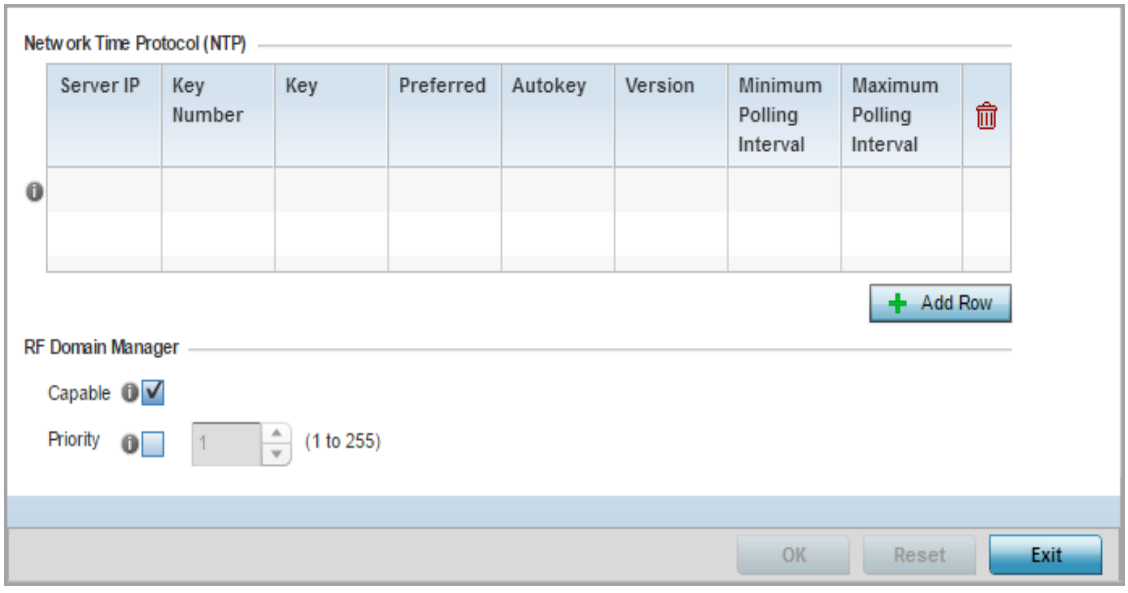


Figure 9: General Profile screen

4 Select **+ Add Row** below the *Network Time Protocol* (NTP) table to define the configurations of NTP server resources used to obtain system time. Up to 3 NTP servers can be configured. Set the following parameters to define the NTP configuration:

Server IP	Set the IP address or hostname of each server added as a potential NTP resource. Use the drop-down located next to this field to select from either *IP Address* or *Hostname*. When *Hostname* is selected, provide the hostname of the NTP server in this field.
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 access point and NTP resource share to securely interoperate.
Preferred	Select this option designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources are given first opportunity to connect and provide NTP calibration.
AutoKey	Select this option 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 which indicates *ignore*.
Minimum Polling Interval	Use the drop-down menu to select the minimum polling interval. Once set, the NTP resource is polled no sooner then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 64 seconds.
Maximum Polling Interval	Use the drop-down menu to select the maximum polling interval. Once set, the NTP resource is polled no later then the defined interval. Options include 64, 128, 256, 512 or 1024 seconds. The default setting is 1024 seconds.

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

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

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

Profile Radio Power

"System Profile Configuration"

Use the *Power* screen to set one of two power modes (*3af* or *Auto*) for the access point profile. When *Automatic* is selected, the access point safely operates within available power. Once the power configuration is determined, the access point configures its operating power characteristics based on its model and power configuration.

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

the access point. The CPLD also determines the access point hardware SKU (model) and the number of radios.

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

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

To define an access point's power configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Power.**

A screen displays where the access point profile's power mode can be defined.

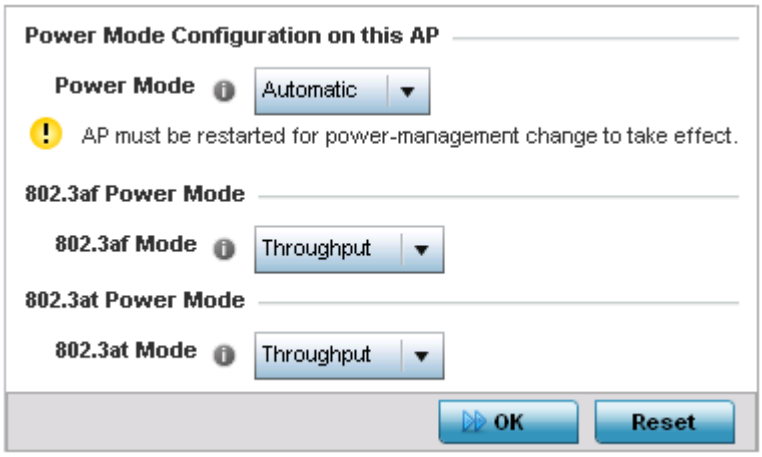


Figure 10: Profile - Power screen

5 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.

6 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.

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

Profile Adoption (Auto Provisioning) Configuration

"System Profile Configuration"

Adoption is the process an access point uses to discover Virtual Controller APs available in the network, pick the most desirable Virtual Controller, establish an association with the Virtual Controller and optionally obtain an image upgrade, obtains its configuration and considers itself provisioned. This is a configurable activity that can be supported within an access point profile and applied to other access points (of the same model) supported by the profile.

At adoption, an access point solicits and receives multiple adoption responses from Virtual Controller APs available on the network. These adoption responses contain loading policy information the access point uses to select the optimum Virtual Controller AP for adoption.



NOTE

An access point configuration does not need to be present for an auto provisioning (adoption) policy to take effect. Once adopted, and the access point's configuration is defined and applied by the Virtual Controller. The auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

To define the access point profile's adoption configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Adoption**.

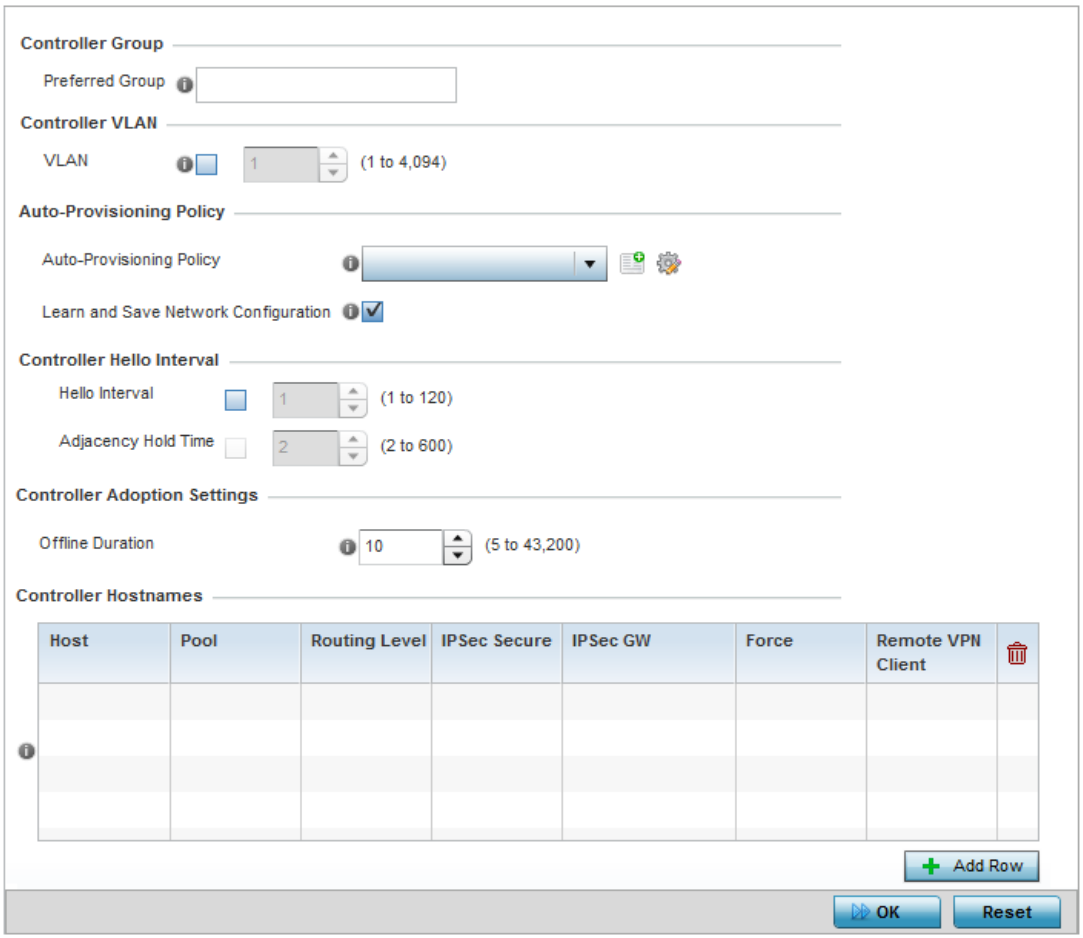


Figure 11: Profile Adoption screen

5 Define the **Preferred Group** used as optimal group of Virtual Controller for adoption. The name of the preferred group cannot exceed 64 characters.

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

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

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

Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.
Learn and Save Network Configuration	Select this option to learn and save the configuration of any device requesting adoption. This setting is enabled by default.

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

The Hello interval is the interval between two consecutive hello keep alive messages exchanged between the access point and the adopting wireless controller. These messages

serve as a connection validation mechanism to ensure the availability of the adopting wireless controller. Use the spinner to set a value from 1 - 120 seconds.

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

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

Host	Use the drop-down menu to specify whether the controller 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 controller to set a pool of either 1 or 2. This is the pool the target Virtual Controller belongs to. The default setting is 1.
Routing Level	Use the spinner controller to set the routing level for the Virtual Controller link. The default setting is 1.
IPSec Secure	Select to enable secure communication between the access point and wireless controllers.
IPSec GW	Use the drop-down menu to specify if the IPSec gateway 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.
Force	Select to enable the link to the adopting controller or the controller group to be created even when not required.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

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

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

Profile Wired 802.1X Configuration

"System Profile 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 **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Wired 802.1x**.

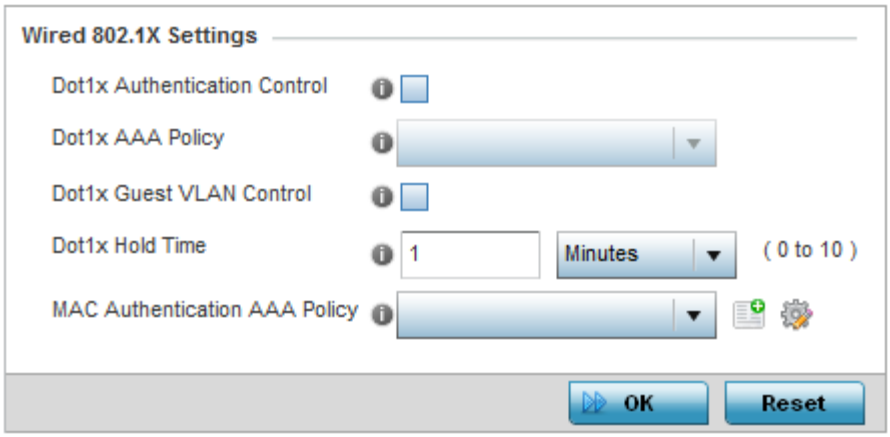


Figure 12: Profile Wired 802.1X screen

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 wired 802.1x traffic. If a suitable AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.
Dot1x Guest VLAN Control	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
Dot1X Hold Time	Set a hold time value (after the last hello packet) in either *Seconds* (0 - 600) or *Minutes* (0 - 10). When exceeded, the controller's 802.1X enabled port and its destination end-point connection is defined as lost and the connection must be re-established.
MAC Authentication AAA Policy	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.

6 Select **OK** to save the changes to the 802.1x configuration. Select **Reset** to revert to the last saved configuration.

Profile Interface Configuration

"System Profile Configuration"

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

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

- "Ethernet Port Configuration"
- "Virtual Interface Configuration"
- "Port Channel Configuration"
- "Access Point Radio Configuration"
- "WAN Backhaul Configuration"

- "PPPoE Configuration"
- "Bluetooth Configuration"

Additionally, deployment considerations and guidelines for profile interface configurations are available for review prior to defining a configuration that could significantly impact the performance of the network. For more information, see "WAN Backhaul Deployment Considerations" on page 140.

Ethernet Port Configuration

"Profile Interface Configuration"

Displays the physical port reporting runtime data and statistics. The following ports are available depending on model:

- AP6521 - GE1/POE (LAN)
- AP6522/AP6522M - GE1/POE (LAN)
- AP6532 - GE1/POE (LAN)
- AP6562 - GE1/POE (LAN)
- AP7131 - GE1/POE (LAN), GE2 (WAN)
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7181 - GE1/POE (LAN), GE2 (WAN)
- AP7502 - GE1, fe1, fe2, fe3
- AP7522- GE1/POE (LAN)
- AP7532 - GE1/POE (LAN)
- AP7562 - GE1/POE (LAN)
- AP8122/AP8132/AP8232/AP8163 - GE1/POE (LAN), GE2 (WAN)
- AP8222/AP8232 - GE1/POE (LAN), GE2 (WAN)

To define a profile's Ethernet port configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

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

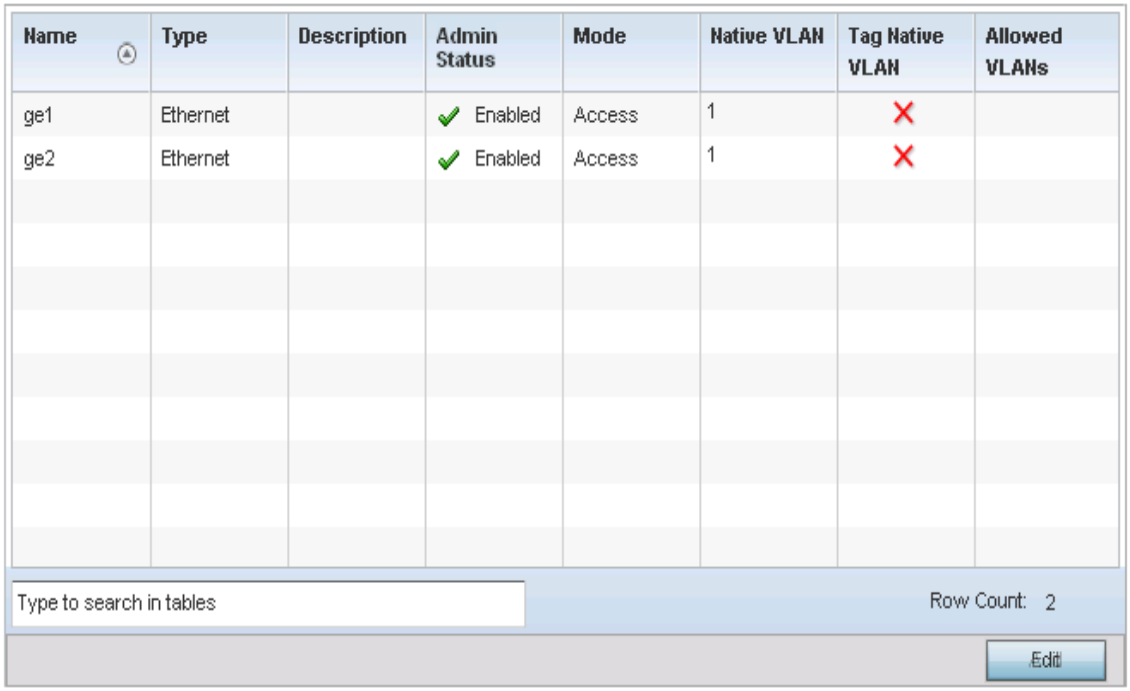


Figure 13: Profile Interfaces - Ethernet Ports screen

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

Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on model.
Type	Displays the physical port type.
Description	Displays an administrator defined description for each listed port.

Admin Status	A green check mark 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 required.
Mode	Displays the profile's current switching mode as either *Access* or *Trunk*. If *Access* is listed, the 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 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 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 the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to *Trunk*.

6 To edit an access point profile's port configuration, select it from amongst those displayed and then select the **Edit** button. The Ethernet port *Basic Configuration* screen displays by default.

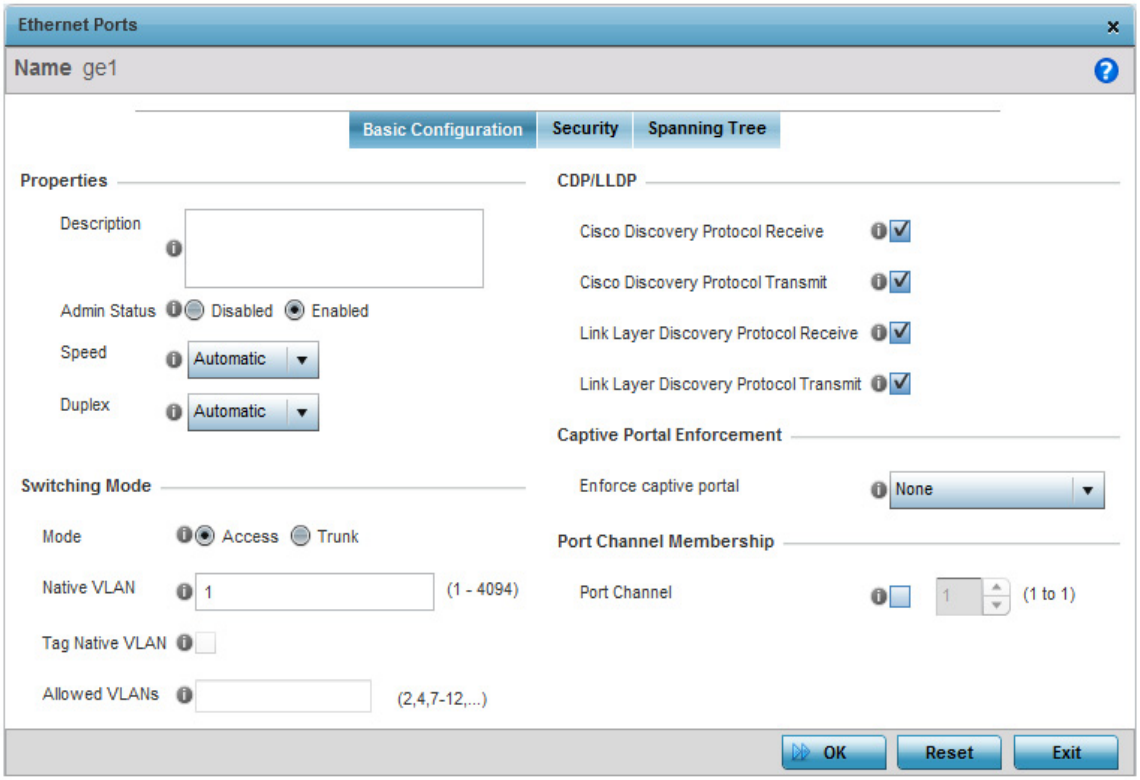


Figure 14: Ethernet Ports - Basic Configuration screen

7 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.
Admin Status	Select the *Enabled* radio button to define this port as active to the 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*, *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 port at the same time. Using full duplex, the port can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port performance needs dictate. Automatic is the default setting.

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 from 1 - 4094. The native VLAN allows the access point 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 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.
Allowed VLANs	Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the listed port.

9 Define the following *Cisco Discovery Protocol* (CDP) and LLDP parameters to apply to the Ethernet port configuration:

Cisco Discover 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. This option is enabled by default.
Cisco Discover 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. This option is enabled by default.
Link Layer Discovery Protocol Receive	Select this option to snoop LLDP 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 transmit LLDP PDUs on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.

10 Select **Enforce Captive Portal** to apply captive portal access permission rules to data transmitted over this specific Ethernet port. Use the drop-down list to select the

appropriate event when to enforce captive portal. Select from *Never*, *Authentication Failure* or *Always*.

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. For information on configuring a captive portal policy, see "Configuring Captive Portal Policies" on page 759.

11 Optionally select the **Port Channel** option and define a setting using the spinner control. This sets the channel group for the port.

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

13 Select the **Security** tab.

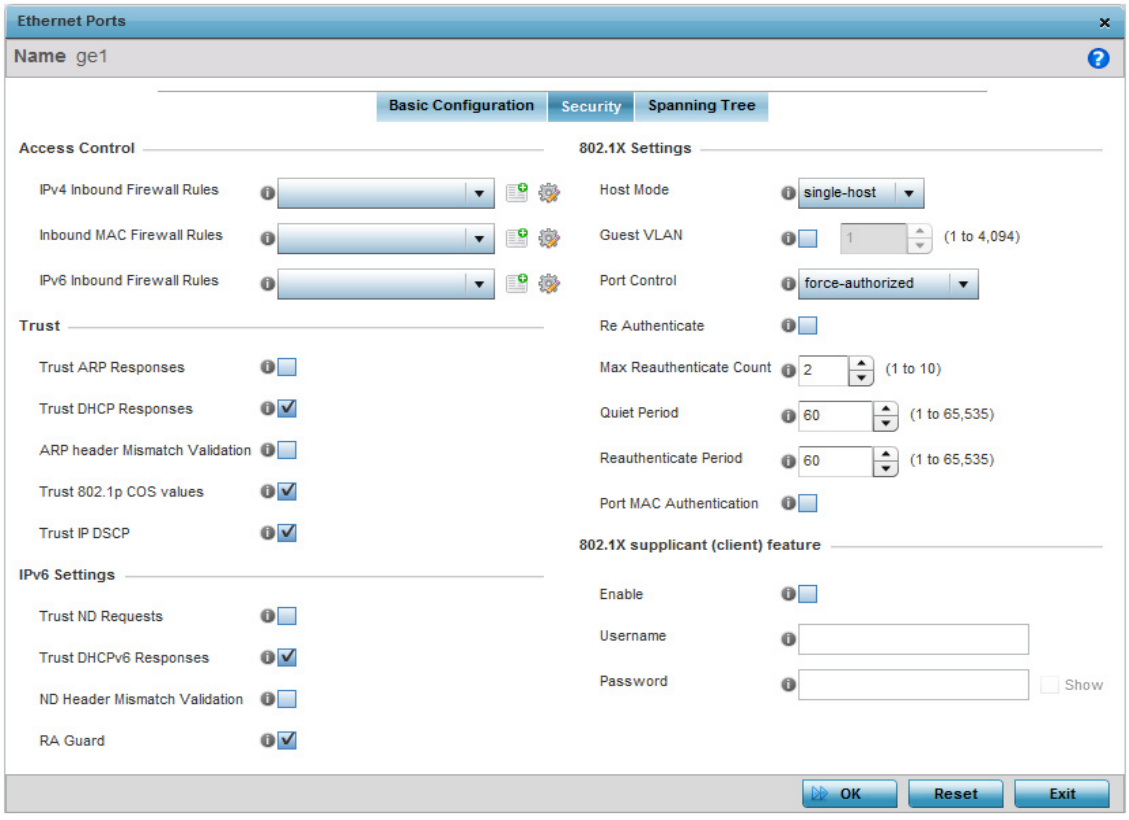


Figure 15: Ethernet Ports - Security tab

14 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 MAC 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.

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 connection less 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. For more information on creating IPv4 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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* (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.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances. For more information on creating IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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.

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

Trust ARP Responses	Select this option to enable ARP trust on this access point 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 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. 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 this option to enable 802.1p COS values on this port. The default value is enabled.
Trust IP DSCP	Select this option 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.

16 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 setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the 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 setting 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 setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This setting is enabled by default.

17 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 port-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.
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 RFS4000, RFS6000 model controllers and NX4500, NX6500 and NX9000 series service platforms. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

18 Select the **Enable** option within the **802.1x supplicant (client) feature** to enable a username and password pair to be used when authenticating users on this port. Use the **Show** option to view the actual characters comprising the password entered in the **Password** field.

19 Select the **Spanning Tree** tab.

Spanning Tree Protocol (STP) (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.

STP calculation happens when a port comes up. As the port comes up and STP calculation happen, 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 there by effecting the network behind the port. Once the STP calculation is complete, the port's state is changed to *Forwarding* and traffic is allowed.

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w standard) is an evolution over the standard STP where the primary aim was to reduce the time taken to respond to topology changes while being backward compatible with STP. *PortFast* quickly changes the port state from *Blocked* to *Forwarding* to allow traffic while the STP calculation occurs.

Multiple Spanning Tree Protocol (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 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 *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST)

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. 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.

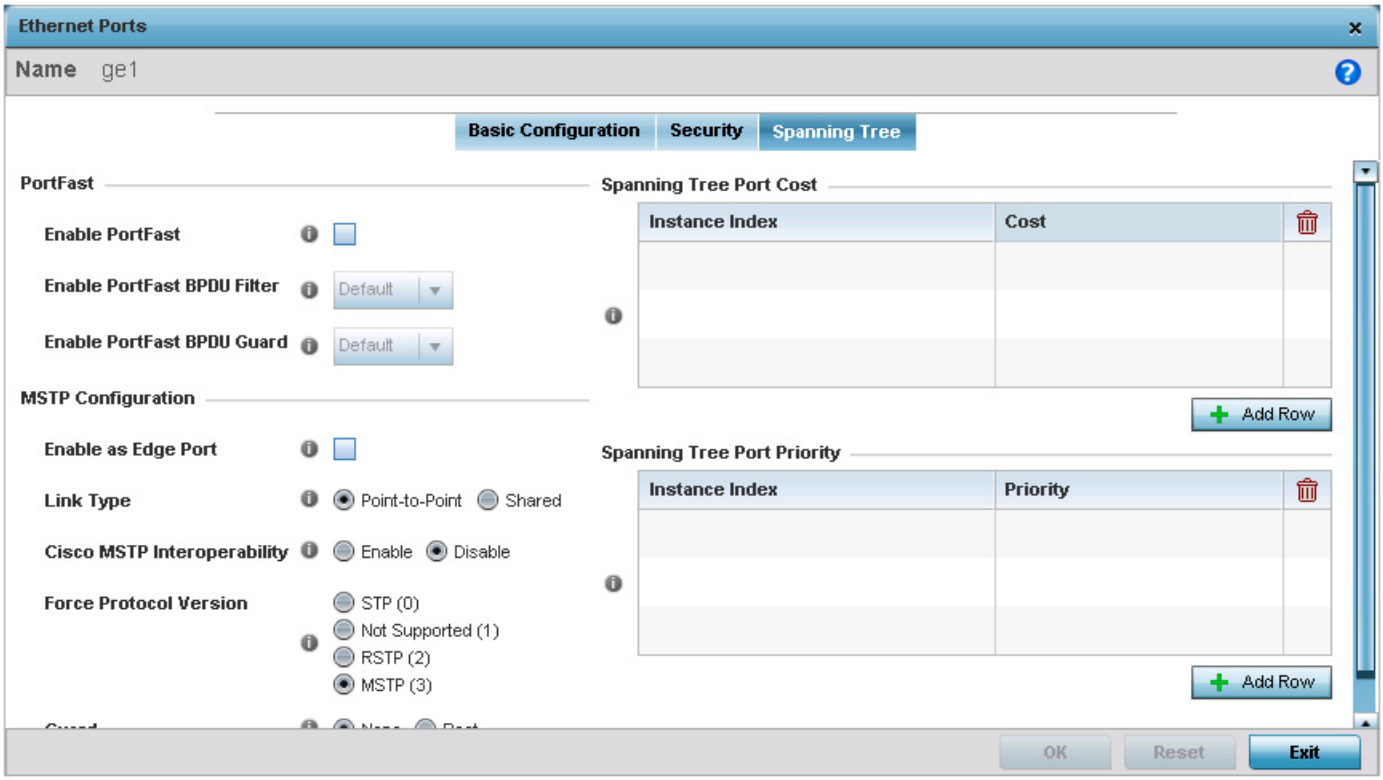


Figure 16: Ethernet Ports - Spanning Tree tab

20 Refer to the **PortFast** field to define the following:

Enable PortFast	PortFast reduces the time taken for a port to complete STP. PortFast must only be enabled on ports on the wireless controller which are directly connected to a server/workstation and not to another hub or controller. PortFast can be left unconfigured on the access point. Select this option to enable drop-down menus for both the *Enable PortFast BPDU Filter* and *Enable PortFast BPDU Guard* options. This setting is disabled by default.
Enable PortFast BPDU Filter	MSTP BPDUs are messages exchanged when controllers gather information about the network topology during STP scan. When enabled, PortFast enabled ports do not transmit or receive BPDU messages. *Default* sets the PortFast BPDU Filter value to the bridge's BPDU filter value. Select *Enable* to invoke a BPDU filter for this PortFast enabled port channel. Set *Disable* to disable this feature.
Enable PortFast BPDU Guard	When set to *Enable*, PortFast enabled ports are forced to shut down when they receive BPDU messages. When set to *Default* sets the PortFast BPDU Guard value to the bridge's BPDU guard value. Set *Disable* to disable this feature.

21 Refer to the **MSTP Configuration** field to define the following:

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* means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point is a point-to-point link. Point-to-Point is the default setting.
Cisco MSTP Interoperability	Select to enable or disable interoperability with CISCO's implementation of MSTP which is incompatible with standard MSTP.
Force Protocol Version	Select the STP protocol to use with this port. Select *Not Supported* to disable STP on this port.
Guard	The Root Guard mechanism prevents election of roots other than those designated as roots in a network. When this port receives a better BPDU, port state becomes *Blocked*. It retains this state till the port no longer receives the better BPDUs and the state is changed to *Forwarding*. Select *Root* to enable this feature. Select *None* to disable this feature.

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

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

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

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

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

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

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

Virtual Interface Configuration

"Profile Interface Configuration"

A Virtual Interface is required for layer 3 (IP) access to provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each VLAN ID the access point 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 networks for routing.

To review existing Virtual Interface configurations and either create a new Virtual Interface configuration, modify an existing configuration or delete an existing configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

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

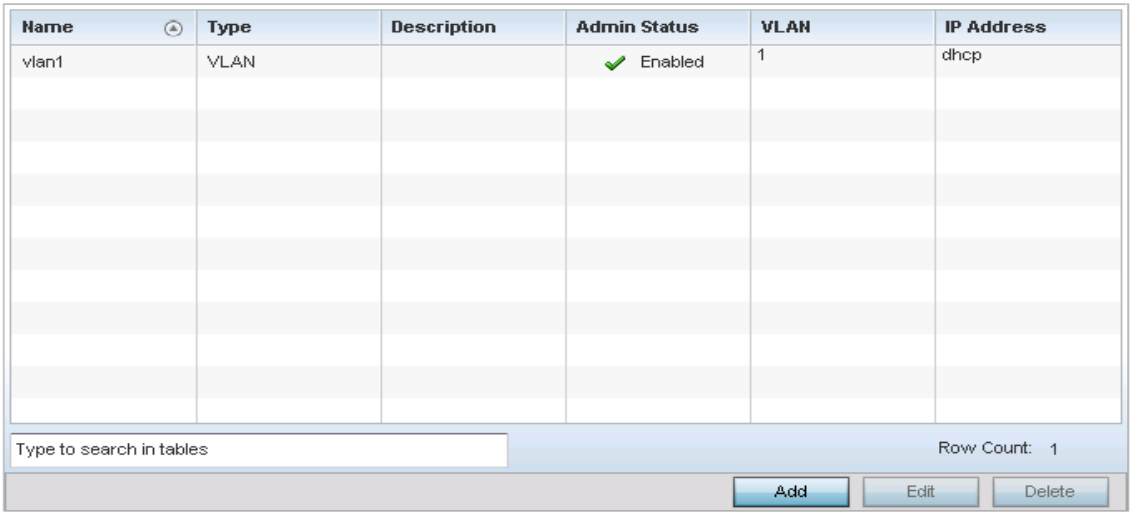


Figure 17: Profile Interfaces - Virtual Interfaces screen

5 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 from 1 - 4094, and cannot be modified as part of a Virtual Interface edit.

Type	Displays the type of Virtual Interface for each listed access point interface.
Description	Displays the description defined for the Virtual Interface when it was either initially created or edited.
Admin Status	A green check mark 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.

Once the configurations of existing Virtual Interfaces have been reviewed, determine whether a new interface requires creation, or an existing Virtual Interface requires edit or deletion.

6 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.

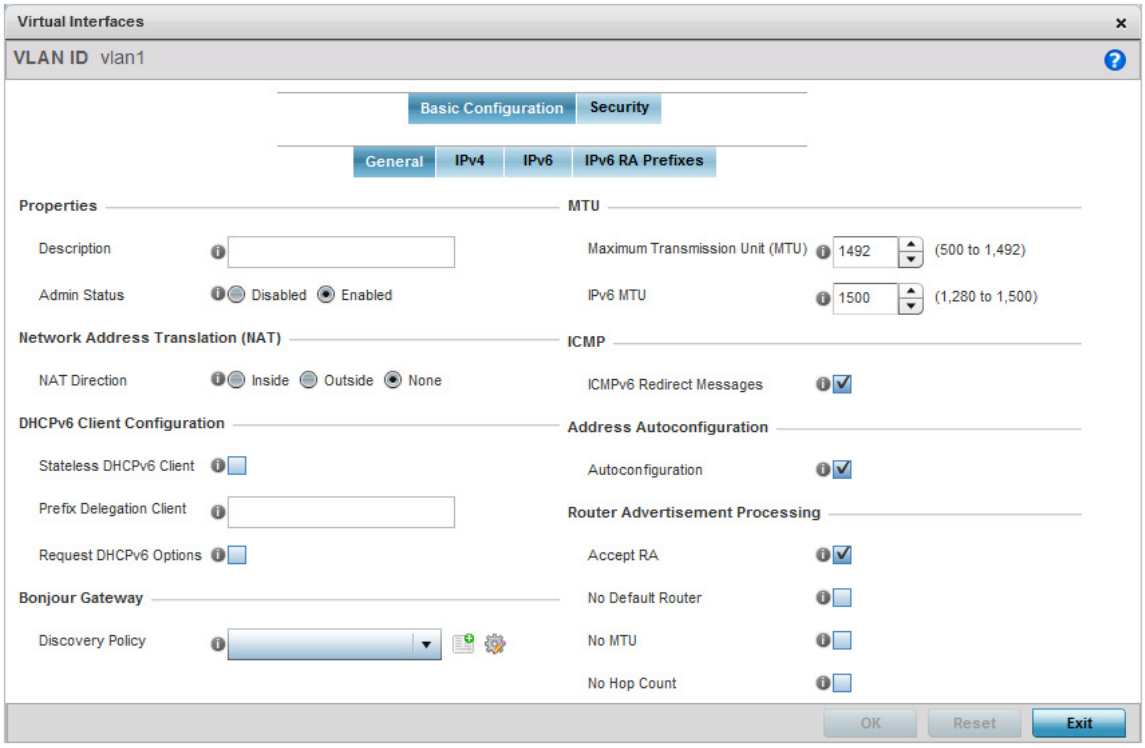


Figure 18: Virtual Interfaces - Basic Configuration tab

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.

7 If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID from 1 - 4094.

8 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.

9 Define the **Network Address Translation (NAT)** direction.

Select either the *Inside*, *Outside* or *None* radio buttons.

- *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.

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

11 Set the following **MTU** settings for the virtual interface:

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.
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.

12 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.

13 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.

14 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 Router Advertisement	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.

15 Use the drop-down menu to define the **Bonjour Gateway Discovery Policy**. Bonjour is Apple's service discovery protocol.

16 Select **OK** button to save the changes to the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.

17 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

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

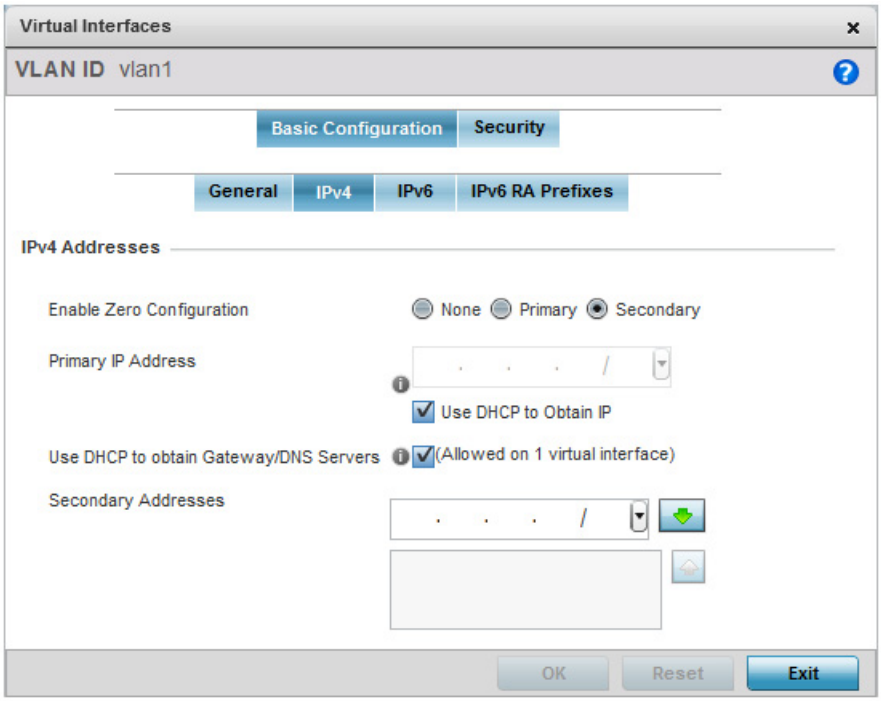


Figure 19: Virtual Interfaces - Basic Configuration screen - IPv4 tab

18 Set the following network information from within 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 the *Secondary Addresses* 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.

19 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

20 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

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. 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

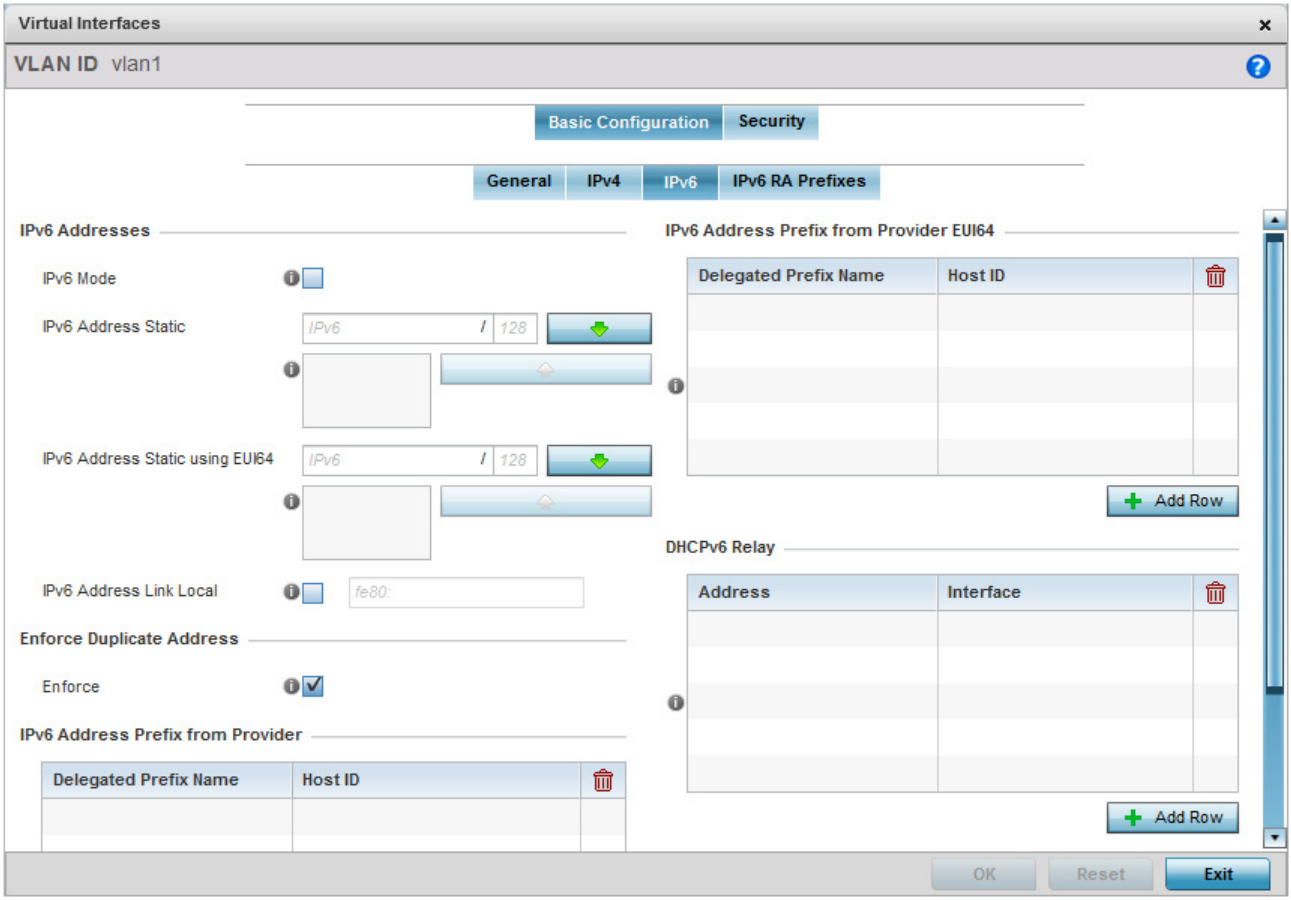


Figure 20: Virtual Interfaces - Basic Configuration screen - IPv6 tab

21 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.

22 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.

23 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 sub screen wherein a new delegated prefix name and host ID can be defined.

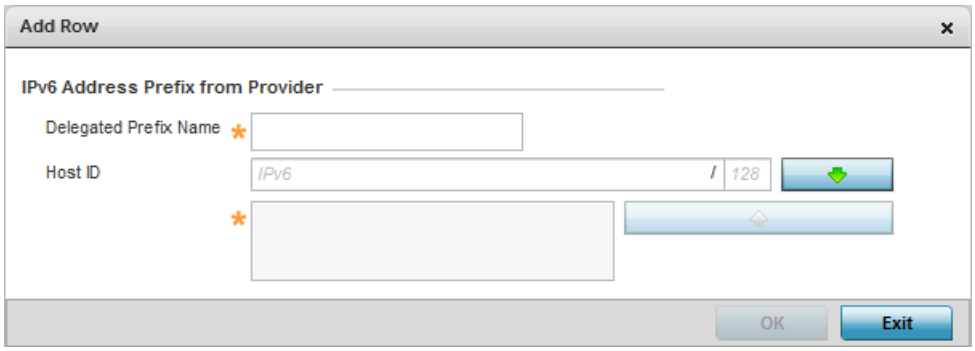


Figure 21: Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider

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.

Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

24 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 sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

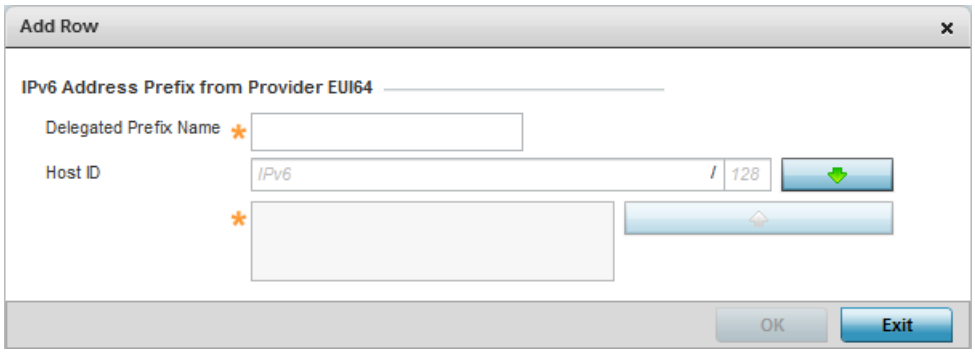


Figure 22: Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64

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.

Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

25 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 sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.



Figure 23: 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.

Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

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

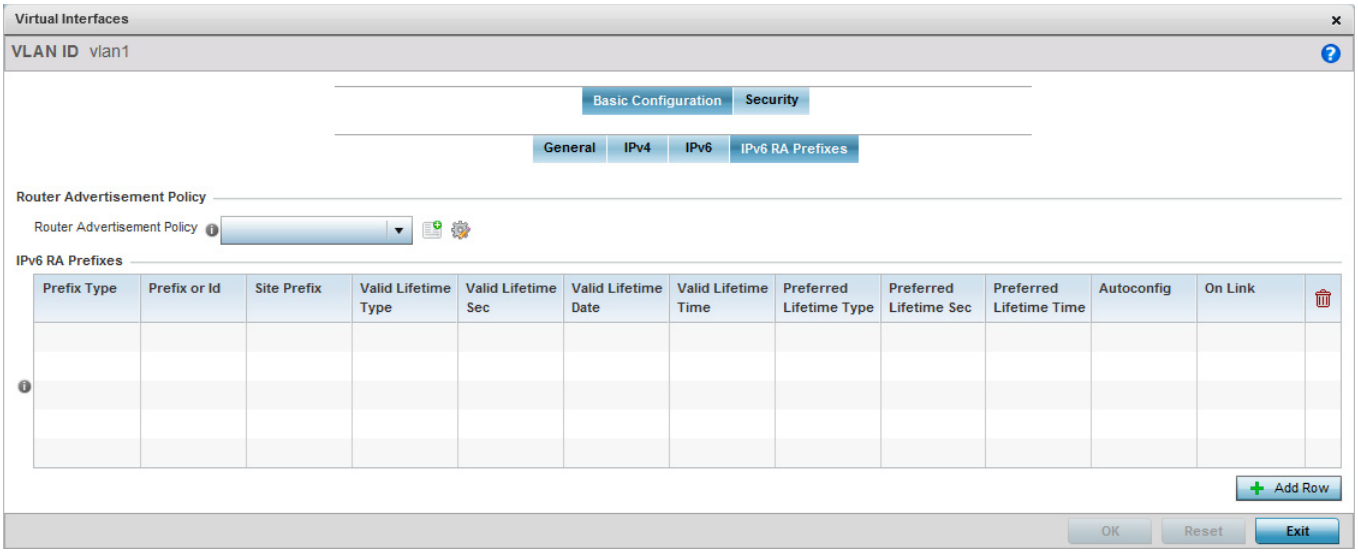


Figure 24: Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab

27 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.

28 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

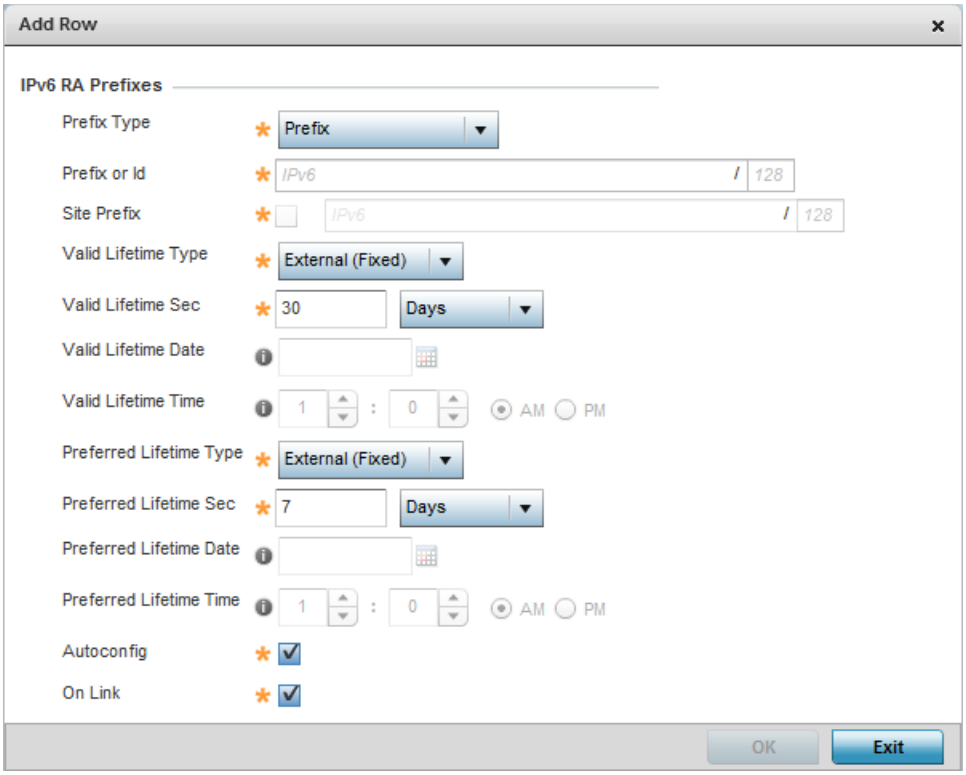


Figure 25: Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix

29 Set 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 *Internet Service Provider* (ISP) 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 measurement 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.

30 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

31 Select the **OK** button to save the changes and overrides to the basic configuration. Select **Reset** to revert to the last saved configuration.

32 Select the **Security** tab.



Figure 26: Virtual Interfaces - Security tab

33 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 creating IPv4 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on creating IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

34 Use the **VPN Crypto Map** drop-down menu to select and assign a VPN crypto map entry to this virtual interface. The VPN Crypto Map entry defines the type of VPN connection and its parameters. For more information, see "Defining Profile VPN Settings" on page 218.

35 Use the **URL Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

Web filtering is used to restrict access to resources on the Internet. For more information on URL filters, see "URL Filtering" on page 692.

36 Select the **OK** button located at the bottom right of the screen to save the changes to the *Security* screen. Select **Reset** to revert to the last saved configuration.

Port Channel Configuration

"Profile Interface Configuration"

The access point's profile can be applied to customize the port channel configurations as part of its interface configuration.

To define a port channel configuration for an access point profile:

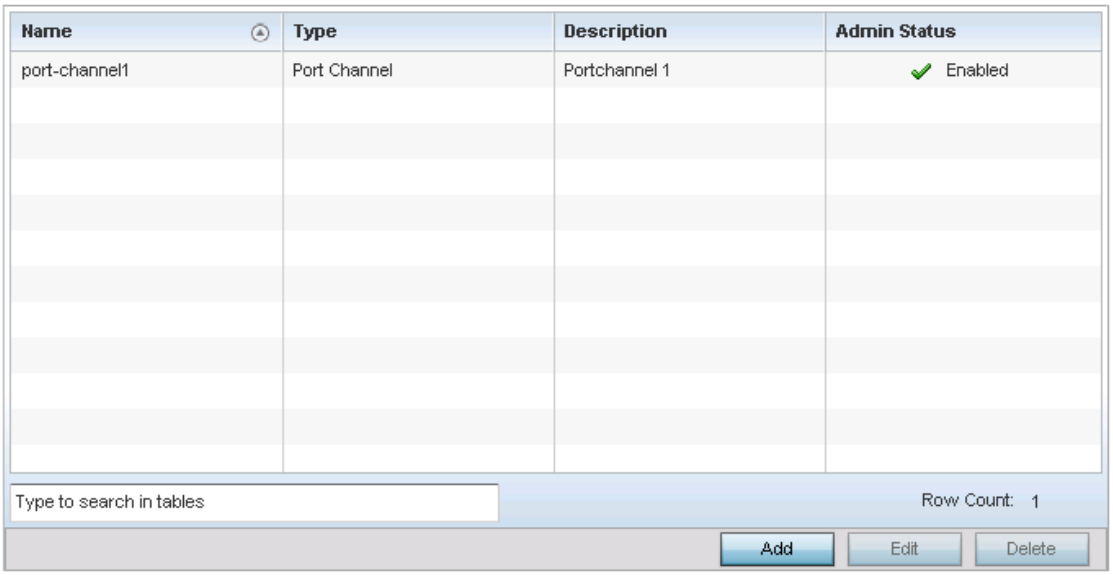


Figure 27: Profile Interfaces - Port Channels screen

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices.**

3 Select **System Profile** from the options on left-hand side of the UI.

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

5 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 a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed port channel as active and currently enabled with the access point's 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

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

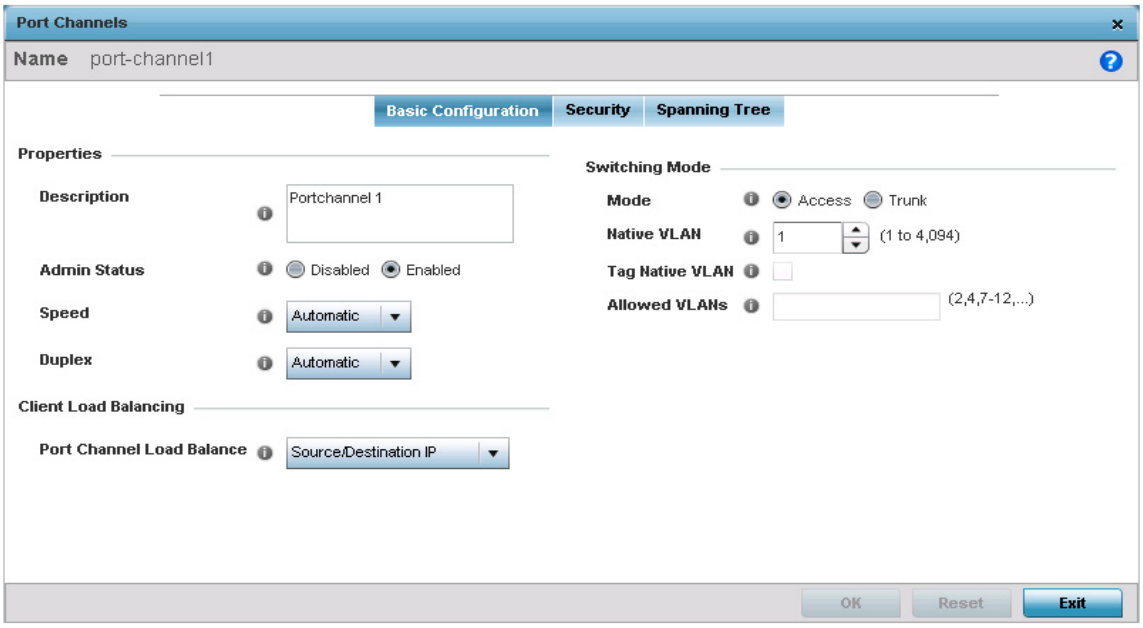


Figure 28: Port Channels - Basic Configuration tab

7 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 controller 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 disabled.
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 Auto 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 enable to the access point to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.

8 Use the **Port Channel Load Balance** drop-down menu within the **Client Load Balancing** field to define whether port channel load balancing is conducted using a *Source/*

Destination IP or a *Source/Destination MAC* as criteria. Source/Destination IP is the default setting.

9 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 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 which 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. Access points 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.

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

11 Select the **Security** tab.

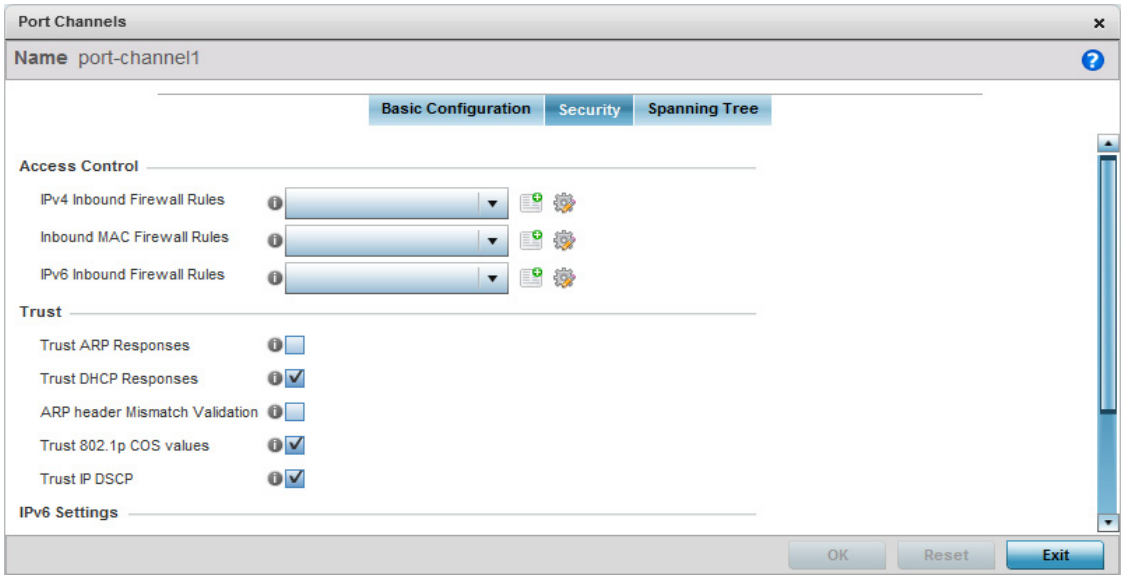


Figure 29: Port Channels - Security tab

12 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 **IPv4 Inbound Firewall Rules, IPv6 Inbound Firewall Rules** and **Inbound MAC Firewall Rules** drop-down menus to select the 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

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. For more information on creating IPv4 firewall rules, see "Configuring IP Firewall Rules" on page 724.

Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on creating IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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.

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

Trust ARP Responses	Select this option 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 managed network. The default value is disabled.
Trust DHCP Responses	Select this option 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 this option 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 this option to enable 802.1p COS values on this port channel. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this port channel. The default value is enabled.

14 Refer to the **IPv6 Settings** field to define the following:

Trust ND Requests	Select the check box 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 the check box 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 the check box to enable a mismatch check for the source MAC in both the ND header and link layer option. The default value is disabled.
RA Guard	Select this option to allow router advertisements or IPv6 redirects from this 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 setting is enabled by default.

15 Select **OK** to save the change

16 s to the security configuration. Select Reset to revert to the last saved configuration.

17 Select the **Spanning Tree** tab.

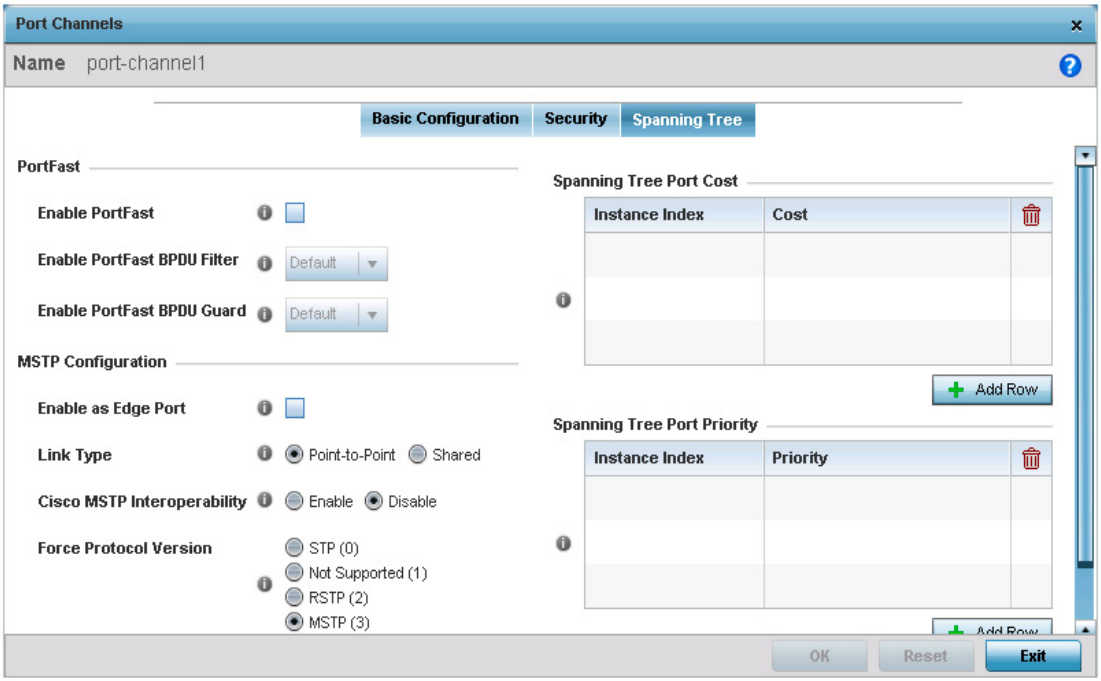


Figure 30: Port Channels - Spanning Tree tab

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

Enable PortFast	PortFast reduces the time required for a port to complete a MSTP state change from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller directly connected to a server/workstation and not another hub or controller. PortFast can be left unconfigured on an access point. Select this option to enable drop-down menus for both the *Enable PortFast BPDU Filter* and *Enable PortFast BPDU Guard* options. This setting is disabled by default.
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 *Default*. Select *Disable* to disable this feature.
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 *Default*. Select *Disable* to disable this feature.

19 Set the following **MSTP Configuration** parameters for the port channel:

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* means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point 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 *Bridge Protocol Data Units* (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.

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

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

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

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

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.

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

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

Access Point Radio Configuration

"Profile Interface Configuration"

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

To define a access point radio configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

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

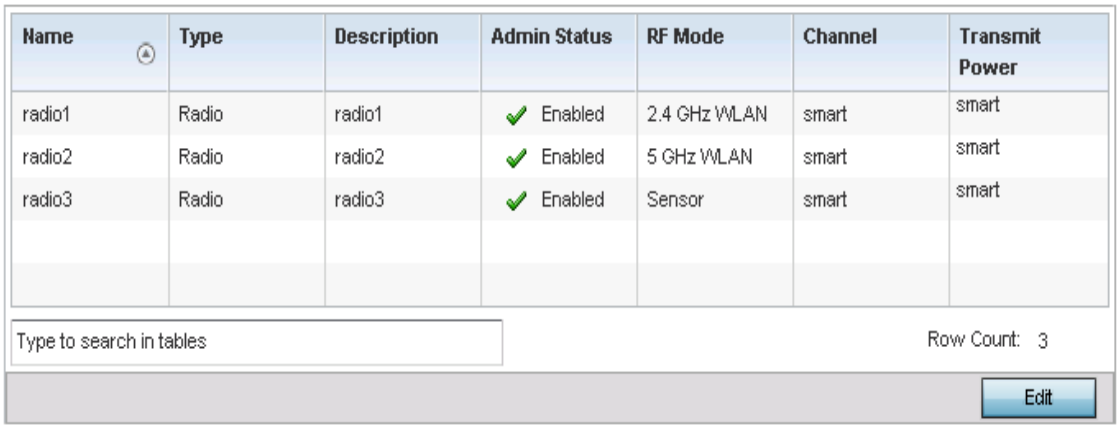


Figure 31: Access Point Radios screen

5 Review the following radio configuration data to determine whether a radio configuration requires modification to better support the network:

Name	Displays whether the reporting radio is radio 1, radio 2 or radio 3. AP6522, AP6522M, AP6532, AP6562, AP8132, AP8232, AP7181 and AP7161 models have 2 radios, while AP6521 model has 1 radio.
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 red "X" defines the radio's status as currently disabled. A green check mark designates the status as enabled.
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 will be listed as a client bridge and does not provide typical 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 will select the channel with the lowest average power level.
Transmit Power	Lists the transmit power for each radio. The column displays *smart* if set for dynamic Smart RF support.

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

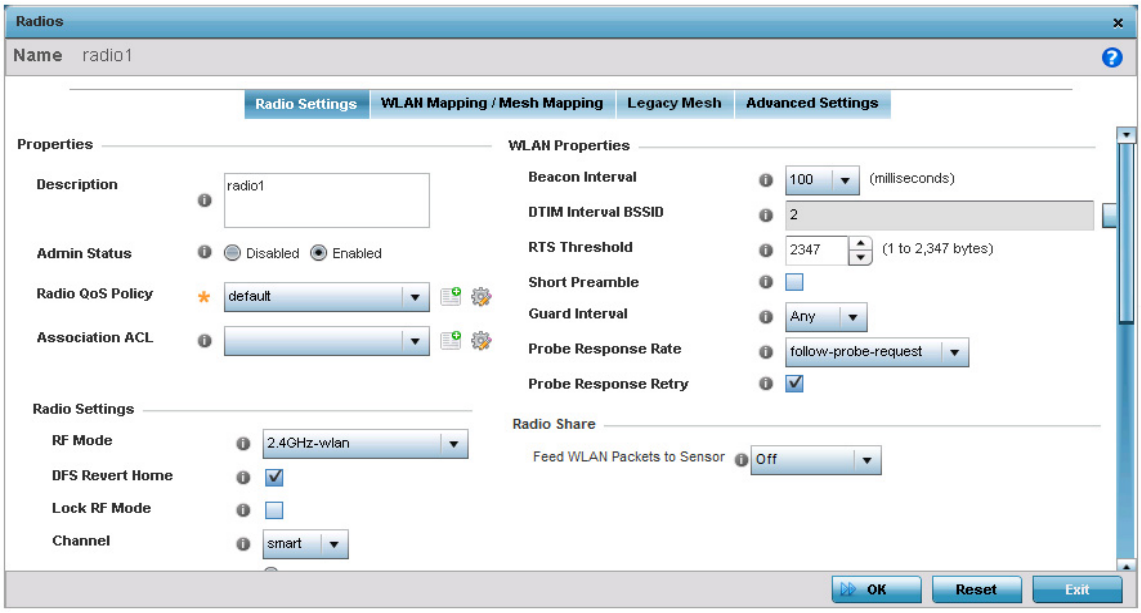


Figure 32: Access Point Radio - Radio Settings tab

The **Radio Settings** tab displays by default.

7 Define the following radio configuration parameters from within the **Properties** field:

Description	Provide or edit a description (1 - 64 characters) for the radio that helps differentiate it from others with similar configurations.
Admin Status	Either select the *Disabled* or *Enabled* radio button to define this radio's current status within the network. When defined as Enabled, the access point is operational and available for client support.
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 Radio QoS Policy exists that suits 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 *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a access point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the packet is compared 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.

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



NOTE

AP6522, AP6522M, AP6532, AP6562, AP8132, AP8232, AP7181 and AP7161 model access points can support up to 256 client connections to a single access point radio. AP6521 model access point (single radio model) can support up to 128 client connections to a single radio.

RF Mode	Set the mode to either *2.4 GHz WLAN* or *5.0 GHz WLAN* support depending on the radio's intended client support. Set the mode to *sensor* if using the radio for rogue device detection. The radio cannot support rogue detection when one of the radios is functioning as a WIPS sensor. To set a radio as a detector, disable Sensor support on the other access point radio. Set the mode to *client-bridge* to configure the radio as a client bridge. A client bridge enables the access point to connect to a 3rd party access point and bridge frames to it.
Lock RF Mode	Select this option to lock Smart RF operation for this radio. The default setting is disabled, as Smart RF utilization will impact throughput.
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 the 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 will select 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, only appear when using an AP8232, and are unique to the 80 MHz band.
DFS Revert Home	Select this option to enable a radio to return back to its original channel. *Dynamic Frequency Selection* (DFS) 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 thirty (30) minutes. When selected, the radio can return back to its original channel of operation once the thirty minute period is over. When not selected, the radio cannot return back to its original channel of operation even after the mandatory thirty minute evacuation period is over.
Transmit Power	Set the transmit power of the selected 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. Set a value in the range 1 - 30 dBm. Set to smart to use Smart RF to determine its output power. The default value is smart.

Antenna Gain	Set the antenna from 0.00 - 30.00 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. It is recommended that only a professional installer 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. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. 1xAll is used when transmission occurs on one antenna and is received on all receiving antennas. The default setting is dynamic based on the access point model deployed and its transmit power settings.
Enable Antenna Diversity	Select this option to enable the radio to have antenna diversity for transmit frames at non 802.11n or 802.11ac data rates. This setting 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 manually set the radio's transmission power (in dBm) to connected clients. The setting 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 drop-down menu populates with rate options depending on the 2.4 or 5.0 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 5.0 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 5.0 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). For more information on the 802.11n rates, see section "MCS Data Rates" on page 137.
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 selected 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 access point radio. The available range is from 1- 256 for AP6522, AP6522M, AP6532, AP6562, AP8132, AP8232, AP7181 and AP7161 models and from 1-128 for AP6521 model.
Rate Selection Methods	Use the drop-down menu to specify the algorithm to use for rate selection. Select *Standard* to use the standard rate selection algorithm. Select *Opportunistic* to use the Opportunistic rate selection algorithm.

9 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. Included in a beacon is information such as the WLAN service area, the radio address, the 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 jitter-sensitive.The default value is 100 milliseconds.
DTIM Interval BSSID	Set a DTIM Interval to specify a period for *Delivery Traffic Indication Messages* (DTIM). 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 acknowledgement, 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 *Request To Send* (RTS) 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 *Clear To Send* (CTS) 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 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 option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink 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 symbols (characters) being transmitted. The guard interval is there to eliminate *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one symbol interfere with another symbol. Adding time between transmissions allows echo's and reflections to settle before the next symbol is transmitted. A shorter guard interval 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 this option to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

10 Use the **Feed WLAN Packets to Sensor** drop-down menu to radio's tap mode of operation. Options include, *Off*, *Inline* and *Promiscuous*. The default setting is Off.

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

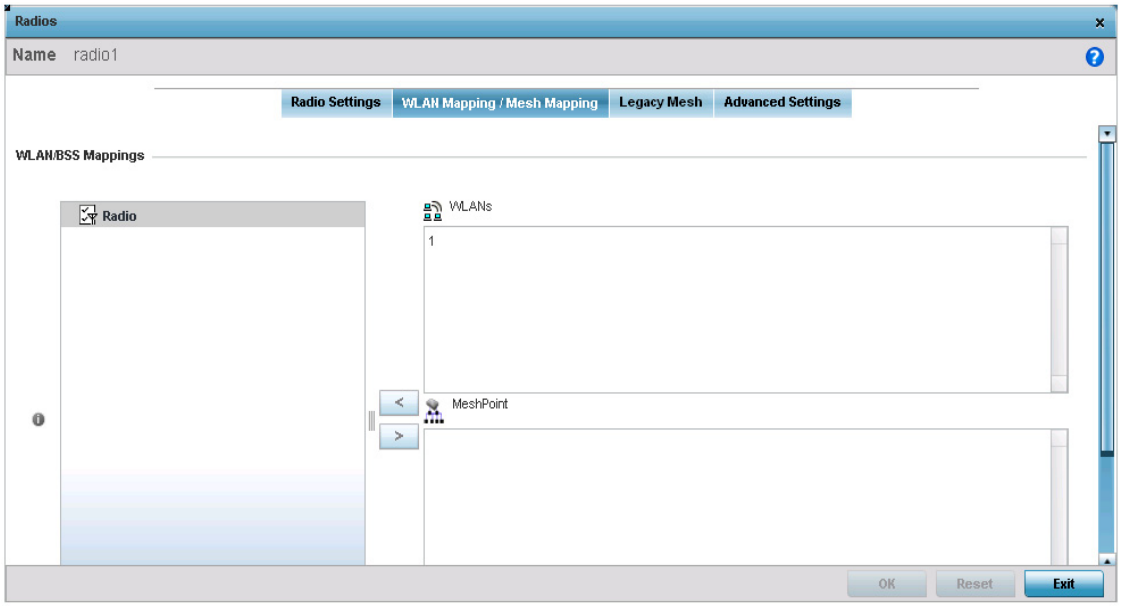


Figure 33: Access Point Radio - WLAN Mapping tab

12 Refer to the **WLAN Mapping/Mesh Mapping** field to set WLAN BSSID assignments for an existing access point deployment.

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.

13 Select **Advanced Mapping** to list all the available BSSIDs for the radio.

14 Select **Create New WLAN** to open a dialog where a new WLAN are created. For more information on creating a WLAN, see "Wireless LANs" on page 527.

15 Select **Create New MeshPoint** to open a dialog where new mesh points are created. For more information on creating a Mesh Point, see "MeshConnex Policy" on page 622.

16 Select the **OK** button located at the bottom right of the screen to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

17 Select the **Legacy Mesh** tab.

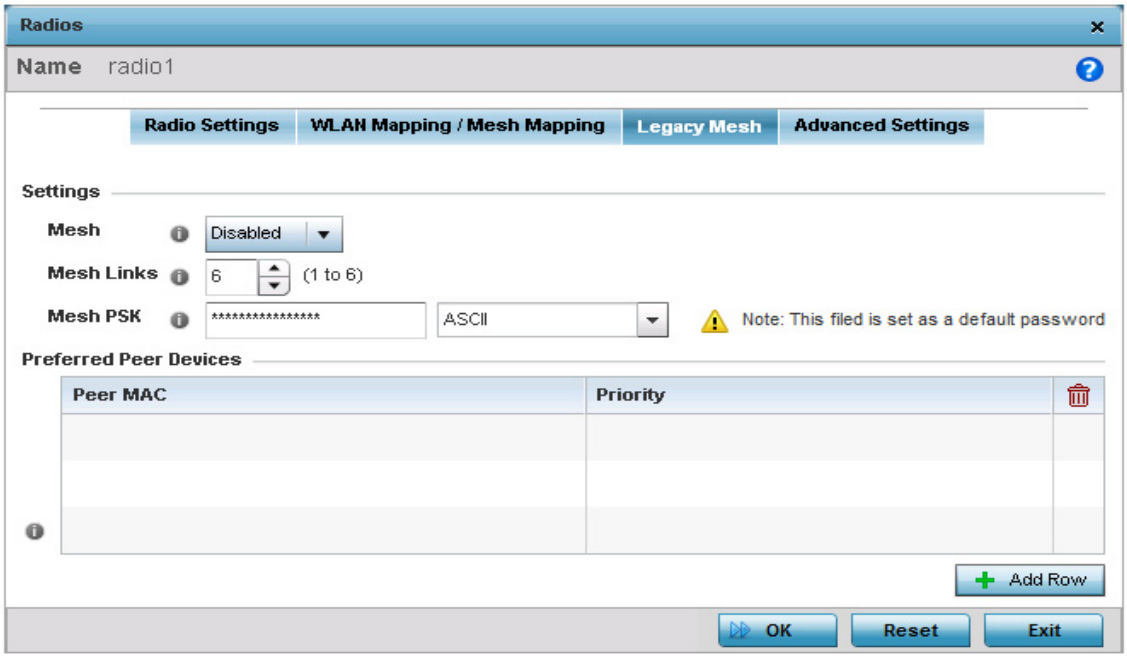


Figure 34: Access Point Radio - Mesh Legacy tab

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

18 Define the following **Mesh Settings:**

Mesh	Options include *Client*, *Portal* and *Disabled*. Select Client to scan for mesh portals, or nodes that have connection to portals, and then connect through them. Portal operation begins beaconing immediately and accepts connections from other mesh supported nodes. Select Portal when setting a mesh connection between two Standalone APs. The default value is Disabled.
Mesh Links	Use the spinner control to define the number of mesh links (1 -6) an access point radio will attempt to create. The default settings is 3 links.
Mesh PSK	Use the text box to enter the mesh's secret key. Select either *ASCII* or *HEX* from the drop-down menu. Click the *Show* option to display the secret key entered in the *Mesh PSK* field.

19 Refer to the **Preferred Peer Devices** table and select **+ Add Row** to define MAC addresses representing peer devices for preferred mesh connection. Use the Priority spinner control to set a priority (1 -6) for connection preference. Up to 6 peer devices can be configured.

20 Select the **OK** button located at the bottom right of the screen to save the changes to the Mesh configuration. Select **Reset** to revert to the last saved configuration.

21 Select the **Advanced Settings** tab.

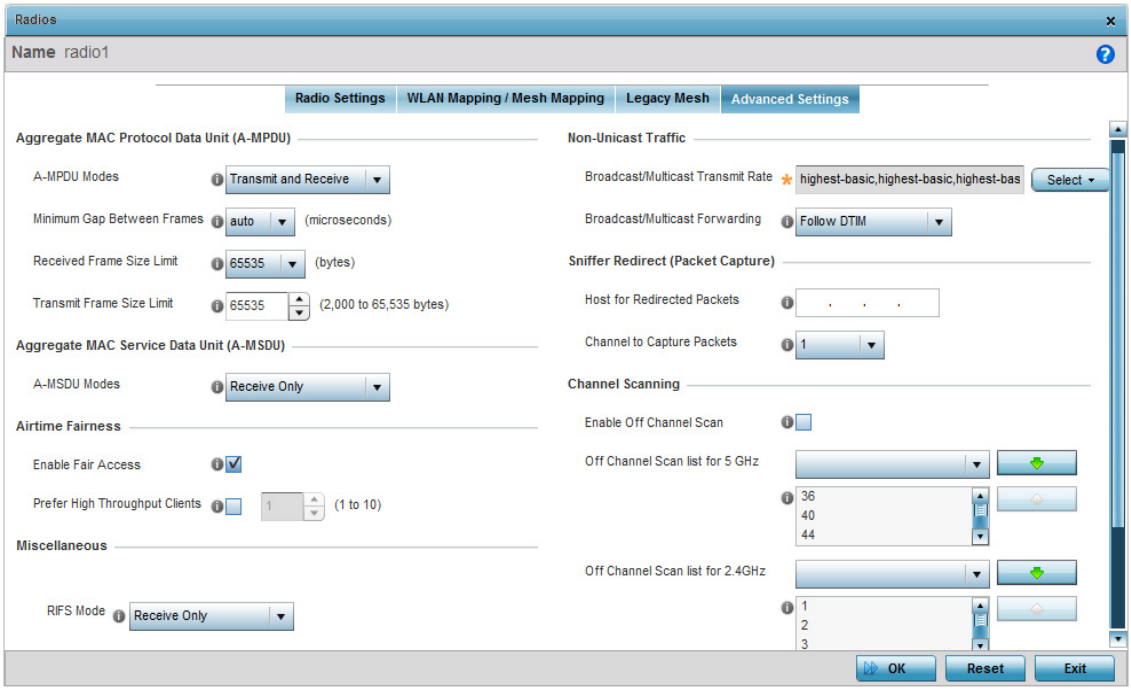


Figure 35: Access Point Radio - Advanced Settings tab

22 Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** 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 the minimum gap between A-MPDU frames (in microseconds). The default value is *auto* which indicates that the minimum gap between frames is selected automatically. The other values are *0, 1, 2, 4, 8* and *16*.
Received Frame Size Limit	If a support mode is enable allowing A-MPDU frames to be received, define an advertised maximum limit for received A-MPDU aggregated frames. Options include 8191, 16383, 32767 or 65535 bytes. The default value is 65535 bytes.
Transmit Frame Size Limit	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is from 2000 - 65,535 bytes). The default value is 65535 bytes.

23 Use the **Aggregate MAC Service Data Unit (A-MSDU)** drop-down menu to set the supported A-MSDU mode.

24 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.

25 Use the **Airtime Fairness** fields to configure wireless access to devices based on their usage.

Select **Enable Fair Access** to enable this feature. Select **Prefer High Throughput Clients** to prefer clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients.

26 Set or override the following **Miscellaneous** advanced radio settings:

RIFS Mode	Define a 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	STBC Mode is available on AP81XX (AP8122, AP8132 and AP8163) model access points only, and is disabled by default. Select a *space–time block coding* (STBC) 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 is 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	Transmit beamforming is available on AP8163 model access points only, and is disabled by default. Enable beamforming to steer signals to peers in a specific direction to enhance signal strength and improve throughput amongst 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.

27 Set the following **Aeroscout Properties** for the selected access point radio:

Forward	Use the Forward option to forward Aeroscout packets to the server.
MAC to be forwarded	Use the text area to provide a MAC address that identifies that the packet is received from Aeroscout tags.

28 Set the following **Ekahau Properties** for the selected access point radio:

Forwarding Host	Use the Forward Host text area to provide the IP address of the Ekahau Engine.
Forwarding Port	Use the Forward Port spinner to configure the port on which to forward captured packets to the Ekahau Engine.
MAC to be forwarded	Use the text area to provide a MAC address that identifies that the packet is received from Ekahau tags.

29 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 *Select* drop-down menu to launch a sub screen 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.

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

31 Select the **Enable Off Channel Scan** radio button to permit scans on non designated channels for this radio. While this affords the access point a greater likelihood of catching an unauthorized device, it does consume more bandwidth. The default setting is disabled. Set the following **Channel Scanning** properties for the selected access point radio:

Off Channel Scan list for 5 GHz	Use the drop-down menu to select the channels to scan in the 5 GHz band when performing off channel scans.
Off Channel Scan list for 2.4 GHz	Use the drop-down menu to select the channels to scan in the 2.4 GHz band when performing off channel scans.
Max Multicast	Use the spinner to set the number of multicast and broadcast packets queued in the radio's queue, when exceeded, off channel scan is skipped during the current scanning interval.
Scan Interval	Use the spinner to set the off channel scan interval in number of dtim periods.
Sniffer Redirect	Use *Sniffer Redirect* text area to provide the IP address of a remote host where the captured off channel scan packets are re-directed.

32 These fields are specific to AP7161 and AP7181 access points:

Enable Antenna Downtilt	Antenna Downtilt is used where there need to be a separation between the 2.4 GHz and 5.0 GHz bands. The 2.4 GHz band is tilted by 15 degrees (up/down tilt) using software. Select to enable downtilt.
Extend Range	Select to enable extending the range of the access points. The access point uses various technologies to extend their service range. Use the spinner to set the range of service. Range can be 1 - 25 Kilometers.

33 Select the **OK** button located at the bottom right of the screen to save the changes to the **Advanced Settings** screen. Select **Reset** to revert to the last saved configuration.

MCS Data Rates

"Access Point Radio Configuration"

802.11n MCS rates are defined as follows both with and without *short guard intervals* (SGI):

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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 Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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

Table 1: 802.11ac MCS rates 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	40MHz With SGI	80 MHz No SGI	80MHz 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

WAN Backhaul Configuration

"Profile Interface 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 point has 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 that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

The following 3G cards are supported:

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

To define a WAN Backhaul configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

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

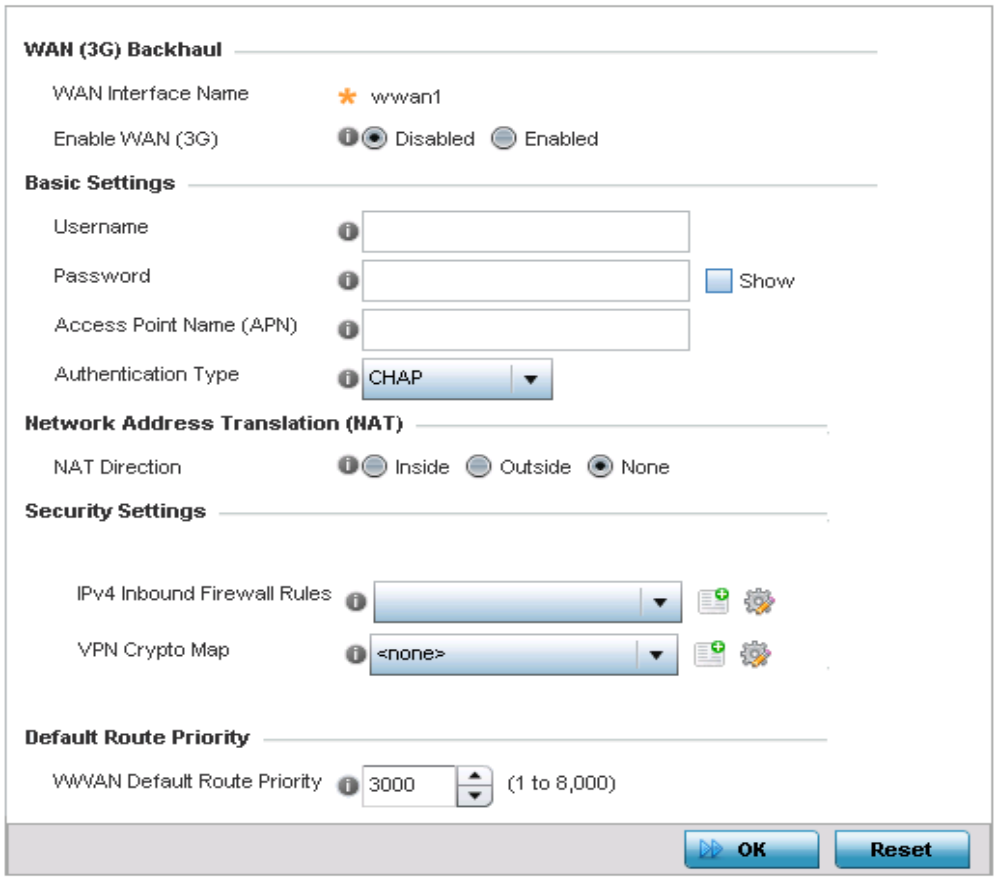


Figure 36: Profile Interface - WAN Backhaul screen

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

WAN Interface Name	Displays the WAN Interface name for the WAN 3G Backhaul card.
Enable WAN (3G)	Select this option to enable 3G WAN card support on the access point. A supported 3G card must be connected for this feature to work.

6 Define the following authentication parameters from within the **Basic Settings** field:

Username	Provide username for authentication support by the cellular data carrier.
Password	Provide password for authentication support by the cellular data carrier.
Access Point Name (APN)	Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols such as Europe, the Middle East and Asia.
Authentication Type	Use the drop-down menu to specify authentication type used by the cellular data provider. Supported authentication options include *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.

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

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

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

10 Use the **WWW Default Route Priority** spinner to set a default route priority for this interface. The default value is 3000.

11 Select **OK** to save the changes to the *Advanced Settings* screen. Select **Reset** to revert to the last saved configuration.

WAN Backhaul Deployment Considerations

"WAN Backhaul Configuration"

Before defining a profile's WAN Backhaul configuration refer to the following deployment guidelines to ensure these configuration are optimally effective:

- If the WAN card does not connect after a few minutes after a *no shutdown*, check the access point's syslog for a *detected ttyUSB0 No such file* event. If this event has occurred, linux didn't detect the card. Re-seat the card.
- If the WAN card has difficulty connecting to an ISP (syslog shows that it retries LCP ConfReq for a long time), ensure the SIM card is still valid and is plugged in correctly.
- If a modem doesn't responding with an OK during the dialing sequence, the WAN card is in an unknown state and will not accept a command. Re-seat the card and begin the dialup sequence again until the card is recognized.
- If encountering a *panic* when conducting a hotplug, power off the access point for one minute. The access point could continue to panic or detect the descriptor of the last utilized WAN card. Thus, it's a good idea to clear the panic state by temporarily disconnecting then re-applying access point power.
- If wanting to unplug the WAN card, ensure sure you shutdown first, as the probability of getting a panic is reduced. With the new high-speed WAN cards currently being utilized, the chances of getting a panic significantly increase.

PPPoE Configuration

"Profile Interface Configuration"

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG supported controllers and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide 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.



NOTE

Access points 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.

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 the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Interface** menu and select **PPPoE**.

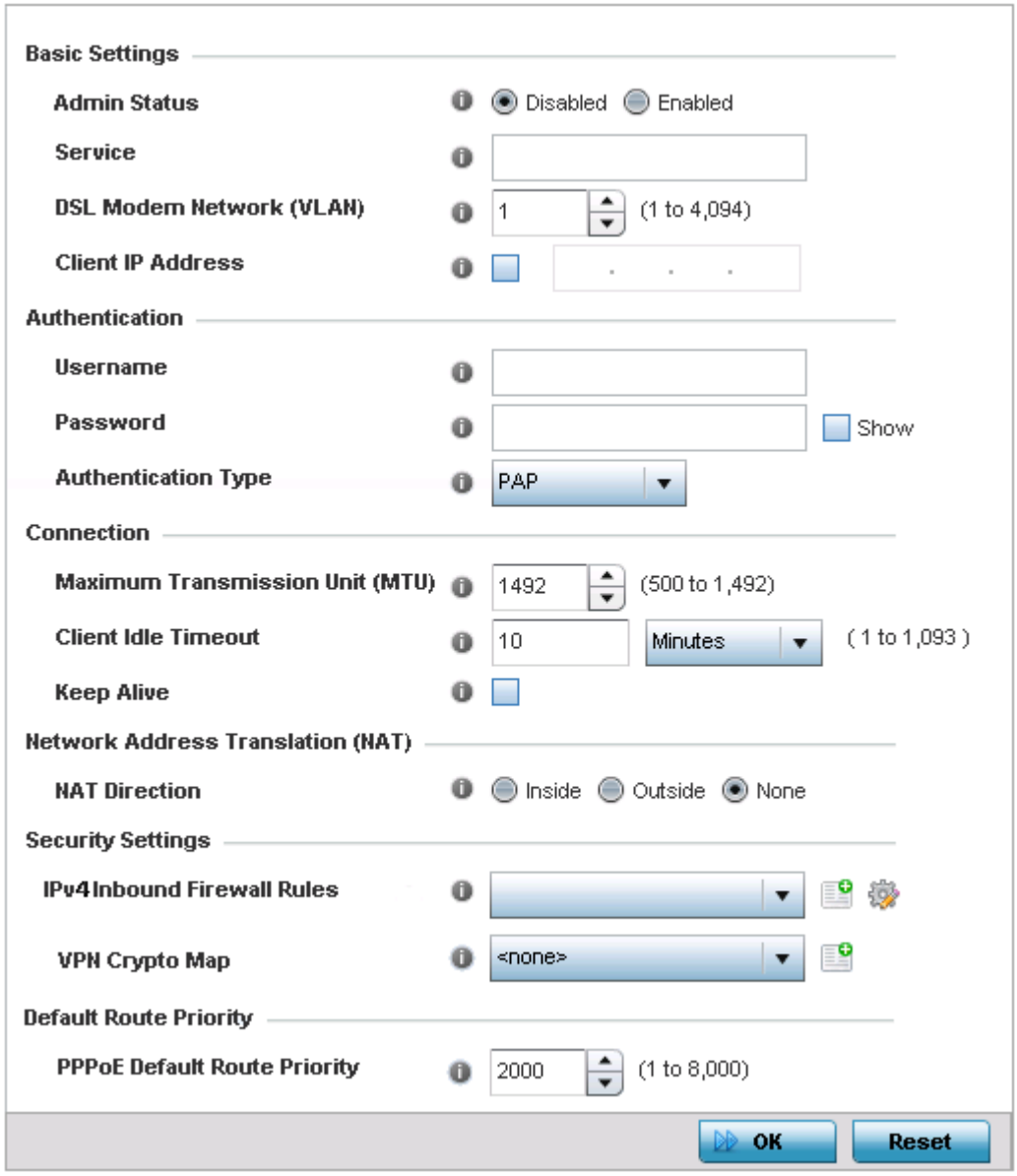


Figure 37: Profile Interface - PPPoE screen

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

Admin Status	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.

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. Use the *Show* option to view the actual characters comprising the password.
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*.

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 - 1,092) 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 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.

Network Address Translation (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 or outside).

9 Define the following **Security Settings** for the PPPoE configuration:

IPv4 Inbound Firewall Rules	Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the *Create* icon to define a new rule configuration or the *Edit* icon to modify an existing rule. For more information, see "Wireless Firewall" on page 709.
VPN Crypto Map	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

10 Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE.

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

11 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.

Bluetooth Configuration

"Profile Interface Configuration"

AP8432 and AP8533 model access point utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP8432 and AP8533 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.



NOTE

AP8132 model access points support an external USB Bluetooth radio providing ADSP Bluetooth sensing functionality only, not the Bluetooth beaconing functionality available for AP8432 and AP8533 model access points described in this section.

AP8432 and AP8533 model access point 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 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 the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Interface** menu and select **Bluetooth**.

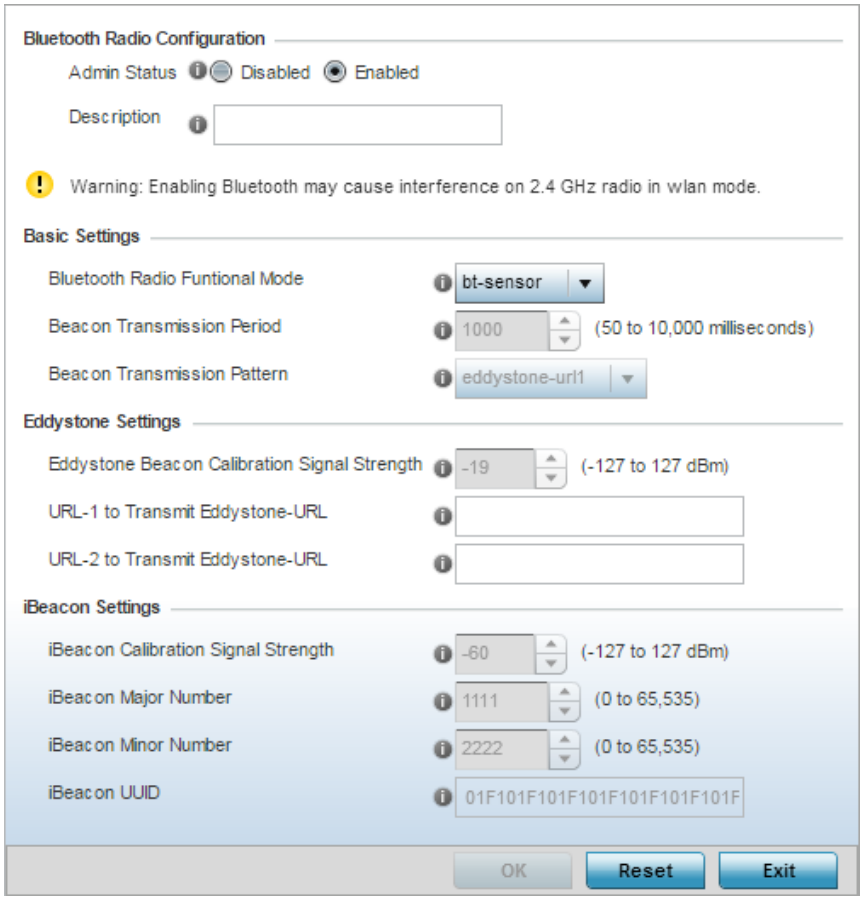


Figure 38: Profile Interface – Bluetooth screen

5 Set the following **Bluetooth Radio Configuration** parameters:

Admin Status	*Enable* or *Disable* Bluetooth support capabilities for AP8432 or AP8533 model access point Bluetooth 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 radios that may be members of the same RF Domain.

6 Set the following **Basic Settings** parameters

Bluetooth Radio Functional Mode	Set the access point's Bluetooth radio functional mode to either *bt-sensor* or *le-beacon*. • *bt-sensors* are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer Bluetooth low energy technology supported devices. • *le-beacons* are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors. le-beacon is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. As the defined period increases, so does the CPU processing time and the number packets incrementally transmitted (typically one per minute). The default setting is 1,000 milliseconds.
Beacon Transmission Pattern	When the Bluetooth radio's mode is set to *le-beacon*, use the enabled drop-down menu to set the beacon's emitted transmission pattern to one of *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. If an eddystone-URL beacon broadcasts https:anysite, then clients receiving the packet can access that URL. iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). There are three data fields Apple has made 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 the Beacon Transmission Pattern has been set to either eddystone_url_1 or eddystone_url_2:

Eddystone Beacon Calibration Signal Strength	Set the Eddystone Beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm.
URL-1 to Transmit Eddystone-URL	Enter a 64 character maximum Eddystone-URL1. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.
URL-2 to Transmit Eddystone-URL	Enter a 64 character maximum Eddystone-URL2. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.

8 Define the following **iBeacon Settings** if the Beacon Transmission Pattern has been set to iBeacon:

iBeacon Calibration Signal Strength	Set the ibeacon measured calibration signal strength, from -127 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 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 *Universally Unique IDentifier* (UUID) classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes. For example, f2468da6-5fa8-2e84-1134-bc5b71e0893e. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

9 Select **OK** to save the changes to the Bluetooth configuration. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

Profile Network Configuration

"System Profile Configuration"

Setting an access point profile's network configuration is a large task comprised of numerous administration activities.

An access point profile network configuration process consists of the following:

- "DNS Configuration"
- "ARP"
- "L2TPv3 Profile Configuration"
- "IGMP Snooping"
- "MLD Snooping"
- "Quality of Service (QoS)"
- "Spanning Tree Configuration"
- "Routing"
- "Dynamic Routing (OSPF)"
- "Forwarding Database"
- "Bridge VLAN"
- "Cisco Discovery Protocol Configuration"
- "Link Layer Discovery Protocol Configuration"
- "Miscellaneous Network Configuration"

- "Alias"
- "IPv6 Neighbor Configuration"

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" on page 217.

DNS Configuration

"Profile Network 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 does not 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 is 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 (www.domainname.com).

To define the DNS configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **DNS**.

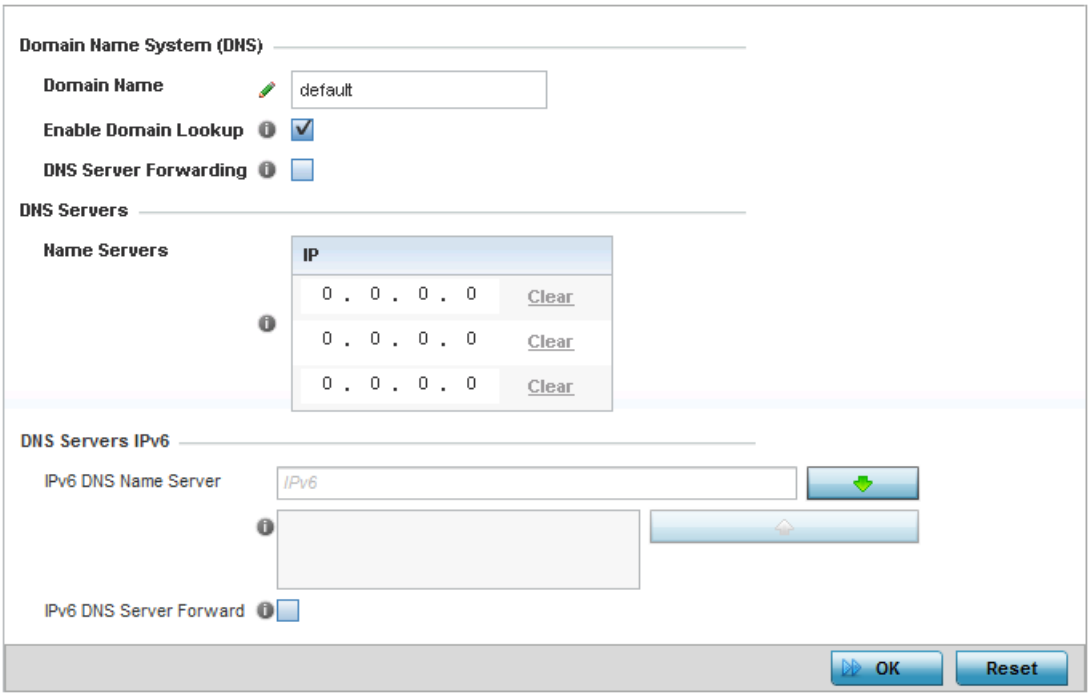


Figure 39: Network - DNS screen

5 Provide a default **Domain Name** used when resolving DNS names. The name cannot exceed 64 characters.

6 Set the following DNS configuration data:

Enable Domain Lookup	Select this option to enable DNS. When enabled, human friendly domain names can be converted into numerical IP destination addresses. This feature is enabled by default.
DNS Server Forwarding	Select to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by the access point's own DNS resources. This feature is disabled by default.

7 In the **Name Servers** field, provide the IP addresses of up to three DNS server resources available to the access point.

8 Set the following **DNS Servers IPv6** configuration data when using IPv6:

IPv6 DNS Name Server	Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted.
IPv6 DNS Server Forward	Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default.

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

ARP

"Profile Network 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, the gateway uses ARP 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 the destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply. 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 the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **ARP**.

5 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.

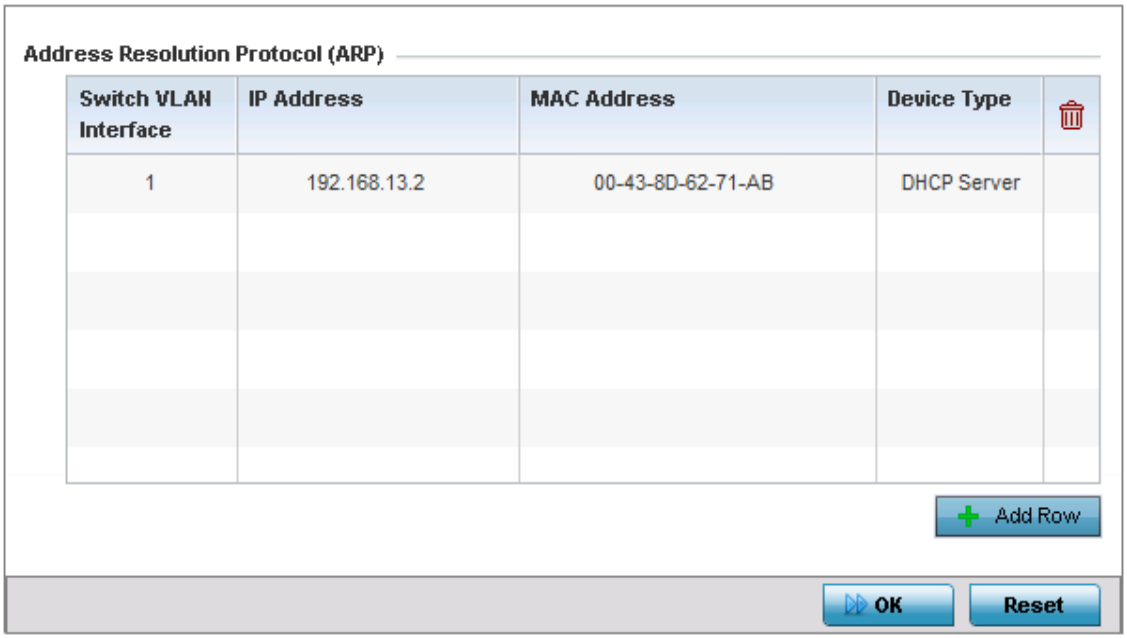


Figure 40: Network - ARP screen

6 Set the following parameters to define the ARP configuration:

Switch VLAN Interface	Use the spinner control to select a VLAN for an address requiring resolution.
IP Address	Define the IP address used to fetch a MAC Address.
MAC Address	Displays the target MAC address that's subject to resolution. This is the MAC used for mapping an IP address to a MAC address that's recognized on the network.
Device Type	Specify the device type the ARP entry supports (*Host*, *Router* or *DHCP Server*). Host is the default setting.

7 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 Profile Configuration

"Profile Network Configuration"

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point 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 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 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 *packet-switching network* (PSN). 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 L2TPV3 configuration for an access point profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **L2TPv3**.

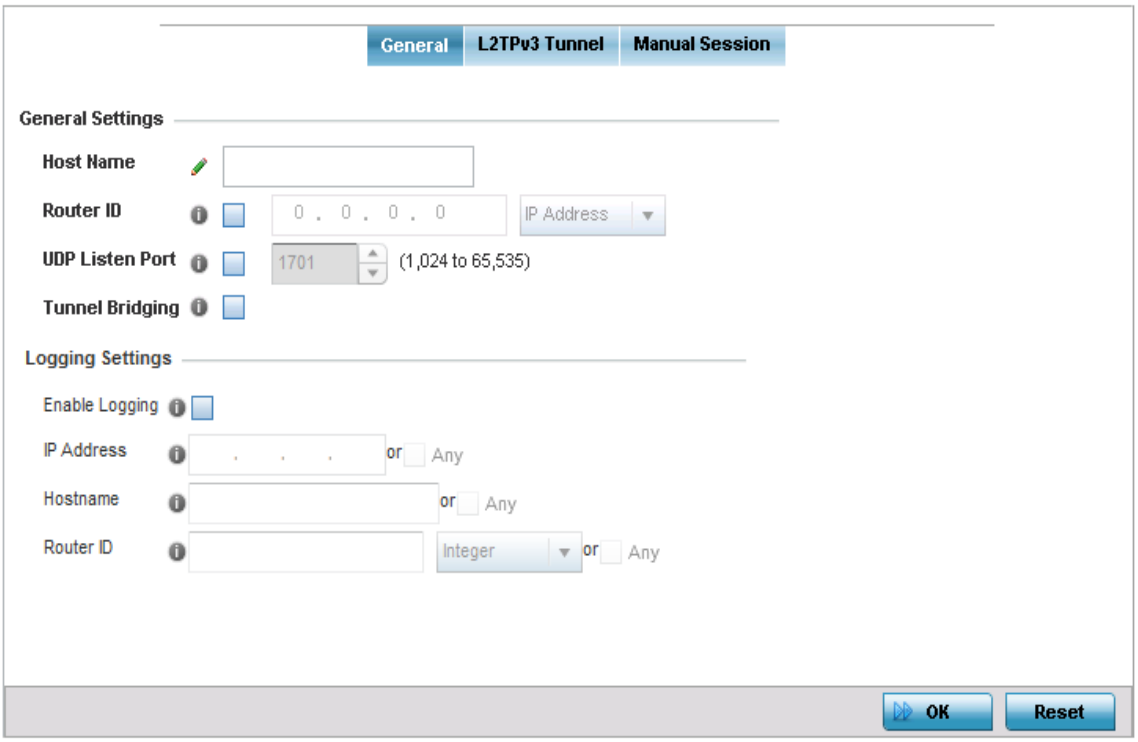


Figure 41: Network - L2TPv3 screen - General tab

5 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.

6 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.

7 Select the **L2TPv3 Tunnel** tab.

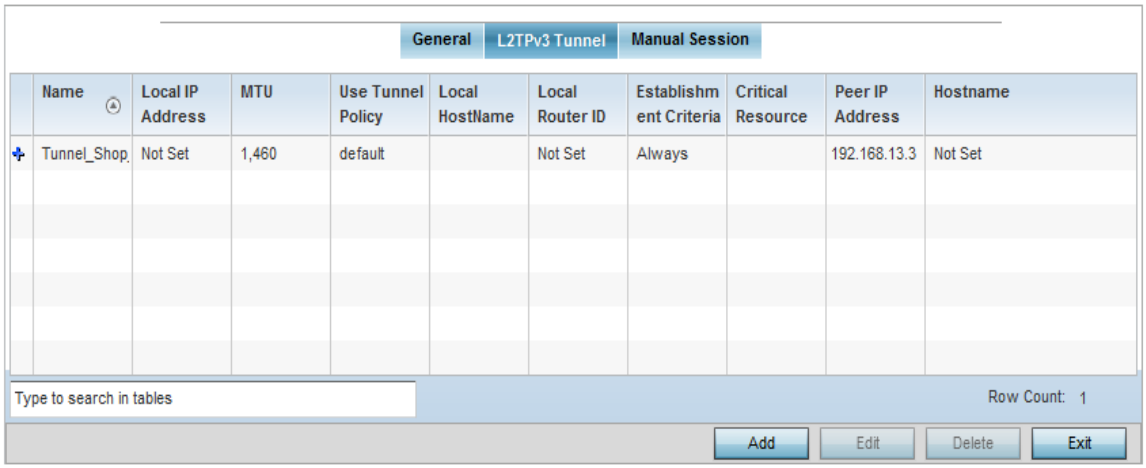


Figure 42: Network - L2TPv3 screen - L2TPv3 tunnel tab

8 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 *maximum transmission unit* (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.

9 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.

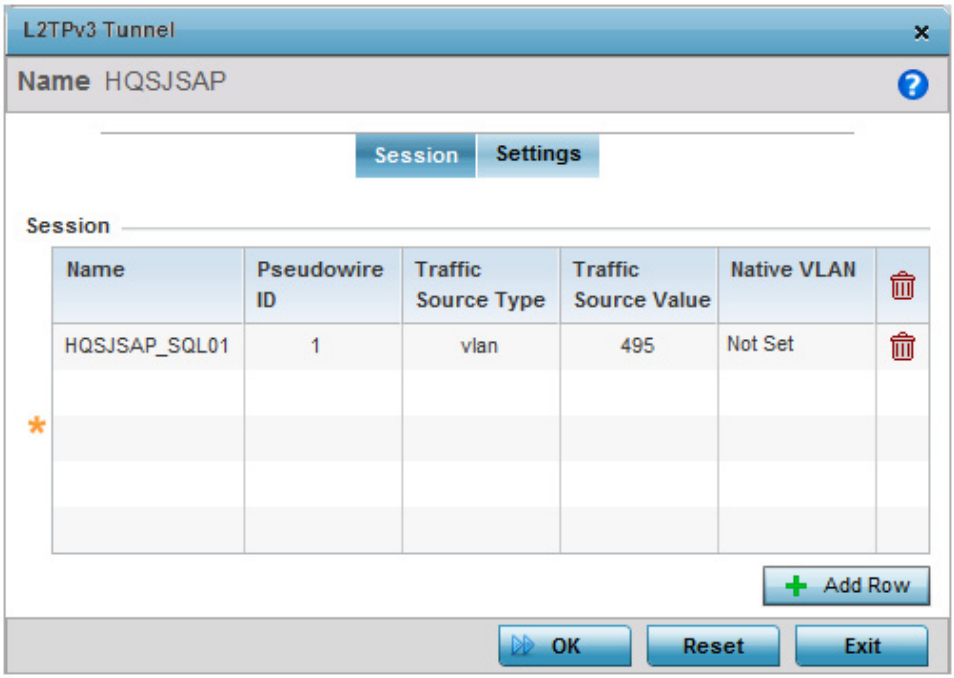


Figure 43: Network - L2TPv3 screen - Add L2TPv3 Tunnel Configuration

10 If creating a new tunnel configuration, assign it a 31 character maximum **Name**.

11 Refer to the **Session** table to review the configurations of the peers available for tunnel connection.

12 Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

13 Define the following **Session** parameters:

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 *packet-switching network* (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 tunnelled 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.

14 Select the **Settings** tab.

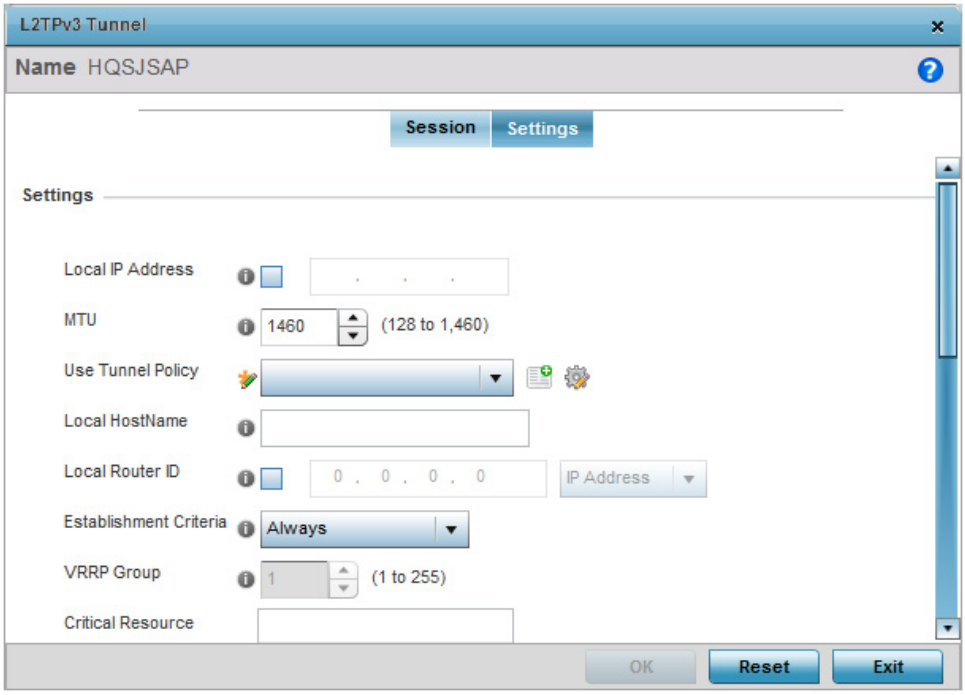


Figure 44: Network - L2TPv3 screen - Add L2TPv3 Tunnel Configuration - Settings screen

15 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 *maximum transmission unit* (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU between 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data.
Use Tunnel Policy	Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available a new policy can be created or an existing one can be modified. For more information, refer to "L2TP V3 Configuration" on page 657.
Local Hostname	Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages.
Local Router ID	Specify the router ID sent in tunnel establishment messages with a potential peer device.
Establishment Criteria	Configure establishment criteria for creating a tunnel between the device and the NOC. This criteria ensures only one tunnel is created between two sites where the tunnel is established between the vrrp-master/cluster master/rf-domain manager at the remote site and the controller at the NOC. The tunnel is created based on the role of the remote peer. • *always* – The tunnel is always created irrespective of the role of the local device. • *vrrp-master* – The tunnel is only created when the local device is a VRRP master. • *cluster-master* – The tunnel is only created when the local device is a cluster master. • *rf-domain-manager* – The tunnel is only created when the local device is a RF-Domain manager. In all the above cases, if the local device goes offline for any reason, the tunnel is brought down.
VRRP Group	This field is enabled only when the *Establishment Criteria* is set to *vrrp-master*. Use the spinner to select the VRRP group.
Critical Resource	Enter the critical resources required for creating and maintaining a L2TPV3 tunnel. A tunnel is only established when all critical resources for the tunnel to be operational are available at the time when the tunnel is created. If any one of the listed critical resources goes down, the tunnel is disabled. When a tunnel is established, the listed critical resources are checked for availability. Tunnel establishment is started if the critical resources are available. Similarly, for incoming tunnel termination requests, listed critical resources are checked and tunnel terminations are only allowed when the critical resources are available. For more information on managing critical resources, see "Profile Critical Resources" on page 257.

16 Define the following **Rate Limit** settings for the L2TP tunnel configuration. 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%.

17 Refer to the **Peer** table to review the configurations of the peers available for tunnel connection.

Select **+ Add Row** to populate the table with a maximum of two peer configurations.

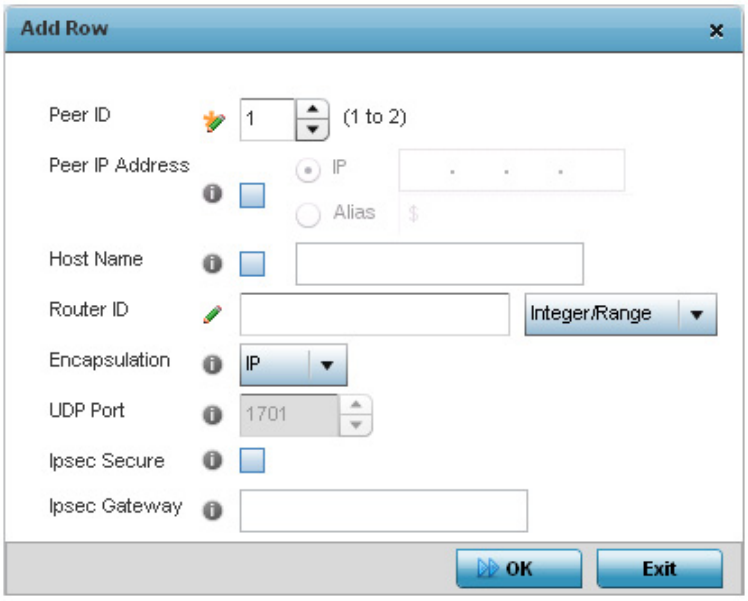


Figure 45: Network - L2TPv3 screen - Add L2TPv3 Peer Configuration

18 Define the following **Peer** parameters:

Peer ID	Define the primary peer ID used to set the primary and secondary peer for tunnel failover. 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.
Peer IP Address	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment. Select the check-box to enable the option to either provide an IP address or an alias for this field.
Host Name	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process.
Router ID	Specify the router ID sent in tunnel establishment messages with this specific peer.
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.
IPSEC Secure	Select this option to provide IPSEC security for the tunnel.
IPSEC Gateway	Enter the IP address/Hostname for the IPSEC gateway.

19 Select **OK** to save the peer configuration.

20 From the **L2TPv3 Tunnel** screen's **Settings** tab, configure the **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.

21 Select **OK** to save the changes within the L2TPv3 Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.

22 Select the **Manual Session** tab.

After 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.

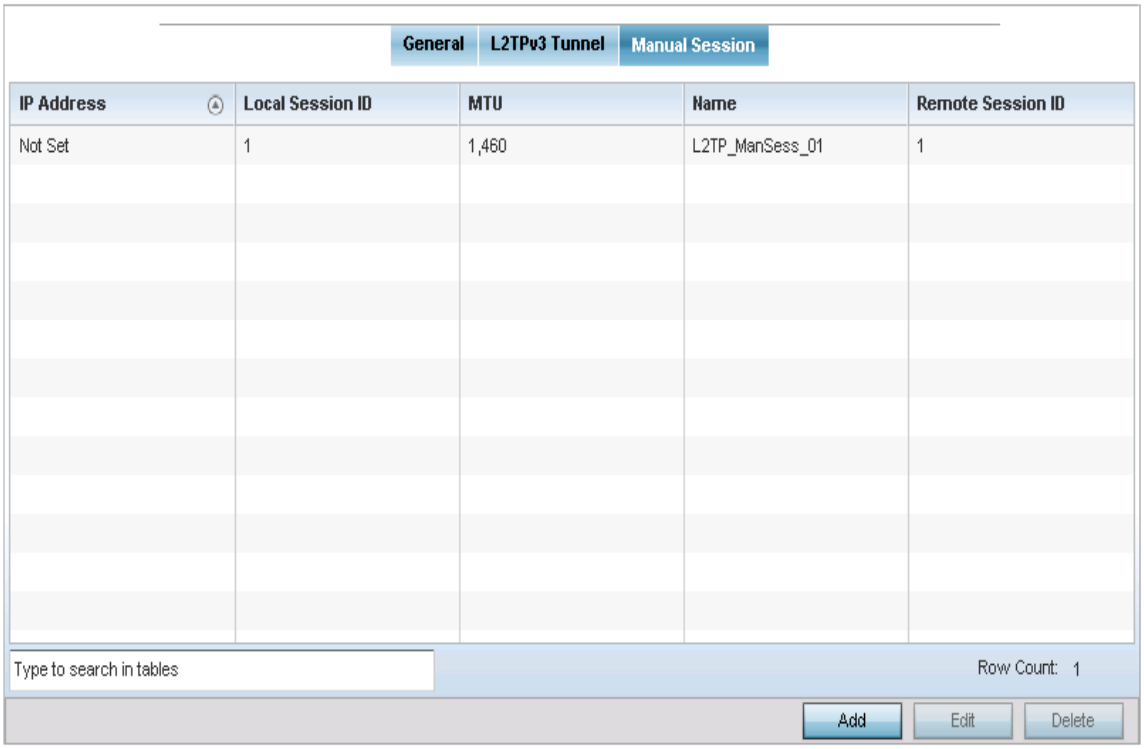


Figure 46: Network - L2TPv3 screen - Manual Session tab

23 Refer to the following 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 sessions's *maximum transmission unit* (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.

24 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

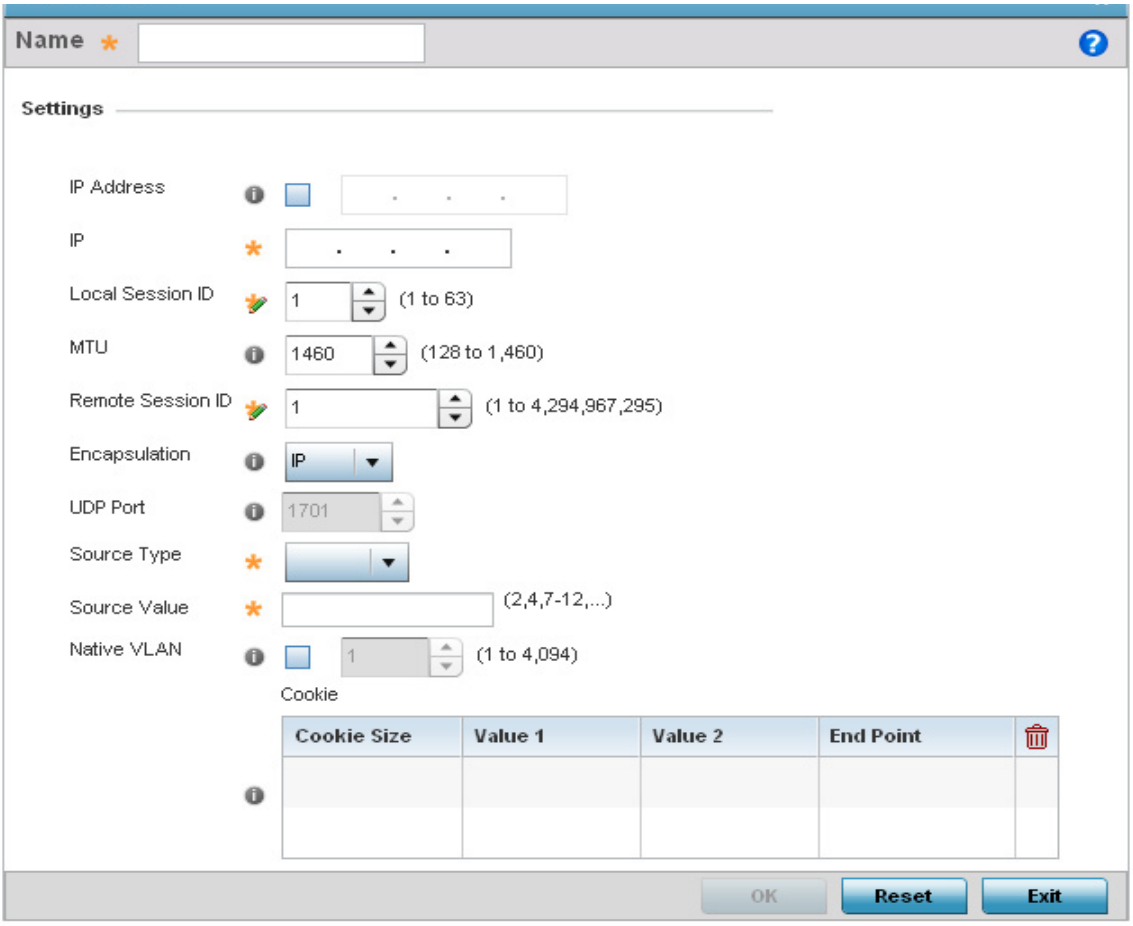


Figure 47: Network - L2TPv3 screen, Add L2TPv3 Peer Configuration

25 Set the following session parameters:

Name	Define a 31 character maximum name for this tunnel session. Each session name represents a single data stream.
IP Address	Specify the IP address used as a 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, the tunnel would use the IP address received in the tunnel create 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 maximum transmission unit (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 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 will not be tagged.

26 Select the **+ Add Row** button 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.

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

IGMP Snooping

"Profile Network Configuration"

Internet Group Management Protocol (IGMP) is a protocol to establish and maintain multicast group memberships to interested members. Multicasting allows a networked computer to send content to multiple computers who have registered to receive the content. IGMP Snooping is for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.

To configure IGMP Snooping:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **IGMP Snooping**.

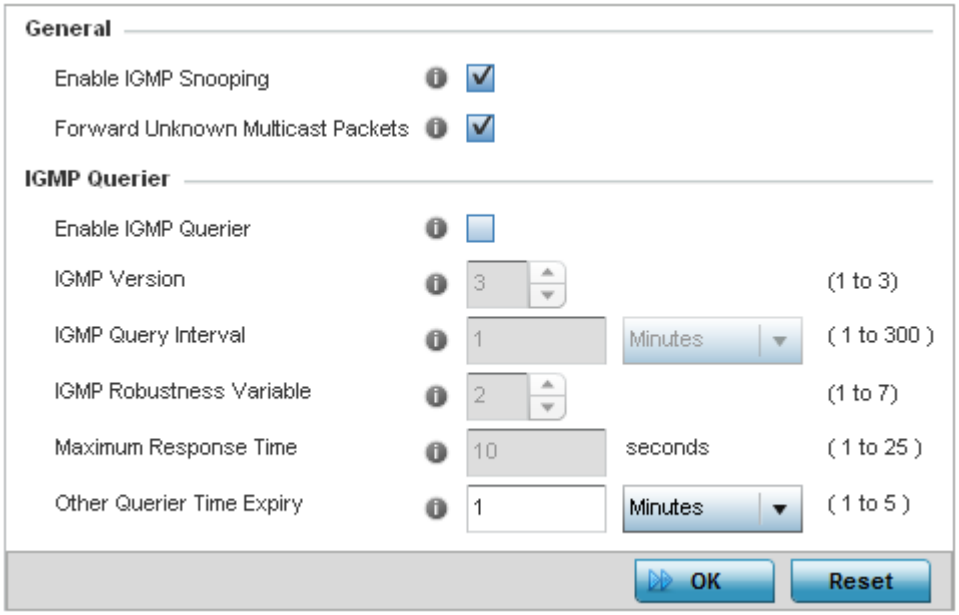


Figure 48: IGMP Snooping screen

5 Set the following parameters to configure **General IGMP Snooping** values:

Enable IGMP Snooping	Select this option to enable IGMP Snooping on the access point. This feature is enabled by default.
Forward Unknown Multicast Packets	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the *Unknown Multicast Forward* feature is also disabled for the selected VLANs. This is enabled by default.

6 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 is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. 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 forwarded on that port. An AP71xx model access point can also be an IGMP querier.
IGMP Version	Use the spinner control to set the IGMP version compatibility to IGMP version 1, 2 or 3. The default IGMP version is 3.
IGMP Query Interval	Sets the IGMP query interval. This parameter is used only when the querier functionality is enabled. Define an interval value in *Seconds* (1 - 18000 seconds), *Minutes* (1 - 300 minutes) or *Hours* (1 - 5 hours) up to maximum of 5 hours. The default value is 60 seconds.
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 time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
Other Querier Time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

7 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.

MLD Snooping

"Profile Network Configuration"

Multicast Listener Discovery (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 set an IPv6 MLD snooping configuration for the profile:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the **Network** menu to display its submenu options.

3 Select **MLD Snooping**.

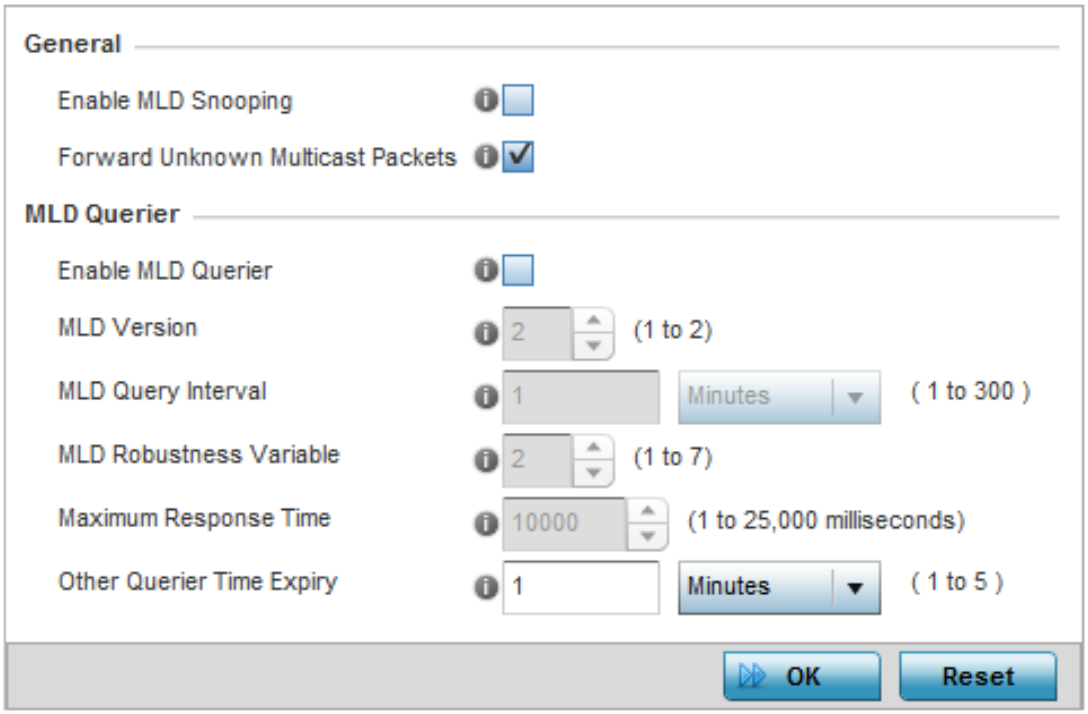


Figure 49: Profile - Network MLD Snooping screen

4 Define the following **General** MLD snooping settings:

Enable MLD Snooping	Enable MLD snooping to examine MLD packets and make content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast. MLD snooping is disabled by default.
Forward Unknown Multicast Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

5 Define the following **MLD Querier** settings for the MLD snooping configuration:

Enable MLD Querier	Select this option to enable MLD querier on the controller, service platform or access point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is disabled by default.
MLD Version	Define whether MLD version *1* or *2* is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2.
MLD Query Interval	Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in either *Seconds* (1 -18,000), *Minutes* (1 - 300) or *Hours* (1 - 5). The default interval is 1 minute.
MLD Robustness Variable	Set a MLD IGMP robustness value (1 - 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2.
Maximum Response Time	Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 milliseconds.
Other Querier time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

6 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

Quality of Service (QoS)

"Profile Network Configuration"

The 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 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Quality of Service (QoS)**.

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

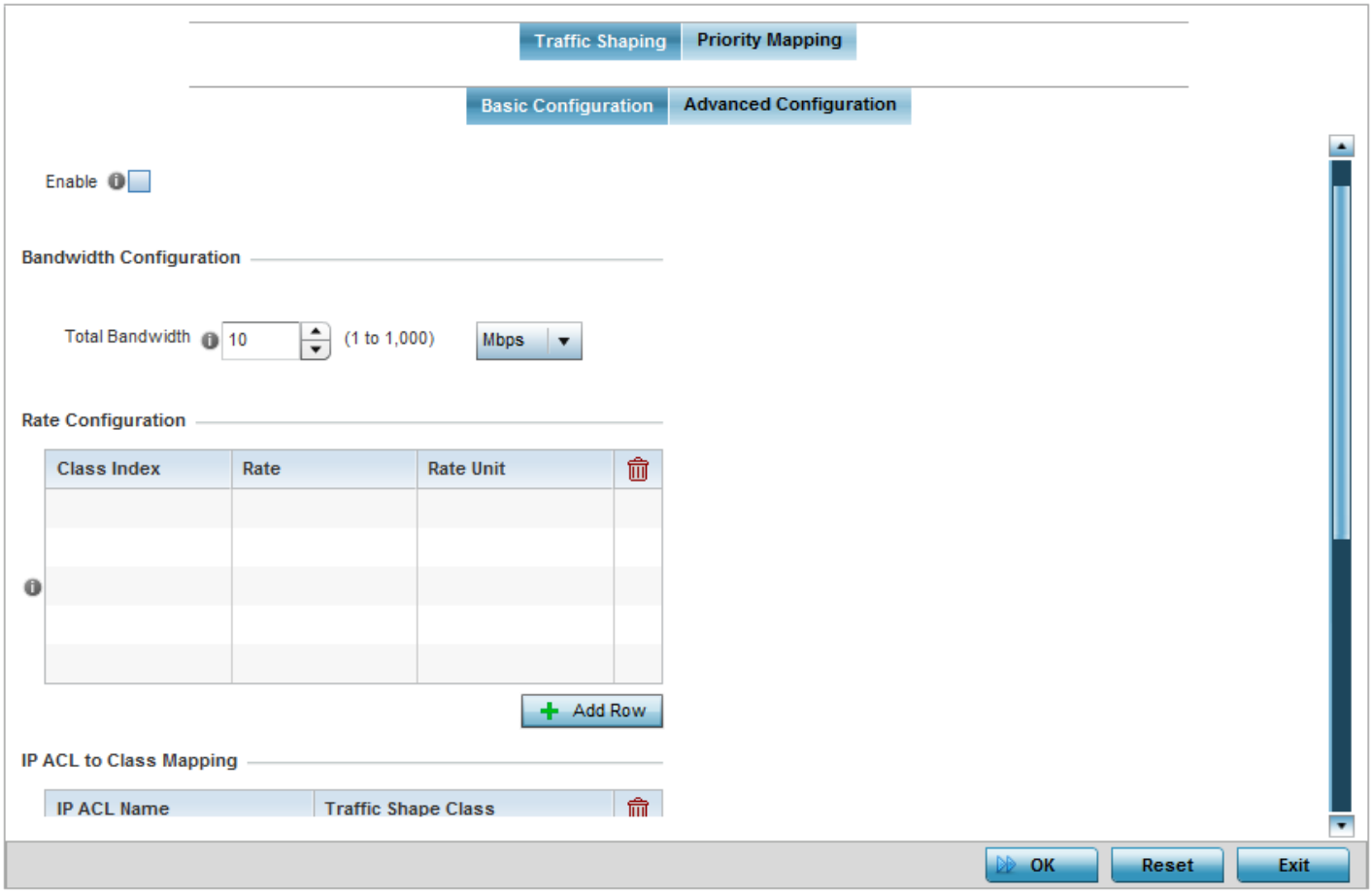


Figure 50: Profile Overrides - Network QoS Traffic Shaping Basic Configuration screen

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 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

6 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.

7 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.

8 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 724 and "Setting an IPv4 or IPv6 Firewall Policy" on page 725.

9 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 724 and "Setting an IPv4 or IPv6 Firewall Policy" on page 725.

10 Select the **OK** button located to save the changes to the traffic shaping basic configuration. Select **Reset** to revert to the last saved configuration.

11 Select the **Advanced Configuration** tab.

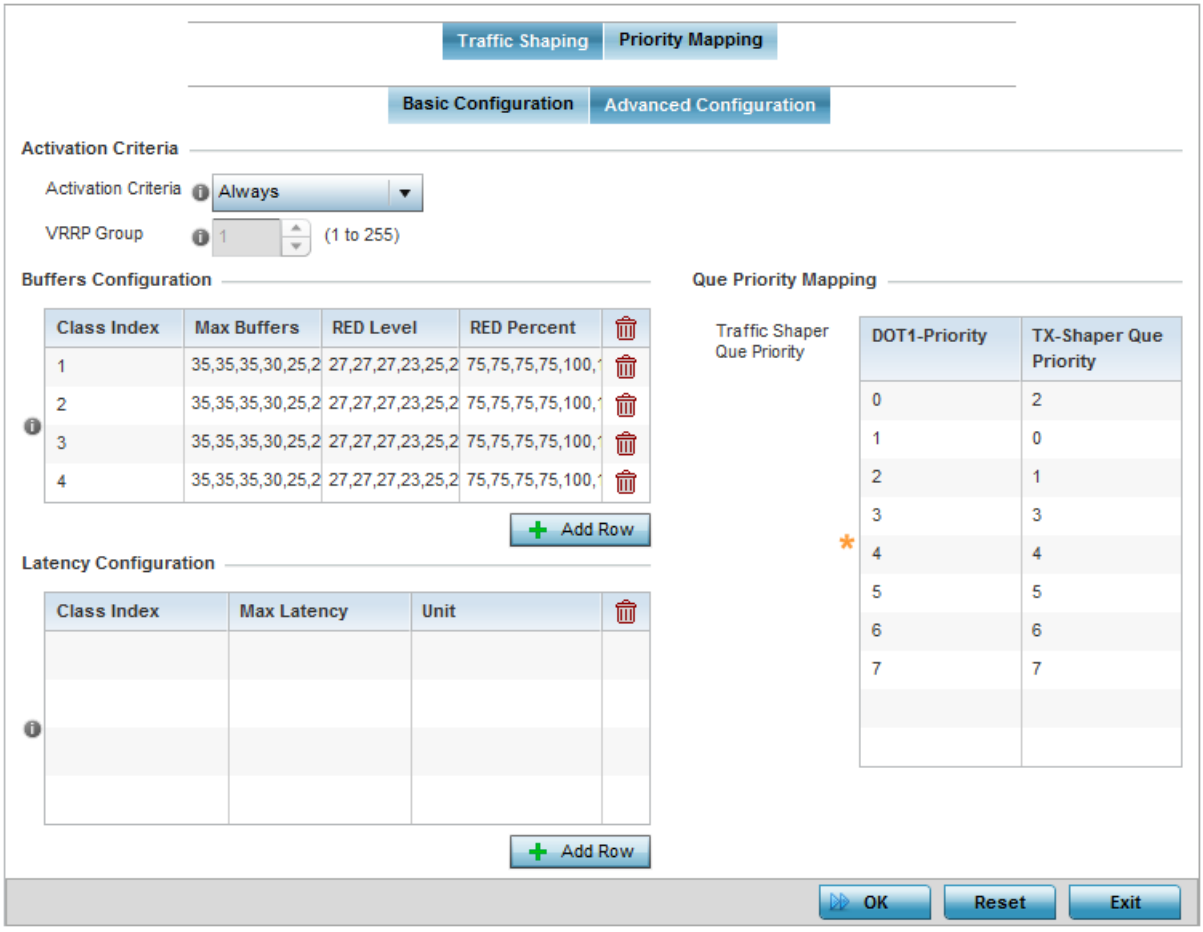


Figure 51: Profile Overrides - Network QoS Traffic Shaping Advanced Configuration screen

12 Set the following **Activation Criteria** for traffic shaper activation:

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.

13 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 *random early detection* (RED) 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.

14 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.

15 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.

16 Select the **OK** button located to save the changes to the traffic shaping advanced configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Priority Mapping** tab.

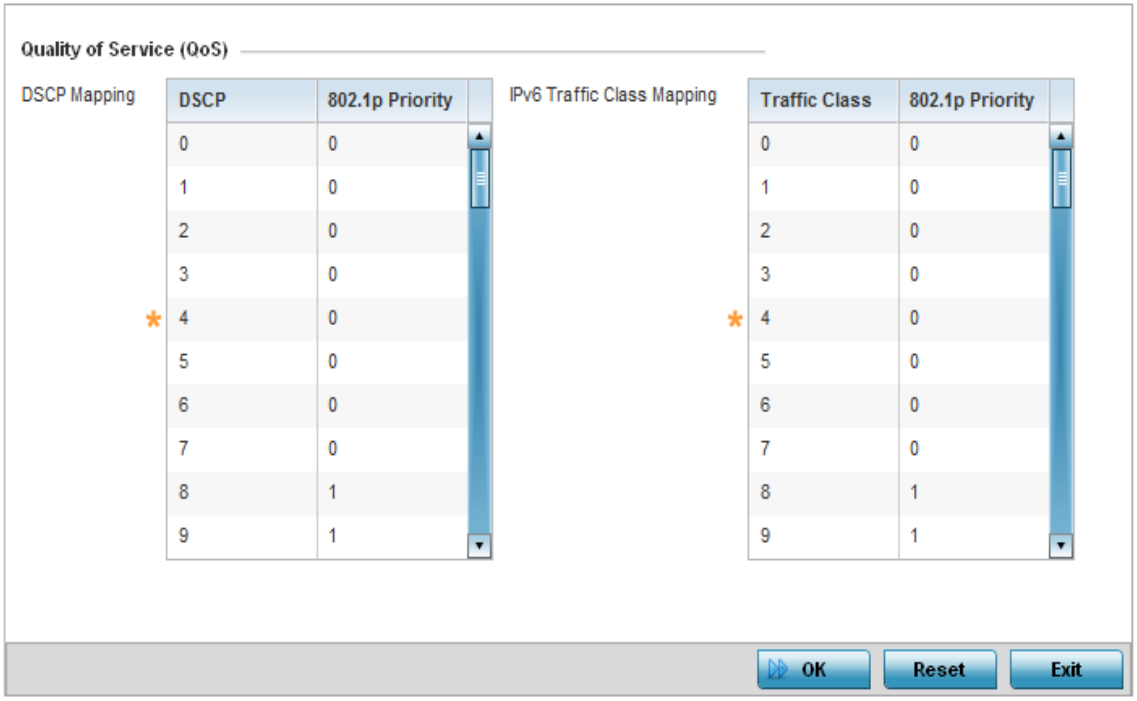


Figure 52: Network - Quality of Service (QoS) screen

18 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.

19 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

20 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.

Spanning Tree Configuration

"Profile Network Configuration"

The *Multiple Spanning Tree Protocol* (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 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 *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. 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 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Spanning Tree**.

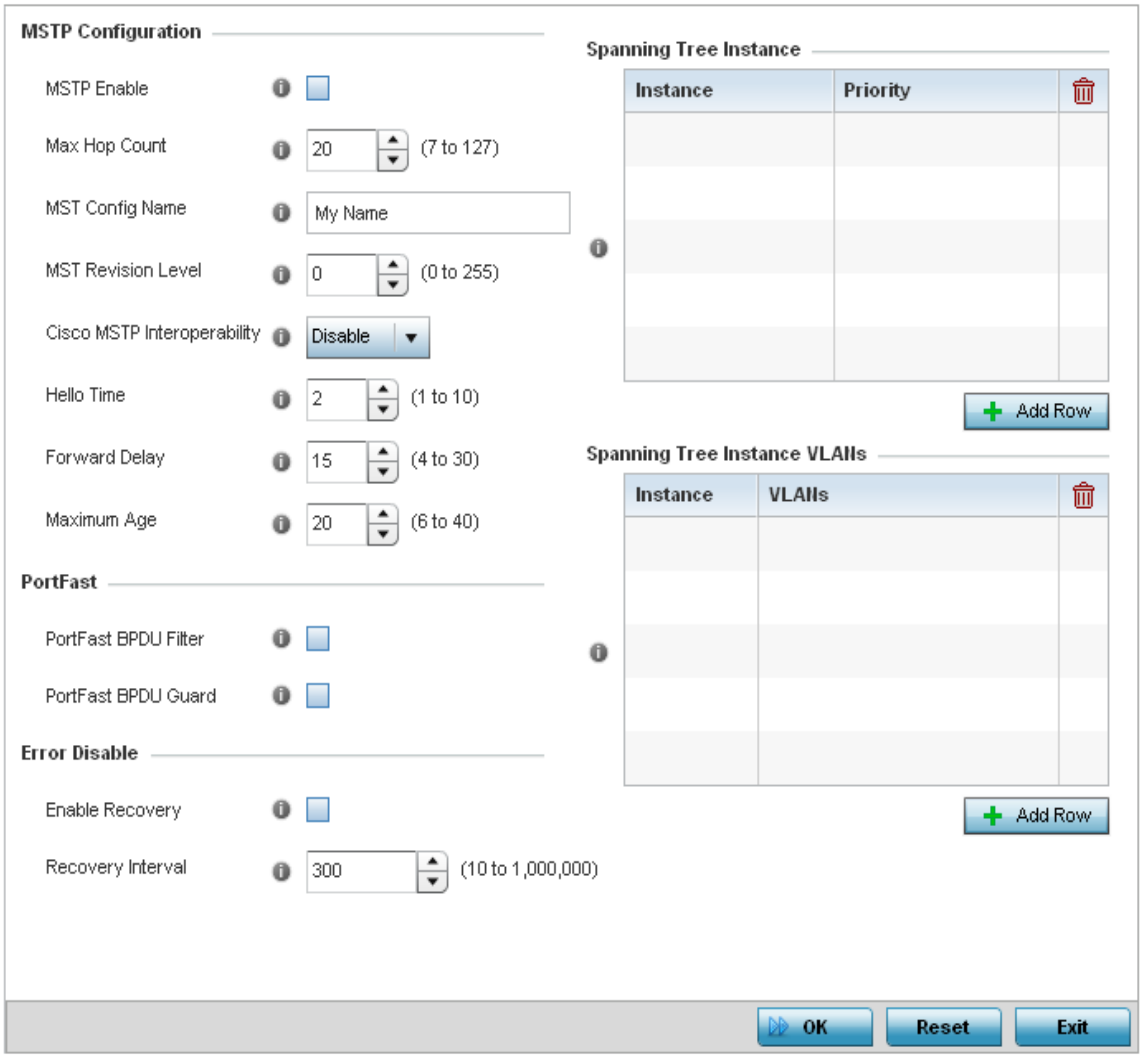


Figure 53: Network - Spanning Tree screen

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

MSTP Enable	Select this option to enable MSTP for this profile. MSTP is disabled by default, so enable this setting if requiring different (groups) of VLANs with the profile supported network segment.
Max Hop Count	Define the maximum number of hops the BPDU considers 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 to use as an identifier for the configuration.
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 start/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 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.

6 Define the following **PortFast** parameters for the profile configuration:

PortFast BPDU Filter	Select *Enable* to invoke a BPDU filter for this PortFast enabled port. Enabling the BPDU filter 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 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*.

7 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 Interval	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.

8 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.

9 Use the **Spanning Tree Instance VLANs** table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.

10 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.

Routing

"Profile Network 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 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Routing**. The **IPv4 Routing** tab displays by default.

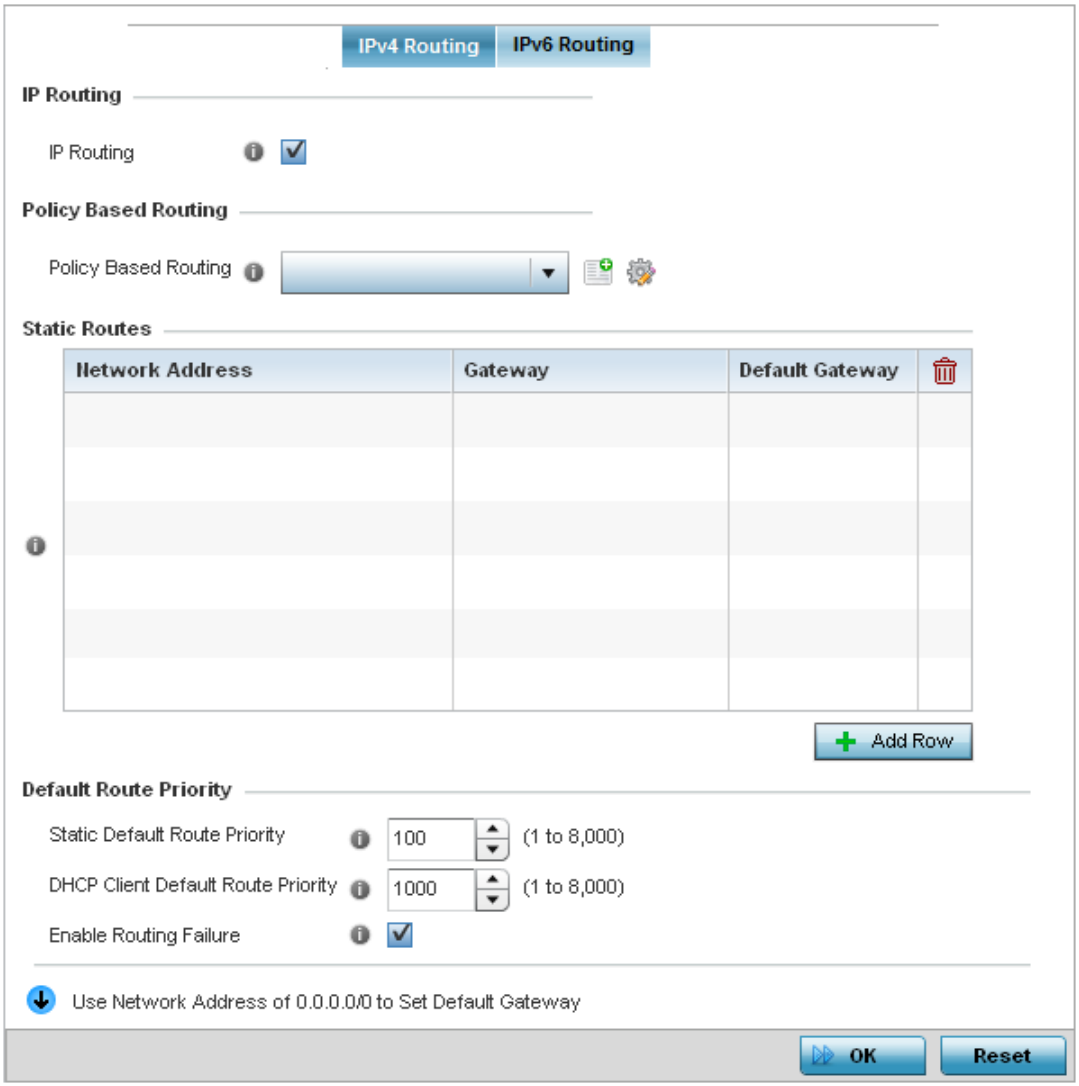


Figure 54: Network - Routing screen

5 Select **IP Routing** to enable static routes using IPv4 addresses. This option is enabled by default.

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 651.

Select **Add Row +** as needed to include single rows with in the static IPv4 route table.

6 Add IP addresses and network masks in the **Network Address** column of the **Static Routes** table.

7 Provide the **Gateway** used to route traffic.

8 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.

9 Select the **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

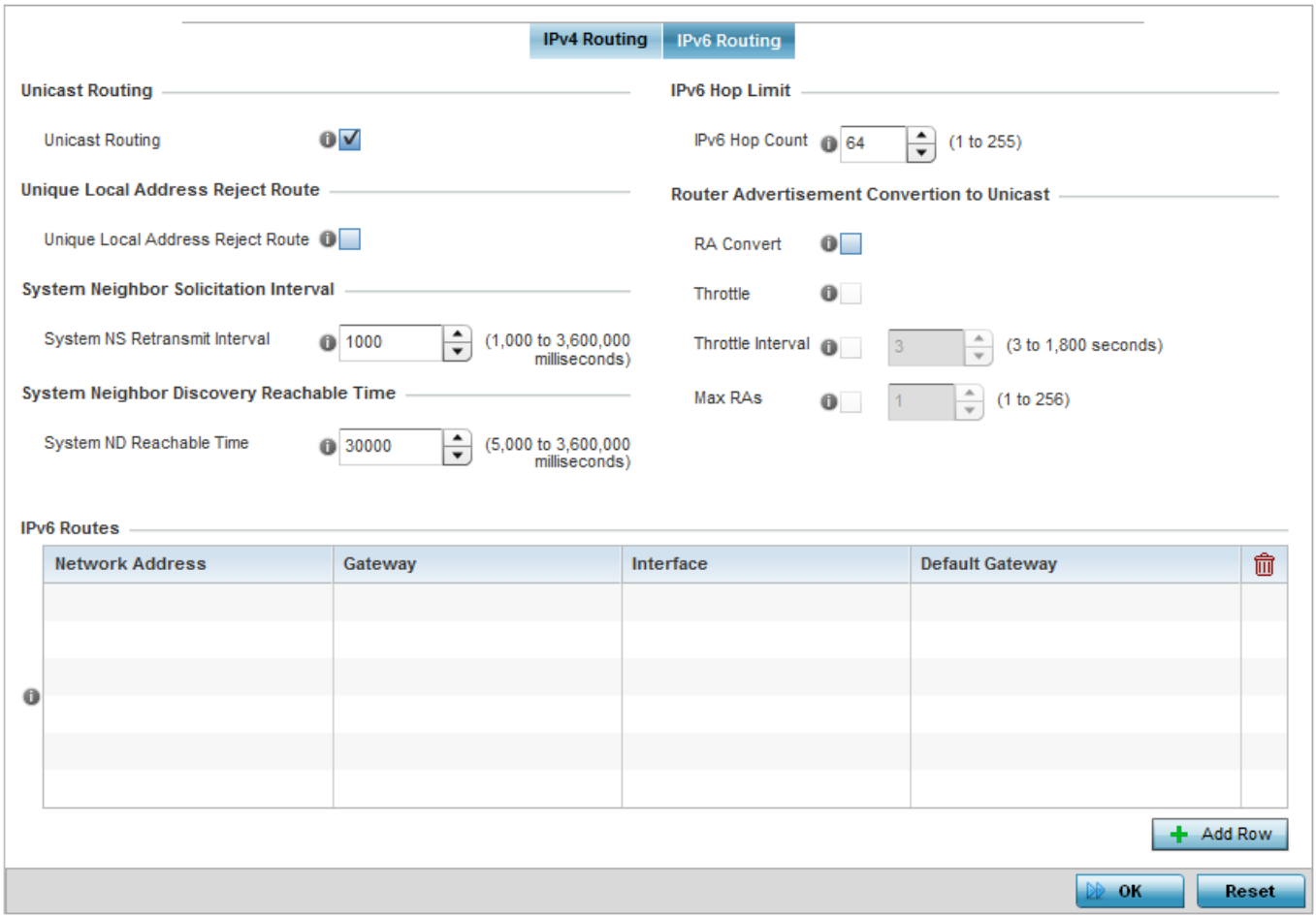


Figure 55: Static Routes screen, IPv6 Routing tab

10 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.

11 Select **Unique Local Address Reject Route** to enable rejecting local routes in the format *FC00::/7*.

12 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.

13 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.

14 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.

15 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.

16 Select **+ Add Row** as needed within the **IPv6 Routes** table to add an additional 256 IPv6 route resources.

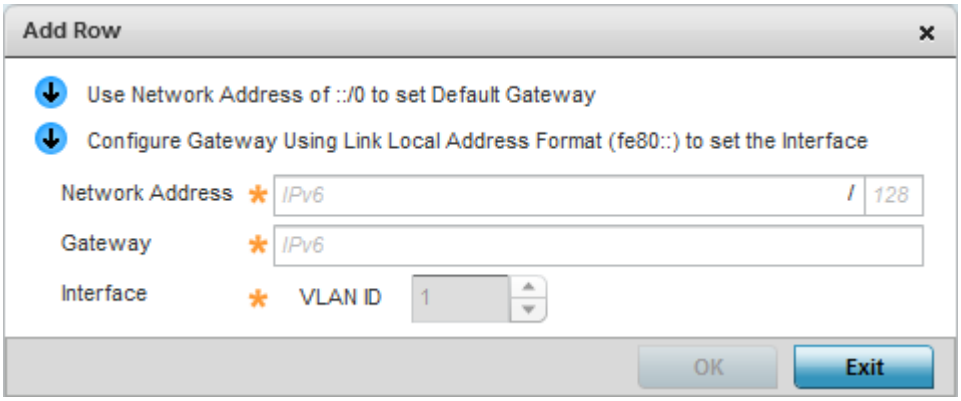


Figure 56: Static Routes screen, Add IPv6 Route

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.
Default Gateway	Use a network address of ::/0 to set the default gateway.

17 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.

Dynamic Routing (OSPF)

"Profile Network Configuration"

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 is 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 sends 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.

NOTE

OSPF is available on the following access points: AP8432, AP8533, AP7522, AP7532, AP7562, AP82XX, AP81XX.

To define a dynamic routing configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Dynamic Routing**.

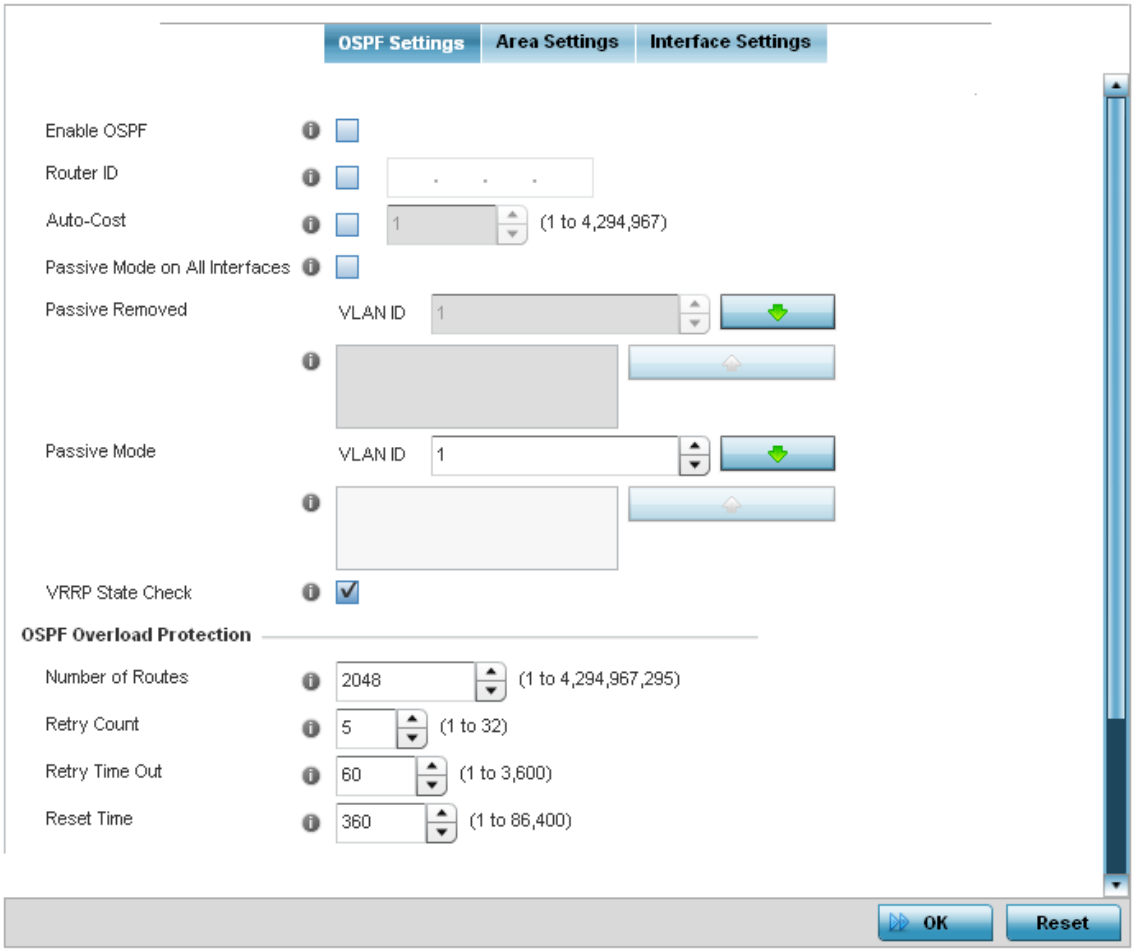


Figure 57: Network - OSPF Settings tab

5 Enable/disable OSPF and provide the following dynamic routing settings:

Enable OSPF	Select this option to enable OSPF for this access point. OSPF is disabled by default.
Router ID	Select this option to define a router ID (numeric IP address) for this access point. 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 VRRP state. If the interface's VRRP state is not *Backup*, then the interface is published via OSPF.

6 Set the following **OSPF Overload Protection** settings:

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.

7 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 is defined by the speed (bandwidth) of the interface supporting a given route.

8 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*, *kernel* and *static*.

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 learnt from OSPF. The default priority is 7000.

11 Select the **Area Settings** tab.

An OSPF *Area* contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.

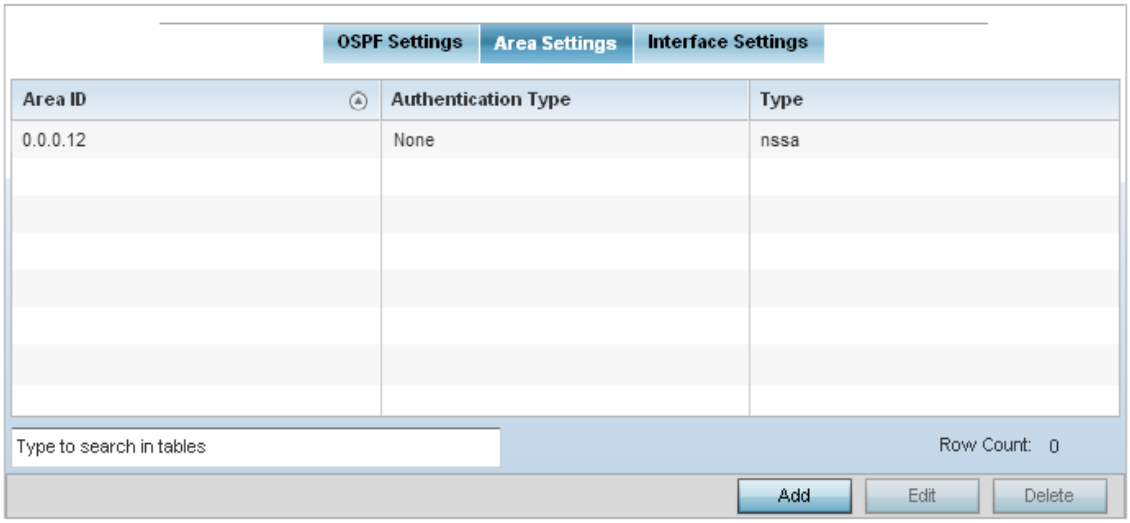


Figure 58: Network - Area Settings tab

12 Review existing **Area Settings** configurations using:

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.

13 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

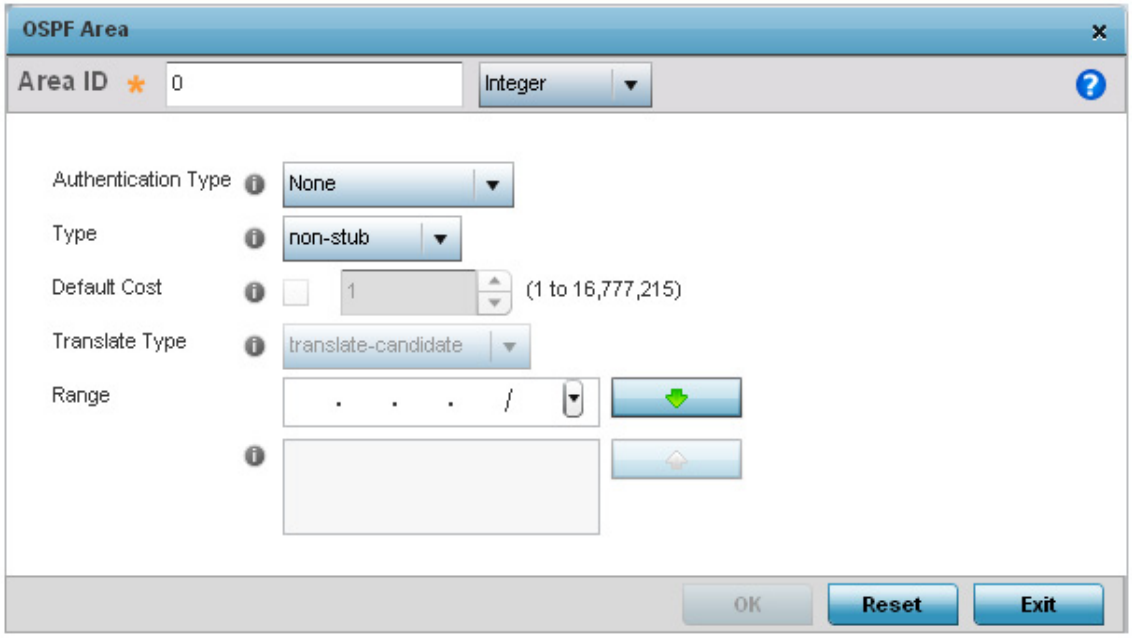


Figure 59: Network - OSPF Area Configuration screen

14 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.

15 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

16 Select the **Interface Settings** tab.

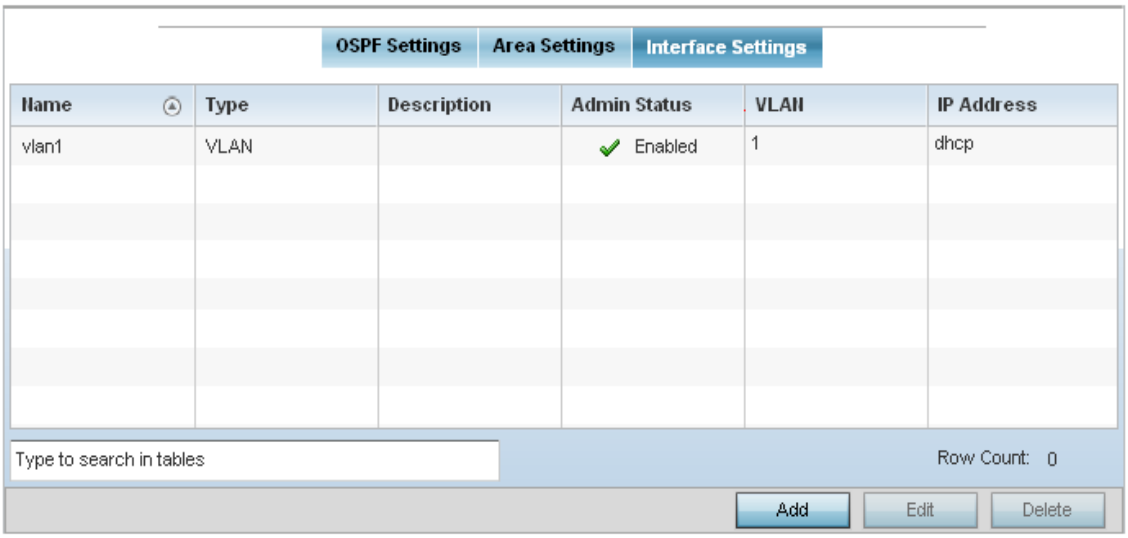


Figure 60: Network - Interface Settings tab

17 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.

18 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.

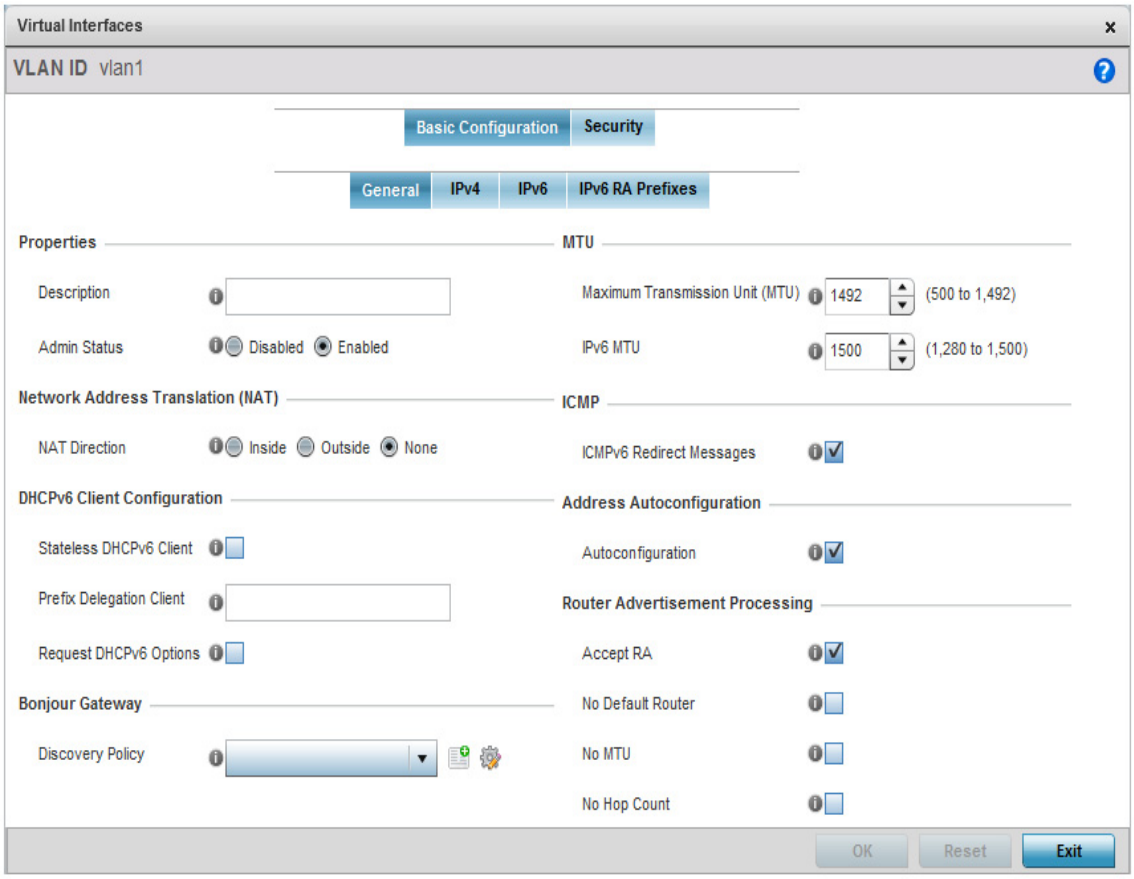


Figure 61: Network - OSPF Virtual Interfaces - Basic Configuration tab

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.

19 If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID from 1 - 4094.

20 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.

21 Define the **Network Address Translation** (NAT) direction.

Select either the *Inside*, *Outside* or *None* radio buttons.

- *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.

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

23 Set the following **MTU** settings for the virtual interface:

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.
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.

24 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.

25 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.

26 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.

27 Use the drop-down menu to define the **Bonjour Gateway Discovery Policy**. Bonjour is Apple's service discovery protocol.

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

29 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

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

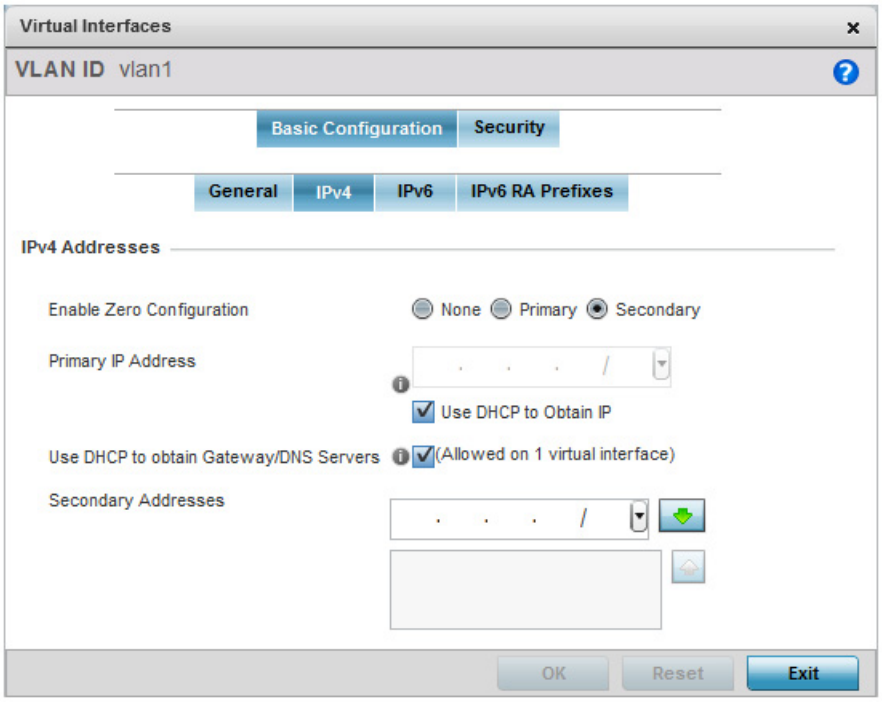


Figure 62: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv4 tab

30 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 the *Secondary Addresses* 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.

31 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

32 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

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. 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

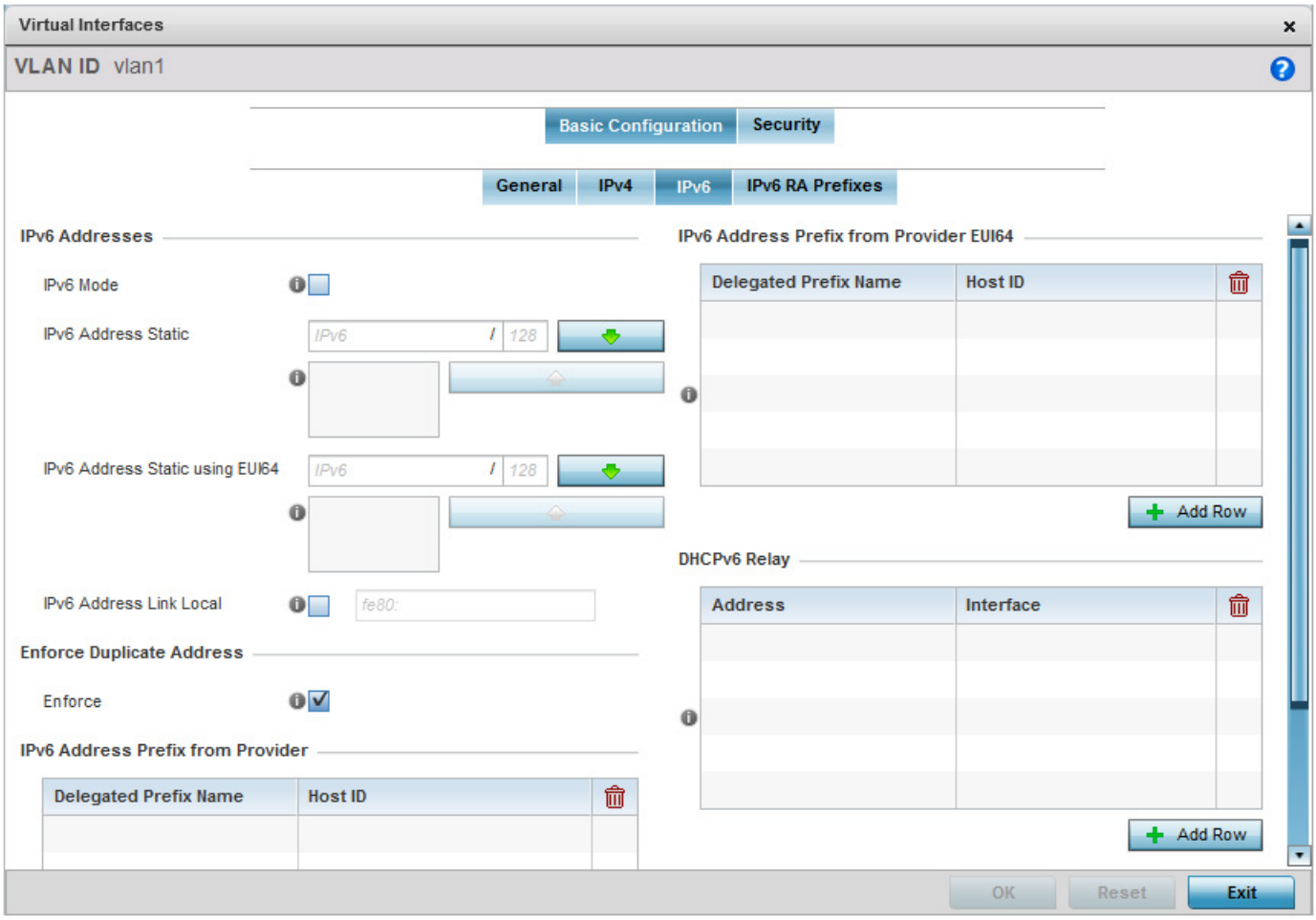


Figure 63: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab

33 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.

34 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.

35 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 sub screen wherein a new delegated prefix name and host ID can be defined.

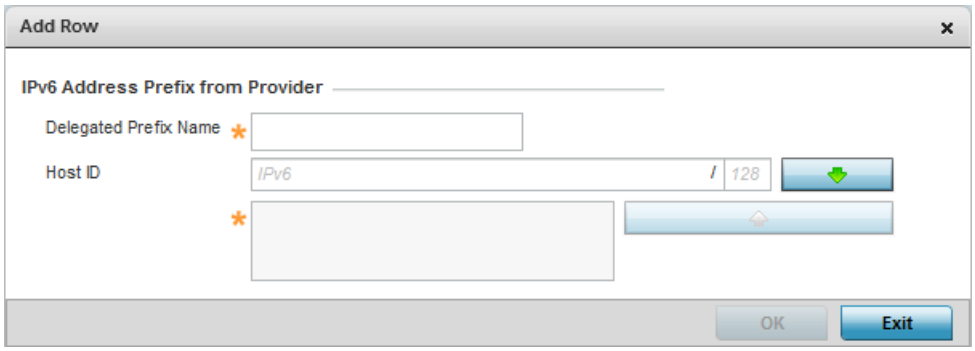


Figure 64: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider

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.

36 Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

37 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 sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

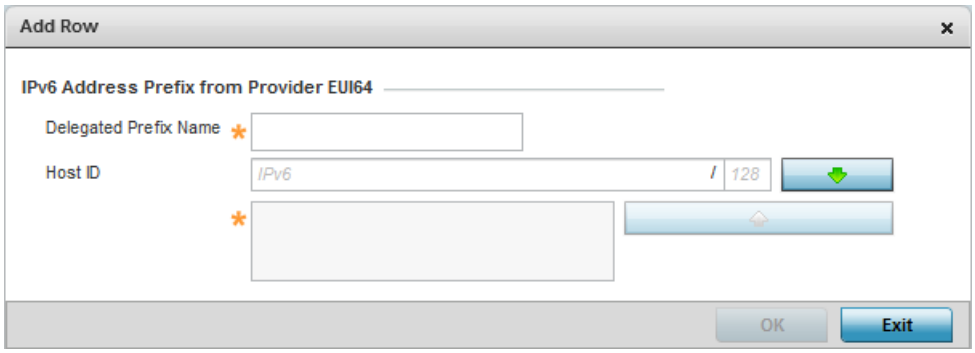


Figure 65: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64

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.

38 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

39 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.

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



Figure 66: Network - OSPF 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.

41 Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

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

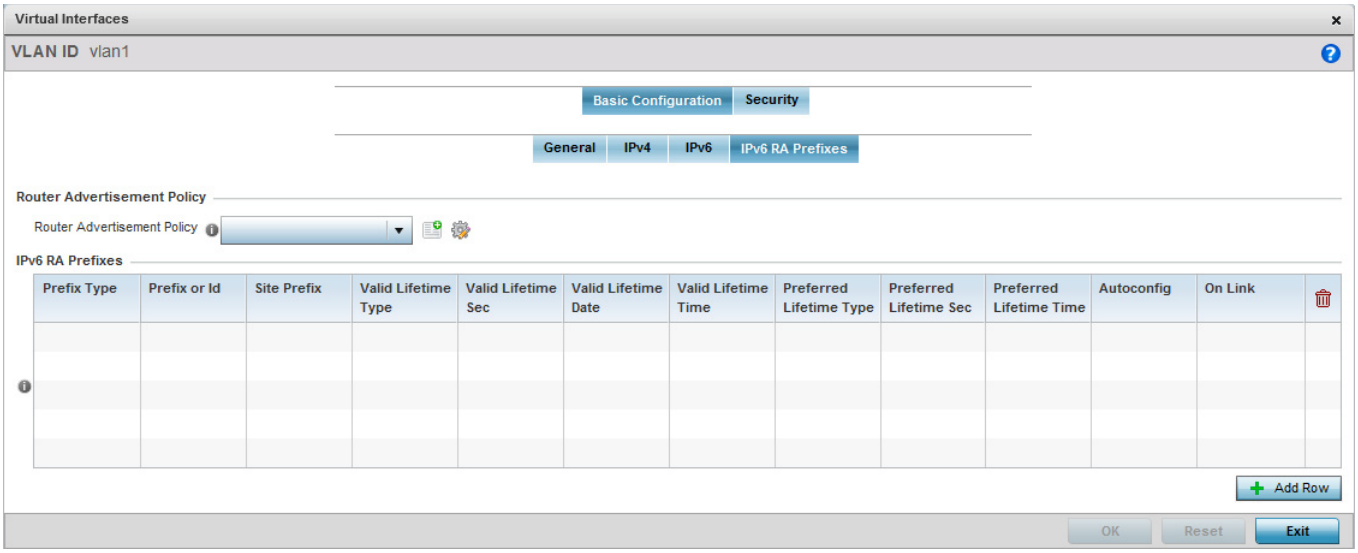


Figure 67: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab

43 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 Advertisement Policy" on page 697.

44 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

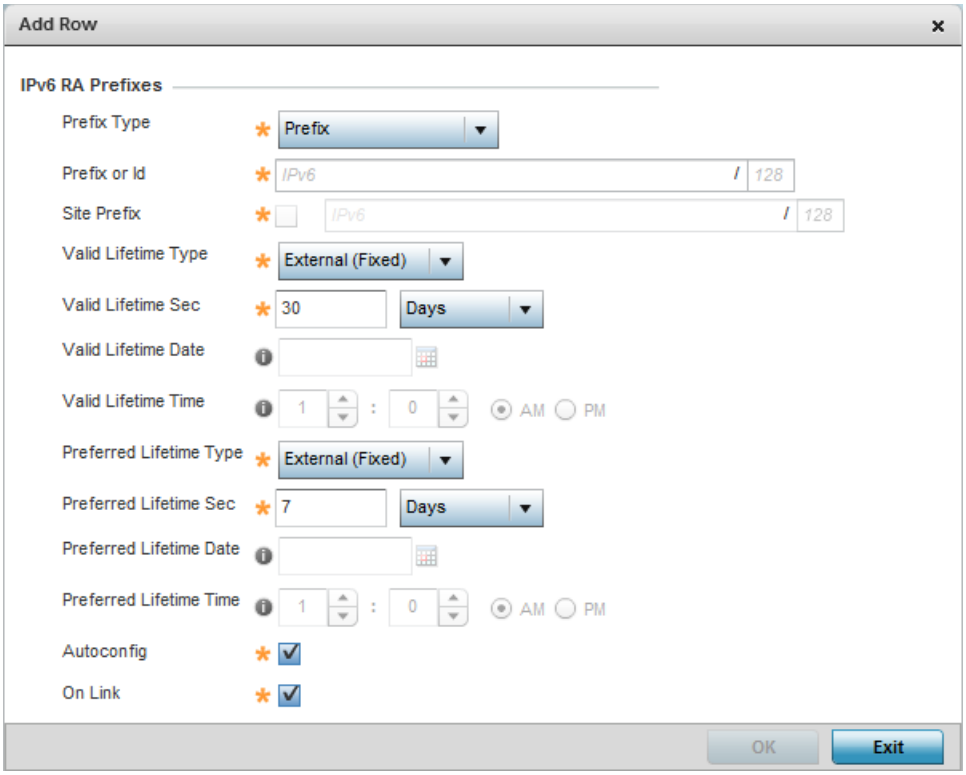


Figure 68: Network - OSPF Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix

45 Set 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 *Internet Service Provider* (ISP) 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 measurement 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.

46 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

47 Select the **OK** button to save the changes and overrides to the basic configuration. Select **Reset** to revert to the last saved configuration.

48 Select the **Security** tab.

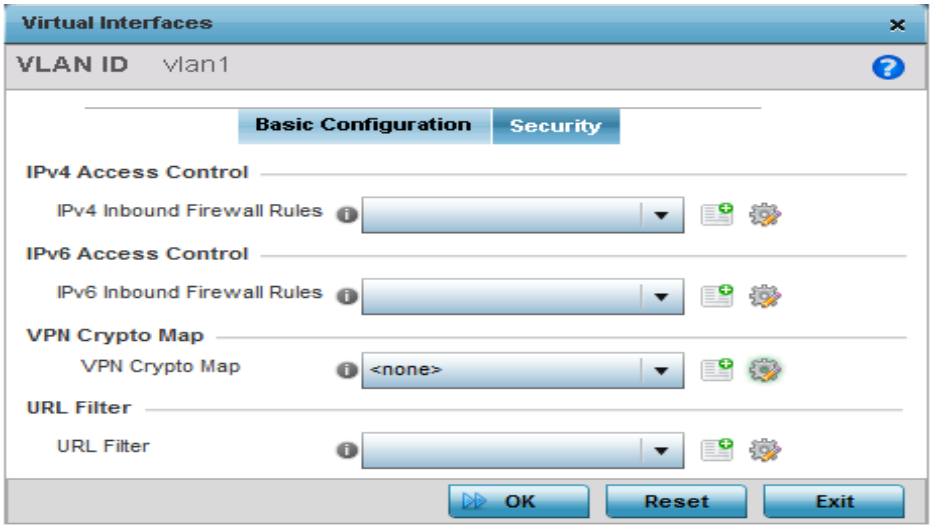


Figure 69: Network - OSPF Virtual Interface - Security tab

49 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 724.

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* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

50 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.

51 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

Forwarding Database

"Profile Network Configuration"

A *Forwarding Database* is used by a bridge to forward or filter packets. The bridge reads the packet's destination MAC address and 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 decide to filter or forward the packet.

To define a forwarding database configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Forwarding Database**.

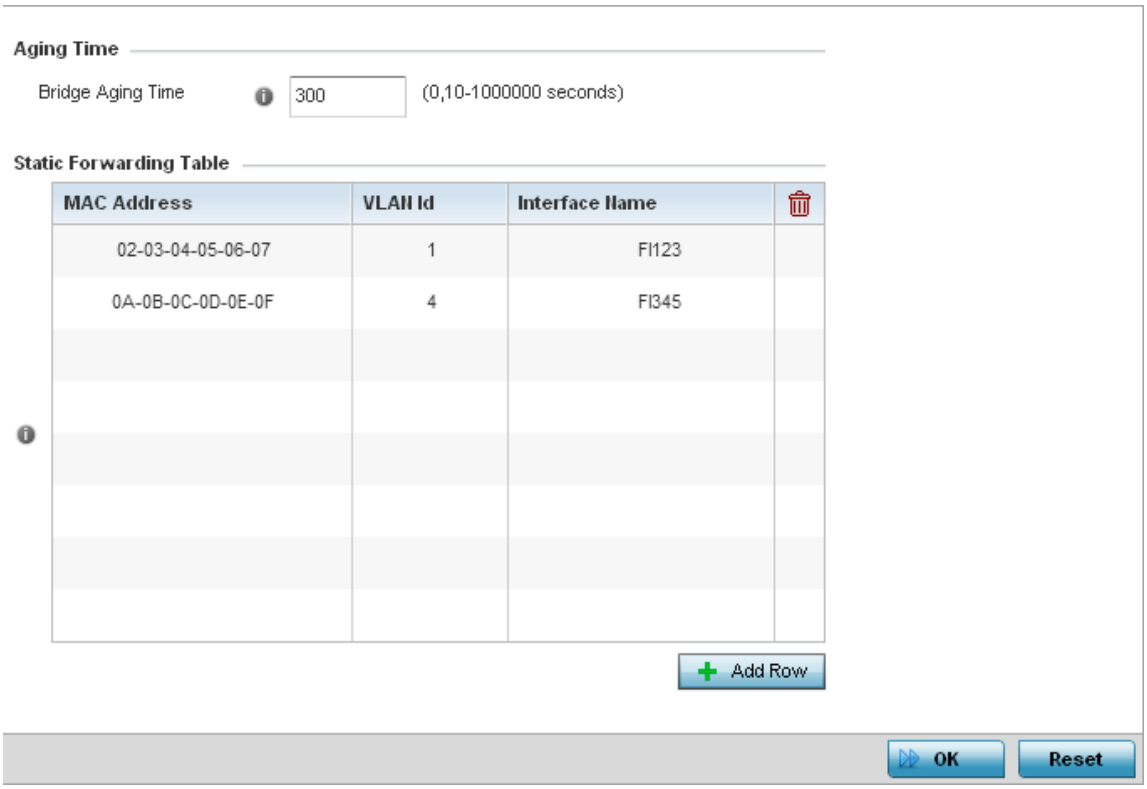


Figure 70: Network - Forwarding Database screen

5 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.

6 Use the **+ Add Row** button to create a new row within the **Static Forwarding 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 is 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

"Profile Network Configuration"

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical managed network. VLANs are broadcast domains 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). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

To define a Bridge VLAN configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Bridge VLAN.**

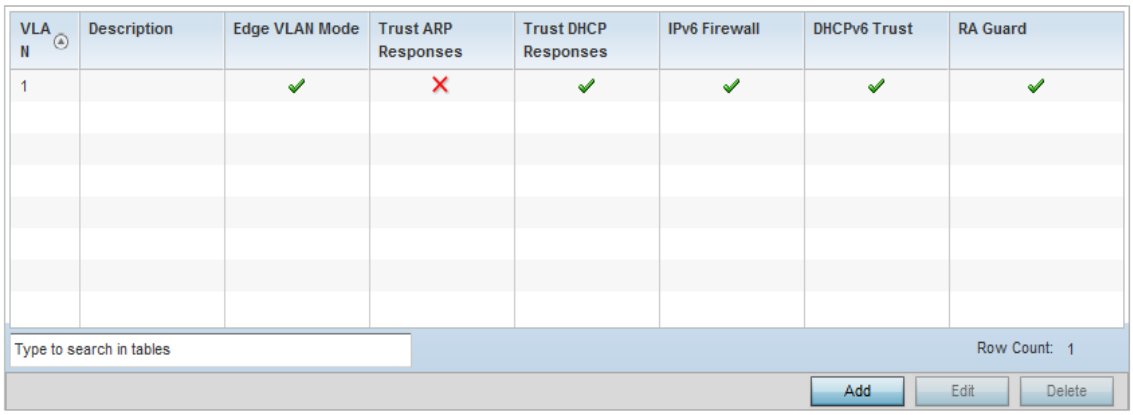


Figure 71: Network - Bridge VLAN screen

VLAN	Lists the numerical identifier defined for the Bridge VLAN when it was 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. 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 be marked as an edge VLAN. When defining a VLAN as 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 Responses	When ARP trust is enabled, a green check mark 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 check mark displays. When disabled, a red “X” displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.
IPv6 Firewall	Lists whether IPv6 is enabled on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. 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.
DHCPv6 Trust	Lists whether DHCPv6 responses are trusted on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. If enabled, only DHCPv6 responses are trusted and forwarded over the Bridge VLAN.
RA Guard	Lists whether *router advertisements* (RA) are allowed on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. RAs are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

5 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify the configuration of an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

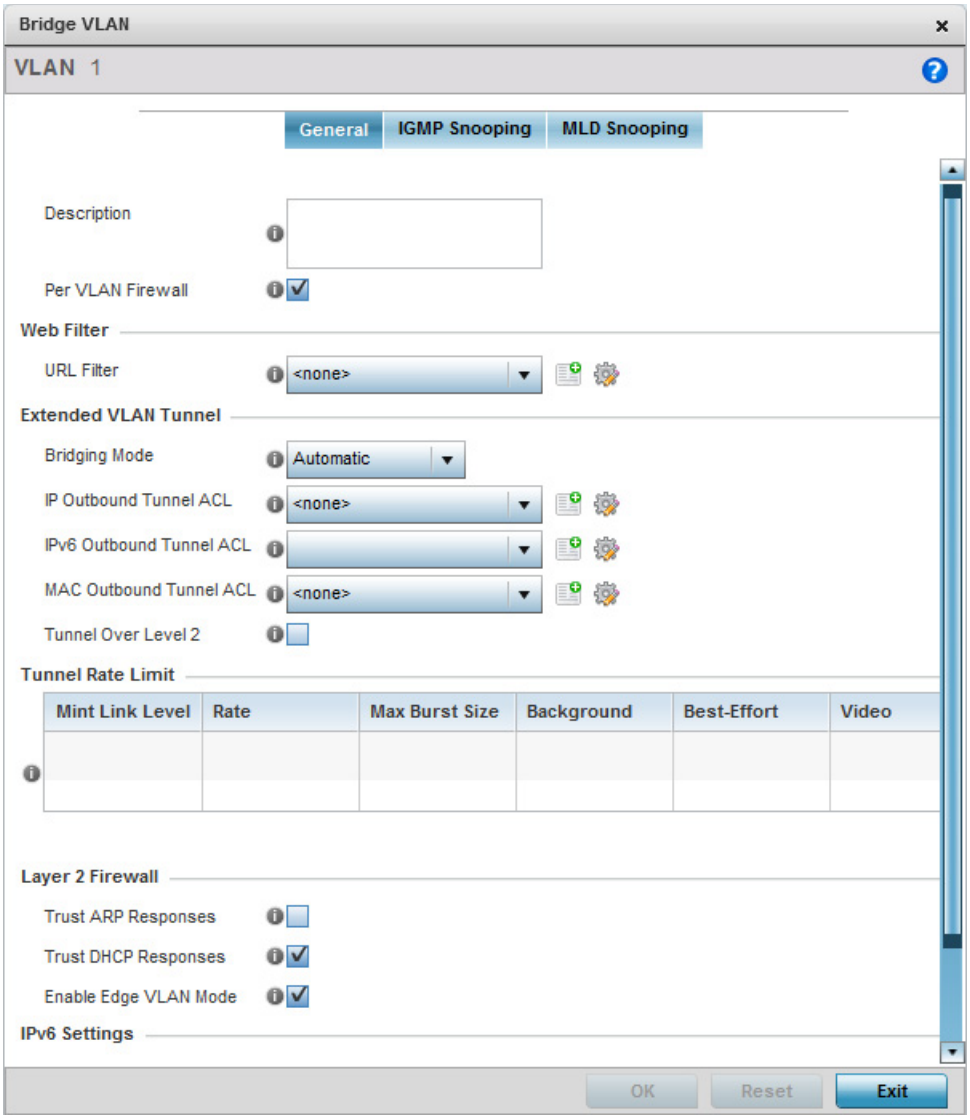


Figure 72: Network - Bridge VLAN Configuration screen

6 If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN ID** from 1 - 4095. This value must be defined and saved before the **General** tab can become enabled and the remainder of the settings defined.

7 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.

8 Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate flow tables that store information on the traffic allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory that could be used for other critical purposes. With the per VLAN firewall feature enabled on an interface, flow tables are only generated for that interface. Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory which can be used for other purposes.

Firewalls can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network. Select the **Per VLAN Firewall** option to enable firewall on this interface.

9 Set or override the following **Web 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.

10 Set or override the following **Extended VLAN Tunnel** parameters:

Bridging Mode	Specify one of the following bridging mode for use on the VLAN. • *Automatic* - Select automatic mode to let the controller or service platform 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 traffic on the VLAN.
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.
IPv6 Outbound Tunnel ACL	Select an *IPv6 Outbound Tunnel ACL* for outbound traffic from the drop-down menu. If an appropriate outbound IPv6 ACL is not available, select the *Create* button.
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, select the *Create* button.
Tunnel Over Level 2	Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default.

11 Set the following **Tunnel Rate Limit** parameters:

Mint Link Level	Select the MINT link level from the drop-down menu.
Rate	Define a transmit 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 Bridge VLAN. 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 0 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion. The default burst size is 320 kbytes.
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%.

12 Define 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 network. DHCP packets update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default.
Enable Edge VLAN Mode	Select this option to enable edge VLAN mode. When selected, the IP address in the VLAN is not used for normal operations, as it is now designated to isolate devices and prevent connectivity. This feature is enabled by default.

13 Set the following **IPv6 Settings**:

IPv6 Firewall	Select this option to enable IPv6 on this Bridge VLAN. This setting is enabled by default.
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this Bridge VLAN. 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.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this Bridge VLAN. This setting is enabled by default.

14 Refer to the **Captive Portal** field to select an existing captive portal configuration to apply access restrictions to the Bridge VLAN configuration.

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.

If an existing captive portal does not suite the Bridge VLAN configuration, either select the **Edit** icon to modify an existing configuration or select the **Create** icon to define a new configuration that can be applied to the Bridge VLAN. For information on configuring a captive portal policy, see "Configuring Captive Portal Policies" on page 759.

15 Select the **IGMP Snooping** tab.

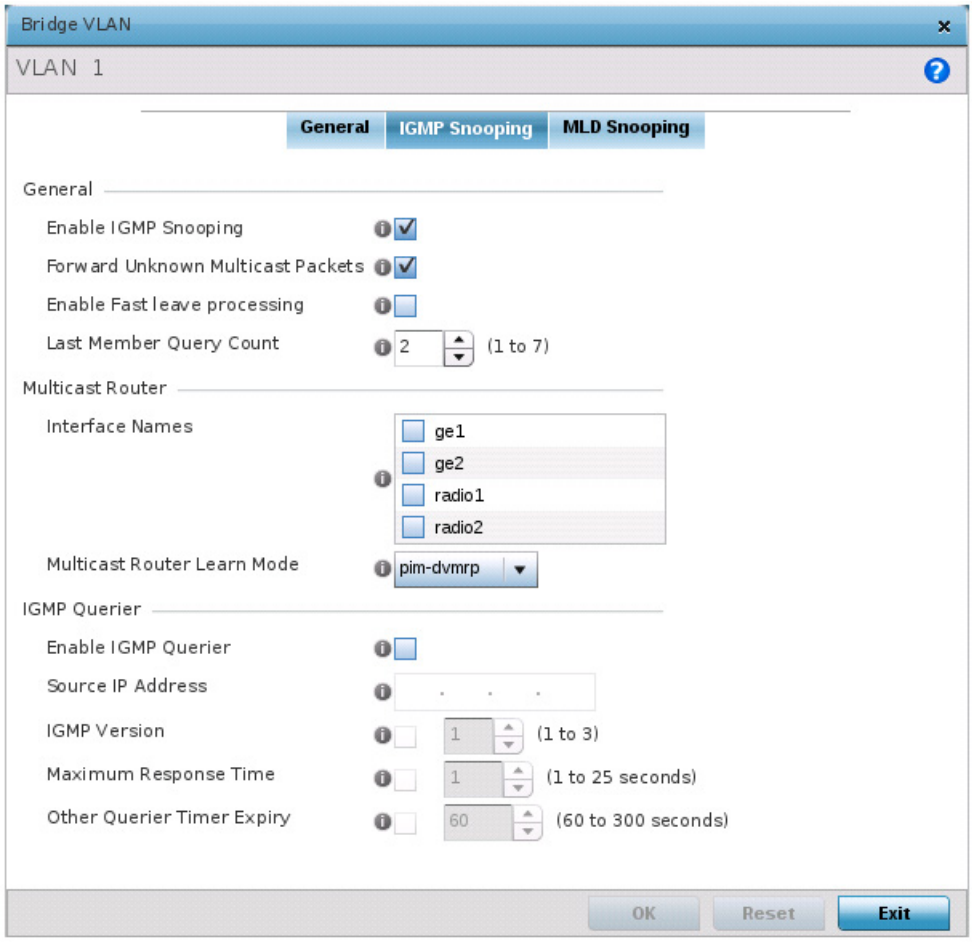


Figure 73: Network - Bridge VLAN - IGMP Snooping screen

16 Define the following IGMP **General** parameters.

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on this Bridge VLAN is disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden.
Forward Unknown Multicast Packets	Select this option to enable forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for this Bridge VLAN. This setting is enabled by default.
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. This setting is disabled by default.
Last Member Query Count	Specify the number (1 - 7) of group specific queries sent before removing an IGMP snooping entry. The default settings is 2.

17 Define the following **Multicast Router** settings:

Interface Names	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
Multicast Router Learn Mode	Select *static* or *pim-dvmrp* as the mode used to determine client multicast traffic levels on specific routes.

18 Set the following **IGMP Querier** parameters for the Bridge VLAN configuration:

Enable IGMP Querier	IGMP snoop querier is used to keep host memberships alive. it is primarily used in a network where there is 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.

19 Select the **MLD Snooping** tab.

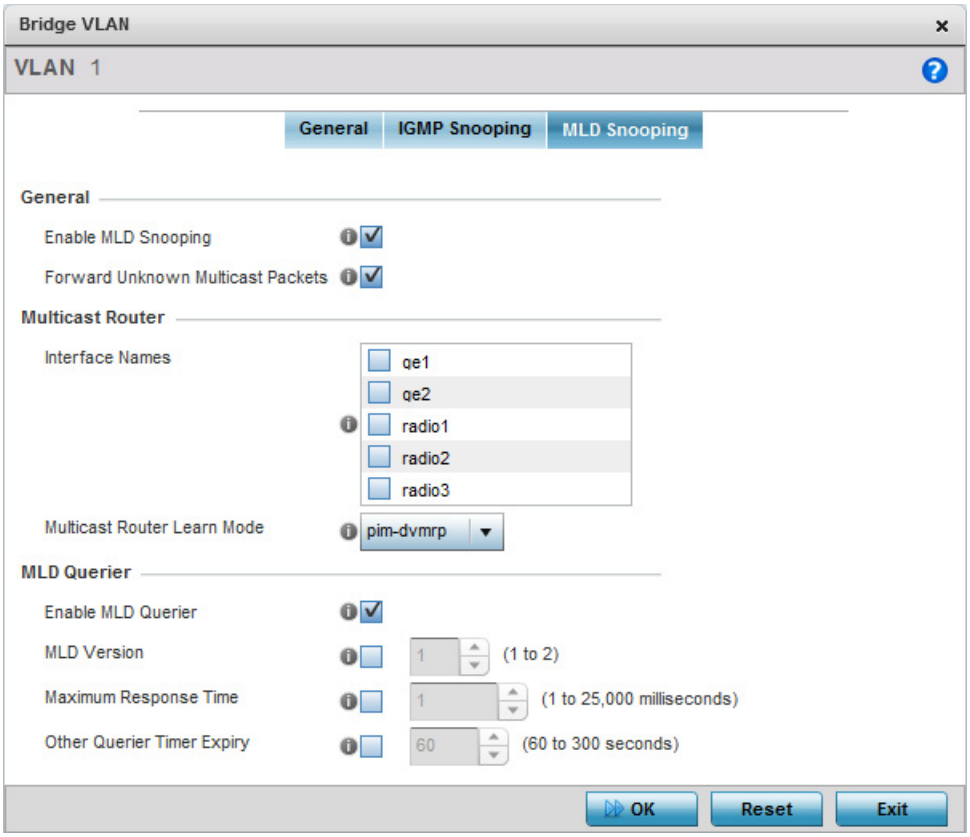


Figure 74: Network Bridge VLAN screen, MLD Snooping tab

20 Define the following **General** MLD snooping parameters for the Bridge VLAN configuration:

Multicast Listener Discovery (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.

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 Multicast Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

21 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.

22 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

23 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

"Profile Network Configuration"

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To define the profile's CDP configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Cisco Discovery Protocol**.



Figure 75: Network - Cisco Discovery Protocol (CDP) screen

5 Enable/disable CDP and set the following settings:

Enable CDP	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default.
Hold Time	Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 1,800 seconds.
Timer	Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds.

6 Select the **OK** button located at the bottom right of the screen to save the changes to the CDP configuration. Select **Reset** to revert to the last saved configuration.

Link Layer Discovery Protocol Configuration

"Profile Network Configuration"

The *Link Layer Discovery Protocol* (LLDP) 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 *Link Layer Discovery Protocol Data Unit* (LLDP PDU). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To set the LLDP configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Link Layer Discovery Protocol**.

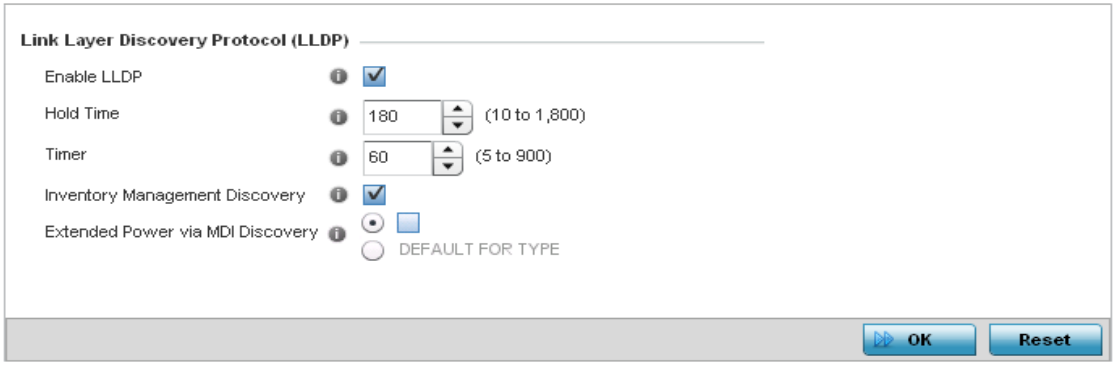


Figure 76: Network - Link Layer Discovery Protocol (LLDP) screen

5 .Set the following LLDP parameters for the profile configuration:

Enable LLDP	Select this option to enable LLDP on the access point. LLDP is enabled by default When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them.
Hold Time	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds.
Timer	Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds.
Inventory Management Discovery	Select this option to include LLPD-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.
Extended Power via MDI Discovery	Select this option to include LLPD-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default.

6 Select the **OK** button to save the changes to the LLDP configuration. Select **Reset** to revert to the last saved configuration.

Miscellaneous Network Configuration

"Profile Network Configuration"

A profile can be configured to include a hostname in a DHCP lease for a requesting device and its profile. This helps an administrator track the leased DHCP IP address by hostname for the supported device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include hostnames in DHCP requests:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Network** menu and select **Miscellaneous**.

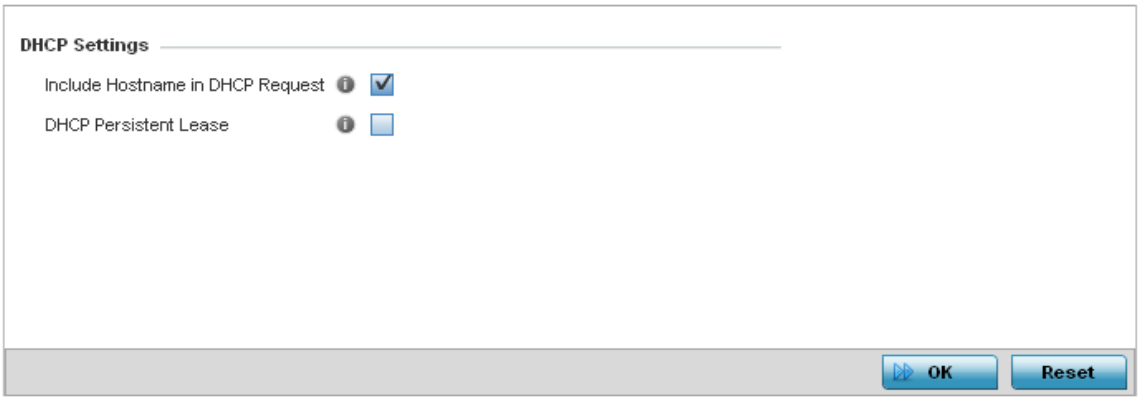


Figure 77: Network - Miscellaneous screen

5 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.

6 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.

7 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

"Profile Network Configuration"

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

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

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

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

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

- *Global aliases* are defined from the **Configuration > Network > Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from **Configuration > Devices > System Profile > Network > Alias** screen. These aliases are available for use to a specific group of wireless controllers

or access points. *Alias* values defined in this profile override alias values defined within global aliases.

- *RF Domain aliases* are defined from **Configuration > Devices > RF Domain > Alias** screen. These aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

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

Alias can be classified as:

- "Network Basic Alias"
- "Network Group Alias"
- "Network Service Alias"

Network Basic Alias

- "Alias"

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

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

To edit or delete a basic alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **System Profiles.**

3 Select **Network** to expand it and display its sub menus.

4 Select the **Alias** item, the **Basic Alias** screen displays.

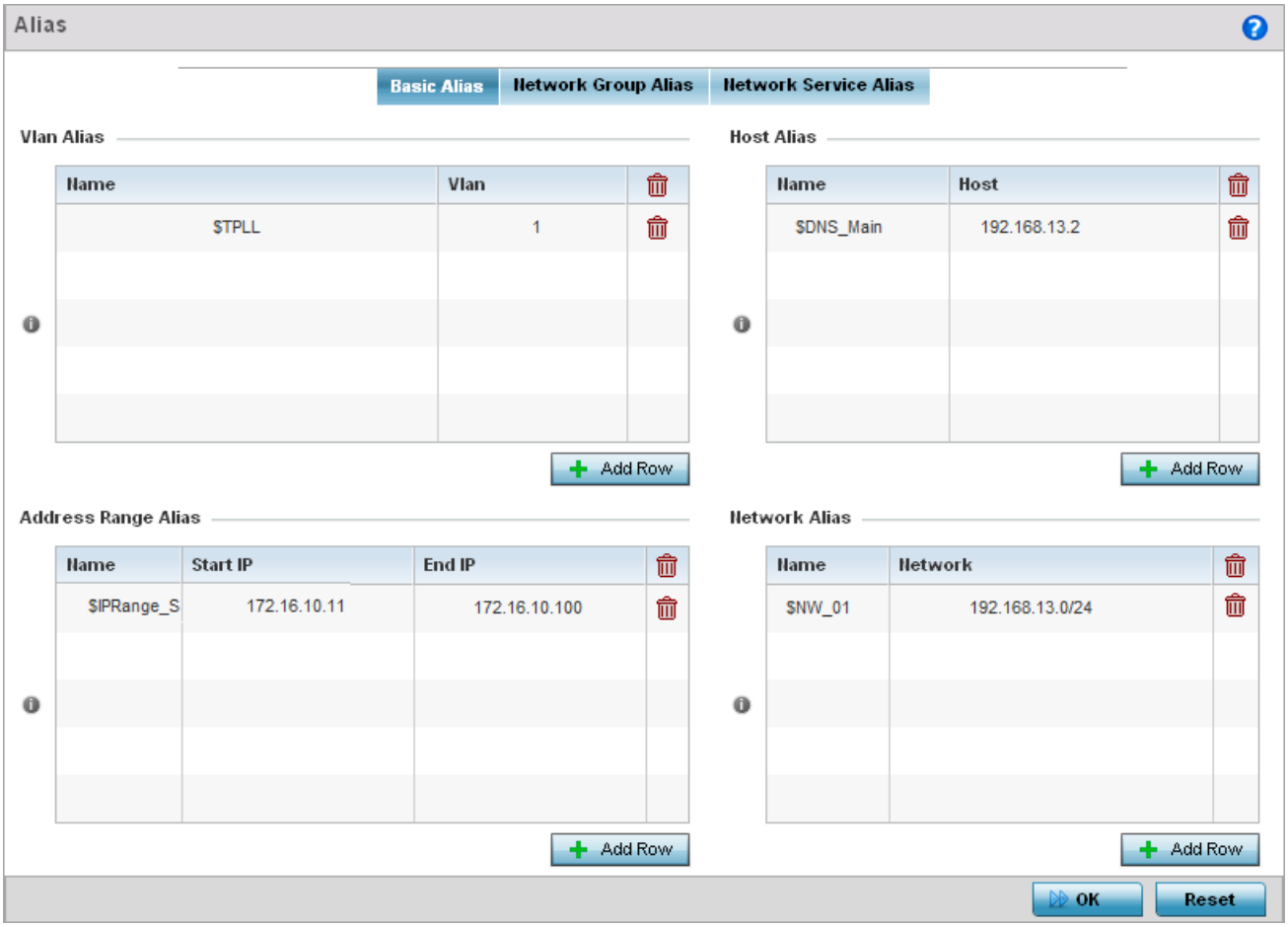


Figure 78: Network - Basic Alias Screen

5 Select **+ Add Row** to define **VLAN Alias** settings:

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

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

A *VLAN alias* is used to replace VLANs in the following locations:

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

6 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 a ending IP address used with a range of addresses utilized with the address range alias.

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

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

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

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

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

- IP Firewall Rules
- DHCP

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

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

- IP Firewall Rules

- DHCP

9 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 string value to use in the alias.

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

10 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

"Alias"

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

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

A *network group alias* 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 **Configuration** tab from the Web user interface.

2 Select **System Profiles.**

3 Select **Network** to expand it and display its sub menus.

4 Select the **Alias** item, the **Basic Alias** screen displays.

5 Select the **Network Group Alias** tab.

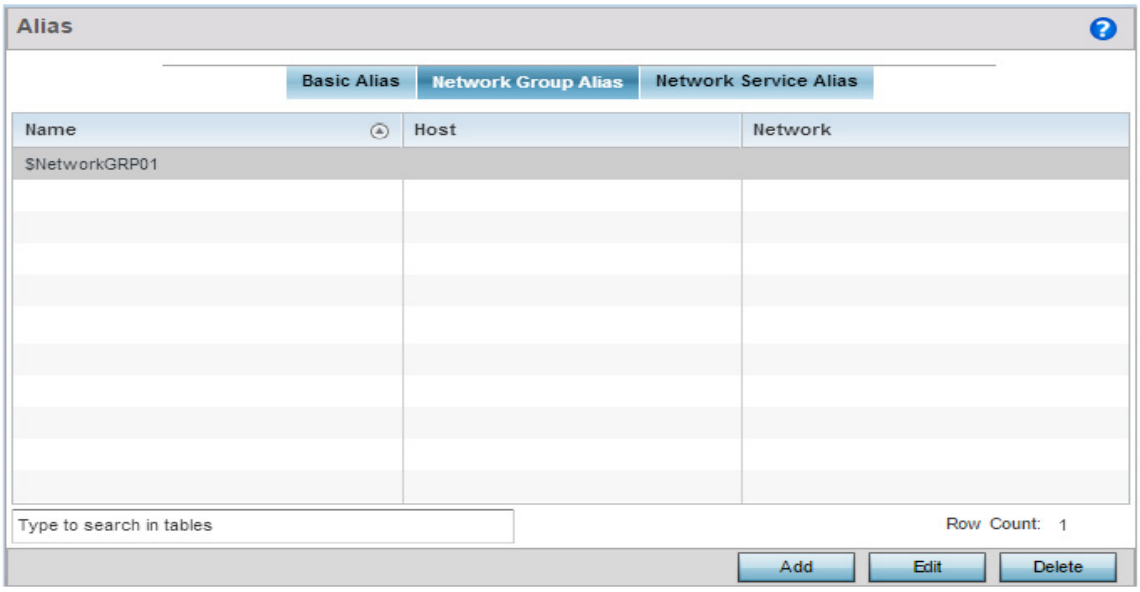


Figure 79: Network - Alias - Network Group Alias screen

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

6 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Group Alias**. **Copy** to copy an existing policy or **Rename** to rename an existing policy.

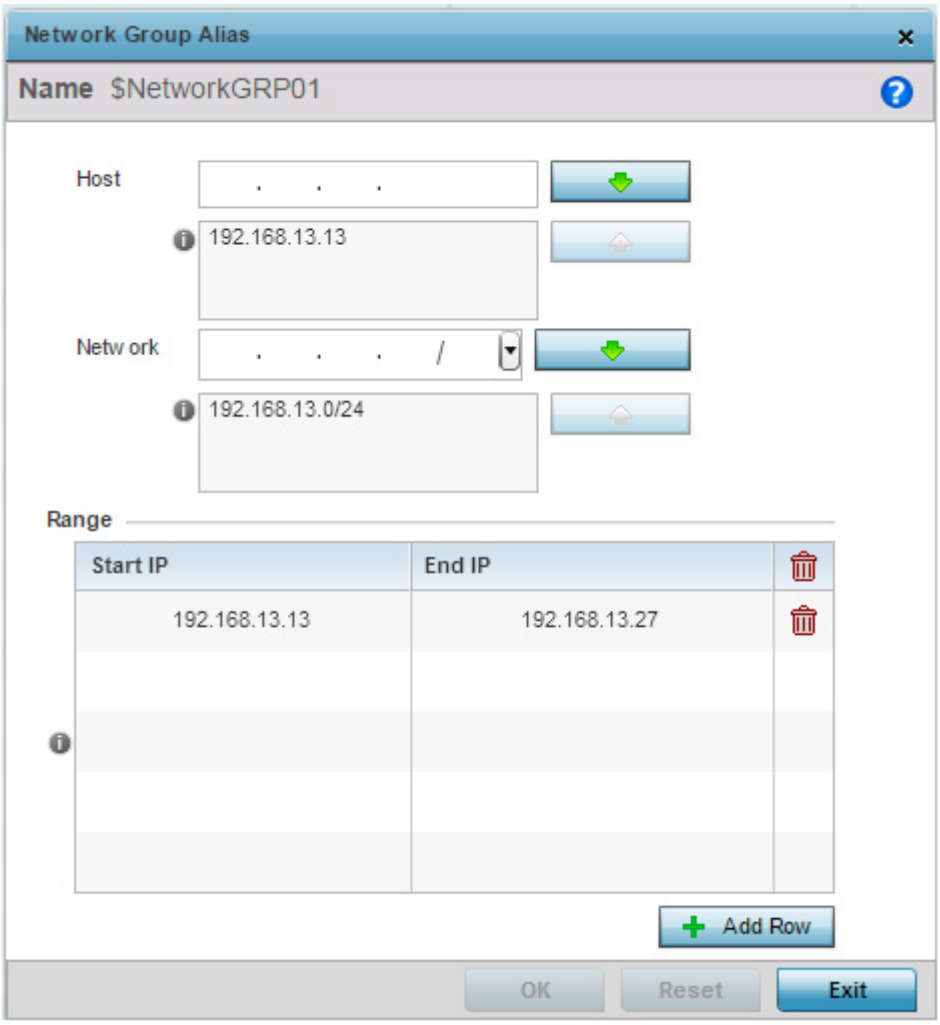


Figure 80: Network - Alias - Network Group Alias Add screen

7 If adding a new **Network Group Alias**, provide it a name of up to 32 characters.

NOTE

The Network Group Alias Name always starts with a dollar sign ($).

8 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.

9 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 an alias range entry to edit it.

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

Network Service Alias

"Alias"

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.

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:

1 Select **Configuration** tab from the Web user interface.

2 Select **System Profiles.**

3 Select **Network** to expand it and display its sub menus.

4 Select the **Alias** item, the **Basic Alias** screen displays.

5 Select the **Network Service Alias** tab.

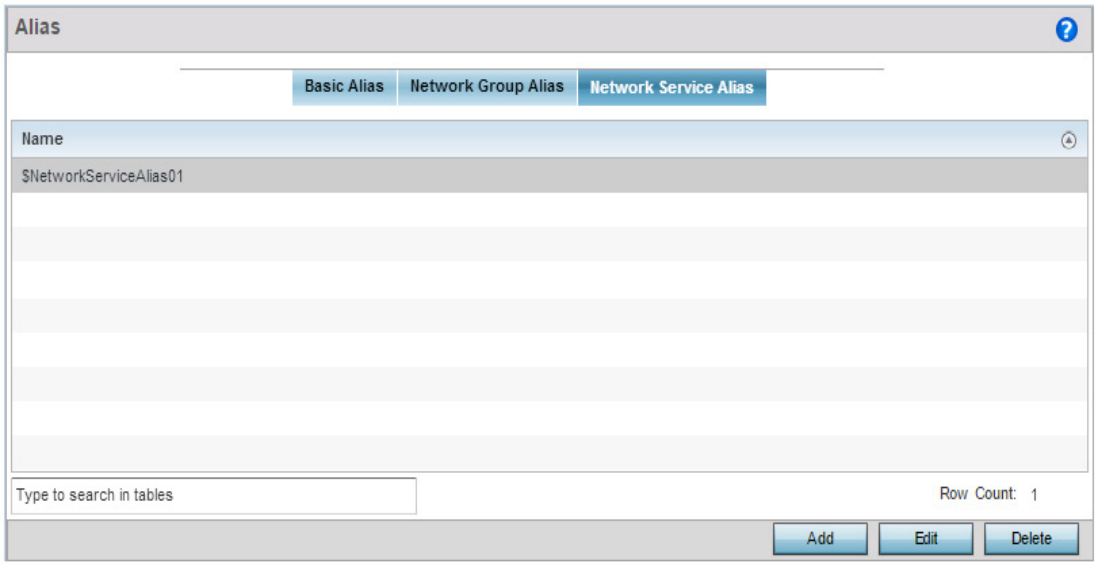


Figure 81: Network - Alias - Network Service Alias screen

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

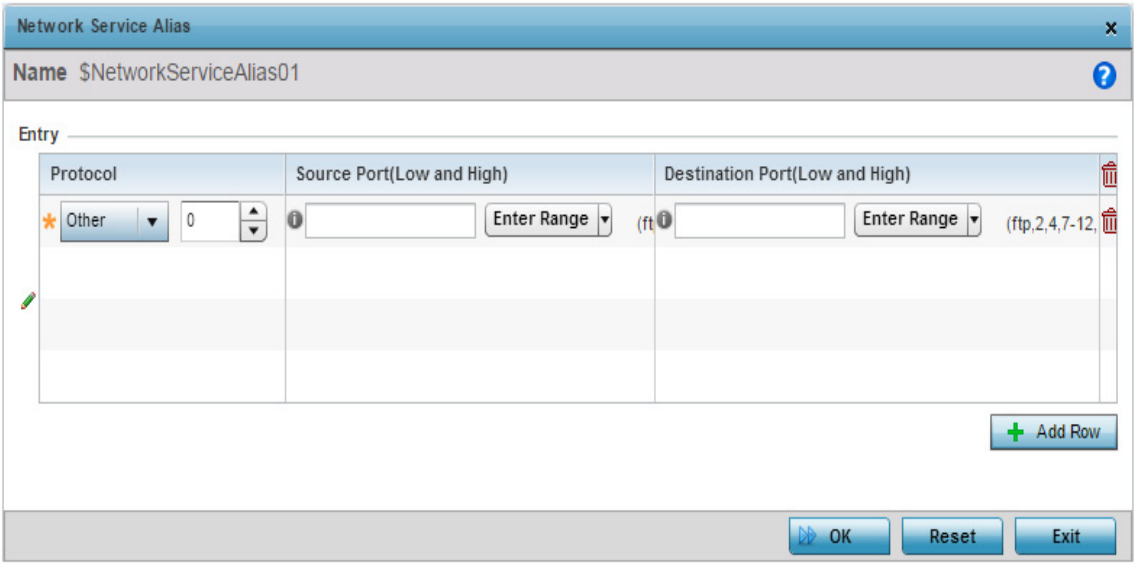


Figure 82: Network - Alias - Network Service Alias Add screen

7 If adding a new **Network Service Alias**, provide it a name up to 32 characters.

NOTE

The **Network Service Alias Name** always starts with a dollar sign ($).

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

Protocol	Specify the protocol for which the alias has to be created. Use the drop-down 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)	Use this field only if the protocol is *tcp* or *udp*. Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	Use this field only if the protocol is *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

9 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

"Profile Network 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 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **IPv6 Neighbor**.

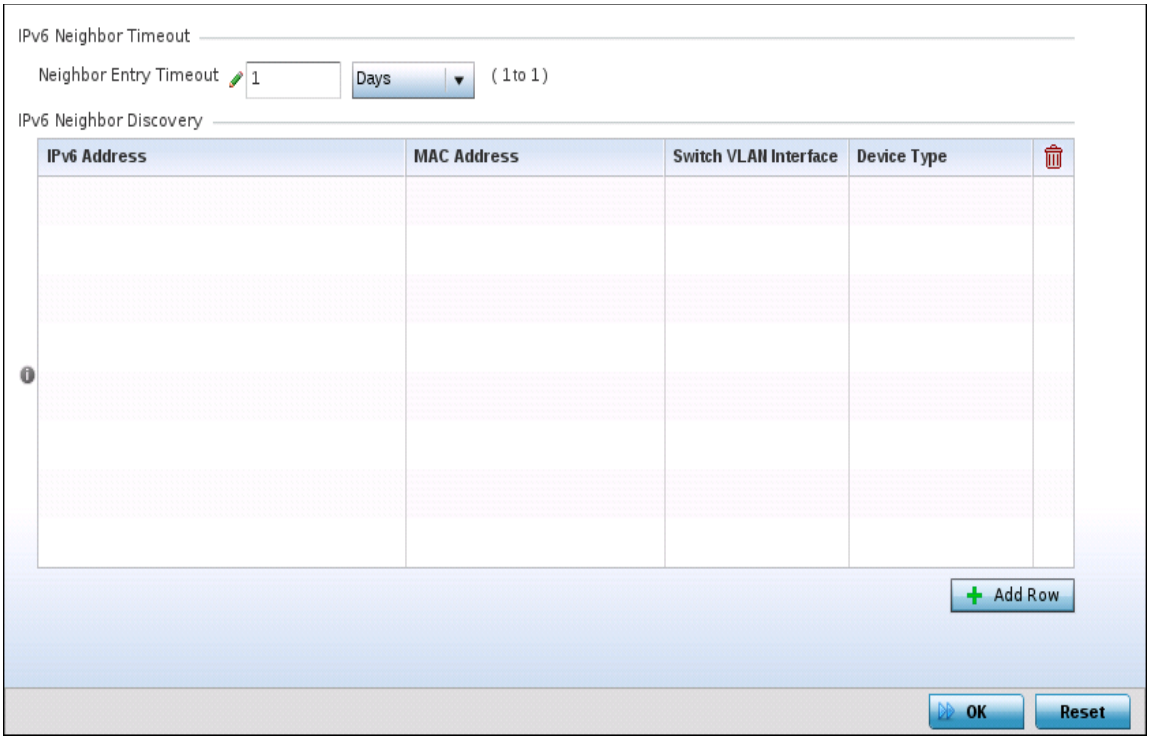


Figure 83: IPv6 Neighbor screen

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** to define the configuration of **IPv6 Neighbor Discovery** configurations. A maximum of 256 neighbor entries can be defined.

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*.

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

Profile Network Configuration and Deployment Considerations

"Profile Network Configuration"

Before defining a profile's network configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception.
- Static routes, while easy, can be overwhelming within a large or complicated network. Each time there is a change, someone must manually make changes to reflect the new route. If a link goes down, even if there is a second path, the router would ignore it and consider the link down.
- Static routes require extensive planning and have a high management overhead. The more routers that exist in a network, the more routes need to be configured. If you have N number of routers and a route between each router is needed, then you must configure N x N routes. Thus, for a network with nine routers, you will need a minimum of 81 routes (9 x 9 = 81).

Profile Security Configuration

"System Profile Configuration"

An access point profile can have its own firewall policy, wireless client role policy, WEP shared key authentication and NAT policy applied.

For more information, refer to the following:

- "Defining Profile VPN Settings"
- "Defining Profile Auto IPSec Tunnel"
- "Defining Profile Security Settings"
- "Setting the Certificate Revocation List (CRL) Configuration"
- "Setting the Profile's RADIUS Trustpoint Configuration"
- "Setting the Profile's NAT Configuration"
- "Setting the Profile's Bridge NAT Configuration"
- "Setting a Profile's Application Visibility Settings"

Defining Profile VPN Settings

"Profile Security Configuration"

IPSec VPN provides a secure tunnel between two networked peer access points or controllers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPSec peer, however for remote VPN deployments one crypto map is used for all the remote IPSec peers.

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 settings:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **VPN**.

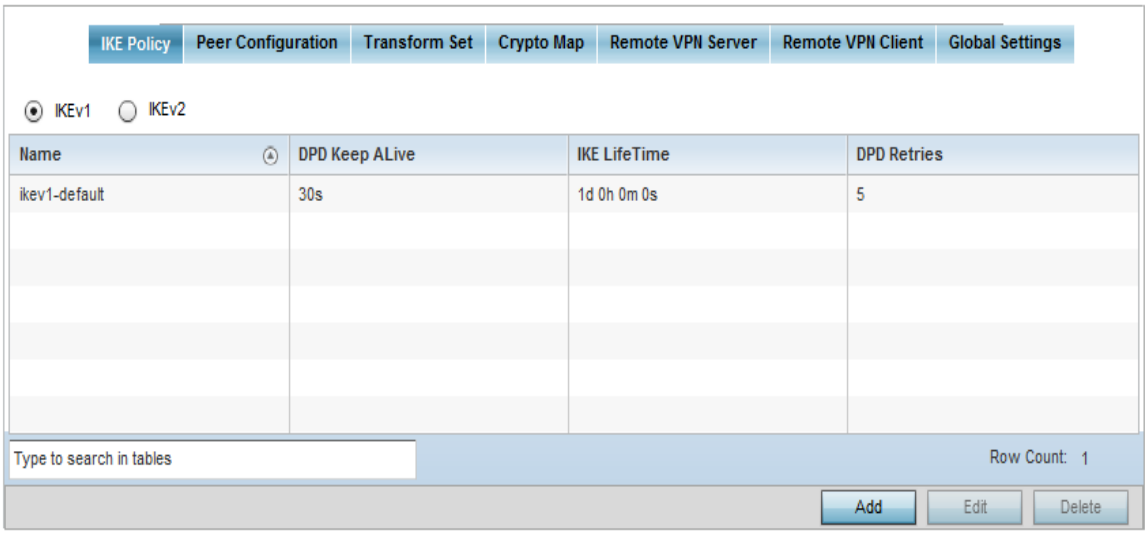


Figure 84: Profile Security - VPN IKE Policy screen

5 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.

6 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 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.

7 Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

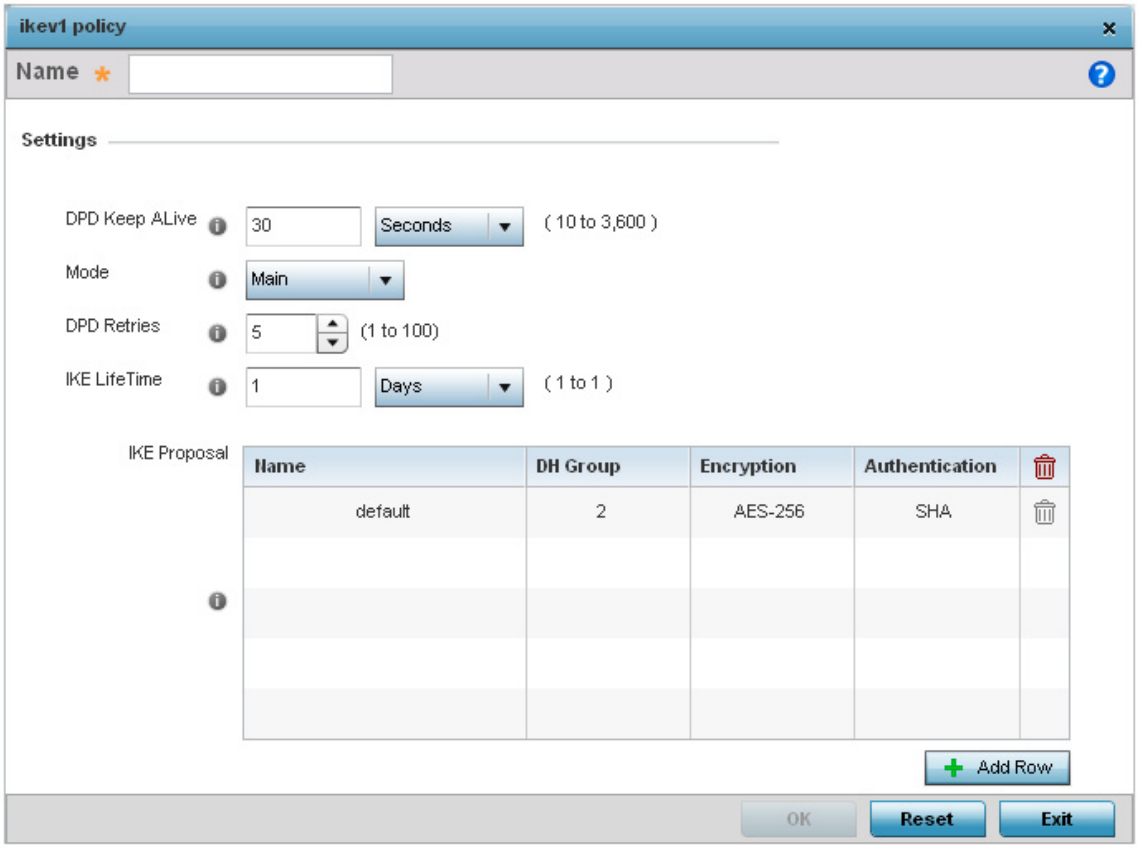


Figure 85: Profile Security - VPN IKE Policy create/modify screen (IKEv1 example)

Name	If creating a new IKE policy, assign it a name (32 character maximum) 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 drop-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.

8 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 tunnelled peers to securely interoperate. Options include *3DES*, *AES*, *AES-192* and *AES-256*. The default setting is AES-256.
Authentication	Select an authentication hash algorithm used by the peers to exchange credential information. Options include *SHA* and *MD5*. The default setting is SHA. The option *aes-xcbc-mac* is only available for IKEv2 and is not available on AP7131, AP7181, AP8132, AP82XX, RFS4000, RFS6000 and RFS7000 platforms.

9 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 to remove a peer configuration.

10 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.

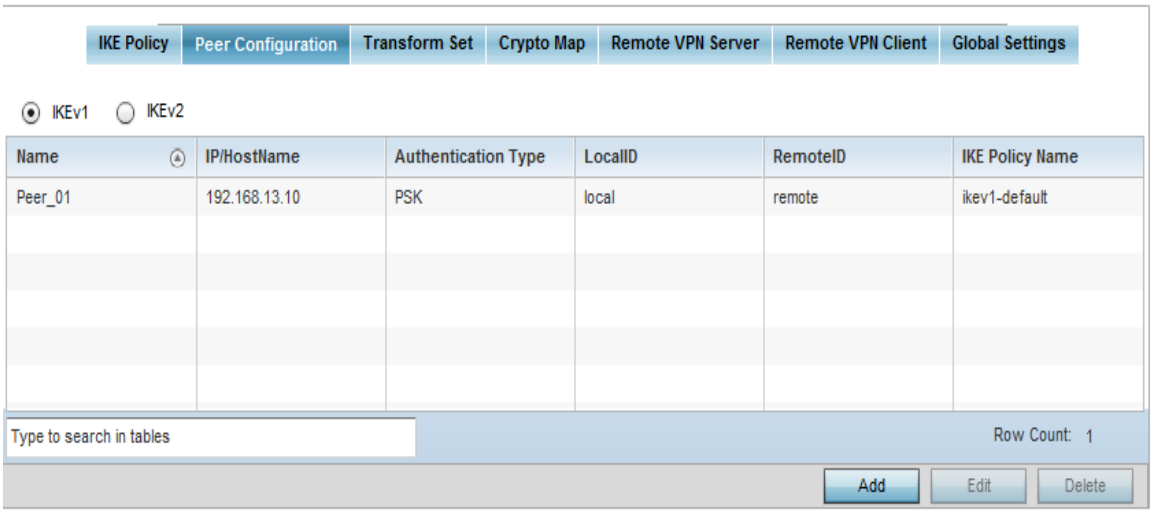


Figure 86: Profile Security - VPN Peer Destination screen (IKEv1 example)

11 Select either the **IKEv1** or **IKEv2** radio button to enforce VPN key exchanges using either IKEv1 or IKEv2.

12 Refer to the following to determine whether a VPN **Peer Configuration** requires creation, modification or removal:

Name	Lists the 32 character maximum name assigned to each listed peer configuration.
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 is the first algorithm known to be suitable for signing, as well as encryption. If using *IKEv2*, this screen displays both local and remote authentication, as both ends of the VPN connection require authentication.
LocalID	Lists the access point's 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.

13 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.

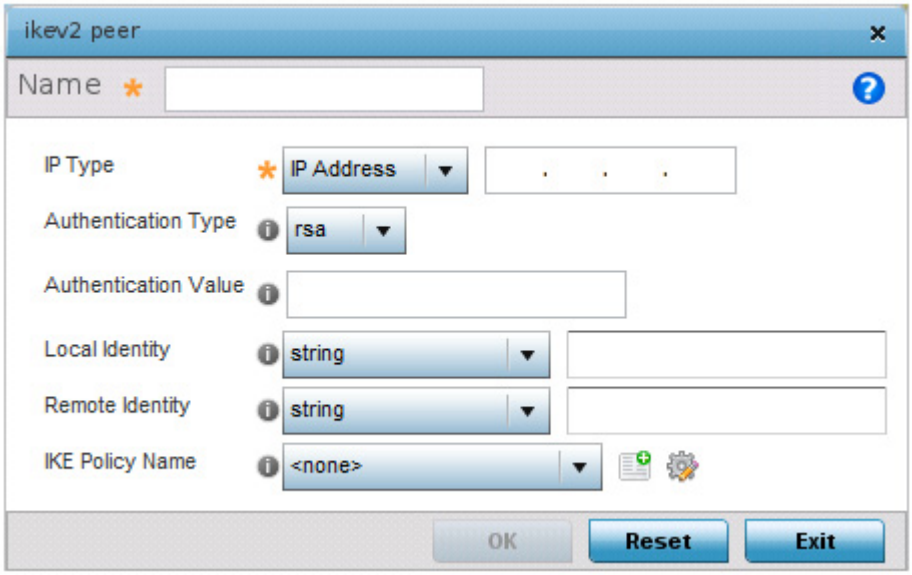


Figure 87: Profile Security - VPN Peer Configuration create/modify screen (IKEv2 example)

Name	If creating a new peer configuration (remote gateway) for VPN tunnel connection, assign it a name (32 character maximum) to distinguish it from others 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 or **Local Authentication Type**	Select either *pre-shared key* (PSK) or RSA. *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 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 or **Local Authentication Value**	Define the authentication string (shared secret) that must be shared by both ends of the VPN tunnel connection. The string must be from 8 - 21 characters long. If using *IKEv2*, both a local and remote string must be specified for handshake validation and both ends (local and remote) of the VPN connection.
Local Identity	Select the access point's 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 access point's 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.

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

15 Select the **Transform Set** tab.

Create or modify **Transform Set** configurations to specify how traffic is protected within crypto ACL defining the traffic that needs to be protected.

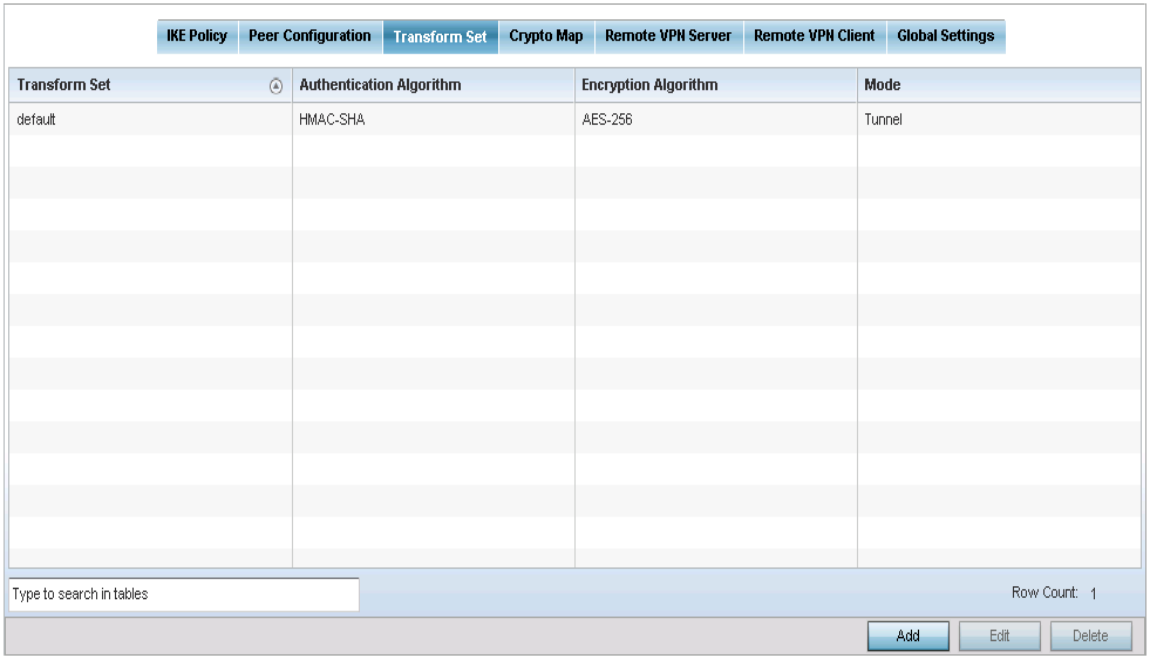


Figure 88: Profile Security - VPN Transform Set tab

16 Review the following attributes of an existing **Transform Set** configurations:

Transform Set	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 is either *sha256-hmac, aes-xcbc-mac, HMAC-SHA* or *HMAC-MD5*. The option *aes-xcbc-mac* is not available on AP7131, AP7181, AP8132, AP82XX, RFS4000, RFS6000 and RFS7000 platforms.
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.

17 Select **Add** to define a new transform set configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing transform set.

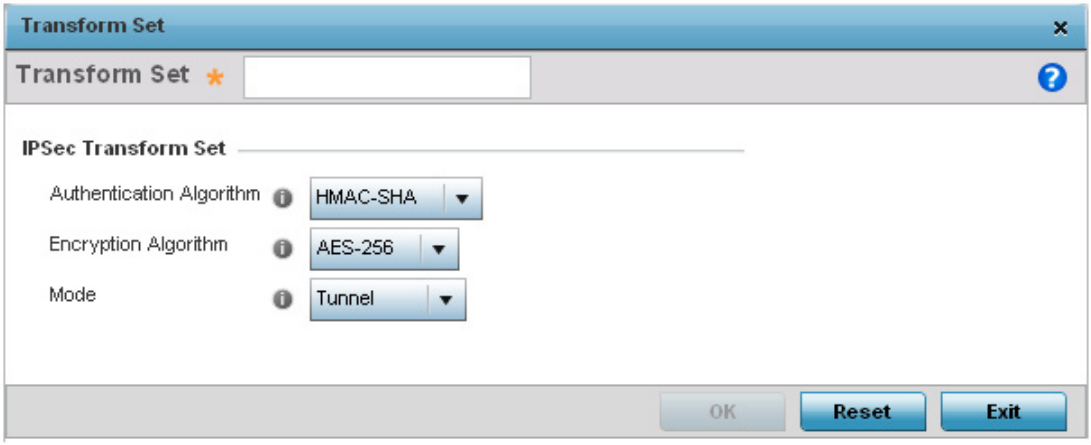


Figure 89: Profile Security - VPN Transform Set create/modify screen

18 Define the following settings for the new or modified **Transform Set** configuration:

Transform Set	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 drop-down menu to select either *sha256-hmac, aes-xcbc-mac, HMAC-SHA* or *HMAC-MD5*. The default setting is HMAC-SHA. The option *aes-xcbc-mac* is not available on AP7131, AP7181, AP8132, AP82XX, RFS4000, RFS6000 and RFS7000 platforms.
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 drop-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.

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

20 Select the **Crypto Map** tab.

Use crypto maps (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).

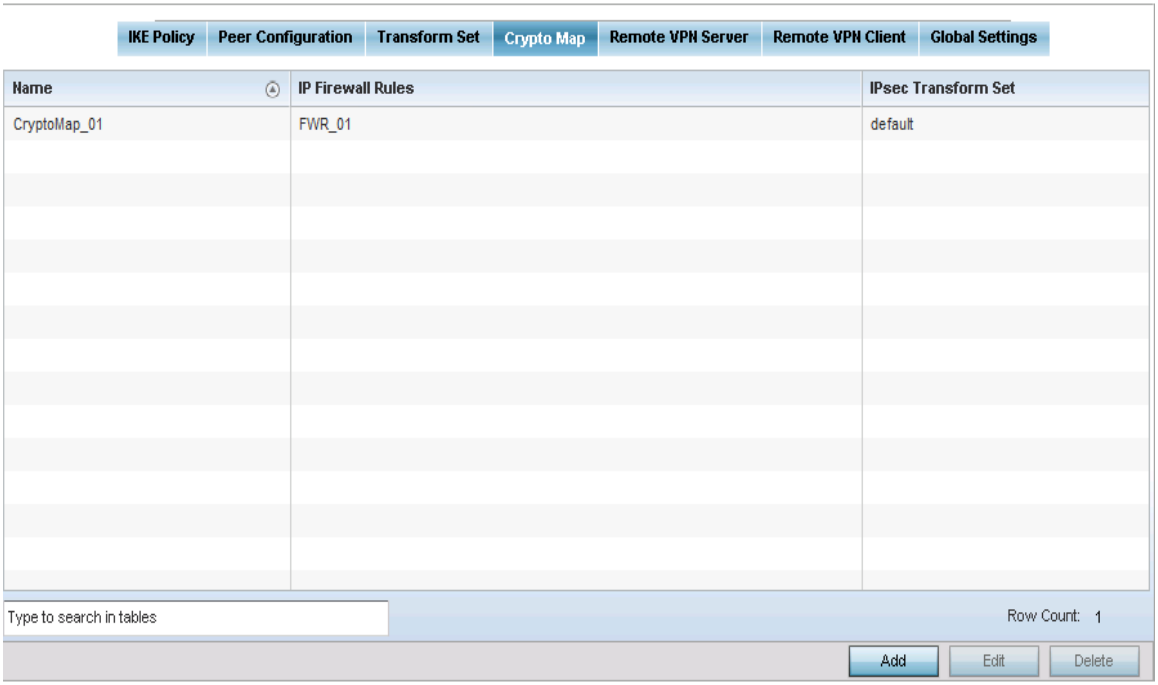


Figure 90: Profile Security - VPN Crypto Map tab

21 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.
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.

22 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.

23 If adding a new crypto map, assign it a name up to 32 characters as a unique identifier. Select the **Continue** button to proceed to the **VPN Crypto Map** screen.

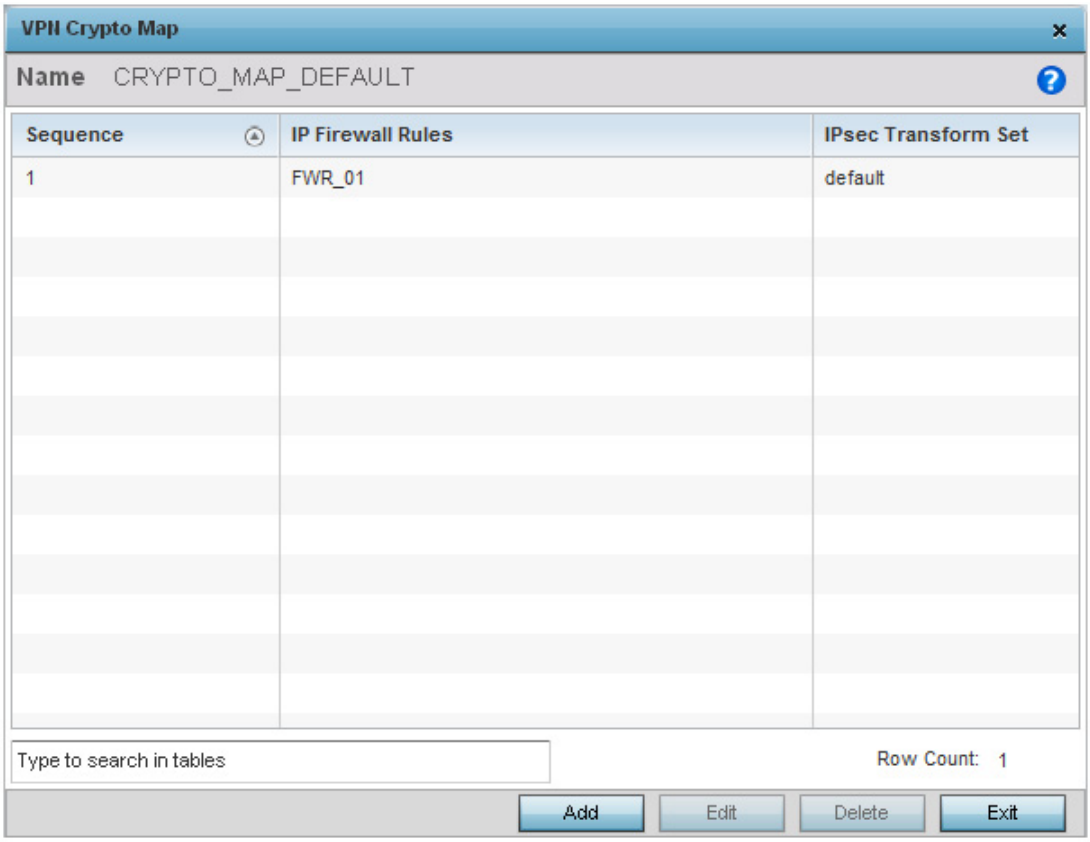


Figure 91: Profile Security - VPN Crypto Map screen

24 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).
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.

25 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.

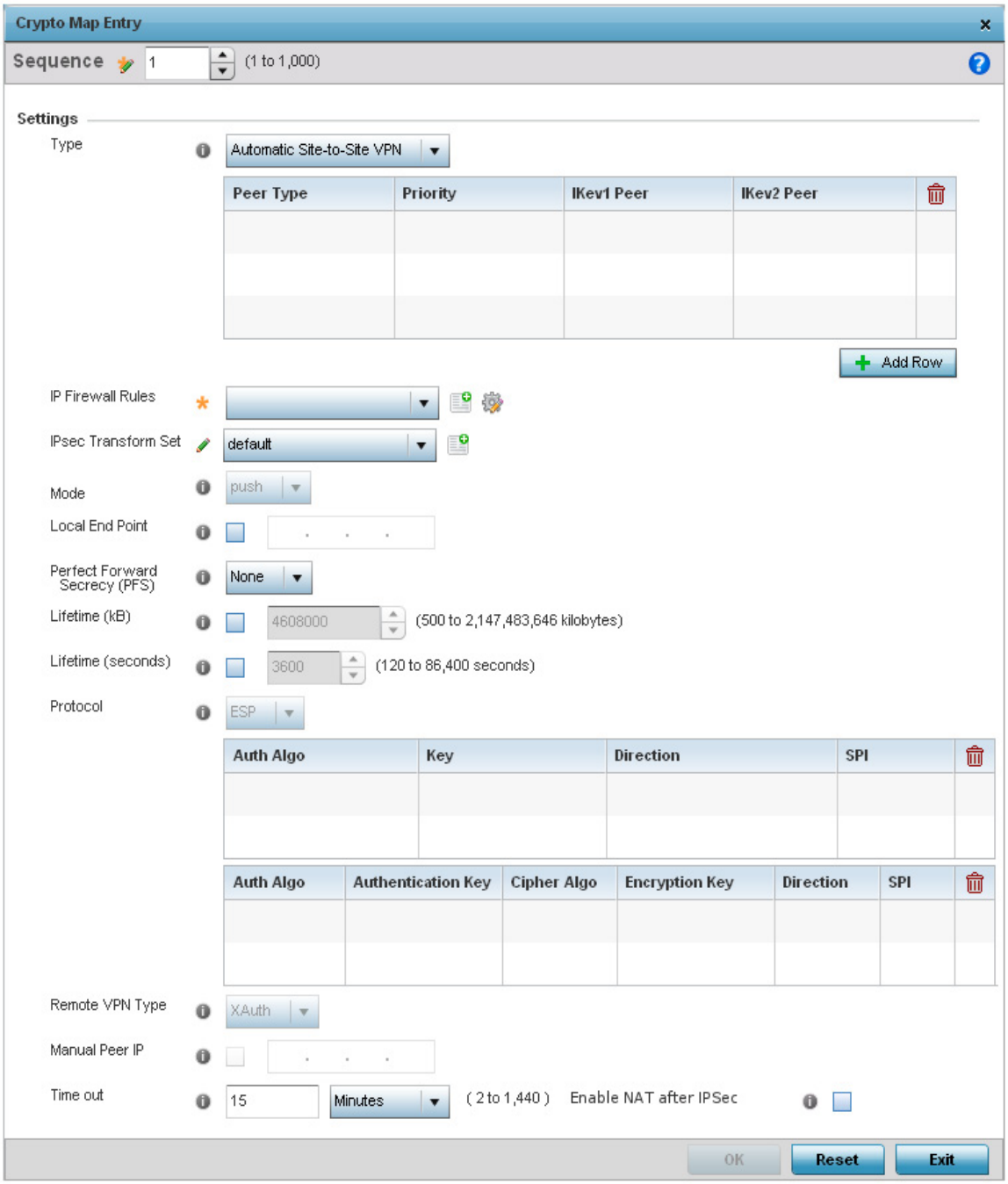


Figure 92: Profile Security - VPN Crypto Map Entry screen

26 Define the following parameters to set the crypto map configuration:

Sequence	Each crypto map configuration uses a list of entries based on a sequence number. Specifying multiple sequence numbers within the same crypto map extends connection flexibility to multiple peers on the same interface, based on this selected sequence number (from 1 - 1,000).
Type	Define the *site-to-site-manual*, *site-to-site-auto* or *remote VPN* configuration defined for each listed crypto map configuration.
IP Firewall Rules	Use the drop-down menu to select the *access list* (ACL) used to protect IPSec VPN traffic. New access/deny rules can be defined for the crypto map by selecting the *Create* icon, or an existing set of firewall rules can be modified by selecting the *Edit* icon.
IPSec Transform Set	Select the transform set (encryption and hash algorithms) to apply to this crypto map configuration.
Mode	Use the drop-down menu to define which mode (pull or push) is used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push.
Local End Point	Select this option to define an IP address as a local tunnel end-point address. This setting represents an alternative to an interface IP address.
Perfect Forward Secrecy (PFS)	PFS is key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must not be used to derive any additional keys. Options include *None*, *2*, *5* and *14*. The default setting is None.
Lifetime (kB)	Select this option to define a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes.
Lifetime (seconds)	Select this option to define a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. The available range is from 120 - 86,400 seconds. The default setting is 120 seconds.
Protocol	Select the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include *ESP* and *AH*. The default setting is *ESP*.
Remote VPN Type	Define the remote VPN type as either *None* or *XAuth*. XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device respond with a failed or passed message. The default setting is XAuth.
Manual Peer IP	Select this option to define the IP address of an additional encryption/ decryption peer.
Time Out	Select this option to set the IPSec SA time out value. Use the textbox and the drop-down list to configure the time out duration.
Enable NAT after IPSec	Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels.

27 Select **OK** to save the updates made to the **Crypto Map Entry** screen. Selecting **Reset** reverts the screen to its last saved setting.

28 Select **Remote VPN Server**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

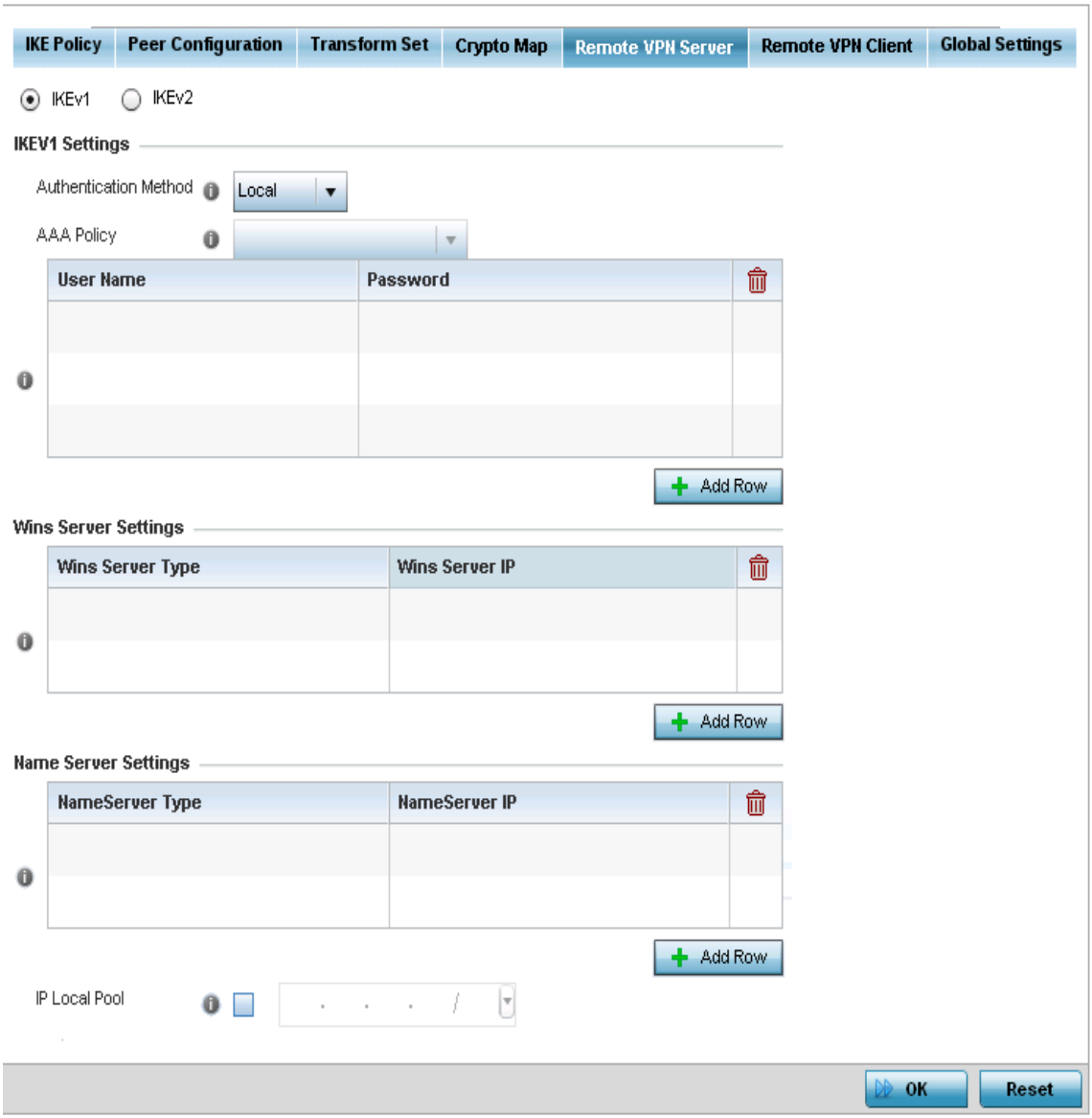


Figure 93: Profile Security - Remote VPN Server tab (IKEv2 example)

29 Select either the **IKEv1** or **IKEv2** radio button to enforce peer key exchanges over the remote VPN server using either IKEv1 or IKEv2.

IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the screen differs depending on the selected IKE mode.

30 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. AP6511 and AP6521 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 information and user authentication data.

31 Refer to the **Username Password Settings** field and specify the username and password for validating RADIUS authentication.

32 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.

33 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.

34 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.

35 If using IKEv2 specify following additional settings (required for IKEv2 only):

DHCP Server Type	Specify whether the *Dynamic Host Configuration Protocol* (DHCP) server is specified as an *IP address*, *Hostname (FQDN)* or *None* (a different classification will be defined). DHCP allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside.
DHCP Server	Depending on the DHCP server type selected, enter either the numerical IP address, hostname or other (if None is selected as the server type).
IP Local Pool	Select this option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients.
Relay Agent IP Address	Select this option to define DHCP relay agent IP address.

36 Select **OK** to save the updates made to the **Remote VPN Server** screen. Selecting **Reset** reverts the screen to its last saved configuration.

37 Select the **Remote VPN Client** tab.

The **Remote VPN Client** screen provides options for configuring the remote VPN client.

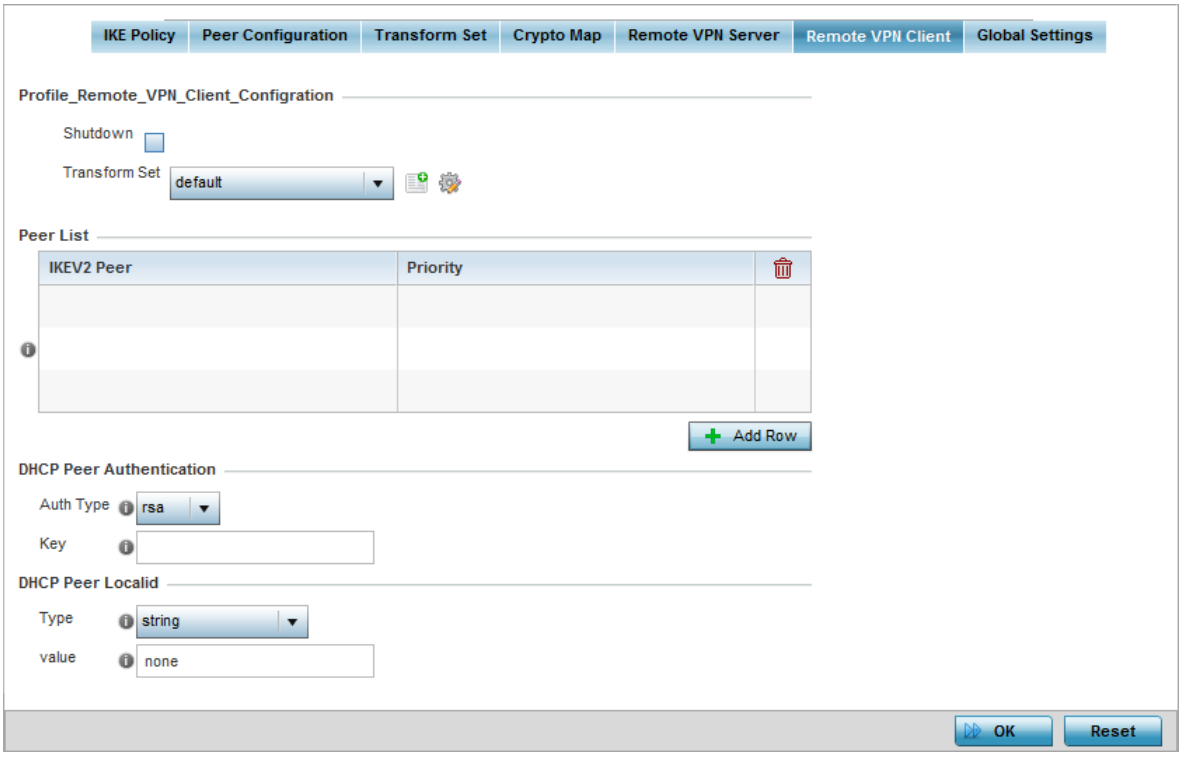


Figure 94: Profile Security - Remote VPN Client tab

38 Refer to the following fields to define **Remote VPN Client Configuration** settings:

Shutdown	Select this option to disable the remote VPN client. The default is *disabled.*
Transform Set	Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down menu or click the icon next to the drop-down menu to create a new transform set.

39 Refer to the following fields to define the Remote VPN Client **Peer list**:

IKEV2 Peer	Use the drop-down menu to select the remote IKE v2 peer. Use the icon next to the drop-down to create a new peer.
Priority	Use the spinner to set the priority in which a remote peer is connected. The lower the number the higher the priority.

40 Set the following **DHCP Peer Authentication** settings:

Auth Type	Use the drop-down menu to specify the DHCP peer authentication type. Options include *PSK* and *rsa*. The default setting is rsa.
Key	Provide a 8 - 21 character shared key password for DHCP peer authentication.

41 Set the following **DHCP Peer Localid** settings:

Type	Select the DHCP peer local ID type. Options include *string* and *autogen-uniqueid*. The default setting is string.
value	Set the DHCP peer local ID. The ID cannot exceed 128 characters.

42 Select **OK** to save the updates made to the **Remote VPN Client** screen. Selecting **Reset** reverts the screen to its last saved configuration.

43 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.

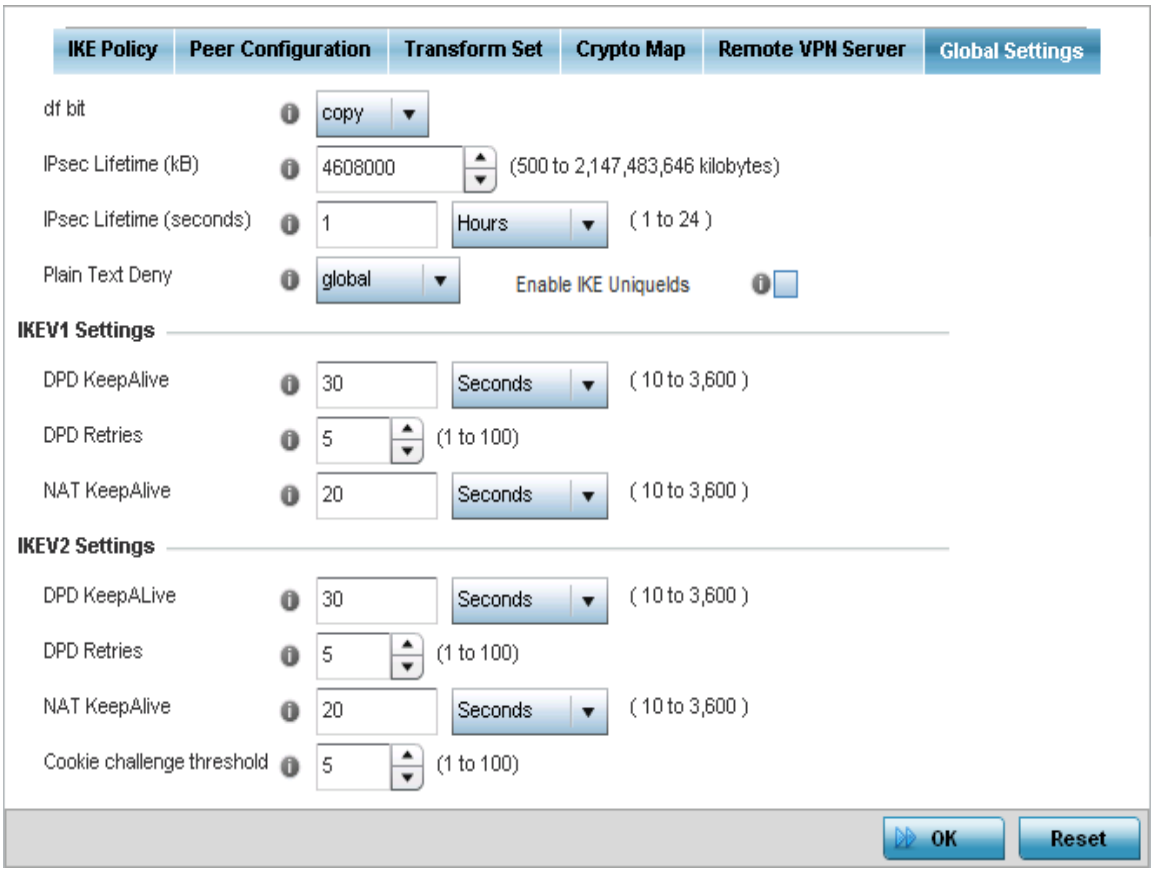


Figure 95: Profile Security - Global VPN Settings tab

44 Refer to the following fields to define IPSec security, lifetime and authentication settings:

df bit	Select the DF bit handling technique used for the ESP encapsulating header. Options include *clear*, *set* and *copy*. The default setting is copy.
IPsec Lifetime (kb)	Set a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes. The default settings is 4,608,000 kilobytes.
IPsec Lifetime (seconds)	Set a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. Options include *Seconds* (120 - 86,400), *Minutes* (2 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 3,600 seconds.
Plain Text Deny	Select *global* or *interface* to set the scope of the ACL. The default setting is global, expanding the rules of the ACL beyond just the interface.
Enable IKE Uniqueids	Select this option to initiate a unique ID check. This is disabled by default.

45 Define the following IKE Dead Peer Detection settings:

DPD Keep Alive	Define the interval (or frequency) of IKE keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 30 seconds.
DPD Retries	Use the spinner control to define the number of keep alive messages sent to an IPSec VPN client before the tunnel connection is defined as dead. The available range is from 1 - 100. The default number of messages is 5.
NAT Keep Alive	Define the interval (or frequency) of NAT keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 20 seconds.
Cookie Challenge Threshold	Use the spinner control to define the threshold (1 - 100) that, when exceeded, enables the cookie challenge mechanism.
Crypto NAT Pool	Use the drop-down menu to select the NAT pool for internal source NAT for IPSec tunnels.

46 Select **OK** to save the updates made to the **Global Settings** screen. Selecting **Reset** reverts the screen to its last saved configuration.

Defining Profile Auto IPSec Tunnel

"Profile Security Configuration"

IPSec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Auto IPSec Tunnel**.

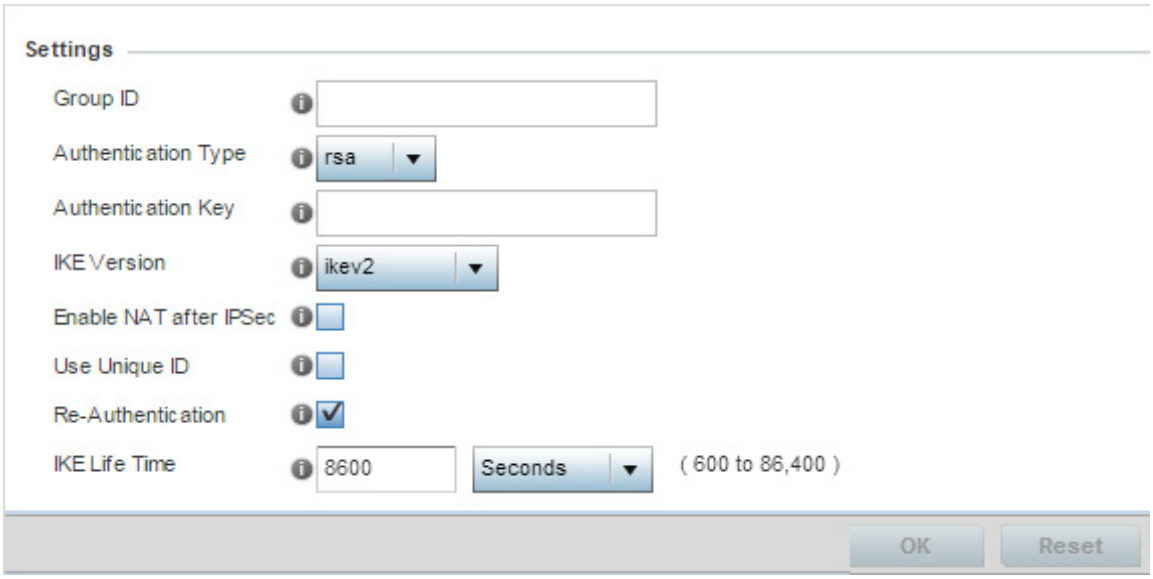


Figure 96: Profile Security – Auto IPSec Tunnel screen

5 Refer to the following table to configure the Auto IPSec Tunnel settings:

Group ID	Configure the ID string used for IKE authentication. String length can be between 1 - 64 characters.
Authentication Type	Set the IPSec Authentication Type. Options include *PSK* (Pre Shared Key) or *rsa.*
Authentication Key	Set the common key for authentication between the remote tunnel peer. Key length is between 8 - 21 characters.
IKE Version	Configure the IKE version to use. The available options are *ikev1-main*, *ikev1-aggr* and *ikev2.*
Enable NAT after IPSec	Select this option to enable NAT after IPSec. Enable this option if there are NATted networks behind VPN tunnels.
Use Unique ID	In scenarios where different access points behind different NAT boxes/ routers have the same IP address, it is not possible to create a tunnel between the wireless controller and access point, as the wireless controller fails to identify the access point uniquely. When selected, each access point behind the same NAT box/router will have a unique ID. This unique ID is used to create the VPN tunnel.
Re-Authentication	Select this option to re-authenticate the key on a IKE rekey. This setting is disabled by default.
IKE Life Time	Set a lifetime in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1) for IKE security association duration. The default is 8600 seconds.

6 Select **OK** to save the updates made to the **Auto IPSec Tunnel** screen. Selecting **Reset** reverts the screen to its last saved configuration.

Defining Profile Security Settings

"Profile Security Configuration"

A profile can leverage existing firewall, wireless client role and WIPS policies and configurations 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 access point's numerous deployment scenarios.

To define a profile's security settings:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Settings**.

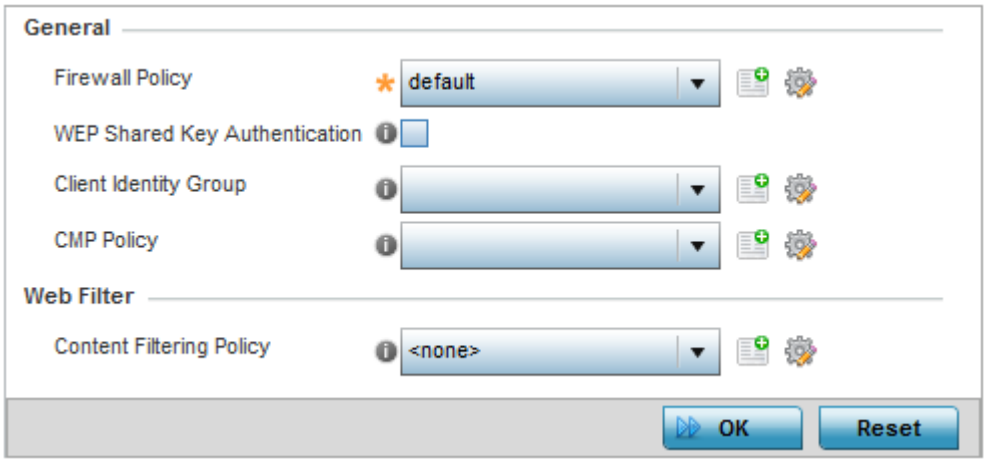


Figure 97: Profile Security - Settings screen

5 Select a firewall policy from the **Firewall Policy** drop-down menu. All devices using this profile must meet the requirements of the firewall policy to access the network. A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. If an existing Firewall policy does not meet your requirements, select the *Create* icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.

6 Select the **WEP Shared Key Authentication** radio button to require profile supported devices to use a WEP key to access the network using this profile. The access point, other proprietary routers, and our clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without our adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

7 Client Identity is a set of unique fingerprints used to identify a class of devices. This information is used to configure permissions and access rules for devices classes in the network. **Client Identity Group** is a collection of client identities that identify devices and applies specific permissions and restrictions on these devices. From the drop-down

menu select the client identity group to use with this device profile. For more information, see "Device Fingerprinting" on page 735.

8 *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. Use the drop-down list to select a CMP policy to apply.

9 Use the **Web Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

Web filtering is used to restrict access to resources on the Internet.

10 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

"Profile Security 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** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Certificate Revocation**.

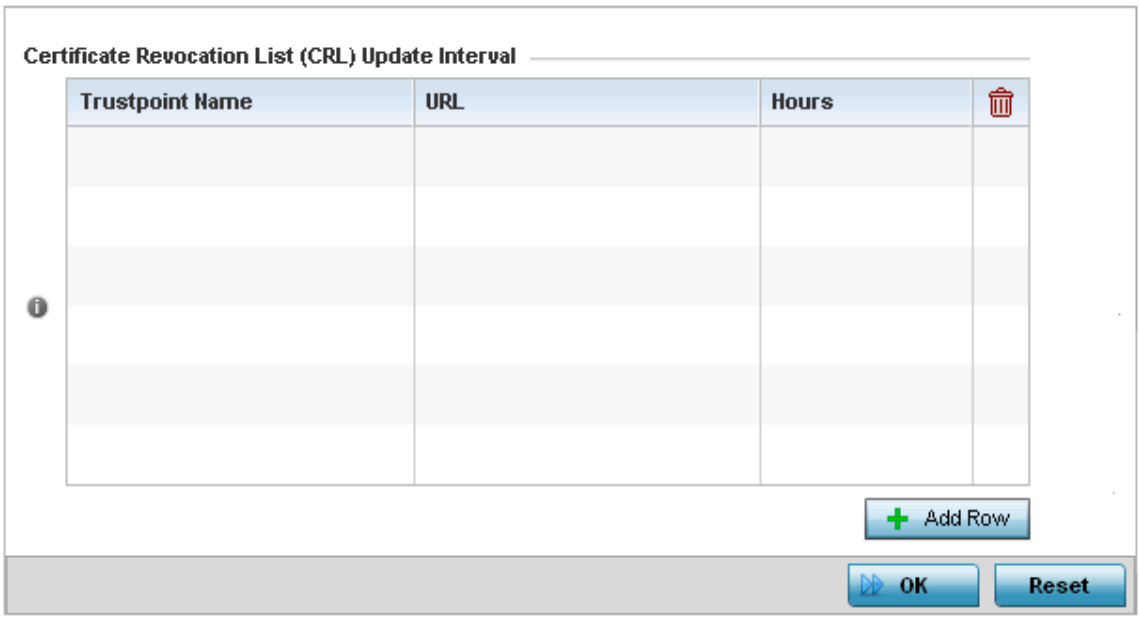


Figure 98: Profile Security - Certificate Revocation List (CRL) Update Interval screen

5 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.

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.

6 Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.

7 Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.

8 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.

9 Select **OK** to save the changes made within the **Certificate Revocation List (CRL) Update Interval** screen. Select **Reset** to revert to the last saved configuration.

Setting the Profile's RADIUS Trustpoint Configuration

"Profile Security Configuration"

A RADIUS 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.

To define a RADIUS Trustpoint configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

3 Select **System Profiles** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **RADIUS Trustpoints**.

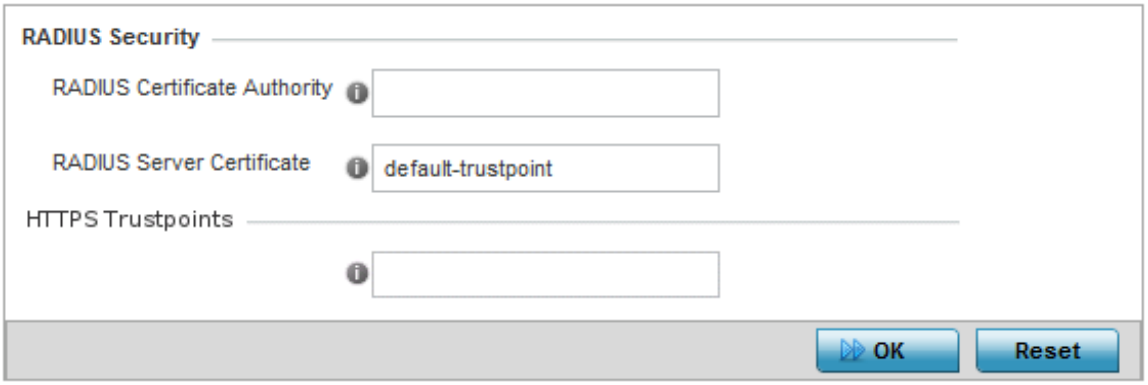


Figure 99: Security - RADIUS Trustpoint screen

5 Set the following **RADIUS Security** certificate settings:

RADIUS Certificate Authority	Either use the *default-trustpoint* or select the *Stored* radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the *Launch Manager* button.
RADIUS Server Certificate	Either use the *default-trustpoint* or select the *Stored* radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the *Launch Manager* button.

6 Set the following **HTTPS Trustpoints**:

HTTPS Trustpoint	Either use the default trustpoint or select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be utilized. To use an existing certificate for this device, select the **Launch Manager** button. For more information, see "Manage Certificates" on page 301.

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

Setting the Profile's NAT Configuration

"Profile Security 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 a profile outbound Internet access to wired and wireless hosts connected to an access point. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an 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 a NAT configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **NAT**.

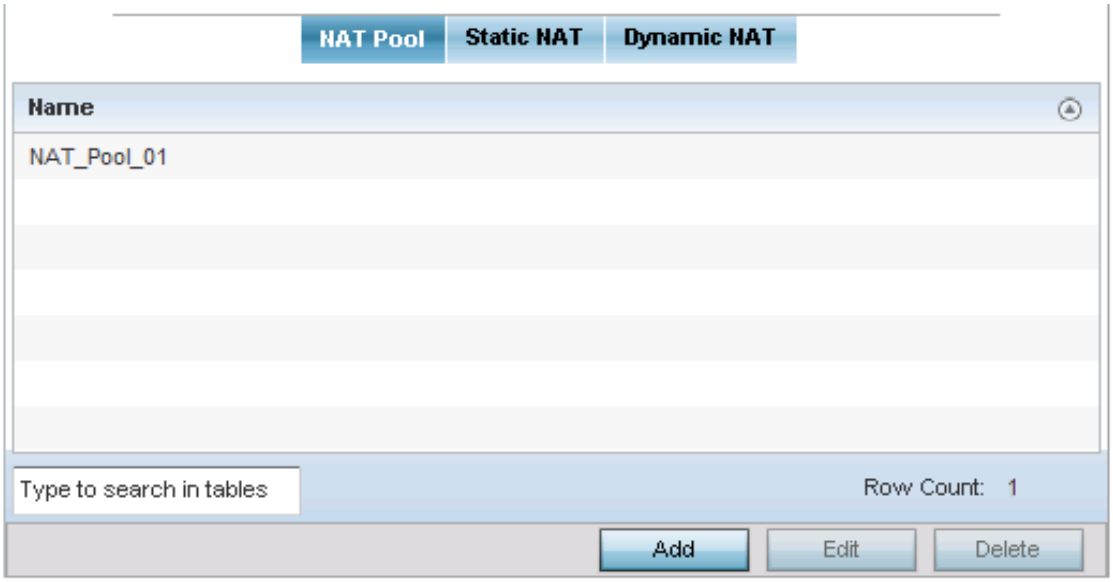


Figure 100: Profile Security - NAT Pool tab

The **NAT Pool** tab displays by default. The NAT Pool tab lists those NAT policies created thus far. Any of these policies can be selected and applied to the access point profile.

5 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.

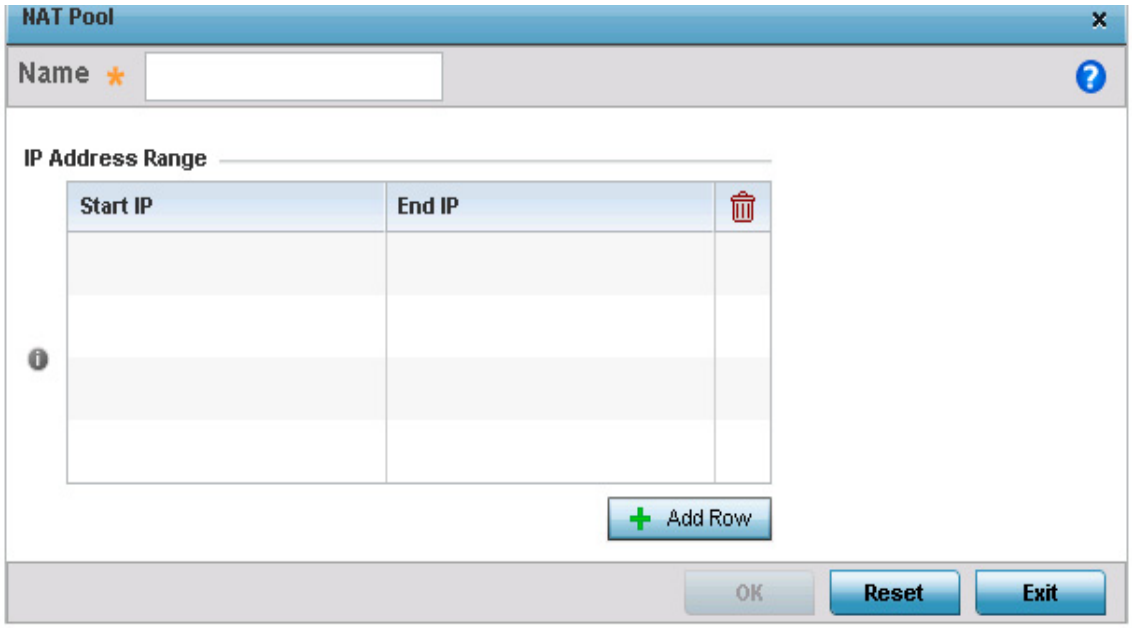


Figure 101: Profile Security - NAT Pool tab - NAT Pool field

6 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 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 being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

7 Select the **+ Add Row** button to append additional rows to the **IP Address Range** table.

8 Select **OK** to save the changes made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.

9 Select the **Static NAT** tab. The **Source** tab displays by default.

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.

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.

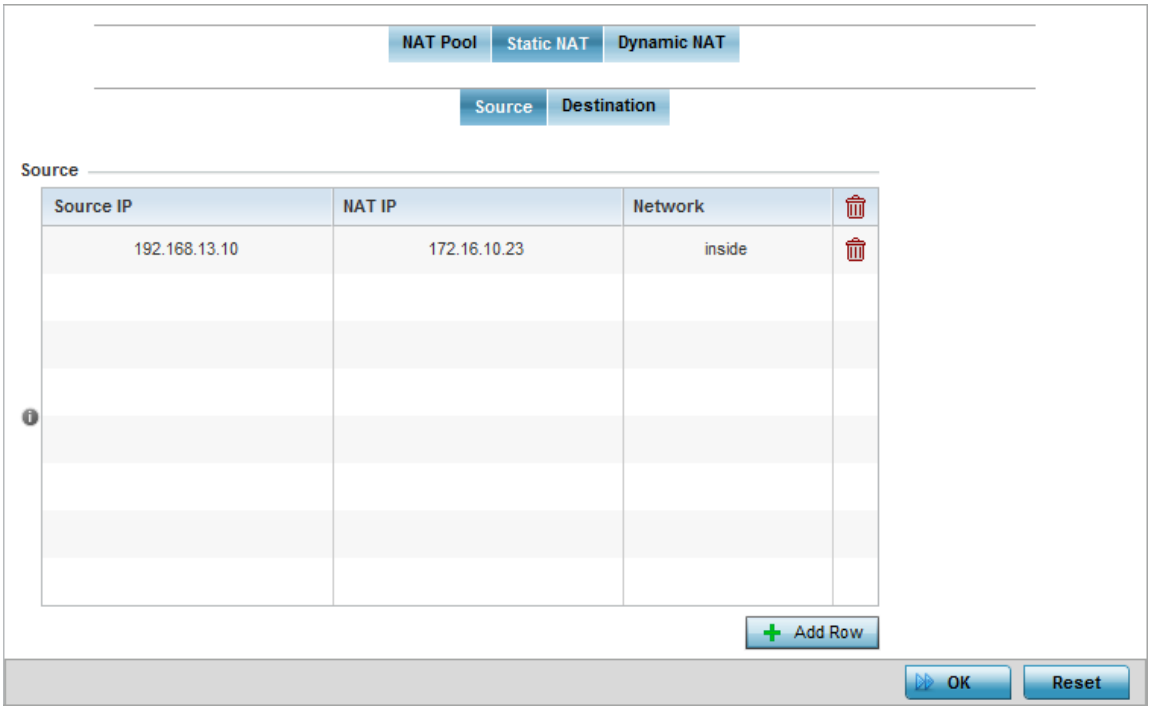


Figure 102: Profile Security - Static NAT screen - Source tab

10 To map a source IP address from an internal network to a NAT IP address click the **Add** button.

11 Define the following Source NAT parameters.

Source IP	Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either *source* or *destination* based on the direction specified.
Network	Select *Inside* or *Outside* NAT as the network direction. The default setting is Inside. 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.

12 Select the **Destination** tab to view destination NAT configurations and define packets passing through the NAT on the way back to the LAN are searched against to 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.

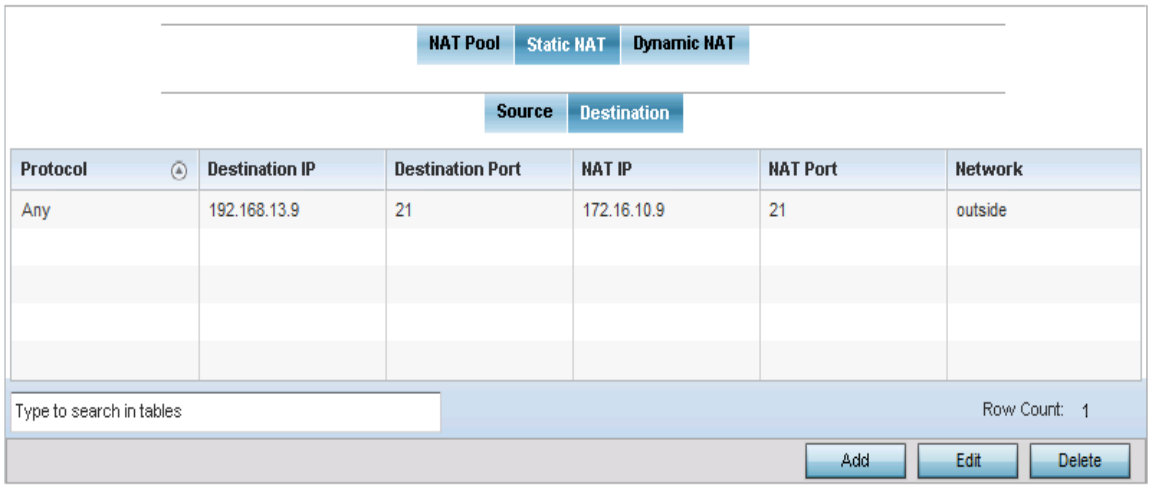


Figure 103: Profile Security - Static NAT screen - Destination tab

13 Select **Add** to create a new NAT destination configuration or **Delete** to permanently remove a NAT destination. Existing NAT destination configurations are not editable.

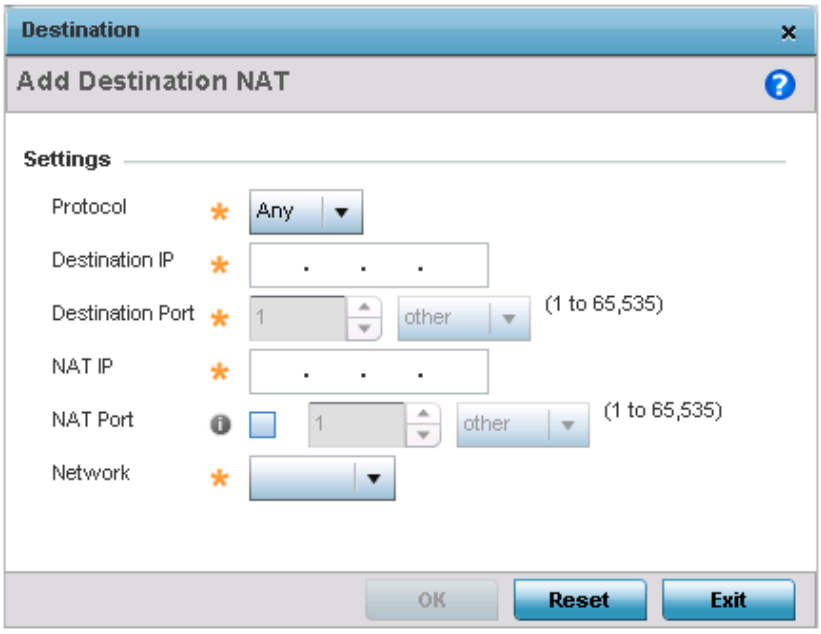


Figure 104: NAT Destination - Add screen

14 Set 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. *TCP*, *UDP* and *Any* are the available options. *Transmission Control Protocol* (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 *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 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	Use the spinner control to 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. *Inside* NAT is the default setting.

15 Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

16 Select the **Dynamic NAT** tab.

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.

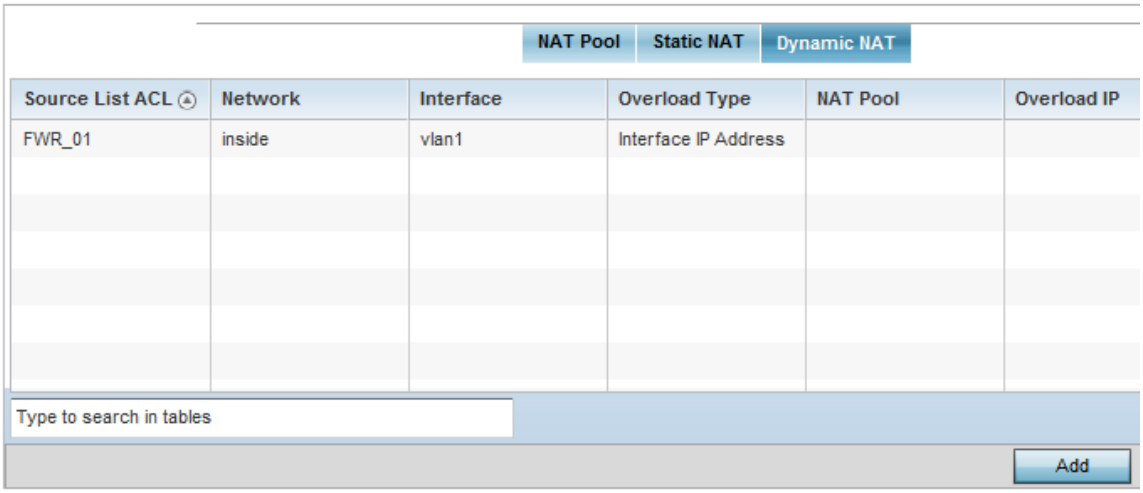


Figure 105: Profile Security - Dynamic NAT tab

17 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

Source List ACL	Lists the ACL defining 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 (from 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*. The default setting is Interface IP Address.
NAT Pool	Displays the name of an existing NAT pool used with the NAT configuration.
Overload IP	Displays the IP address used to represent numerous local addresses in this 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.

18 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove a configuration.

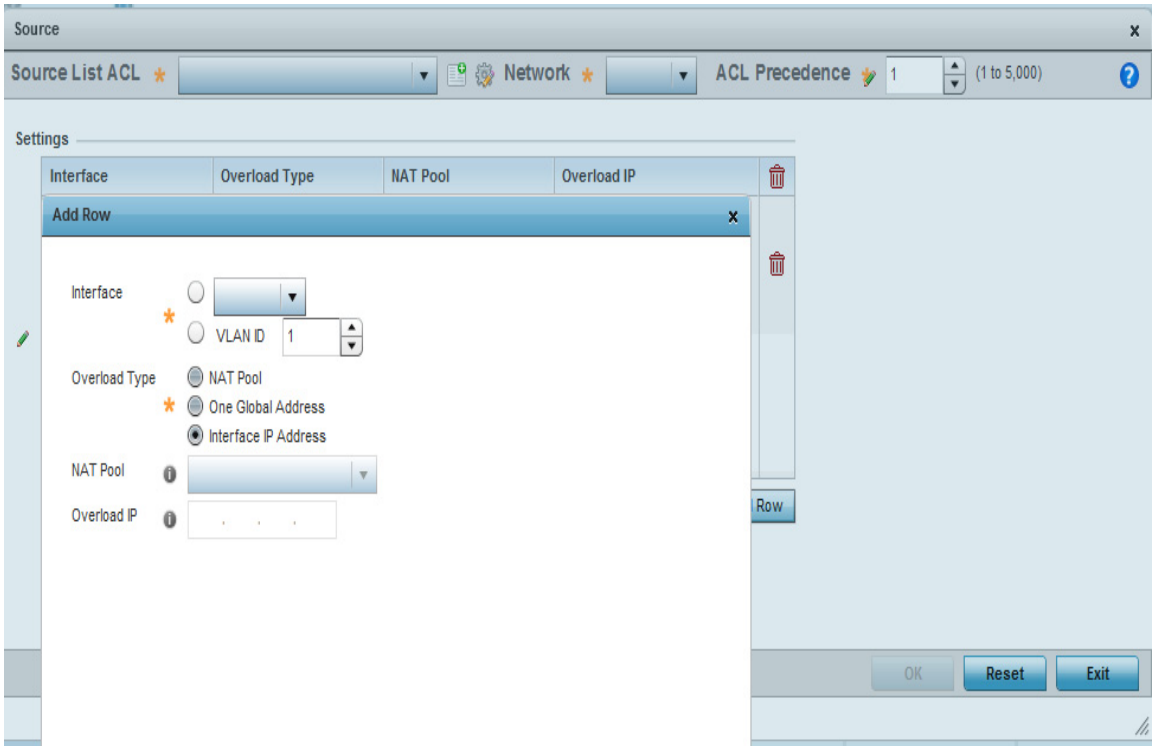


Figure 106: Profile Security - Source ACL List screen

19 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.

20 Select **+ Add Row** to launch a pop up screen used to define the **Interface**, **Overload Type**, **Nat Pool** and **Overload IP** used with the dynamic NAT configuration.

Interface	Use the drop-down menu to select the VLAN ID (from 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. Optionally, select the wwan1 radio button if the access point model supports a wwan interface as the outgoing layer 3 interface for NAT.
Overload Type	Select this option 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. If NAT Pool is selected, provide the Overload IP address.
NAT Pool	Provide the name of an existing NAT pool for use with the NAT configuration. Optionally select the *Create* icon to define a new NAT Pool configuration.
Overload IP	Enables the use of one global address for numerous local addresses. Enter a valid IP address in this field.

21 Select **OK** to save the changes made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

Setting the Profile's Bridge NAT Configuration

"Profile Security Configuration"

Use *Bridge NAT* to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.



NOTE

Bridge NAT supports single AP deployments only. This feature cannot be used in a branch deployment with multiple access points.

To define a Bridge NAT configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Bridge NAT**.

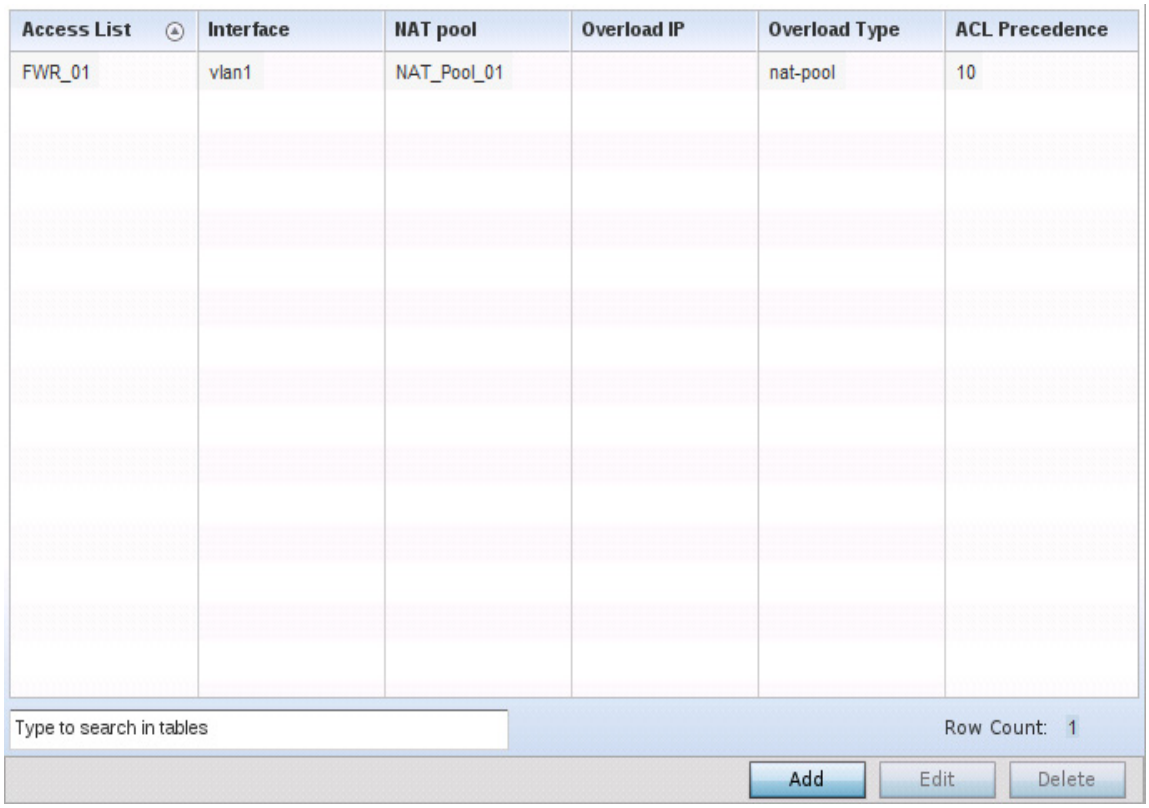


Figure 107: Profile Security - Bridge NAT screen

5 Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration modified or removed:

Access List	Lists the ACL applying IP address access/deny permission rules to the Bridge NAT configuration.
Interface	Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the access point's pppoe1 or wwan1 interface or the VLAN used as the redirection interface between the source and destination.
NAT Pool	Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when Overload Type is NAT Pool.
Overload IP	Lists the IP address used to represent a large number 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 precedence for this ACL. The lower the precedence, the earlier the ACL is applied.

6 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

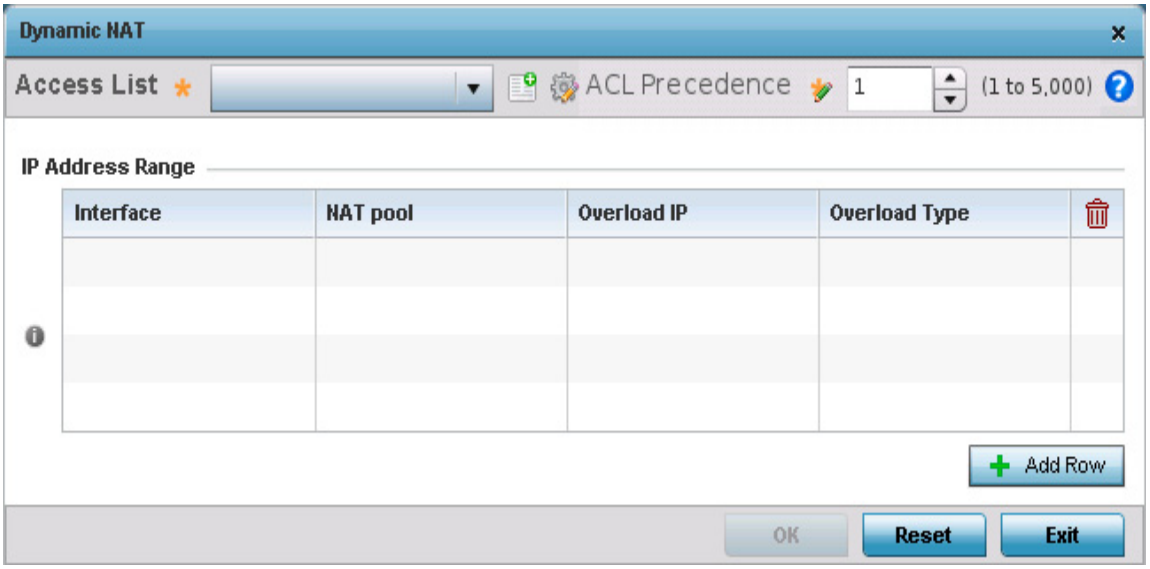


Figure 108: Profile Security - Dynamic NAT screen

7 Select the **ACL** whose IP rules are to be applied to this policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.

8 Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the Internet.

Interface	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN.
NAT Pool	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool.
Overload IP	Lists the IP address used to represent a large number local addresses for this configuration.
Overload Type	Displays the override type for this policy based forwarding rule.

9 Select **+ Add Row** to set the IP address range settings for the Bridge NAT configuration.

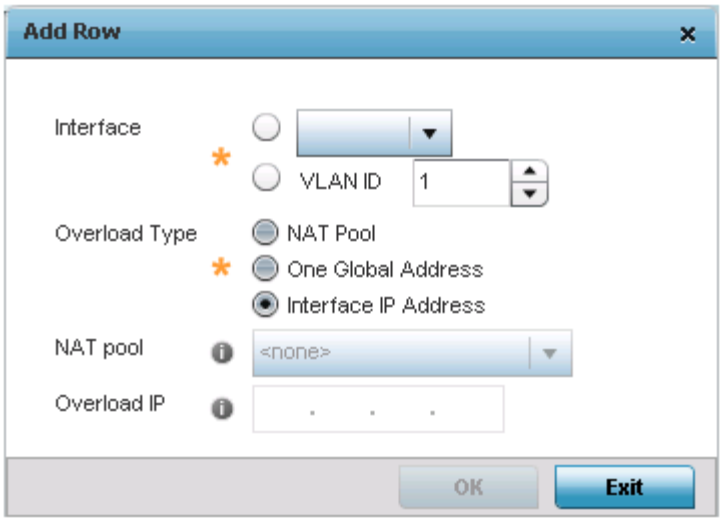


Figure 109: Profile Security - Source Dynamic NAT screen - Add Row field

10 Select **OK** to save the changes made within the **Add Row** and **Dynamic NAT** screens. Select **Reset** to revert to the last saved configuration.

Setting a Profile's Application Visibility Settings

"Profile Security Configuration"

Deep packet inspection (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, *identify*, *classify, reroute* or *block* packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

NOTE

Application Visibility is only available on AP7562, AP8432 and AP8533 access points only.

To configure a profile's application visibility settings and overrides:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Device Overrides** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Bridge NAT**.

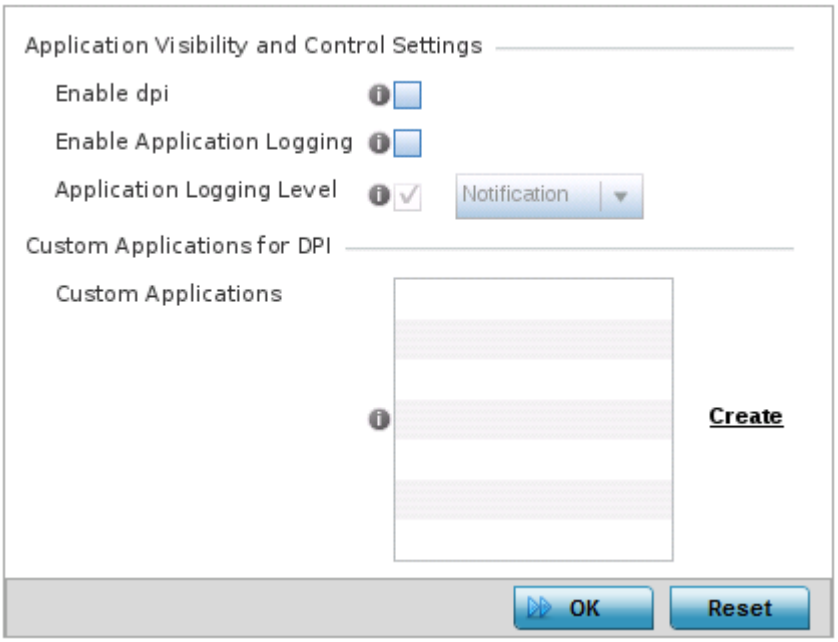


Figure 110: Profile Security - Application Visibility screen

5 Refer the following **Application Visibility and Control** Settings:

Enable dpi	Enable this setting to provide deep-packet inspection (application assurance) by inspecting every byte of each application header packet passing through the controller or service platform. When enabled, application data streams are inspected at a granular level to help prevent viruses and spyware from accessing the WiNG managed network.
Enable Applications Logging	Select this option to enable event logging for deep packet inspection application recognition. This setting is disabled by default.
Application Logging Level	If enabled, 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 of high bandwidth voice and video application data flows. The default setting is disabled.
Enable HTTP Metadata	Select this option to enable the metadata extraction of HTTP application data flows. The default setting is disabled.
Enable SSL Metadata	Select this option to enable the metadata extraction of SSL application data flows. The default setting is disabled.

6 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 704.

7 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

Profile Security Configuration and Deployment Considerations

"Profile Security Configuration"

Before defining a profile's security configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Ensure the contents of the certificate revocation list are periodically audited to ensure revoked certificates remained quarantined or validated certificates are reinstated.
- NAT alone does not provide a firewall. If deploying NAT on a profile, add a firewall on the profile to block undesirable traffic from being routed. For outbound Internet access, a stateful firewall can be configured to deny all traffic. If port address translation is required, a stateful firewall should be configured to only permit the TCP or UDP ports being translated.

Virtual Router Redundancy Protocol (VRRP) Configuration

"System Profile Configuration"

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available on an AP7131, 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 wireless 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.



NOTE

VRRP support is available only on AP7131 model access point, and is not available in other models.

To define the configuration of a VRRP group:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **VRRP**.

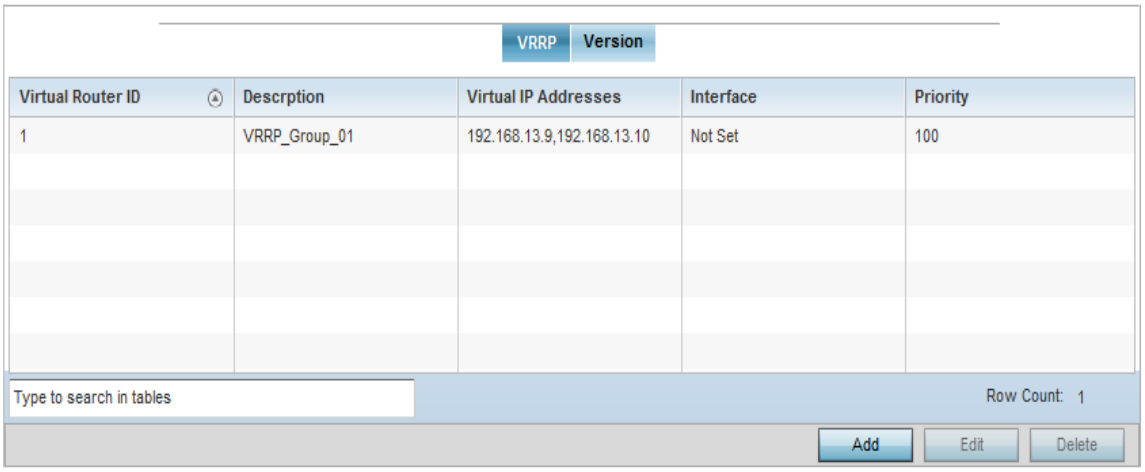


Figure 111: Profiles - VRRP screen - VRRP tab

5 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 (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 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 interfaces selected on the access point to supply VRRP redundancy failover support.
Priority	Lists 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 Select the **Version** tab to define the VRRP version scheme used with the configuration.

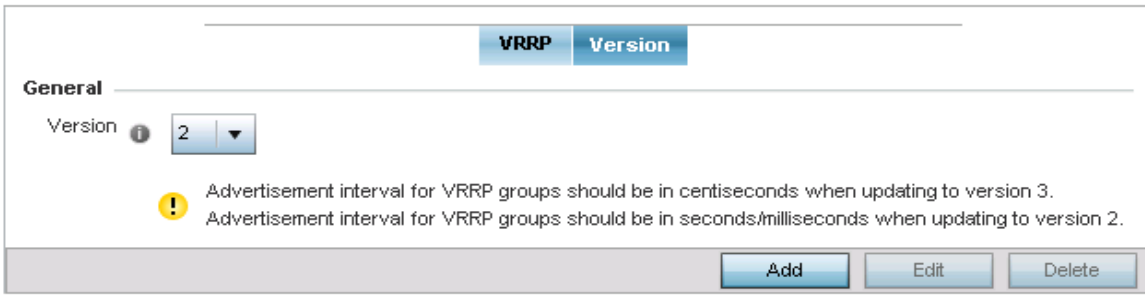


Figure 112: Profiles - VRRP screen - Version tab

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).

7 From within the **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**.

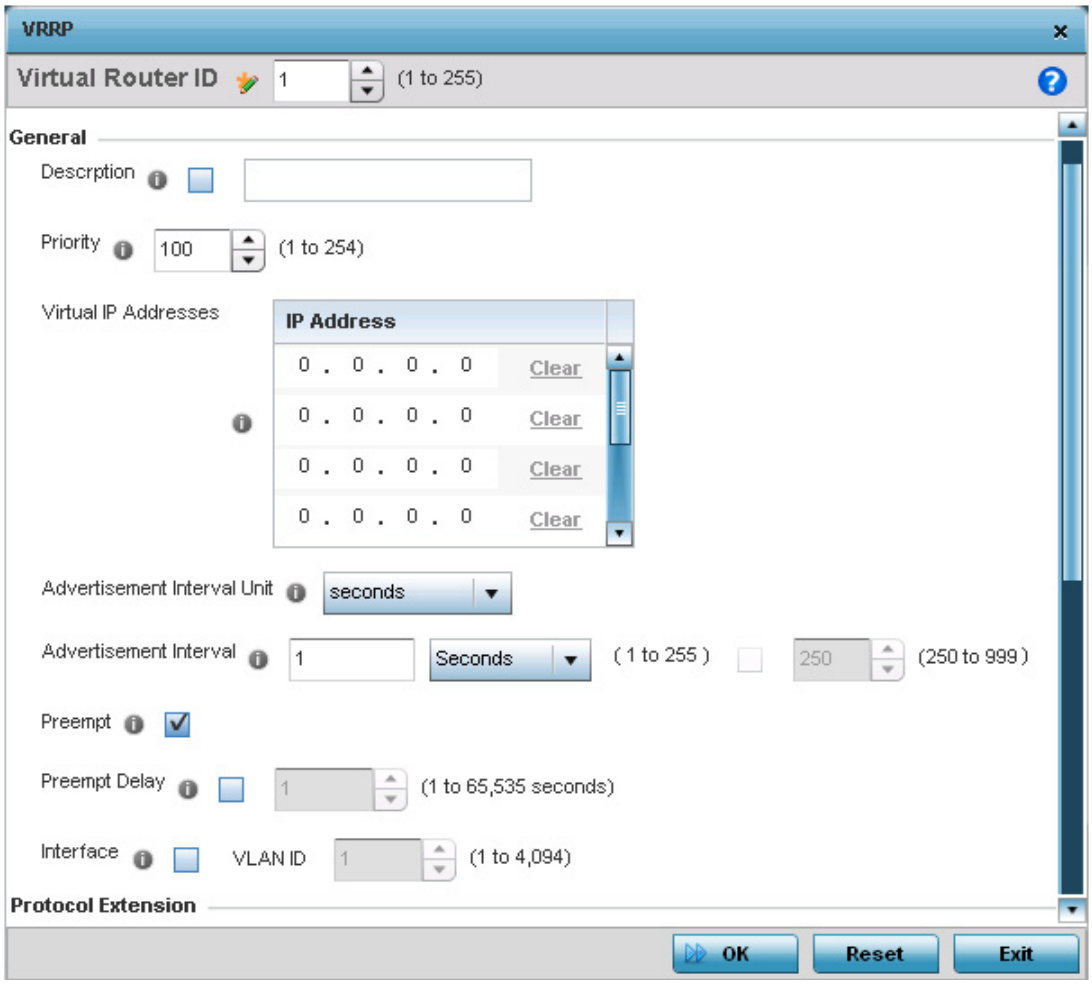


Figure 113: Profiles - VRRP screen

8 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.

9 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 access point 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 8 IP addresses representing the Ethernet switches, routers or security appliances defined as virtual router resources to the AP7131 access point.
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 the *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 preemption.
Interface	Select this value to enable/disable VRRP operation and define the AP7131 VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure.

10 Refer to the **Protocol Extension** field to define the following:

Sync Group	Select this 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 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 within the VRRP group.
Network Monitoring: Critical Resources	Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include *None*, *increment-priority*, and *decrement priority*.
Network Monitoring: Delta Priority	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.

11 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

Profile Critical Resources

"System Profile 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're 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 the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Critical Resources**.

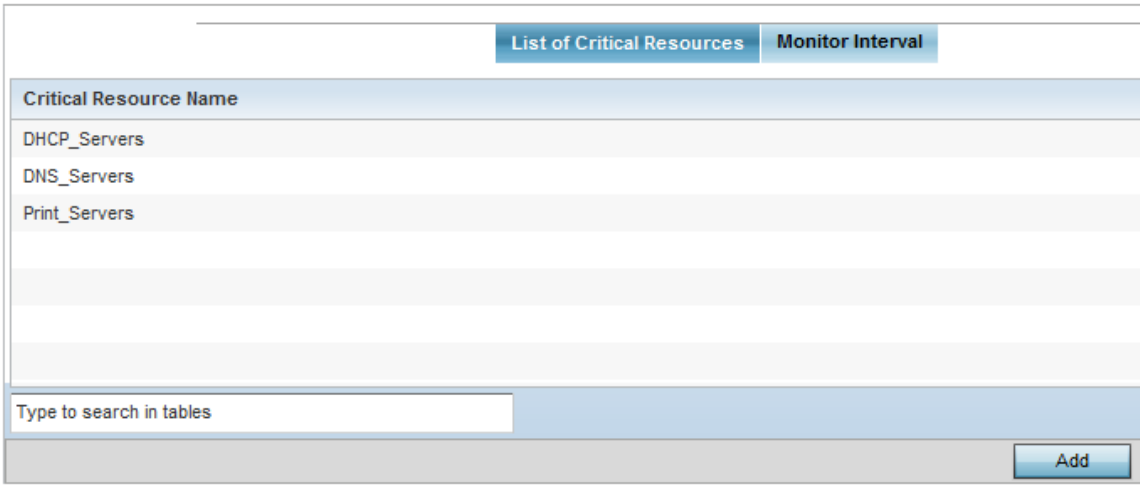


Figure 114: Critical Resources screen - List of Critical Resources tab

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 access point or controller, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5 Select 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.

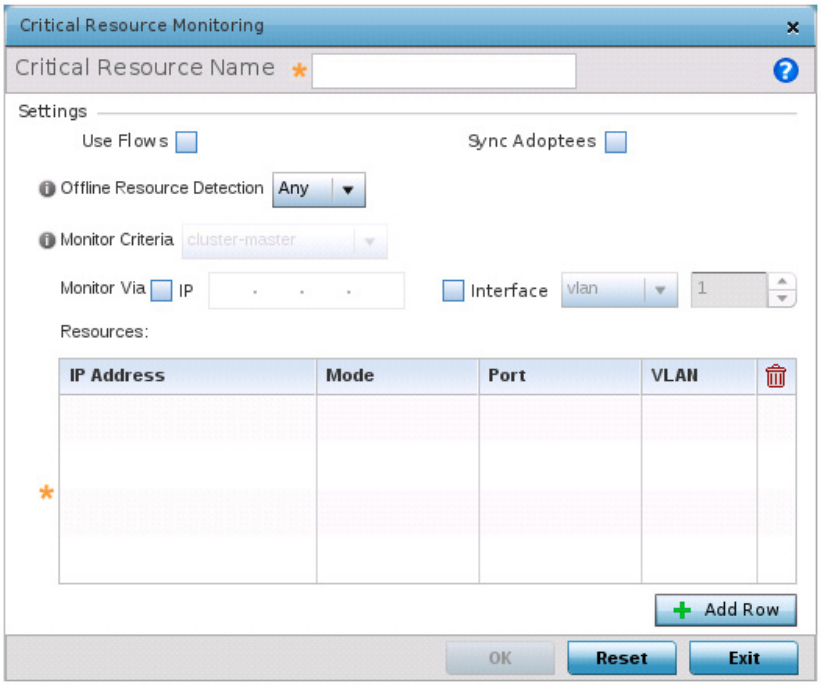


Figure 115: Critical Resources screen - Adding a Critical Resource

6 Select **Use Flows** to configure the critical resource to monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets to reduce the amount of traffic on the network. Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message. These settings are disabled by default.

7 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.

8 Select the **IP** option (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.

9 Select the **Interface** option (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.

10 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 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 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 pinging the critical resource and sending control messages (device not reachable, requested service not available, etc.).
Port	Provide the port on which the critical resource is available. Use the spinner control to set the port number.
VLAN	Define the VLAN on which the critical resource is available using the spinner control.

11 Select the **Monitor Interval** tab.

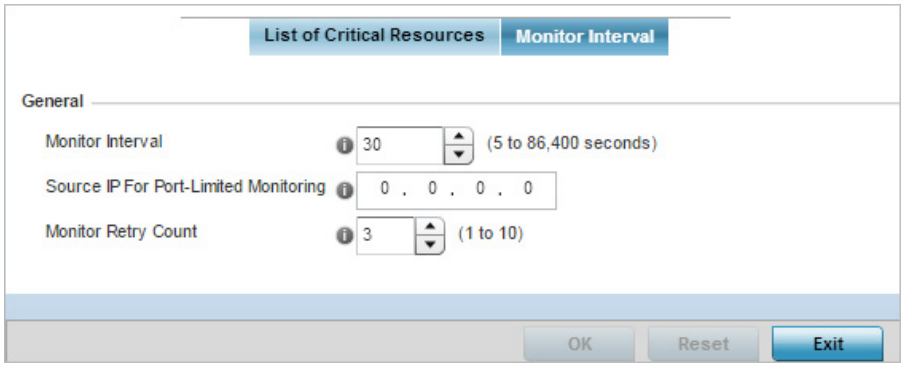


Figure 116: Critical Resources screen - Monitor Interval tab

12 Set the duration between two successive pings from the access point to the critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.

13 Configure the IP address for Port-Limited Monitoring in the **Source IP for Port-Limited Monitoring** field. Sets 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.

14 Select **OK** to save the changes to the critical resource configuration and monitor interval. Select **Reset** to revert to the last saved configuration.

Profile Services Configuration

"System Profile Configuration"

A profile can contain specific guest access (captive portal) server configurations. These guest network access permissions can be defined uniquely as profile requirements dictate.

To define a profile's services configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Services**.

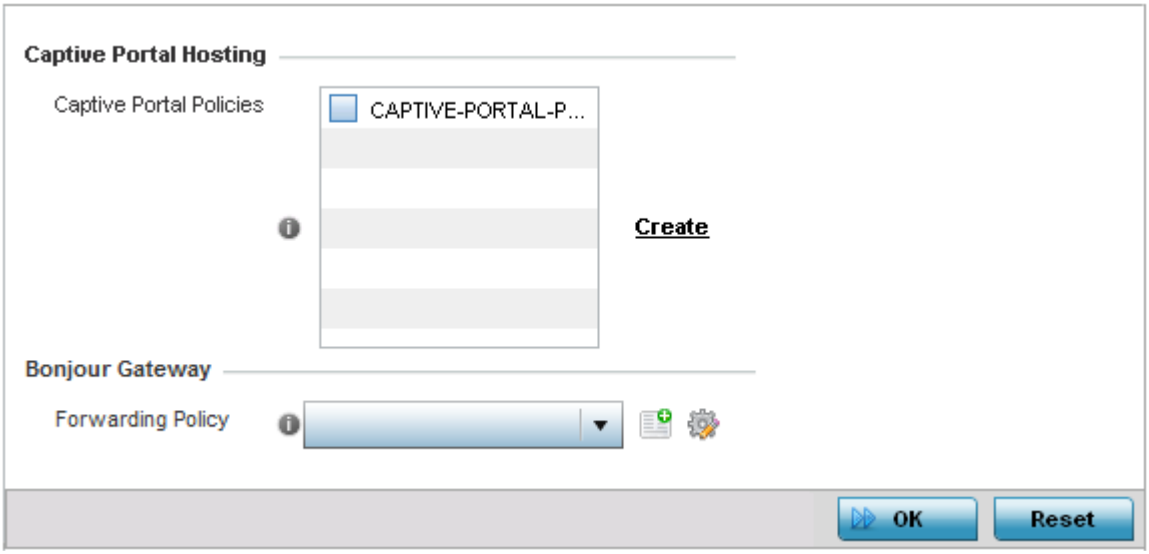


Figure 117: Profile Services - Services screen

5 Refer to the **Captive Portal Hosting** field 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 access point managed network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal configuration that can be applied to this profile. For more information, see "Configuring Captive Portal Policies" on page 759.

6 Refer to the **Bonjour Gateway** field to select or set a Bonjour Gateway **Forwarding Policy**.

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

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.

7 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

"Profile Services Configuration"

Before defining a profile's captive portal and DHCP configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- A profile plan should consider the number of wireless clients allowed on the profile's guest (captive portal) network and the services provided, or if the profile should support guest access at all.
- Profile configurations supporting a captive portal should include firewall policies to ensure logical separation is provided between guest and internal networks so internal networks and hosts are not reachable from guest devices.
- DHCP's lack of an authentication mechanism means a DHCP server supported profile cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. Ensure a profile using DHCP resources is also provisioned with a strong user authorization and validation configuration.

Profile Management Configuration

"System Profile Configuration"

The access point has mechanisms to allow/deny management access to the network for separate 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.

To define a profile's management configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Management** menu item and select **Settings**.

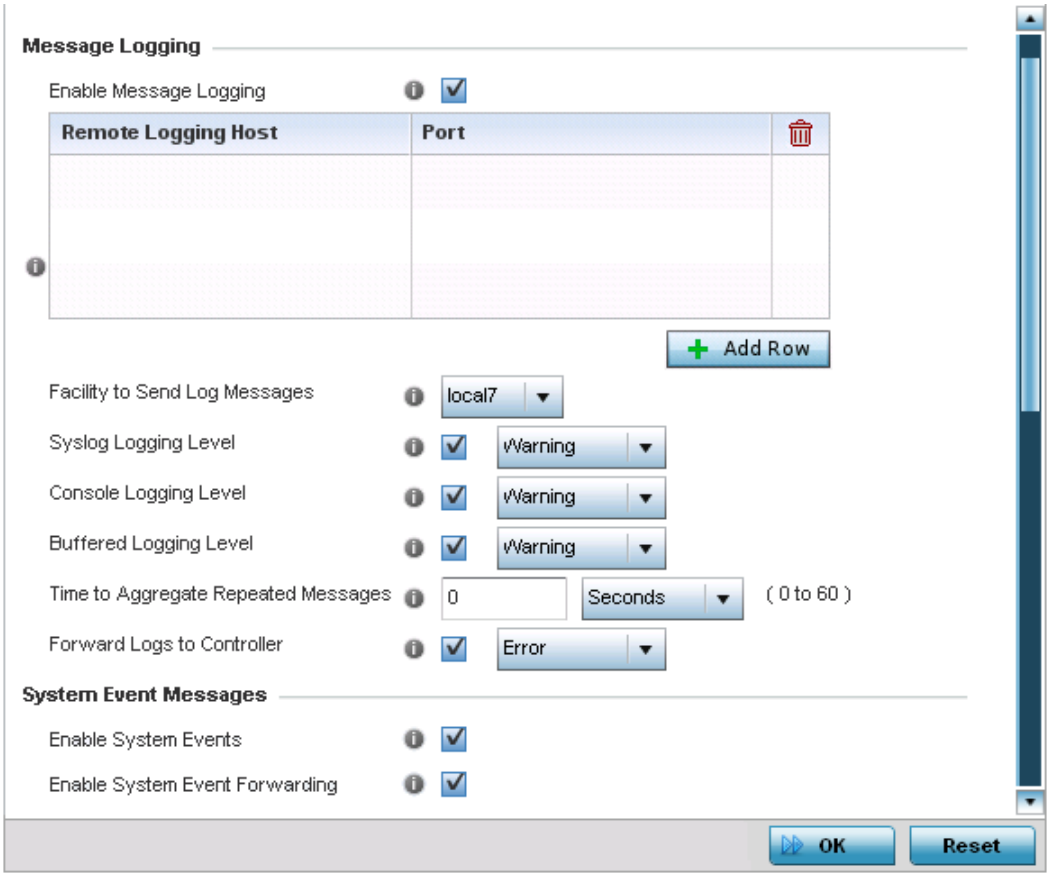


Figure 118: Profile Management - Settings screen

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 may be negatively impacting performance using the configuration defined for the access point's 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 radio button 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* to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the 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 console 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 buffered 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 interval (duration) system events are logged on behalf of the access point 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. 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 how system messages are logged and forwarded on behalf of the access point's profile.

7 Select the **Enable System Event**s radio button 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 the access point's performance. This setting is enabled by default.

8 Select the **Enable System Event Forwarding** radio button to enable the forwarding of system events. This setting is enabled by default.

9 Refer to the **Events E-mail Notification** field to define how system event notification E-mails are sent on behalf of the access point profile.

SMTP Server	Specify either the *Hostname* or *IP Address* of the outgoing SMTP server where notification E-mails are originated.
Port of SMTP	If a non-standard SMTP port is used on the outgoing SMTP server, select this option and specify a port from 1 - 65,535 for the outgoing SMTP server.
Sender E-mail Address	Specify the E-mail address where notification E-mails are originated.
Recipient's E-mail Address	Specify the destination E-mail address where notification E-mails are sent. Multiple E-mail addresses can be specified by typing each address individually and selecting the button next to the E-mail text box to add it to a list.
Username for SMTP Server	Specify the sender's username on the outgoing SMTP server. Many SMTP servers require users to authenticate with a username and password before sending E-mail through the server.
Password for SMTP Server	Specify the sender's username password on the outgoing SMTP server. Many SMTP servers require users to authenticate with a username and password before sending E-mail through the server.

10 Use the **Persist Configuration Across Reloads** option to define how the access point saves (in flash memory) the configuration received from its connected Virtual Controller. Stored configurations can be made available to the access point if the access point's connected Virtual Controller were to be unreachable. Options include *Enabled, Disabled* and *Secure*.

11 Use the **HTTP Analytics** area to configure how analytics is sent to the HTTP analytics server. Select the **Compress** option to send the HTTP analytics compressed. Use the **Update Interval** fields to configure the update interval between two updates to the HTTP analytics server.

12 Select **OK** to save the changes made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.

13 Select **Firmware** from the Management menu.

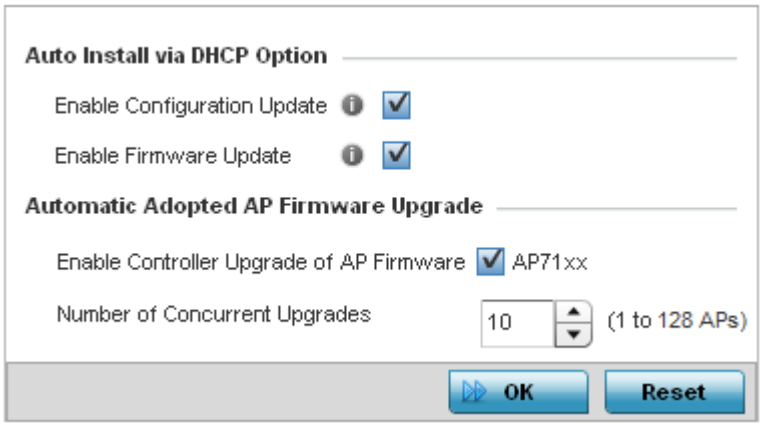


Figure 119: Profile Management - Firmware screen

14 Refer to the **Auto Install via DHCP** field to define the configuration used by the profile to update firmware using DHCP:

Enable Configuration Update	Select this option to enable automatic configuration file updates for the profile from a location external to the access point. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update. To use this option, first create a Virtual Interface in the Interfaces section and enable the *Use DHCP to Obtain Gateway/DNS Servers* option for that Virtual Interface.
Enable Firmware Update	Select this option to enable automatic firmware updates (for this profile) from a location external to the access point. To use this option, first create a Virtual Interface in the Interfaces section and enable the *Use DHCP to obtain Gateway / DNS Servers* option for that Virtual Interface. This value is disabled by default. For information on upgrading an AP6532 from firmware version 5.1, refer to "Upgrading AP6532 Firmware from 5.1" on page 266.

15 Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware configuration.

Enable Controller Upgrade of AP Firmware	Select the access point model to upgrade to a newer firmware version using its associated Virtual Controller AP's most recent firmware file for that model. The only available option is AP71XX.
Number of Concurrent Upgrades	Use the spinner control to define the maximum number (from 1 - 128) of adopted APs 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.

16 Select **OK** to save the changes made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Heartbeat** option from the Management menu.



Figure 120: Profile Management - Device Heartbeat Settings screen

18 Select the **Service Watchdog** option to implement heartbeat messages to ensure other associated devices are up and running. The Service Watchdog is enabled by default.

19 Select **OK** to save the changes made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

Upgrading AP6532 Firmware from 5.1

"Profile Management Configuration"

An existing AP6532 deployment running factory installed 5.1 version firmware can be upgrade to this most recent 5.4 version baseline. To upgrade AP6532 from the 5.1 version baseline:

Ensure you have the following resources:

- A computer with a SSH client and a FTP or TFTP server
- The latest AP6532 5.4 image file in the computer's FTP or TFTP directory
- A PoE hub

1 Calculate the AP6532's IP address.

The AP6532 has an IP of 169.254.<last two digits of its MAC address in decimal>, with subnet mask of 255.255.0.0.
For example, if the MAC address is 00-23-68-86-48-18, the last two digits of its IP address will be 72.24
(48 hexadecimal = 72 decimal, 18 hexadecimal = 24 decimal). So the IP address is 169.254.72.24, with subnet mask of 255.255.0.0.

2 Configure the computer with an IP address in the same subnet. For example, 169.254.0.1, and a subnet mask of 255.255.0.0.

3 Ping the AP6532 from the computer to ensure IP connectivity.

4 Open an SSH session on the computer and connect to the AP6532's IP address.

5 Login with a username and password of admin/admin123. The CLI will prompt for a new password. Re-enter the password and confirm.

6 Within the CLI, type **`enable`**.

7 Enter **`commit write memory`** to save the new password.

8 To upgrade firmware using a FTP server, use the upgrade command.
`ftp://<username>:<password>@169.254.0.1/AP6532-5.4.0.0-047R.img`.

Alternatively, a user can upgrade the AP6532 firmware using a TFTP server using the upgrade command.
`tftp://169.254.0.1/AP6532-5.4.0.0-047R.img`.

The AP6532 downloads the firmware from FTP/TFTP server. This process will take a few minutes.

9 When finished, type **`reload`** to reboot the AP6532. Press '**`y`**' when asked to confirm the reboot.

10 The AP6532 reboots and SSH session is terminated. The reboot takes a couple of minutes.

11 Run a ping from the computer to the AP6532. A ping will be timed out during the reboot.

12 When the ping resumes, start an SSH session again to the AP6532.

13 Login to the AP6532 using the new password and confirm the firmware upgrade is successful by issuing a **`show version`** command.

Profile Management Configuration and Deployment Considerations

"Profile Management Configuration"

Before defining a access point profile's management configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Define profile management access configurations providing both encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide data privacy and authentication.
- It is recommended that SNMPv3 be used for management profile configurations, as it provides both encryption, and authentication.

Mesh Point Configuration

"System Profile Configuration"

The access point can be configured to be a part of a meshed network. A mesh network is one where each node in the network is be able to communicate with other nodes in the network and where the node can maintain more than one path to its peers. Mesh network provides robust, reliable and redundant connectivity to all the members of the network. When one of the participant node in a Mesh Network becomes unavailable, the other nodes in the network are still able to communicate with each other either directly or through intermediate nodes.

Mesh Point is the name given to a device that is a part of a meshed network.

Use the *Mesh Point* screen to configure the parameters that set how this device behaves as a part of the mesh network.

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Mesh Point.**

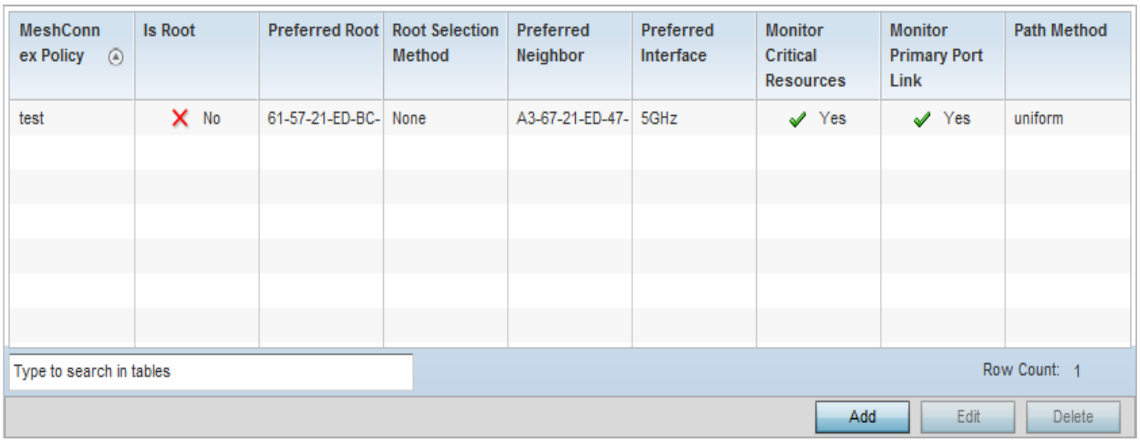


Figure 121: Mesh Point Configuration - Mesh Point screen

The *Mesh Point* screen displays a list of configured MeshConnex policies on this device.

5 Refer to the following for more information on the *Mesh Point* screen:

Mesh Connex Policy	Displays the name of the selected Mesh Connex™ policy.
Is Root	Displays the root status of the mesh point. If the device is a mesh root, then this field displays “True”.
Preferred Root	Displays the MAC address of the preferred root. A Preferred Root is a root node that this mesh point prefers to join over other root nodes in the mesh network.
Root Selection Method	Displays the root selection method that determines if this meshpoint is a root or not.
Preferred Neighbor	Displays the MAC address of the preferred neighbor. A Preferred Neighbor is a node that this mesh point prefers to have a mesh connection with over other nodes in the mesh network.
Preferred Interface	Displays the name of the preferred interface. A Preferred Interface is an interface on this mesh point that is preferred over other interfaces on the device when forming a mesh network.
Monitor Critical Resource	Displays if this mesh point monitors critical resources for maintaining a mesh connection.
Monitor Primary Port Link	Displays if this mesh point monitors link status on the primary port.
Path Method	Displays the path selection method used to select the path to the root node.

6 Select the **Add** button to create a new Mesh Connex policy.

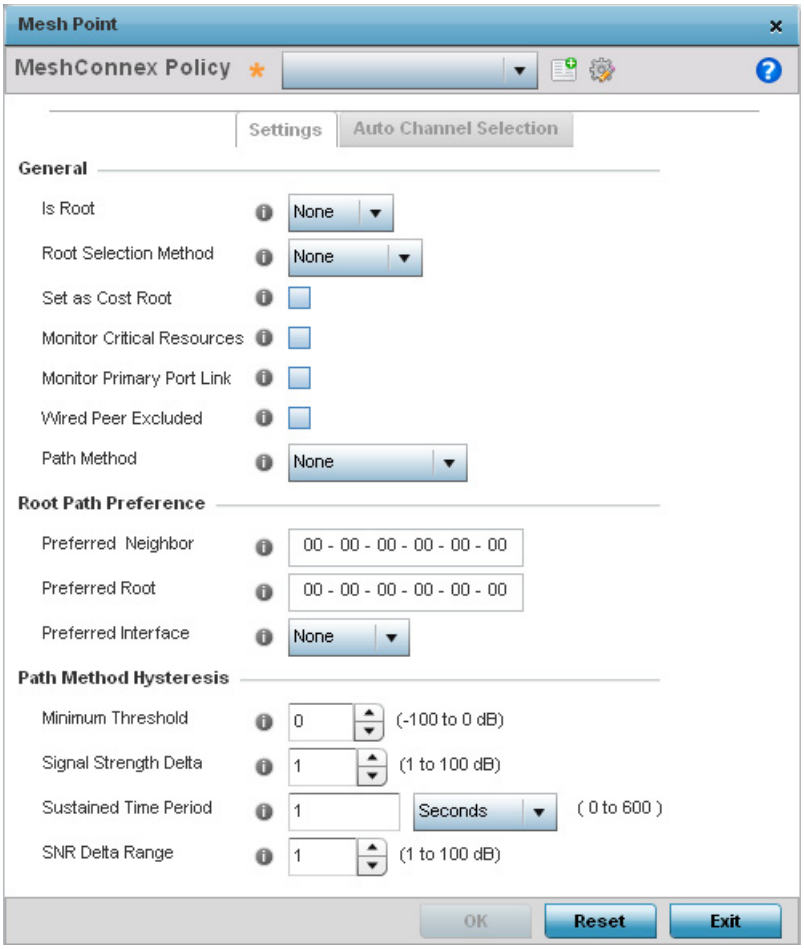


Figure 122: Mesh Point Configuration - Add Mesh Point Mesh Connex Policy screen

7 Refer to the following for more information on the *Mesh Point Mesh Connex Policy* screen:



NOTE

With this release of the WiNG software, an AP7161 model access point can be deployed as a *Vehicle Mounted Modem* (VMM) 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. For VMM deployment considerations, see "Vehicle Mounted Modem (VMM) Deployment Consideration" on page 277.

MeshConnex Policy	Provide a name for the Mesh Connex Policy. Use the *Create* icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the drop-down and click the *Edit* icon. For more information on creating or editing a Mesh Connex policy, see "MeshConnex Policy" on page 622
Is Root	From the drop-down menu, select the root behavior of this access point. Select *True* to indicate this access point is a root node for this mesh network. Select *False* to indicate this access point is not a root node for this mesh network.
Root Selection Method	Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either *None* (the default setting) or *auto-mint*.
Set as Cost Root	Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default.
Monitor Critical Resource	Select this option to monitor critical resources. If a configured critical resource becomes unavailable, the mesh point is removed from the mesh network.
Monitor Primary Port Link	Select this option to indicate this mesh point monitors the link on the primary port. If the link on the primary port becomes unavailable, the mesh network is brought down.
Wired Peer Exclude	Select this option to exclude wired peers when creating mesh links.
Path Method	From the drop-down menu, select the method to use for path selection in a mesh network. The available options are: • *None* – Select this to indicate no criteria used in root path selection. • *uniform* – Indicates 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 (AP7161 models only). When selected, the path to the route will be selected based on the *Signal To Noise Ratio* (SNR) to the neighbor device. • *pcr-weighted* – Select this to choose a neighbor path based on the packet completion rate from a neighbor device. A device with a higher packet completion rate is chosen over a device with a lower packet completion rate. • *snr-leaf* – Select this to indicate the path with the best signal to noise ratio is always selected.
Preferred Neighbor	Enter the MAC address of the mesh point device that is the preferred neighbor.
Preferred Root	Enter the MAC address of the mesh point root that is the preferred root.

Preferred Interface	From the drop-down menu, select the preferred interface for forming a mesh network.
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* is used to dynamically select the next hop in a dynamic mesh network.
Sustained Time Period	Indicates the duration (in minutes) 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.
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 Mesh Connex *Auto Channel Selection* policy.

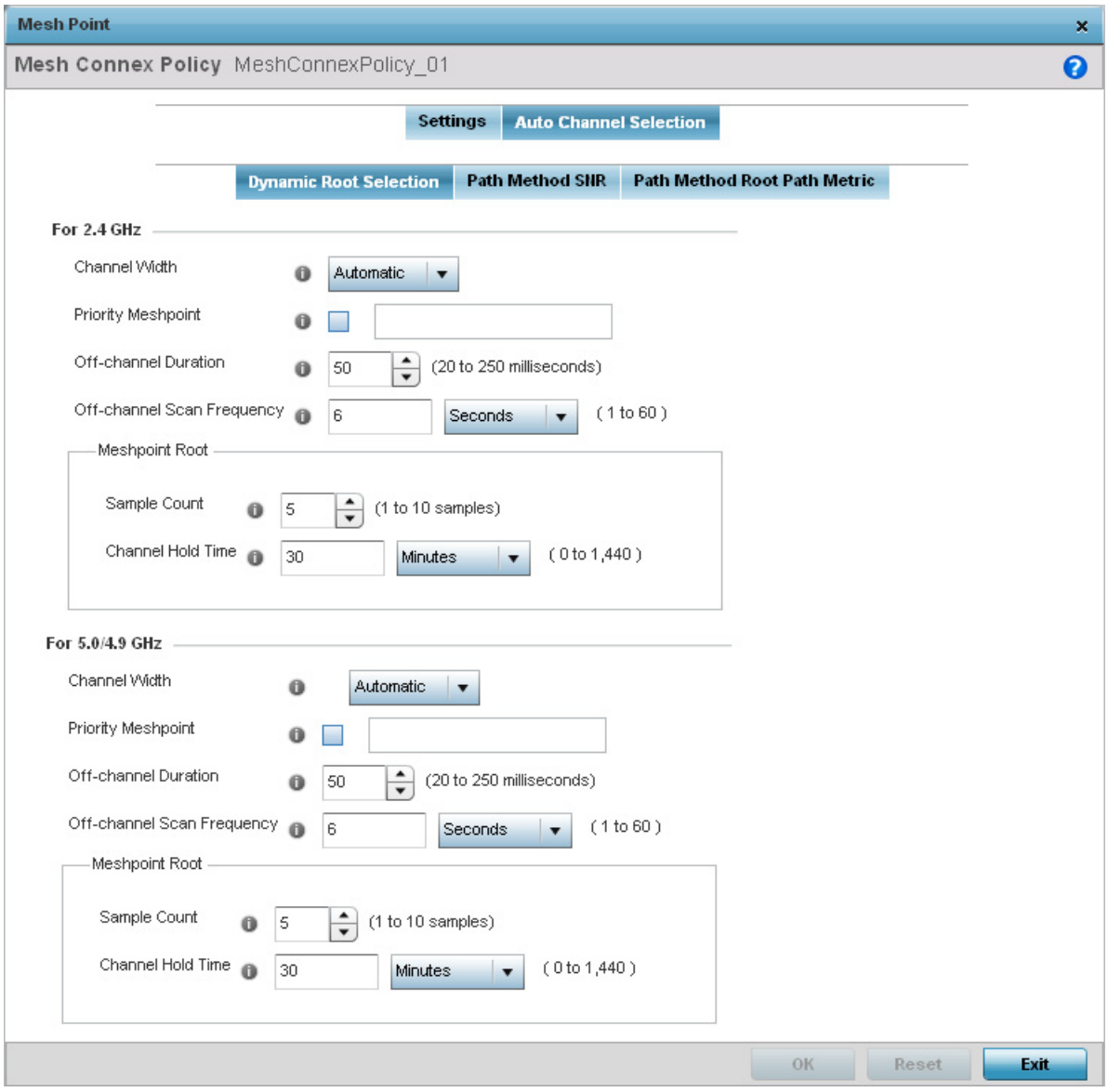


Figure 123: Mesh Connex Auto Channel Selection screen

9 By default, the **Dynamic Root Selection** screen displays.

This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies. 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	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
Off-channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field. This is the duration the scan dwells on each channel when performing an off channel scan. The default value is 50 milliseconds.
Off-channel Scan Frequency	Configure the time duration in seconds between two consecutive Off Channel Scans. Set a duration between 1 - 60 seconds.
Meshpoint Root - Sample Count	Configure the number of scans to be performed for data collection before a mesh channel is selected. Set a value between 1 - 10 scans.
Meshpoint Root - Channel Hold Time	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

10 Click the **Path Method SNR** tab to configure the signal to noise ratio values when selecting the path to the mesh point root.

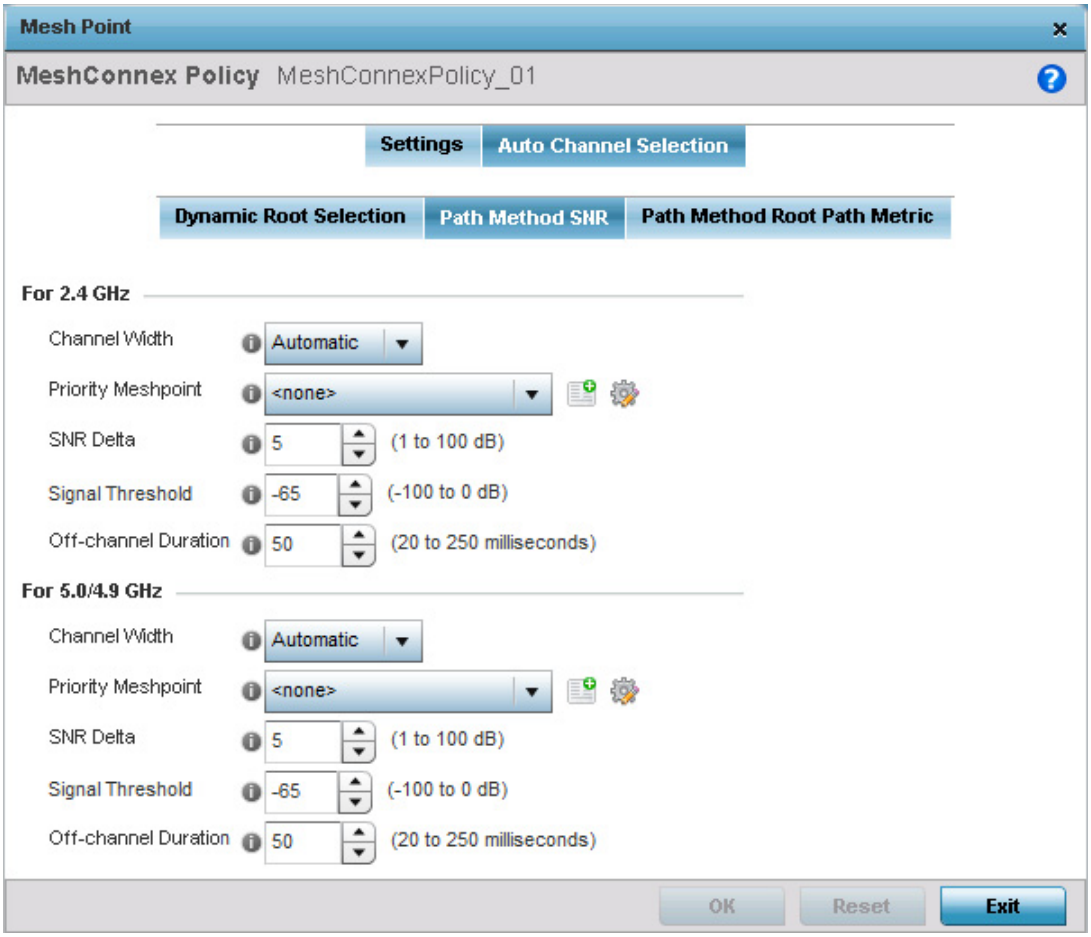


Figure 124: Mesh Point Auto Channel Selection Path Method SNR screen

11 Refer to the following for more information on the Path Method SNR screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

Channel Width	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
SNR Delta	Configure the signal to noise ratio delta value for path selection. When path selection happens, this value is considered 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.
Signal Threshold	Configure the signal to noise threshold value for path selection. When the signal strength of the next hop in the mesh network goes below this value, a scan is triggered to select a better next hop.
Off-channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field. This is the duration that the scan dwells on each channel when performing an off channel scan.

12 Click the **Path Method Root Path Metric** tab to configure the parameters controlling the calculation of the root path metrics.

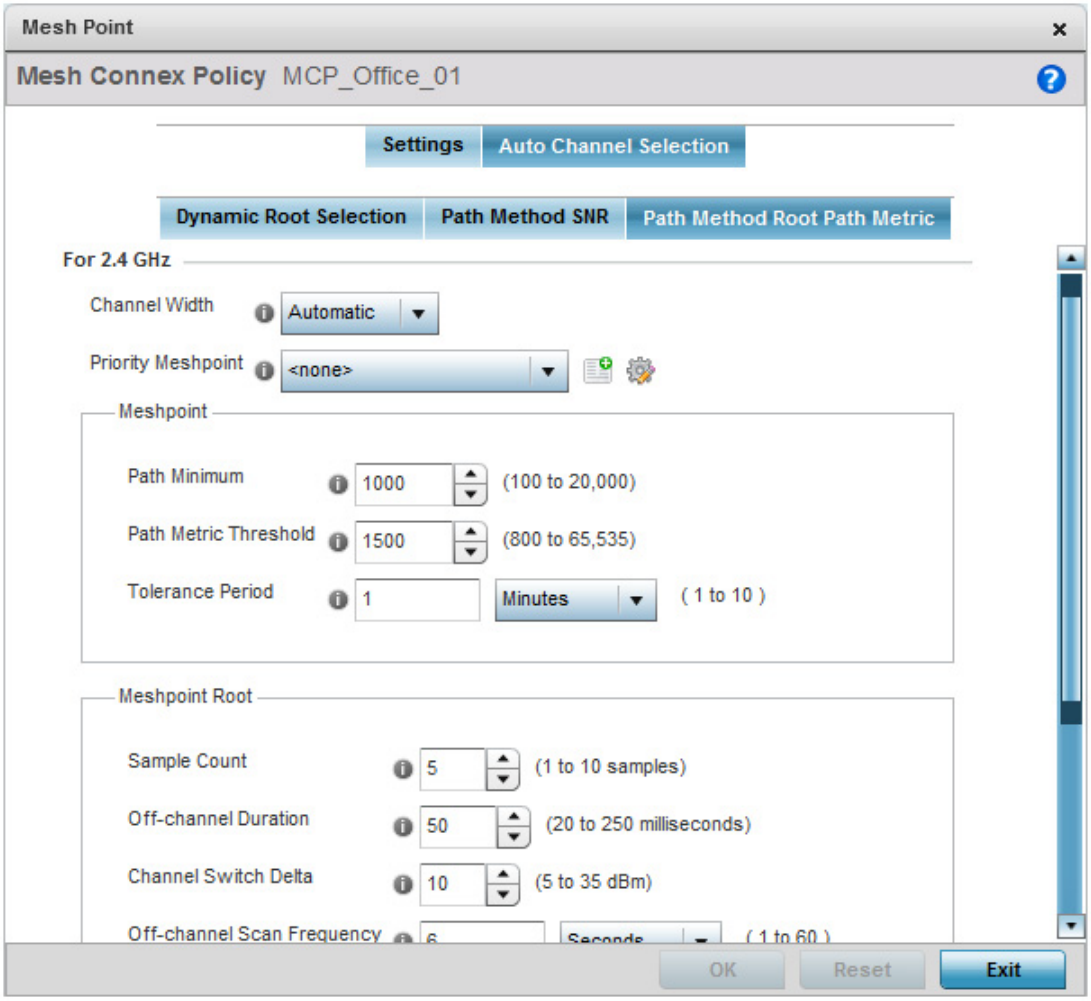


Figure 125: Mesh Point Auto Channel Selection Path Method Root Path Metric screen

13 Refer to the following for more information on the Path Method Root Path Metric screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

Channel Width	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point monitored for automatic channel scan. This is the mesh point given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
Meshpoint: Path Minimum	Configure the minimum path metric value for a mesh connection to be established. Set a value between 100 - 20,000.
Meshpoint: Path Metric Threshold	Configure a minimum threshold value for triggering an automatic channel selection for mesh point selection. Set a value in between 800 - 65535.
Meshpoint: Tolerance Period	Configure the time duration in seconds to wait before triggering a automatic channel selection for the next hop.
Meshpoint Root: Sample Count	Configure the number of scans performed for data collection before a mesh point root is selected. Set a value between 1 - 10 scans.
Meshpoint Root: Off-channel Scan Frequency	Configure the time duration in seconds between two consecutive Off Channel Scans for mesh point root. Set a duration between 1 - 60 seconds.
Meshpoint Root: Channel Hold Time	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change for mesh point root. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.
Meshpoint Root: Channel Switch Delta	Configure the delta value in dBm in the range 5 - 35 dBm which when crossed triggers a mesh point root automatic channel selection.

14 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this screen.

Vehicle Mounted Modem (VMM) Deployment Consideration

"Mesh Point Configuration"

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 124.

- Use *Opportunistic* as the rate selection settings for the AP7161 radio The default is *Standard*. For more information on defining this setting, see “Radio Override Configuration” on page 360.
- Disable *Dynamic Chain Selection* (radio setting). The default value is enabled. This setting is disabled from the *Command Line Interface* (CLI) using the **`dynamic-chain-selection`** command, or, in the UI (refer “Radio Override Configuration” on page 360.
- Disable *A-MPDU Aggregation* if the intended vehicular speed is greater than 30 mph. For more information, see “Radio Override Configuration” on page 360.

Advanced Profile Configuration

“System Profile Configuration”

An access point profile’s advanced configuration is comprised of defining connected client load balance settings, a MINT protocol configuration and miscellaneous settings (NAS ID, access point LEDs and RF Domain Manager).

To set an access point profile’s advanced configuration:

Select the Configuration tab from the Web UI.

Select **Devices**.

Select **System Profile** from the options on left-hand side of the UI.

Expand the **Advanced** menu item.

The following items are available as advanced access point profile configuration options:

- “Advanced Profile Client Load Balancing”
- “Configuring MINT Protocol”
- “Advanced Profile Miscellaneous Configuration”

Advanced Profile Client Load Balancing

“Advanced Profile Configuration”

Use the screen to administer the client load across an access point’s radios. When a large number of clients congest a particular channel, Client Load Balancing moves some of the clients to a channel that is less congested increasing the quality of service for all clients on that particular radio.

1 Select **Client Load Balancing** from the expanded **Advanced** menu.

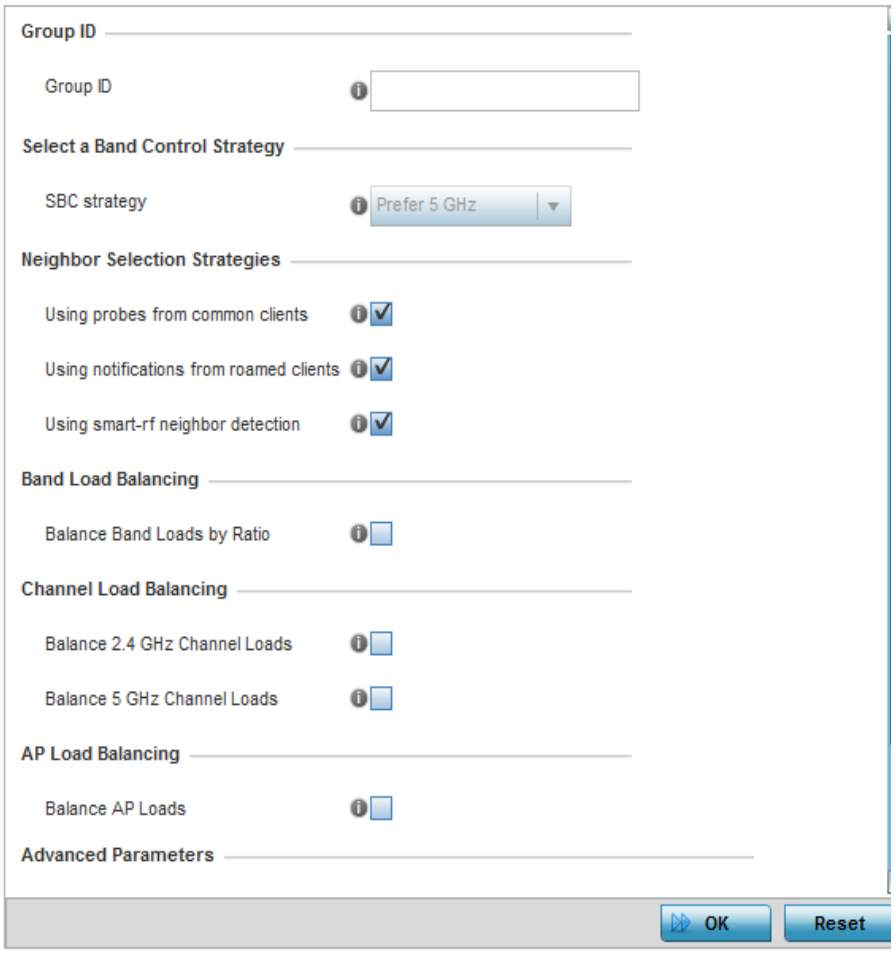


Figure 126: Advanced Profile Configuration - Client Load Balancing screen

2 Use the **Group ID** field to define a group ID of up to 32 characters.

3 Use the drop-down menu to define a **SBC strategy**. Options include *Prefer 5GHz, Prefer 2.4 GHz*, and *distribute-by-ratio*. The default value is *Prefer 5GHz*.

4 Set the following **Neighbor Selection Strategies**:

Use probes from common clients	Select this option to use probes from shared clients in the neighbor selection process. This feature is enabled by default, to provide the best common group of available clients amongst access points in neighbor selection.
Use notifications from roamed clients	Select this option to use roamed client notifications in the neighbor selection process. This feature is enabled by default, allowing access points in the neighbor selection process to consider device roaming counts as selection criteria.
Use smart-rf neighbor detection	Select this option to use SMART RF access point transmission adjustments as criteria in the neighbor selection process. This feature is enabled by default.

5 Select the **Balance Band Loads by Ratio** radio button to balance the radio load, by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio

allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5.0 GHz band. This setting is enabled by default.

6 Set the following **Channel Load Balancing** settings:

Balance 2.4GHz Channel Loads	Select this option to balance loads across channels in the 2.4 GHz radio band. This can prevent congestion on the 2.4 GHz radio if a channel is over utilized. This setting is enabled by default. Selecting this feature enables parameters within the *Channel Load Balancing* field for assigning weightage and throughput values.
Balance 5GHz Channel Loads	Select this option to balance loads across channels in the 5.0 GHz radio band. This can prevent congestion on the 5.0 GHz radio if a channel is over utilized. This setting is enabled by default. Selecting this feature enables parameters within the *Channel Load Balancing* field for assigning weightage and throughput values.

7 Select the **Balance AP Loads** radio button to distribute this access point's radio load amongst other access point radios. This setting is disabled by default, keeping the load on this access point radio.

8 Set the following **Band Control** values within the **Advanced Parameters** field:

Max. Band Load Difference Considered Equal	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing 2.4 and 5GHz radio band load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing 2.4 and 5.0 GHz load balances on this access point. This setting is not available if the *Steering Strategy* has been set to *Disable*.
Band Ratio (2.4GHz)	Use the spinner control to set a loading ratio (from 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight the traffic load if wishing to prioritize client traffic on the 2.4 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1. This setting is enabled only when *Steer by ratio* is selected as the steering strategy.
Band Ratio (5GHz)	Use the spinner control to set a loading ratio (from 0 - 10) the access point 5.0 GHz radio uses in respect to radio traffic on the 5.0 GHz band. This allows an administrator to weight client traffic if wishing to prioritize client traffic on the 5.0 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 5.0 GHz radio band. The default setting is 1. This setting is enabled only when *Steer by ratio* is selected as the steering strategy.
5 GHz load at which both bands enabled	When the *Steering Strategy* is set to Steer at 5.0 GHz, use the spinner control to set a value (from 0 - 100%) at which the load on the 2.4 GHz radio is equally preferred to this 5.0 GHz radio load. The default is 10%.
2.4 GHz load at which both bands enabled	When the *Steering Strategy* is set to Steer at 2.4 GHz, use the spinner control to set a value (from 0 - 100%) at which the load on the 5.0 GHz radio is equally preferred to this 2.4 GHz radio load. The default is 10%.

9 Set the following **Neighbor Selection** values within the **Advanced Parameters** field:

Minimum signal strength for common clients	When *Using probes from common clients* is selected as a neighbor selection strategy, use the spinner control to set a value from -100 - 30 dBM as signal strength criteria for a client to be regarded as a common client in the neighbor selection process.
Minimum number of clients seen	When *Using probes from common clients* is selected as a neighbor selection strategy, use the spinner control to set the number of clients (from 0 -256) that must be shared by at least 2 access points to be regarded as neighbors in the neighbor selection process. The default value is 1.
Max confirmed neighbors	Use the spinner control to set the maximum number of access point neighbors (from 0 - 16) of the same model available for load balance distributions. The default setting is 10.
Minimum signal strength for smart-rf neighbors	When *Using smart-rf neighbor detection* is selected as a neighbor selection strategy, use the spinner control to set a minimum signal strength value (from -100 - 35dBm) for a SMART RF detected access point to be qualified as a neighbor.

10 Set the following **Channel Load Balancing** values within the **Advanced Parameters** field:

Max. 2.4GHz Load Difference Considered Equal	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing access point 2.4GHz radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances exclusively on the 2.4GHz radio band.
Min. Value to Trigger 2.4GHz Channel Balancing	Use the spinner control to define a threshold (from 1 - 100%) the access point uses (when exceeded) to initiate channel load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within their current channel designations. The default is 5%.
Weightage given to Client Count	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 2.4GHz radio client count in the 2.4GHz radio load calculation. Assign this value higher this 2.4GHz radio is intended to support numerous clients and their throughput is secondary to maintaining association. The default setting is 90%.

Weightage given to Throughput	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 2.4 radio throughput in the access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical and more important than a high client connection count. The default setting is 10%.
Max. 5GHz Load Difference Considered Equal	Use the spinner control to set a value (from 0 - 100) considered an adequate discrepancy (or deviation) when comparing access point 5GHz radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances exclusively on the 5GHz radio band.
Min. Value to Trigger 5GHz Channel Balancing	Use the spinner control to define a threshold (from 1 - 100) the access point uses (when exceeded) to initiate channel load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within their current channel designations. The default is 5%.
Weightage given to Client Count	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize 5GHz radio client count in the 5GHz radio load calculation. Assign this value higher this 5GHz radio is intended to support numerous clients and their throughput is secondary to maintaining client association. The default setting is 90%.
Weightage given to Throughput	Use the spinner control to assign a weight (from 0 - 100%) the access point radio uses to prioritize 5GHz radio throughput in the load calculation. Assign this value higher if throughput and radio performance are considered mission critical and more important than a high client connection count. The default setting is 10%.

11 Set the following **AP Load Balancing** values within the **Advanced Parameters** field:

Min Value to Trigger Load Balancing	Use the spinner control to set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other radios. When the radio load exceeds the defined threshold, load balancing is initiated. The default is 5%.
Max. AP Load Difference Considered Equal	Use the spinner control to set a value (from 0 - 100%) considered an adequate discrepancy (or deviation) when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 10% means 10% is considered inconsequential when comparing access point radio load balances.
Weightage given to Client Count	Use the spinner control to assign a weight (from 0 - 100%) the access point uses to prioritize client count in the radio load calculation (on both the 2.4 and 5.0 GHz radio bands). Assign this value higher if this radio is intended to support numerous clients and their throughput is secondary to maintaining client association. The default setting is 90%.
Weightage given to Throughput	Use the spinner control to assign a weight (from 0 - 100%) the access point radio uses to prioritize radio throughput in the load calculation (on both the 2.4 and 5.0 GHz radio bands). Assign this value higher if throughput and radio performance are considered mission critical and of more importance than a high client connection count. The default setting is 10%.

12 Select **OK** to save the changes made to the Client Load Balancing configuration. Select **Reset** to revert to the last saved configuration.

Configuring MINT Protocol

"Advanced Profile Configuration"

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.

Virtual Controller AP managed access points can communicate with each other exclusively over a MINT security domain. Keys can also be generated externally using any application (like openssl). These keys must be present on the access point 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 know about certificates and PKI. However, administrators do not need to define security parameters for access points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MINT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

To define an access point profile's MINT configuration:

1 Select **MINT Protocol** from the expanded **Advanced** menu. The **Settings** tab displays by default.

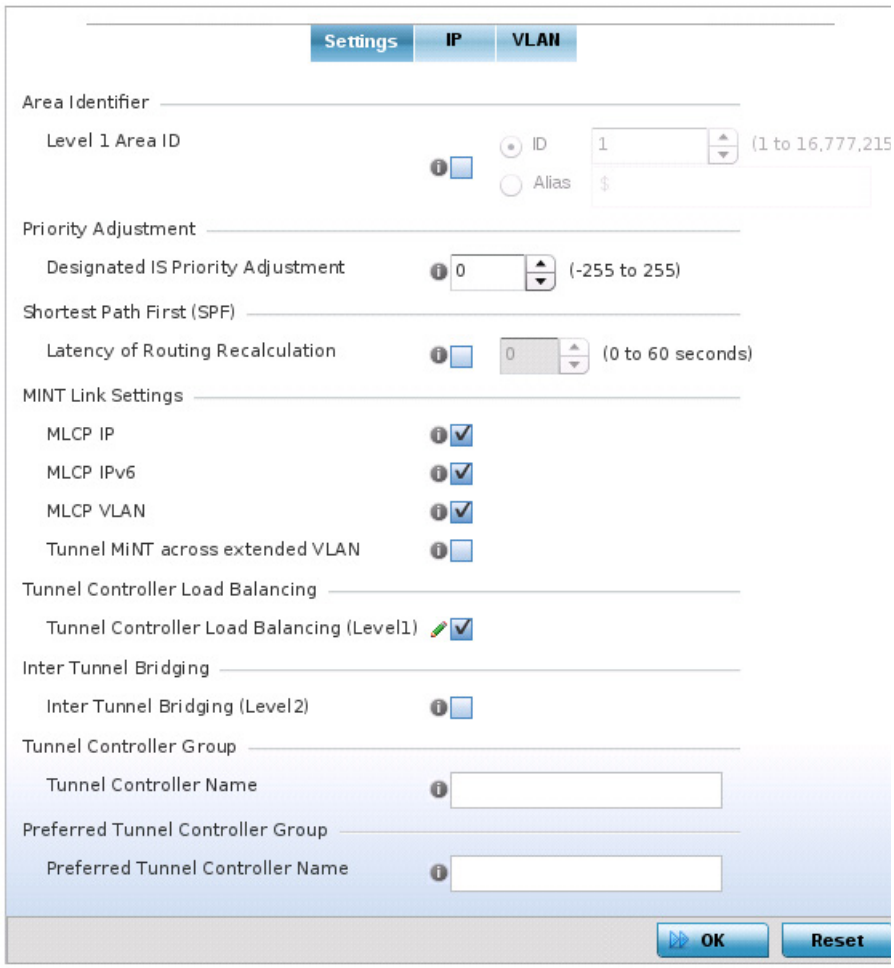


Figure 127: Advanced Profile Configuration - MINT Protocol screen - Settings tab

2 Refer to the **Area Identifier** field to define the Level 1 Area IDs used by the profile's MINT configuration.

Level 1 Area ID	Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 16,777,215. The default value is disabled. Alternatively provide an Alias by selecting the *Alias* option and adding the alias name to this field.

3 Define the following Device Heartbeat Settings in respect to devices supported by the profile:

Designated IS Priority Adjustment	Use the spinner control to set a Designated IS Priority Adjustment setting from -255 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.

4 Select the **Latency of Routing Recalculation** option (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 option disabled.

5 Define the following MINT Link Settings in respect to devices supported by the profile:

MLCP IP	Select this option to enable *MINT Link Creation Protocol* (MLCP) by IP Address. MLCP by IP is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a Virtual Controller, it can be an standalone access point.
MLCP IPv6	Select this option to enable *MINT Link Creation Protocol* (MLCP) by IPv6 Address. MLCP by IPv6 is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a Virtual Controller, it can be an standalone access point.
MLCP VLAN	Select this option to enable MLCP by VLAN. MLCP by VLAN is used to create one VLAN link from the device to a neighbor. The neighboring device does not need to be a Virtual Controller, it can be an standalone access point.
Tunnel MiNT across extended VLAN	Select this option to enable tunneling MiNT protocol packets across extended VLANs.

6 Select the **Tunnel Controller Load Balancing (Level1)** option to enable load balancing on the tunnel controller.

7 Select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging. This setting is disabled by default.

8 Enter a 64 character maximum **Tunnel Controller Name** for this tunneled-WLAN-controller interface.

9 Define a 64 character maximum group name for clustered tunnel controllers in the **Preferred Tunnel Controller Name** field.

10 Select **OK** to save the changes made to the **Settings** tab. Select **Reset** to revert to the last saved configuration.

11 Select the **IP** tab to display the link IP network address information shared by the devices managed by the access point's MINT configuration. The **IP** tab displays the *IP* address, *routing level*, *link cost*, *hello packet interval* and *adjacency hold time* settings used by managed devices to securely communicate amongst one another within the IPSec network.

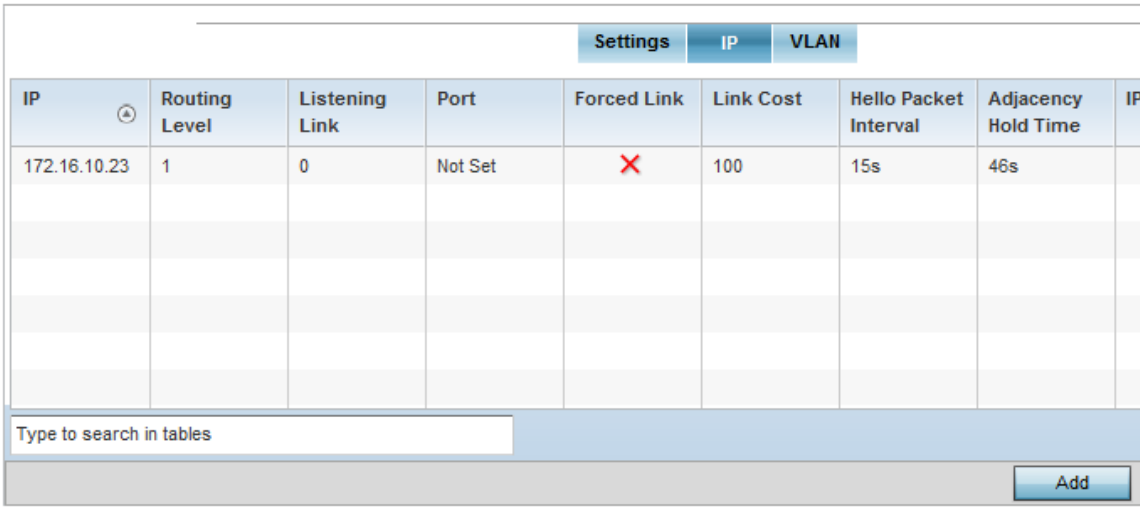


Figure 128: Advanced Profile Configuration - MINT Protocol screen - IP tab

12 Select **Add** to create a new Link IP configuration or **Edit** to modify an existing MINT configuration.

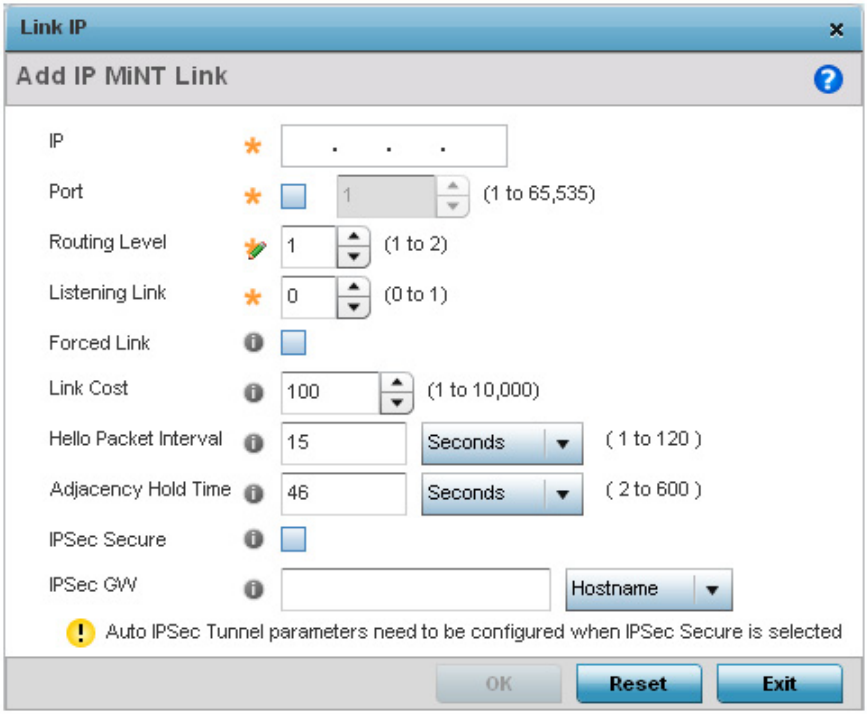


Figure 129: Advanced Profile Configuration- MINT Protocol screen - Add IP MiNT Link field

13 Set the following **Link IP** parameters to complete the MINT network address configuration:

IP	Define the IP address used by peer access points for interoperation when supporting the MINT protocol. Select IPv4 Address/IPv6 Address option to specify the IP address.
Port	Select this option to specify a custom port for MiNT links. Use the spinner control to define the port number (from 1 - 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 does not scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted.
Forced Link	Select this option to specify the MiNT link as a forced link.
Link Cost	Use the spinner control to define a link cost from 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	Select this option to use a secure link for IPSec traffic. This setting is disabled by default. When enabled, both the header and the traffic payload are encrypted.
IPSec GW	Define either an IP address or hostname for the IPSec gateway.

14 Select the **VLAN** tab to display the link IP VLAN information shared by the devices managed by the MINT configuration.

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.

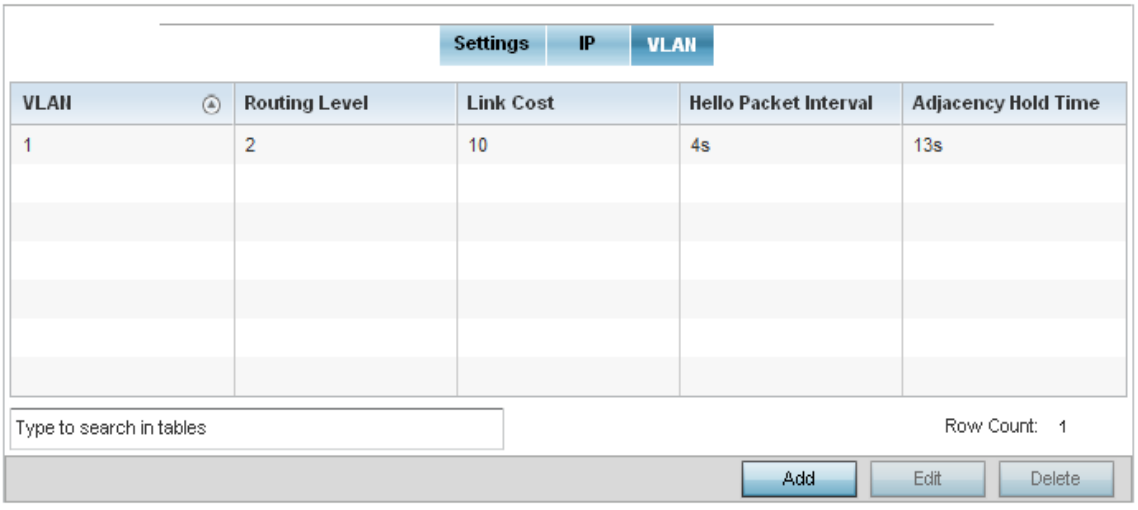


Figure 130: Advanced Profile Configuration - MINT Protocol screen - VLAN tab

15 Select **Add** to create a new VLAN link configuration or **Edit** to modify an existing configuration.

NOTE

If creating a mesh link between two access points in Standalone AP mode, you will need to ensure a VLAN is available to provide the necessary MINT link between the two Standalone APs.

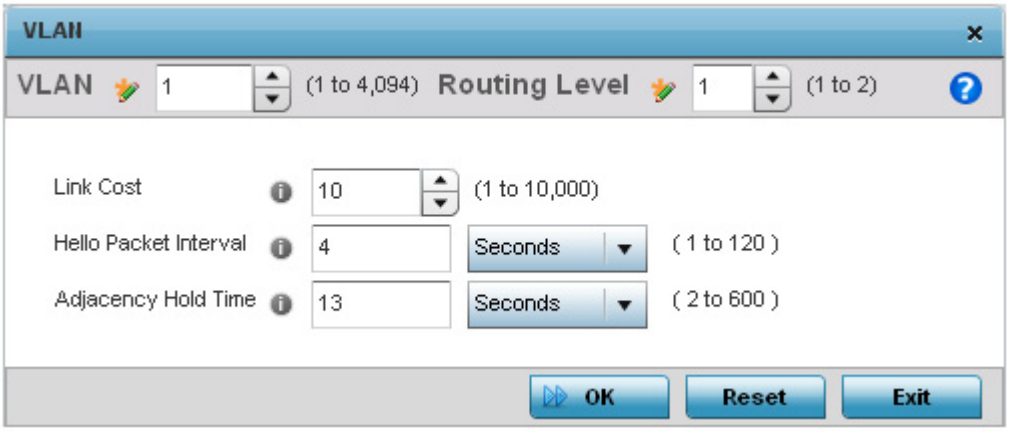


Figure 131: Advanced Profile Configuration - MINT Protocol screen - Add/ edit VLAN field

16 Set the following parameters to add or modify MINT VLAN configuration:

VLAN	If adding a new VLAN, define a VLAN ID from 1 - 4,094 used by peers for interoperation when supporting the MINT protocol.
Routing Level	If adding a new VLAN, use the spinner control to define a routing level of either 1 or 2.
Link Cost	Use the spinner control to define a link cost from 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 4 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 13 seconds.

17 Select **OK** to save the updates to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

18 Select the **Rate Limits** tab to display data rate limits configured on extended VLANs and optionally add or edit rate limit configurations.

Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using

vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the wireless controller, service platforms or access point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).

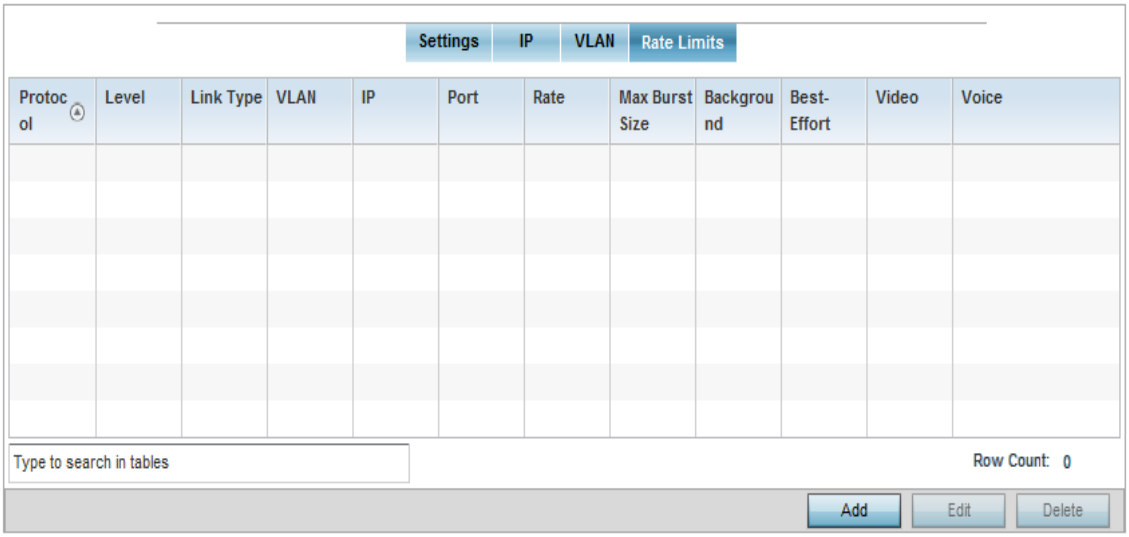


Figure 132: Advanced Profile - MINT screen - Rate Limits tab

Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

19 Select **Add** to create a new rate limit configuration or **Edit** to update the configuration of an existing configuration.

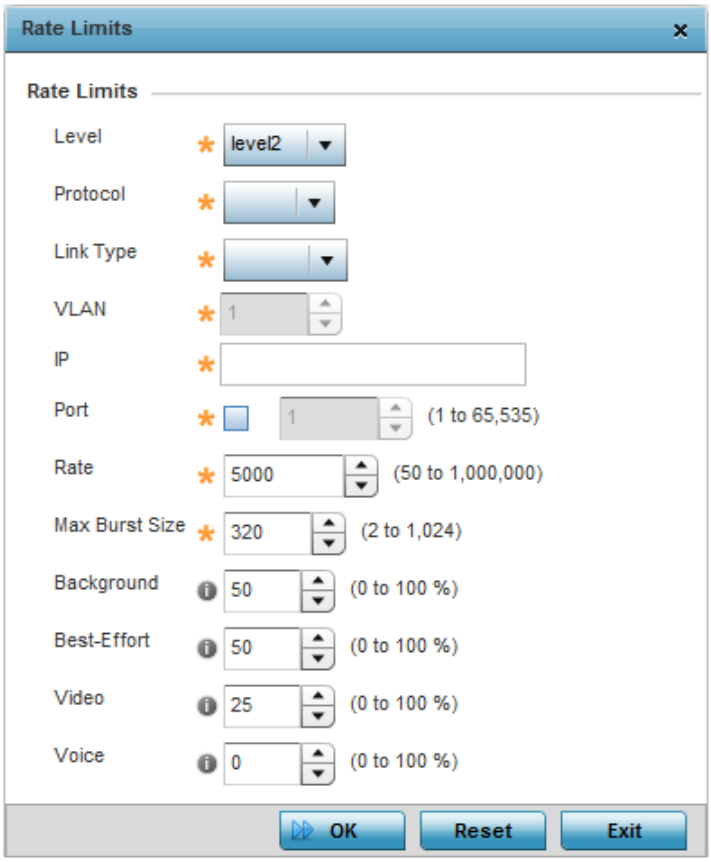


Figure 133: Advanced Profile - MINT screen - Add/Edit Rate Limits screen

20 Set the following **Rate Limits** to complete the MINT configuration:

Level	Select *level2* to apply rate limiting for all links on level2.
Protocol	Select either mlcp or link as this configuration's rate limit protocol. Mint Link Creation Protocol (MLCP) creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a wireless controller or service platforms, it can be an access point with a path to the wireless controller or service platforms. Select *link* to rate limit using statically configured MiNT links.
Link Type	Select either *VLAN*, to configure a rate limit configuration on a specific virtual LAN, or *IP* to set rate limits on a static IP address/Port configuration.
VLAN	When the *Protocol* is set to *link* and the *Link Type* is set to *VLAN*, use the spinner control to select a virtual LAN from *1 - 4094* to refine the rate limiting configuration to a specific VLAN.
IP	When the *Protocol* is set to *link* and the *Link Type* is set to *VLAN*, enter the IP address as the network target for rate limiting.
Port	When the *Protocol* is set to *link* and the *Link Type* is set to *VLAN*, use the spinner control to set the virtual port (1 - 65,535) used for rate limiting traffic.
Rate	Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Max Burst Size	Use the spinner to set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.
Background	Configures the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.
Best-Effort	Configures the random early detection threshold (as a percentage) for low priority best-effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%.
Video	Configures the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%.
Voice	Configures the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%.

21 Select **OK** to save the updates and overrides to the MINT Protocol's rate limit configuration. Select **Reset** to revert to the last saved configuration.

Advanced Profile Miscellaneous Configuration

"Advanced Profile 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 the wireless controller authorizes users, it queries the user profile database using a username representative of the physical NAS port making the connection.

1 Select **Miscellaneous** from the expanded **Advanced** menu.

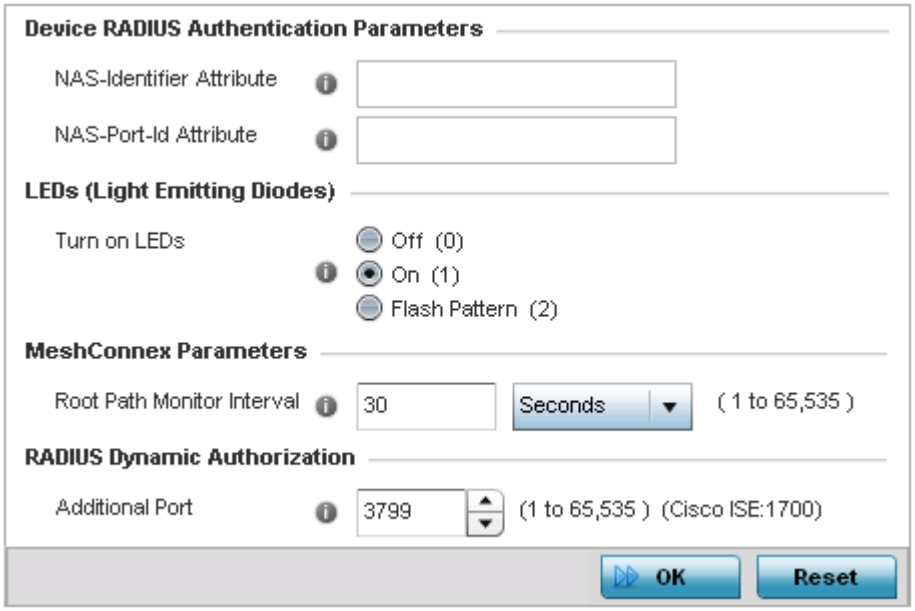


Figure 134: Advanced Profile Configuration - Miscellaneous screen

2 Set a **NAS-Identifier Attribute** up to 253 characters.

This is the RADIUS NAS-Identifier attribute that typically identifies the access point where a RADIUS message originates.

3 Set a **NAS-Port-Id Attribute** up to 253 characters.

This is the RADIUS NAS port ID attribute which identifies the port where a RADIUS message originates.

4 Select the **Turn on LEDs** radio button to ensure this access point's LED remain continuously illuminated. Deployments such as hospitals prefer to keep their wireless devices from having illuminating LEDs, as they have been reported to disturb their patients. this setting, however, is enabled by default.

Select the **Flash Pattern** radio button to enable the access point to blink in a manner that is different from its operational LED behavior. Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate that the initial configuration is complete.

5 Set the appropriate **Meshpoint Behavior** value by selecting either *external* (Fixed) or *vehicle-mounted* from the drop-down menu. The value vehicle-mounted indicates that the mesh point is mobile. This feature is only available on an AP7161 model access point.

6 Set the appropriate **Root Path Monitor Interval** value. This setting configures the frequency at which the path to the root mesh point is monitored.

7 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 of their definition files (this checking is called posture). If the client device complies, then it is allowed access to the network.

8 Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

Environmental Sensor Configuration

"System Profile Configuration"



NOTE

This feature is available on the AP8132 model only.

An AP8132 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 AP8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using the *Environmental Sensor* screen.

To set an environmental sensor configuration for an AP8132 model access point:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Select **Environmental Sensor.**

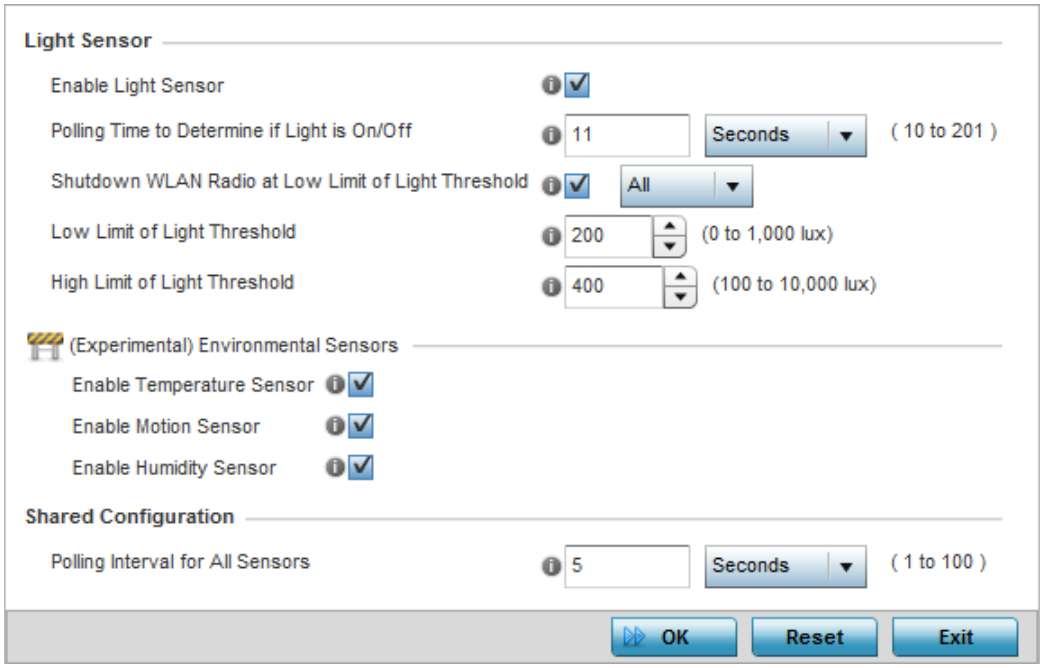


Figure 135: Profile - Environmental Sensor screen

5 Set the following **Light Sensor** settings for the AP8132'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 access point has its light sensor powered on or off.
Polling Time to Determine if Light is On/Off	Define an interval in *Seconds* (2 - 201) or *Minutes* (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 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 AP8132's radios if the light intensity falls below the set threshold. If enabled, select *All* (both AP8132 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 AP8132's deployment location. The default is 100.
High Limit of Light Threshold	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the AP8132's deployment location. The default is 500.

6 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 within the Statistics node. This setting is enabled by default.
Enable Motion Sensor	Select this option to enable the module's motion sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
Enable Humidity Sensor	Select this option to enable the module's humidity sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.

7 Define or override the following **Shared Configuration** setting:

Polling Interval for All Sensors	Set an interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between all environmental polling (both light and environment). The default setting is 5 seconds.

8 Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

Managing Virtual Controllers

"Device Configuration"

Access points set to function as Standalone APs can be re-defined as Virtual Controllers as required, and Virtual Controllers can reverted back to Standalone APs. Consider setting the access point to a Virtual Controller when more than one access points (of the same model) are deployed are require management from a centralized access point. Up to 64 Dependent mode access points can be connected to, and managed by, a single Virtual Controller AP of the same model.



NOTE

If designating the access point as a Standalone AP, it is recommended that the access point's UI be used exclusively to define its device configuration, and not the CLI. The CLI provides the ability to define more than one profile, while the UI only provides one per access point model. Consequently, the two interfaces cannot be used collectively to manage profiles without an administrator encountering problems.



NOTE

The recommended way to administer a network populated by numerous access points is to configure them directly from the designated Virtual Controller AP. If an access point's configuration requires an exception from the Virtual Controller AP's assigned profile configuration the administrator should apply a Device Override to change just that access point's configuration. For more information on applying an override to an access point's Virtual Controller AP assigned configuration profile, see "Device Overrides" on page 319.

To define a Standalone AP as a Virtual Controller AP:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Virtual Controller AP**.

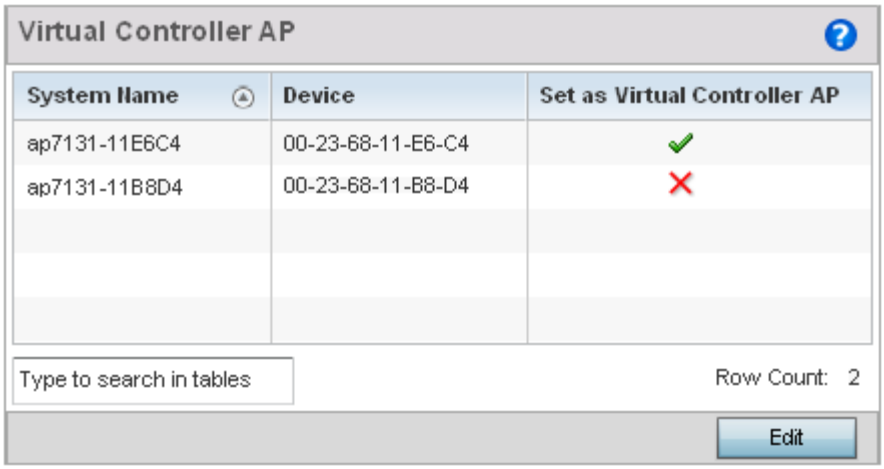


Figure 136: Virtual Controller AP screen

4 The **Virtual Controller AP** screen lists all peer access points within this Virtual Controller's radio coverage area. Each listed access point is listed by its assigned System Name, MAC Address and Virtual Controller designation. Only Standalone APs of the same model can have their Virtual Controller AP designation changed.

5 Either select an access point from those displayed and select **Edit**, or use the device browser in the lower left-hand side of the UI to select an access point.

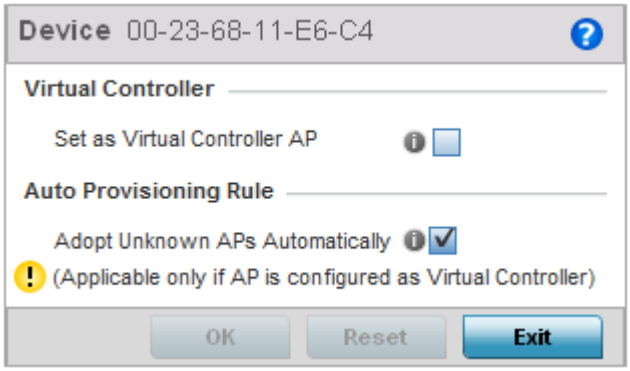


Figure 137: Managing Virtual Controller - AP Designation screen

6 Select the **Set as Virtual Controller AP** radio button to change the selected access point's designation from Standalone to Virtual Controller AP. Remember, only one Virtual Controller can manage (up to) 64 access points of the same model. Thus, an administrator should take care to change the designation of a Virtual Controller AP to Standalone AP to compensate for a new Virtual Controller AP designation.

7 Select the **Adopt Unknown APs Automatically** option to allow a Virtual Controller to adopt APs it does not recognize. While this option may help in the administration and management of all the APs in the network, it introduces the risk of allowing device association to a potential rogue device. Consequently, this setting is disabled by default.

8 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Delete** to remove obsolete rows as needed.

Overriding a Device Configuration

"Device Configuration"

Devices within the access point managed network can have an override configuration defined and applied. New devices can also have an override configuration defined and applied once



NOTE

The best way to administer a network populated by numerous access points is to configure them directly from the designated Virtual Controller AP. If an access point's configuration requires an exception from the Virtual Controller AP's assigned profile configuration the administrator should apply a Device Override to change just that access point's configuration. For more information on applying an override to an access point's Virtual Controller AP assigned configuration profile, see "Device Overrides" on page 319.

Refer to the following configuration overrides, applicable to devices within a access point managed network:

- "Basic Configuration"
- "Certificate Management"
- "Wired 802.1X Overrides"
- "RF Domain Overrides"
- "Device Overrides"

Basic Configuration

"Overriding a Device Configuration"

Applying a basic configuration override to a device entails changing (overriding) the device's system name, deployment area, building floor and system clock.

When a device is initially deployed, it requires several basic configuration parameters be set and its deployment location defined. Additionally, the number of permitted licenses needs to be accessed to determine whether new devices can be adopted (if in Virtual Controller AP mode).

To override a managed device's basic configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Device Overrides**.

4 Select a target device MAC address from either the device browser in the lower, left-hand side of the UI or within the *Device Overrides* screen.

The *Basic Configuration* screen displays by default.

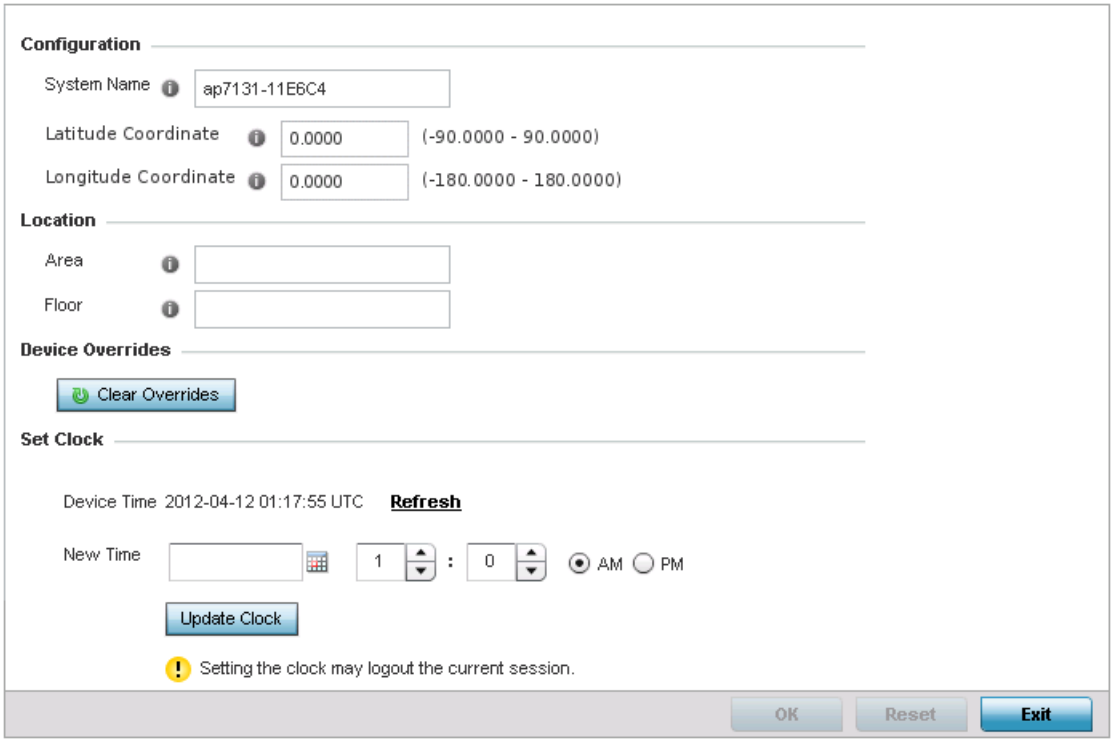


Figure 138: Device Overrides - Basic Configuration screen

5 Set the following **Configuration** settings for the target device:

System Name	Provide the selected device a system name up to 64 characters in length. This is the device name that appears within the RF Domain or Profile the access point supports and is identified by.
Latitude Coordinate	Optionally provide the latitude coordinate where the device is located. The valid value for this field is in the range -90.0000 degrees to +90.0000 degrees. When provided, this enables the device to be mapped on the geolocation map.
Longitude Coordinate	Optionally provide the longitude coordinate where the device is located. The valid value for this field is in the range -180.0000 degrees to +180.0000 degrees. When provided, this enables the device to be mapped on the geolocation map.
Area	Assign the access point an *Area* representative of the location the access point is physically deployed. The name cannot exceed 64 characters. Assigning an area is helpful when grouping access points in profiles, as access points in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.
Floor	Assign the target access point a building *Floor* name representative of the location the access point was physically deployed. The name cannot exceed 64 characters. Assigning a building floor name is helpful when grouping devices in profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

6 Refer to the **Device Overrides** field to assess whether overrides have been applied to the device's configuration. Use the **Clear Overrides** button to clear all device overrides and reset the configuration to its default values.

7 Refer to the **Set Clock** field to update the system time.

Refer to the **Device Time** parameter to assess the device's current time. If the device's time has not been set, the device time is displayed as unavailable. Select **Refresh** to update the device's system time.

Use the **New Time** parameter to set the calendar day, hour and minute. Use the AM and PM radio buttons to refine whether the updated time is for the AM or PM. This time can be synchronized with the use of an external NTP resource.

When completed, select **Update Clock** to commit the updated time to the device.

8 Select **OK** to save the changes to the basic configuration. Selecting **Reset** reverts the screen to its last saved configuration.

Certificate Management

"Overriding a Device Configuration"

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 resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides with the licensed device, while the private portion remains on the client.

The certificate configuration used by an access point managed device can be changed (overridden) as changes in security credentials require modification in the management of the device.

To override a managed device's certificate configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Device Overrides**.

4 Select a target device's MAC address from the device browser in the lower, left-hand side of the UI.

5 Select **Certificates** from the **Device** menu.

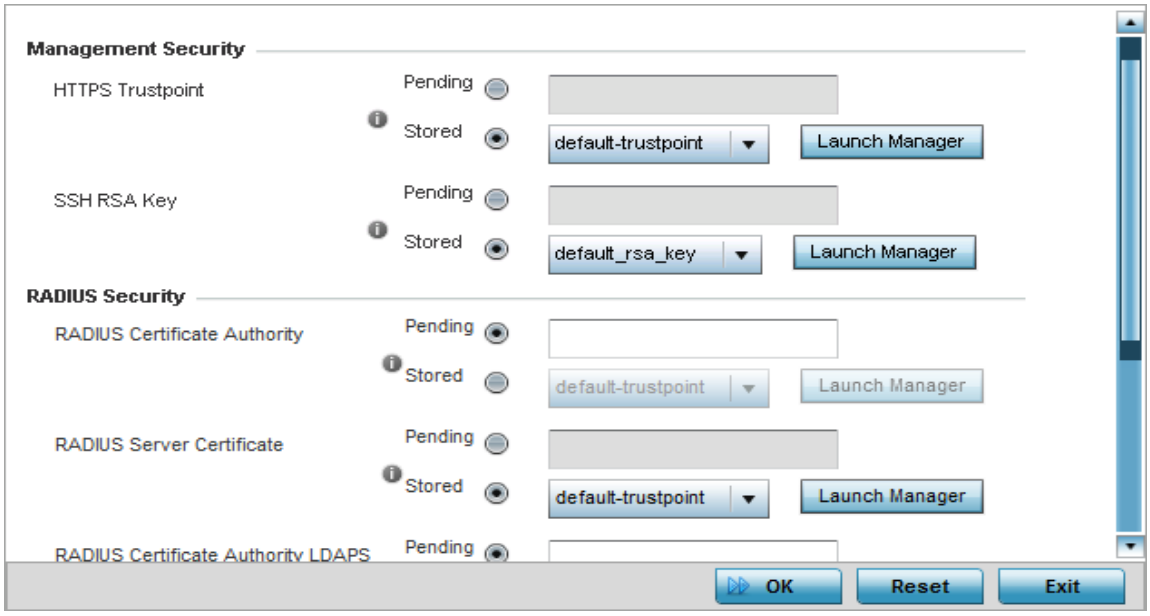


Figure 139: Device Overrides - Certificates screen

6 Set the following **Management Security** certificate configurations:

HTTPS Trustpoint	Either use the default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To leverage an existing device certificate for use with this target device, select the *Launch Manager* button. For more information, see "Manage Certificates" on page 301.
SSH RSA Key	Either use the default_rsa_key or select the *Stored* radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing key, select the *Launch Manager* button. For more information, see "RSA Key Management" on page 306.

7 Set the **RADIUS Security** certificate configuration. Select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be leveraged. To

leverage an existing device certificate for use with this target device, select the **Launch Manager** button.



NOTE

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

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

8 Use the **Authenticate Operator Certificate** to validate the operator's cross-certificate with the existing vendor certificate installed on the device. Use the **Launch Manager** to view more information on the installed vendor certificates. For more information on managing vendor certificates, see "Crypto CMP Policy" on page 660.

9 Select **OK** to save the changes made to the certificate configurations. Selecting **Reset** reverts the screen to its last saved configuration.

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

- "Manage Certificates"
- "RSA Key Management"
- "Certificate Creation"
- "Generating a Certificate Signing Request"

Manage Certificates

- "Certificate Management"

If not wanting to use an existing certificate or key with a selected device, an existing stored certificate can be leveraged from a different device. Device certificates can be imported and exported to a secure remote location for archive and retrieval as required for application to other devices.

To configure trustpoints for use with certificates:

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

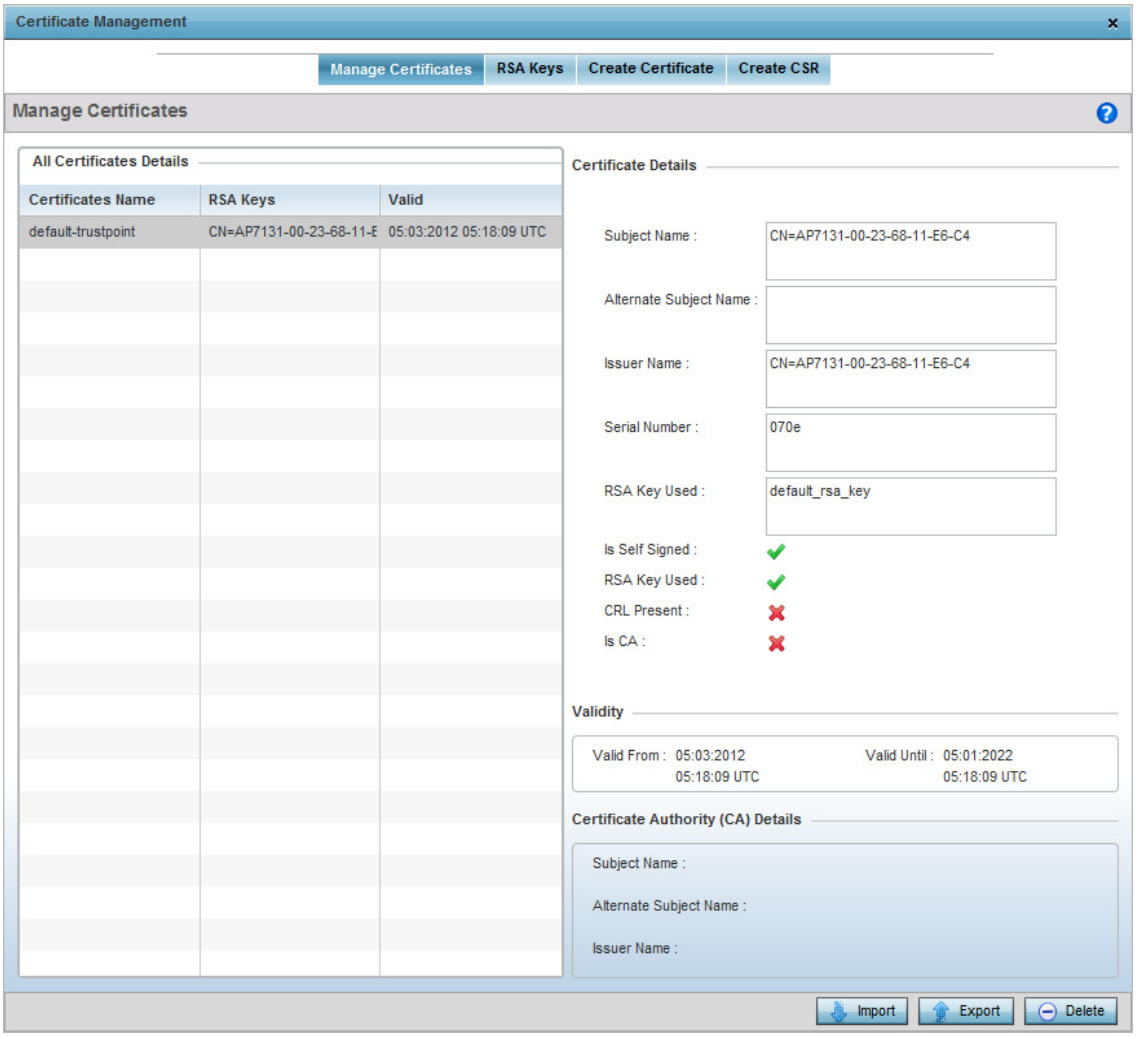


Figure 140: Certificate Management - Trustpoints screen

The **Certificate Management** screen displays with the **Trustpoints** section displayed by default.

2 Select a device from amongst those displayed to review its certificate information.

Refer to **Certificate Details** to review the certificate's properties, self-signed credentials, validity period and CA information.

3 To optionally import a certificate, select the **Import** button from the **Certificate Management** screen.

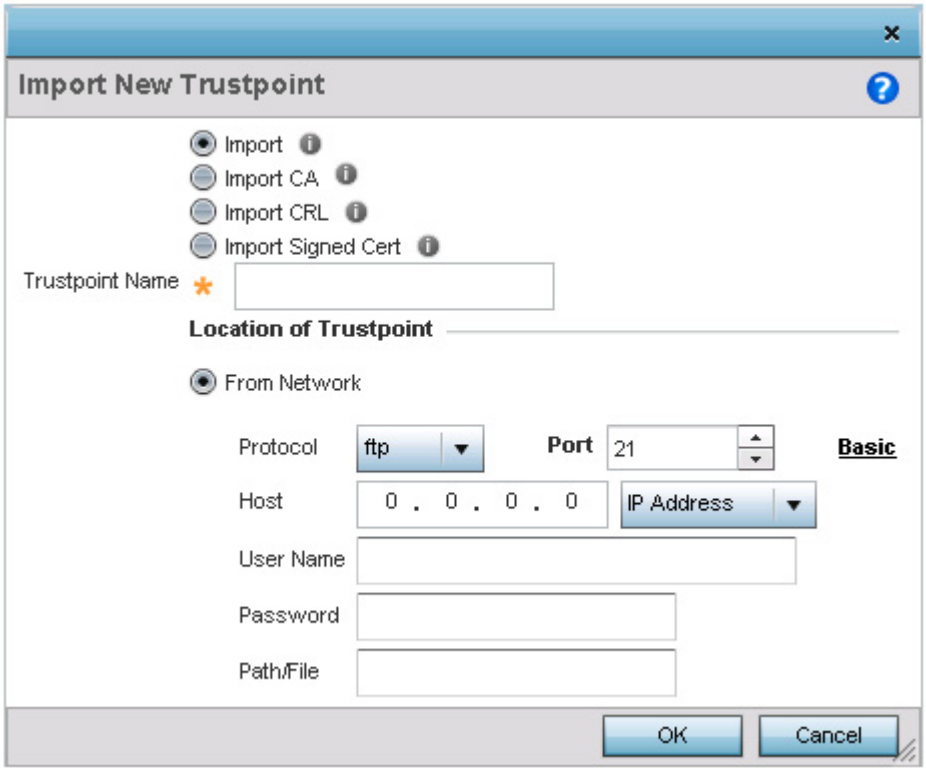


Figure 141: Certificate Management - Import New Trustpoint screen

4 Define the following configuration parameters required for the Import of the trustpoint:

Import	Select the type of Trustpoint to import. The following Trustpoints can be imported: • *Import* – Select to import any trustpoint. • *Import CA* – Select to import a *Certificate Authority* (CA) certificate on to the access point. • *Import CRL* – Select to import a *Certificate Revocation List* (CRL), CRLs are used to identify and remove those installed certificates that have been revoked or are no longer valid. • *Import Signed Cert* – Select to import a self signed certificate.
Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.

A *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.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A *certificate revocation list* (CRL) is a list of revoked certificates, or certificates no longer valid. A certificate can be revoked if the CA improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

5 Define the following configuration to import the Trustpoint from a location on the network. To do so, select **From Network** and provide the following information.

URL	Provide the complete URL to the location of the trustpoint. This option is available by default. Click the *Advanced* link next to this field to display more fields to provide detailed trustpoint location information. This option is only available when the *Basic* link is clicked.
Protocol	If using *Advanced* settings, select the protocol used for importing the target trustpoint. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If using *Advanced* settings, use the spinner control to set the port. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Host	If using *Advanced* settings, provide the hostname of the server used to import the trustpoint. Select *IPv4 Address* or *IPv6 Address* to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If using *Advanced* settings, specify the path to the trustpoint. Enter the complete path to the file on the server.

6 Select the **Cut and Paste** option to paste the trustpoint information in text. When this option is selected, the text box next to it is enabled. Paste the trustpoint details into the text box. This option is only available when *Import CA, Import CRL* or *Import Signed Cert* is selected.

7 Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

8 To optionally export a trustpoint to a remote location, select the **Export** button from the **Certificate Management** screen.

Once a certificate has been generated on the authentication server, export the self-signed certificate.

A digital CA certificate is different from a self-signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an Active Directory Group Policy for automatic root-certificate deployment.

Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication servers, export the certificate and do not generate a second key unless you want to deploy two root certificates.

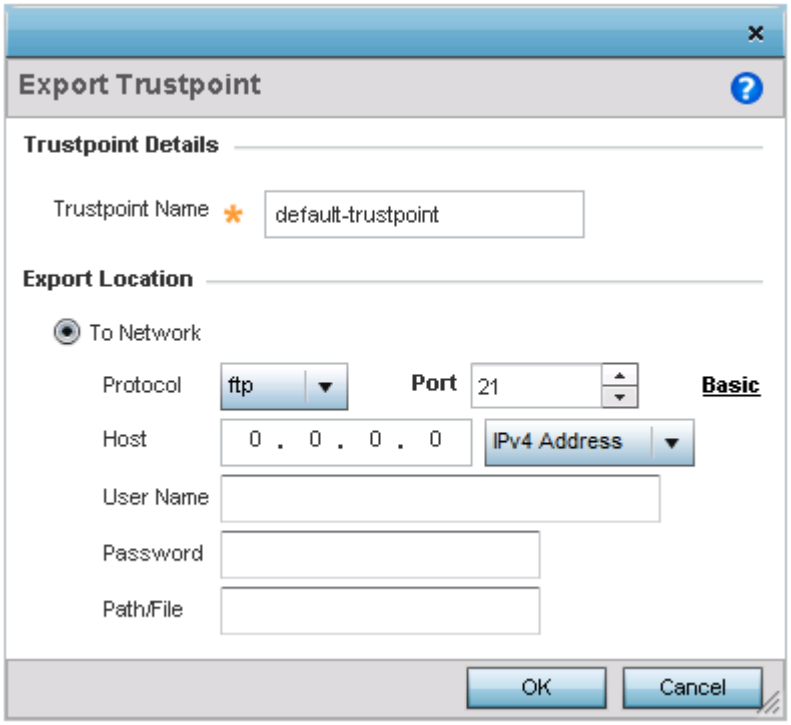


Figure 142: Certificate Management - Export Trustpoint screen

9 Define the following configuration parameters to export a trustpoint:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol. This option is only available when the *Basic* link is clicked.
Protocol	Select the protocol used for exporting the target trustpoint. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If using *Advanced* settings, use the spinner control to set the port. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Host	If using *Advanced* settings, provide the hostname of the server used to export the trustpoint. Select *IPv4 Address* or *IPv6 Address* to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If using *Advanced* settings, specify the path to the trustpoint. Enter the complete relative path to the file on the server.

10 Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

To optionally delete a trustpoint, select the **Delete** button from within the **Certificate Management** screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select the **Delete RSA Key** option to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the *Certificate Management* screen.

RSA Key Management

"Certificate Management"

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

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It is an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).

2 Select **RSA Keys** tab from the menu on the **Certificate Management** screen.

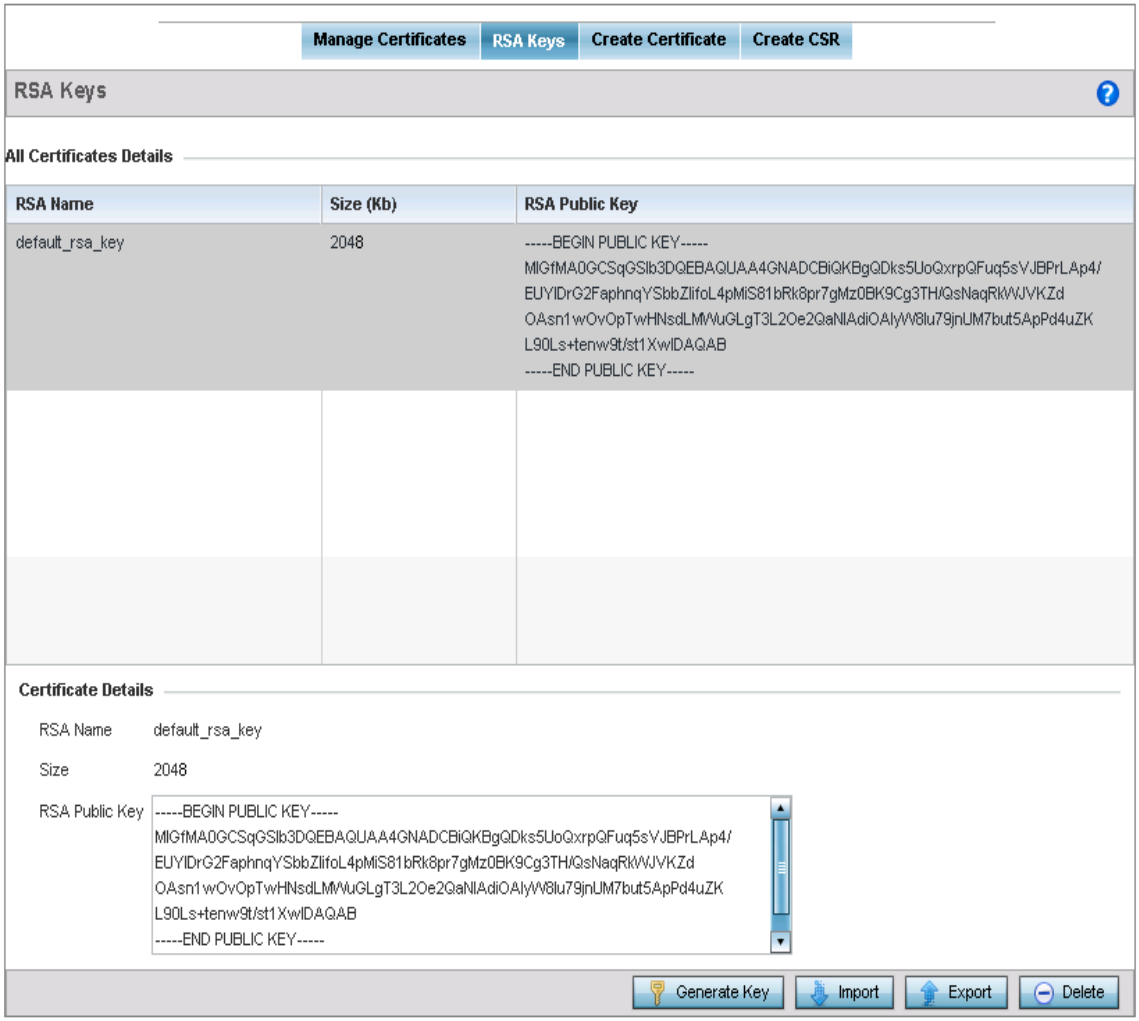


Figure 143: Certificate Management - RSA Keys screen

3 Select a listed device to review its current RSA key configuration.

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

4 Select the **Generate Key** button to create a new key.

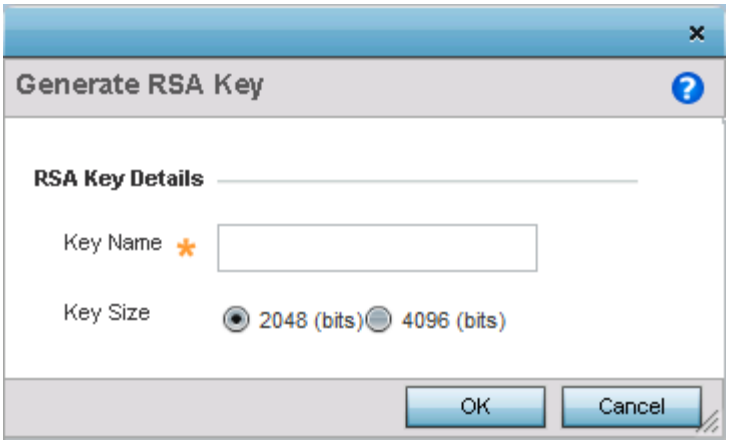


Figure 144: Certificate Management - Generate RSA Key screen

5 Define the following configuration parameters required to generate a key:

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Size	Use the spinner control to set the size of the key (from 2,048 or 4096 bits). It is recommended leaving this value at the default setting of 2048 to ensure optimum functionality.

6 Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

7 To optionally import a CA certificate, select the **Import** button from the RSA Keys screen.

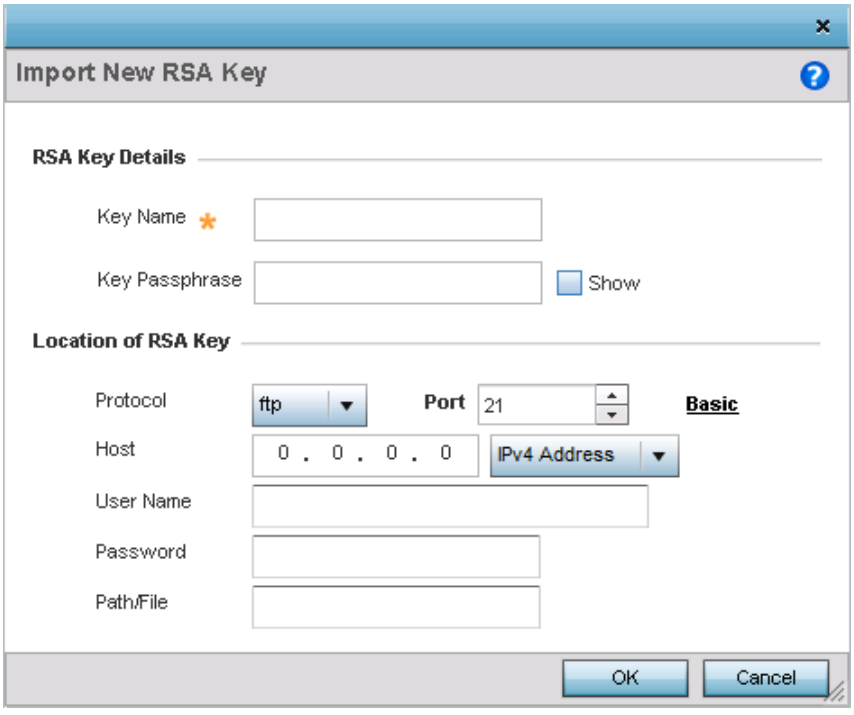


Figure 145: Certificate Management - Import New RSA Key screen

8 Define the following configuration parameters required to import a RSA key:

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Passphrase	Define the key used by both the access point and the server (or repository) of the target RSA key. Select the *Show* option to expose the actual characters used in the passphrase. Leaving the *Show* option unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the RSA key. This option is only available when the *Basic* link is clicked.
Protocol	If selecting *Advanced*, select the protocol used for importing the target key. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If selecting *Advanced*, use the spinner control to set the port. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Host	If selecting *Advanced*, provide the hostname of the server used to import the RSA key. Select *IPv4 Address* or *IPv6 Address* to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If selecting *Advanced*, specify the path to the RSA key. Enter the complete relative path to the key on the server.

9 Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

10 To optionally export a **RSA key** to a remote location, select the **Export** button from the RSA Keys screen.

11 Export the key to a RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

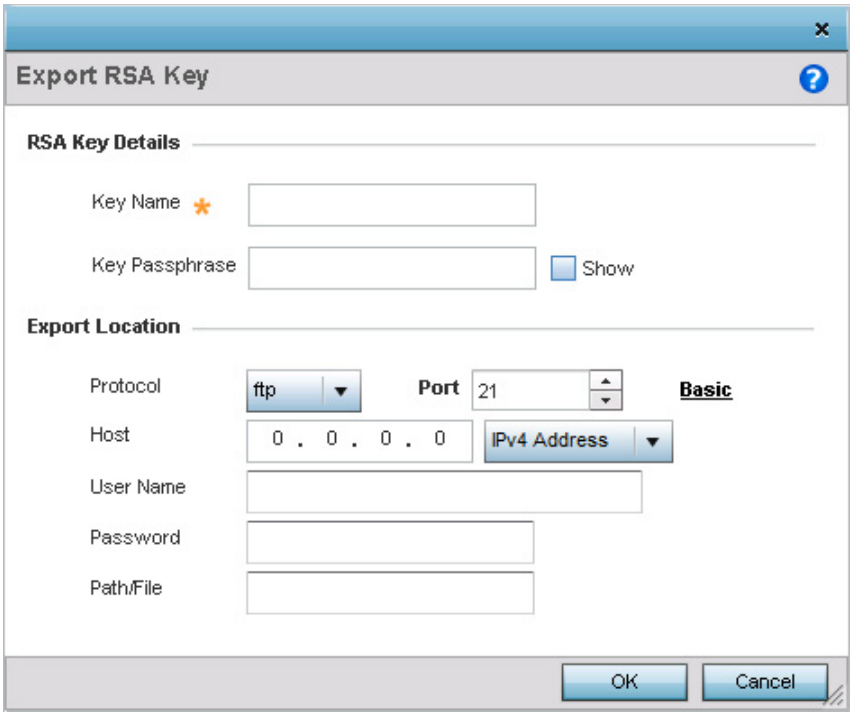


Figure 146: Certificate Management - Export RSA Key screen

12 Define the following configuration parameters required to export a RSA key:

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Passphrase	Define the key passphrase used by both the access point and the server. Select the *Show* option to expose the actual characters used in the passphrase. Leaving the *Show* option unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the key. This option is only available when the *Basic* link is clicked.

Protocol	If selecting *Advanced*, select the protocol used for exporting the RSA key. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If selecting *Advanced*, use the spinner control to set the port. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Host	If selecting *Advanced*, provide the hostname of the server used to export the RSA key. Select *IPv4 Address* or *IPv6 Address* to provide the IP address of a host device appropriately. This option is not valid for *cf*, *usb1, usb2, usb3* and *usb4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols,. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If selecting *Advanced*, specify the path to the key. Enter the complete relative path to the key on the server.

13 Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

14 To optionally delete a key, select the **Delete** button from within the RSA Keys screen. Provide the key name within the **Delete RSA Key** screen and select the **Delete Certificates** option to remove the certificate and the supported key. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

Certificate Creation

"Certificate Management"

The *Certificate Management* screen provides the facility for creating new self-signed certificates. Self-signed certificates (often referred to as root certificates) do not use public or private CAs. A self-signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate:

1 Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).

2 Select **Create Certificate** tab from the menu on the **Certificate Management** screen.

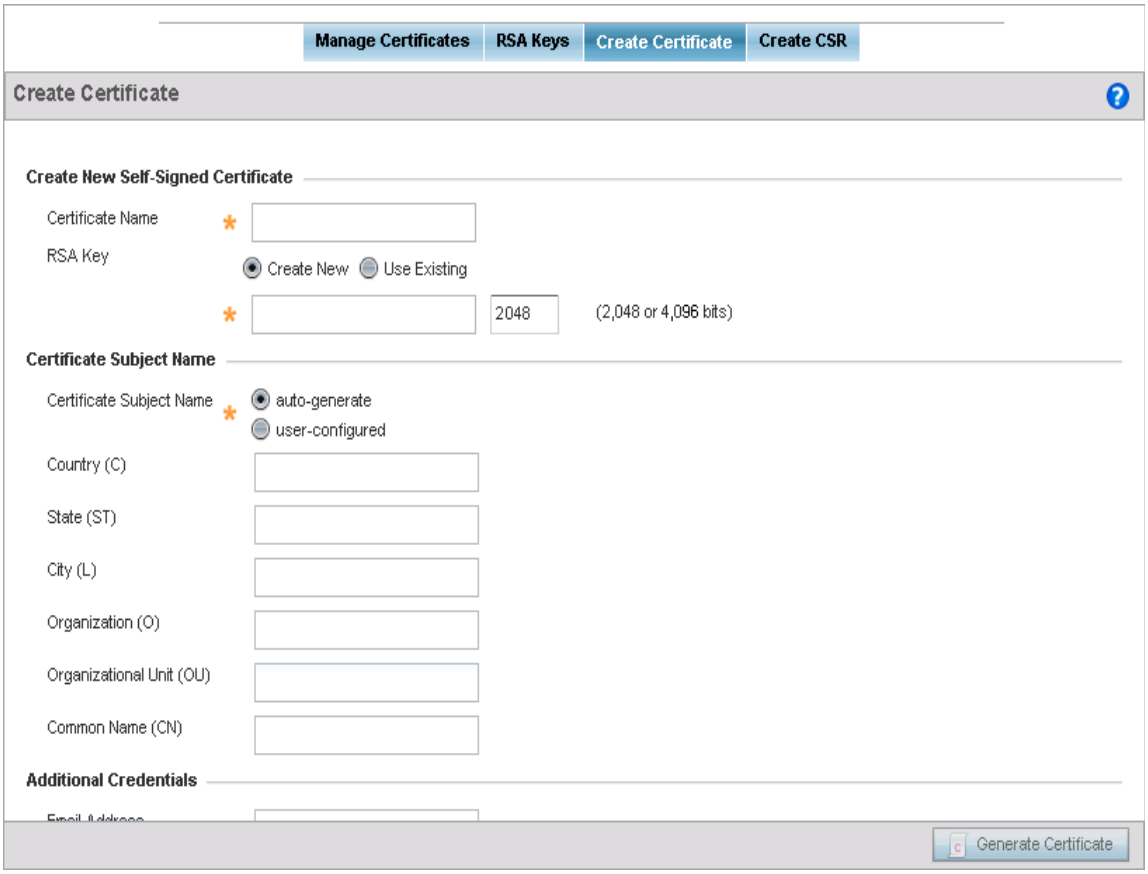


Figure 147: Certificate Management - Create Certificate screen

3 Set the following **Create New Self-Signed Certificate** configuration parameters:

Certificate Name	Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/ identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
Use Existing	Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key.
Create New	Select this option to create a new RSA key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 2,048 or 4,096 bits). It is recommended leaving this value at the default setting (2048) to ensure optimum functionality. For more information on creating a new RSA key, see "RSA Key Management" on page 306.

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or select *user-configured* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the Country of deployment for the certificate. The field can be modified by the user. This is a required field and must not exceed 2 characters.
State (ST)	Enter a State for the state or province name used in the certificate. This is a required field.
City (L)	Enter a City to represent the city name used in the certificate. This is a required field.
Organization (O)	Define an Organization for the organization used in the certificate. This is a required field.
Organizational Unit (OU)	Enter an Organizational Unit for the name of the organization unit used in the certificate. This is a required field.
Common Name (CN)	If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5 Set the following **Additional Credentials** required for the generation of the self-signed certificate:

Email Address	Provide an E-mail address used as the contact address for issues relating to this certificate request.
Domain Name	Enter a *fully qualified domain name* (FQDN) as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since s a suffix is not added.
IP Address	Specify the IP address used as the destination for certificate requests.

6 Select the **Generate Certificate** button at the bottom of the screen to generate the certificate.

Generating a Certificate Signing Request

"Certificate Management"

A *certificate signing request* (CSR) is an application from a requestor to a certificate authority to issue a digitally signed identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate

authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 Select the **Launch Manager** button from either the *SSH RSA Key* or *RADIUS Server Certificate* parameters (within the **Certificate Management** screen).

2 Select **Create CSR** tab from the menu on the **Certificate Management** screen.

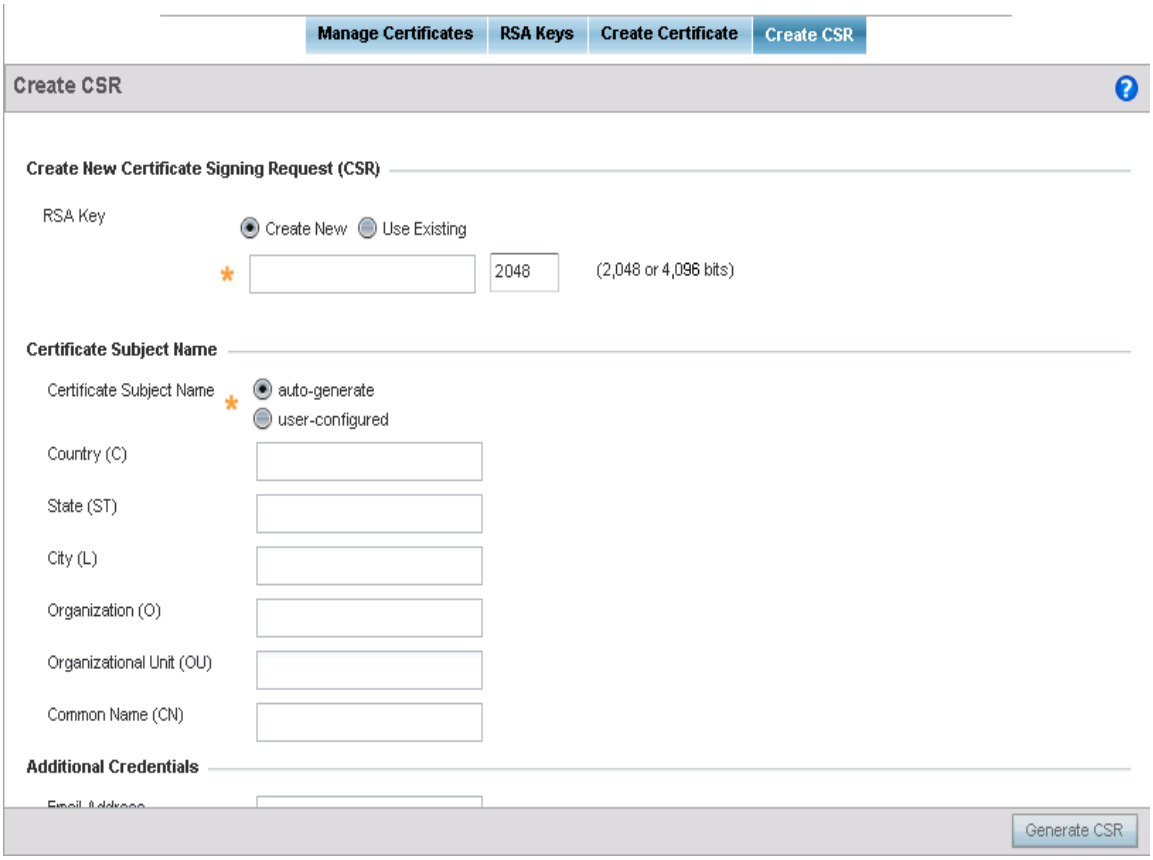


Figure 148: Certificate Management - Create CSR screen

3 Set the following **Create New Certificate Signing Request (CSR)** configuration parameters:

Create New	Select this option to create a new RSA Key. Provide a 32 character name to identify the RSA key. Use the spinner control to set the size of the key (from 2,048 or 4,096 bits). It is recommended leaving this value at the default setting (2048) to ensure optimum functionality. For more information on creating a new RSA key, see "RSA Key Management" on page 306.
Use Existing	Select this option to use an existing RSA key. Use the drop-down menu to select the existing key used by both the device and the server (or repository) of the target RSA key.

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or select *user-configured* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the Country used in the CSR. The field can be modified by the user. This is a required field and must not exceed 2 characters.
State (ST)	Enter a State for the state or province name used in the CSR. This is a required field.
City (L)	Enter a City to represent the city name used in the CSR. This is a required field.
Organization (O)	Define an Organization for the organization used in the CSR. This is a required field.
Organizational Unit (OU)	Enter an Organizational Unit for the name of the organization unit used in the CSR. This is a required field.
Common Name (CN)	If there is a Common Name (IP address) for the organizational unit issuing the certificate, enter it here.

5 Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an E-mail address used as the contact address for issues relating to this CSR.
Domain Name)	Enter a FQDN as an unambiguous domain name that specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
IP Address	Specify the IP address used as the destination for certificate requests.

6 Select the **Generate CSR** button at the bottom of the Create CSR screen to generate the CSR.

Wired 802.1X Overrides

"Overriding a Device 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 **Devices**.

3 Select **Device Overrides** from the options on left-hand side of the UI.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Wired 802.1x**.

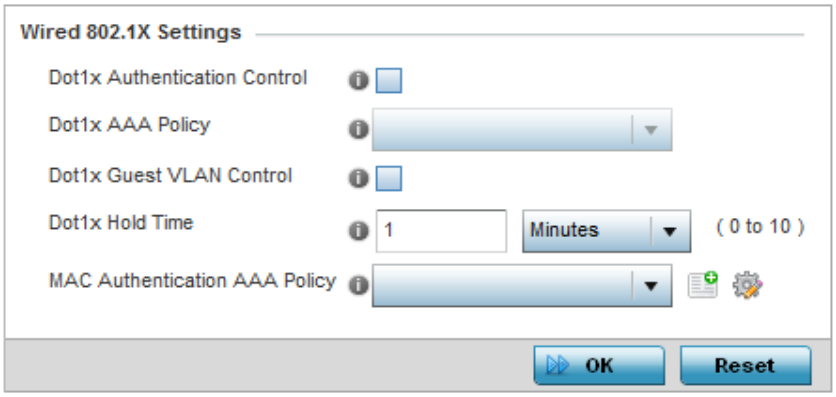


Figure 149: Profile Wired 802.1X screen

6 Set the following **Wired 802.1x Settings**:

Dot1x Authentication Control	Select this option to globally enable 802.1x authentication for the access point. This setting is disabled by default.
Dot1x AAA Policy	Use the drop-down menu to select an AAA policy to associate with the wired 802.1x traffic. If a suitable AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.
Dot1x Guest VLAN Control	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
Dot1x Hold Time	Set a hold time value (after the last hello packet) in either Seconds (0 - 600) or Minutes (0 - 10). When exceeded, the controller's 802.1X enabled port and its destination end-point connection is defined as lost and the connection must be re-established.
MAC Authentication AAA Policy	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.

7 Select **OK** to save the changes to the 802.1x override configuration. Select **Reset** to revert to the last saved configuration.

RF Domain Overrides

"Overriding a Device Configuration"

Use *RF Domain Overrides* to define settings overriding a target device's original RF Domain configuration.

An RF Domain allows an administrator to assign configuration data to multiple access points (of the same model) deployed in a common coverage area (floor, building or site). In such instances, there are many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement from their original RF Domain administered design. Unlike a RFS series controller, an access point supports a single RF domain. An access point RF Domain cannot be used on a different model access point. For example, an AP6532 RF Domain override can only be applied to another AP6532 model access point.

To define a device's RF Domain override configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **RF Domain Overrides**.

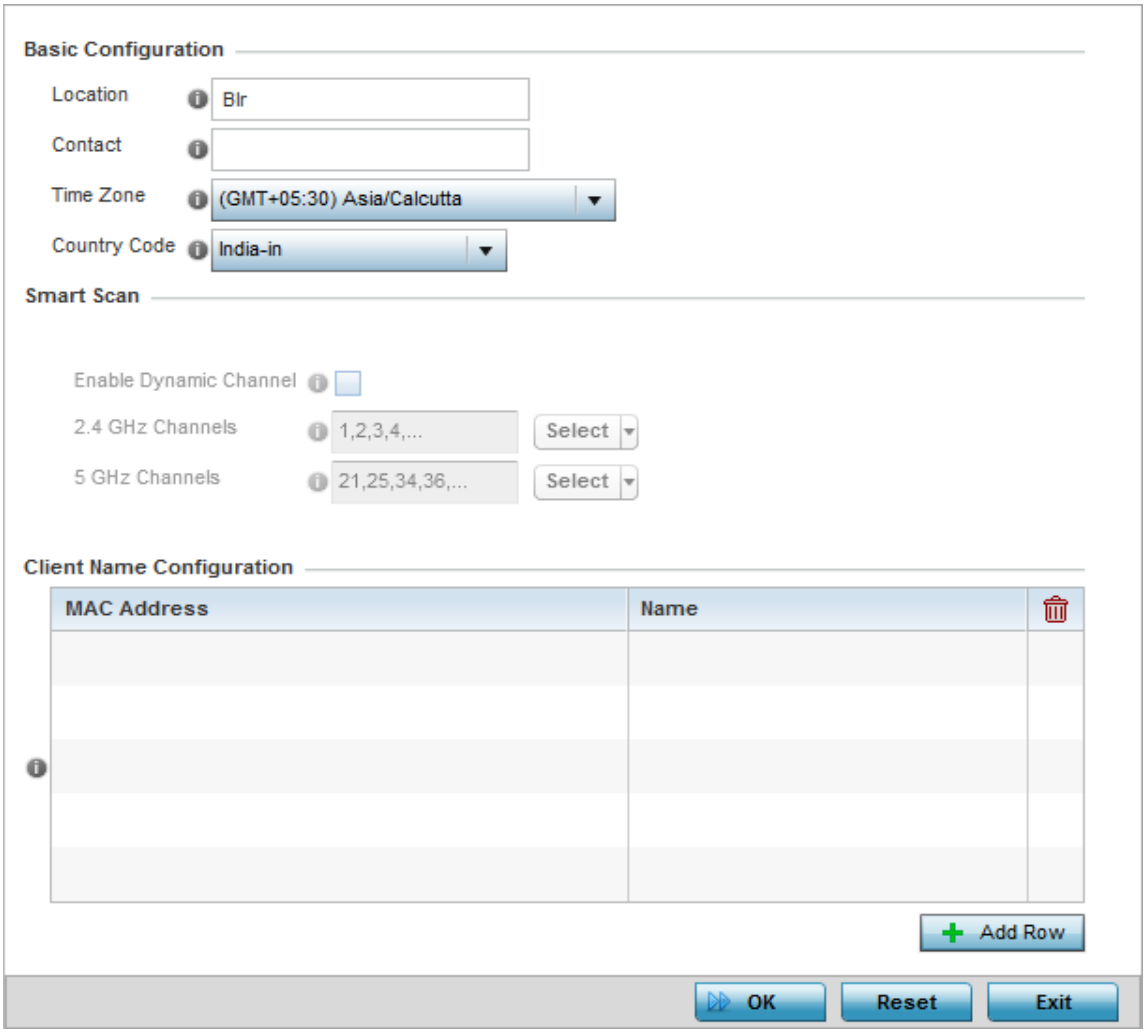


Figure 150: Device Overrides - RF Domain Overrides screen

NOTE

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove a device's override, go to the *Basic Configuration* screen's *Device Overrides* field, and then select the *Clear Overrides* button.

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

Location	Set the deployment location for the access point as part of its RF Domain configuration.
Contact	Set the administrative contact for the access point. This should reflect the administrator responsible for the access point's configuration and wireless network.
Time Zone	Use the drop-down menu to select the geographic time zone supporting its deployment location.
Country Code	Use the drop-down menu to select the country code supporting its deployment location.

7 Refer to the **SMART Scan** field to review the settings defined for SMART RF. Optionally assign/remove overrides to and from specific parameters.

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

8 Refer to the **Client Name** table to view the clients connected to RF Domain member access points adopted by networked controllers or service platforms. Use the table to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

Enter the client's factory coded MAC address in the **MAC Address** field. Assign a name to the RF Domain member access point's connected client to assist in its easy recognition in the **Name** field.

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

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



NOTE

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

Select the **Create** icon to create a new sensor policy to apply to this RF Domain or select the **Edit** icon to update the configuration of an existing policy before applying it to the RF Domain. For more information, see "Sensor Policy" on page 646

11 Within a **MPact Appliance** architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated MPact Server resource, as opposed to an ADSP server. Select the **+ Add Row** button to populate the screen with up to three rows for MPact server credentials.

Server Id	Use the spinner control to assign a numeric ID for up to three MPact servers designated to receive RSSI scan data from a WiNG dedicated server. The server with the lowest defined ID is the first reached. The default ID is 1.
IP Address/Hostname	Provide the numeric (non DNS) IP address or hostname of up to three MPact server resources for receiving RSSI scan data. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of the MPact sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443.

12 For an **ADSP Appliance** sensor architecture, select the **+ Add Row** button to populate the screen with up to three rows for ADSP server credentials:

Server Id	Use the spinner control to assign a numeric ID for up to three ADSP servers designated to receive RSSI scan data from a WiNG dedicated server. The server with the lowest defined ID is the first reached. The default ID is 1.
IP Address/Hostname	Provide the numeric (non DNS) IP address or hostname of up to three ADSP server resources for receiving RSSI scan data. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of the ADSP sensor server resource receiving RSSI scan data from a dedicated sensor. The default port is 443.

13 Select **OK** to save the changes and overrides made to the RF Domain configuration. Selecting **Reset** reverts the screen to its last saved configuration.

Device Overrides

"Overriding a Device Configuration"

A profile enables an administrator to assign a common set of configuration parameters and policies to another access point of the same model. Profiles can be used to assign shared or unique network, wireless and security parameters to access points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

However, device profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could require modification from a profile configuration shared amongst numerous devices deployed within a particular site.

Refer to the following to complete the override of the access point's entire profile configuration:

- "Radio Power Overrides"

- "Adoption Overrides"
- "Profile Interface Override Configuration"
- "Overriding the Network Configuration"
- "Overriding Security Configuration"
- "Overriding the Virtual Router Redundancy Protocol (VRRP) Configuration"
- "Profile Critical Resources"
- "Overriding a Services Configuration"
- "Overriding Management Configuration"
- "Overriding Mesh Point Configuration"
- "Overriding Environmental Sensor Configuration"
- "Overriding an Advanced Configuration"

Use device overrides to define configurations overriding the parameters set by the target device's original profile configuration.

To define a general profile override configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Device Overrides** from the Device menu to expand it into sub menu options.

6 Select **General** if it does not display by default.

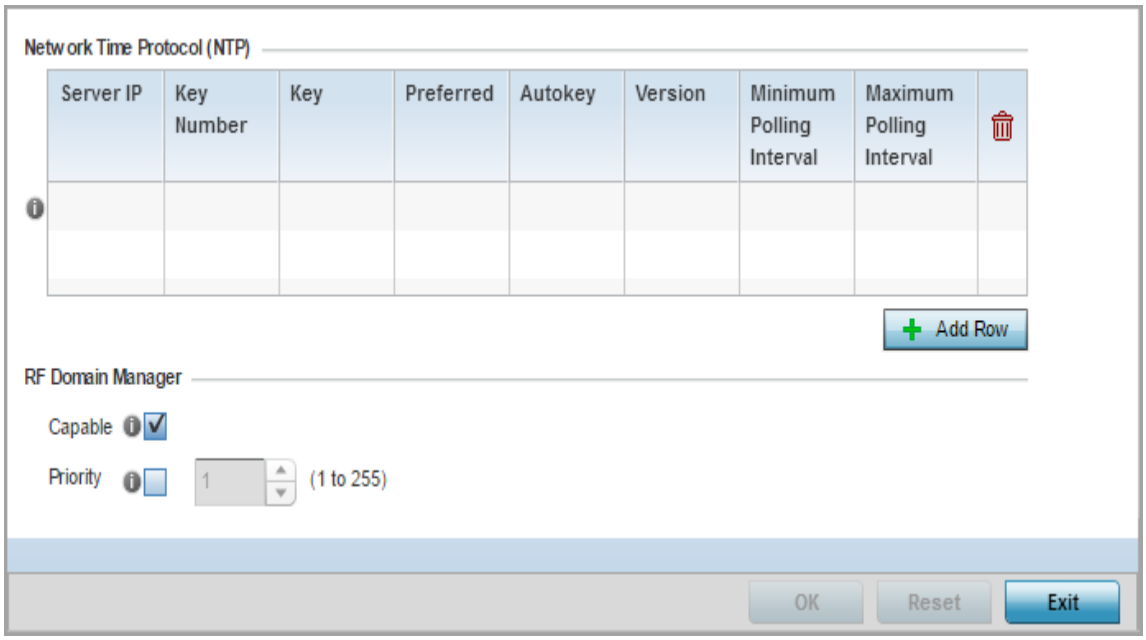


Figure 151: Device Overrides - General screen

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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

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

Server IP	Set the IP address or hostname of each server added as a potential NTP resource. Use the drop-down located next to this field to select from either *IP Address* or *Hostname*. When *Hostname* is selected, provide the hostname of the NTP server in this field.
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 access point and NTP resource share to securely interoperate.

Preferred	Select this option designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources are given first opportunity to connect and provide NTP calibration.
AutoKey	Select this option 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 which indicates *ignore*.
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.

8 Refer to the **RF Domain Manager** field to configure this device as a RF Domain manager.

9 Select the **Capable** option to enable or disable this device as a RF Domain manager.

10 Select the **Priority** option to enable configuring a priority value for this device when election to become a Domain Manager is conducted. Set a value using the spinner control. Setting a low value increases the chance of this device becoming the RF Domain manager.

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

Radio Power Overrides

"Device Overrides"

Use the *Power* screen to set or override one of two power modes (*3af* or *Auto*) for an 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 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 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 or apply an override to an existing parameter:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Device Overrides** from the Device menu to expand it into sub-menu options.

6 Select **Power**.

A screen displays where an access point's power configuration can be defined or overridden.

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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

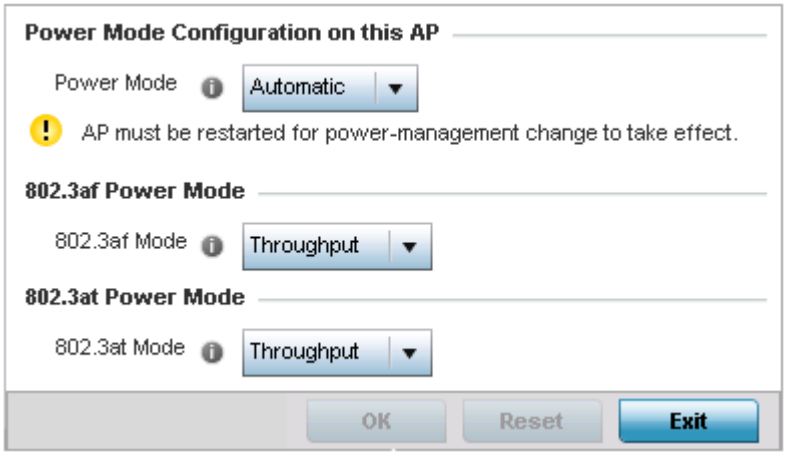


Figure 152: Device Overrides - Power screen

7 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. 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.

8 Set or override the access point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

Use the drop-down menu 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.

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

Adoption Overrides

"Device Overrides"

Use the *Adoption* screen to define the configuration of a preferred Virtual Controller, wireless controller, or service platform resource used for access point adoption. A Virtual Controller can adopt up to 64 access points of the same model. The Virtual Controller must also share its VLAN to peer access points wishing to adopt to it. The Virtual Controllers IP address (or hostname), pool and routing level must also be defined and made available to connecting peers.

Adoption is the process an access point uses to discover Virtual Controllers available in the network, pick the most desirable Virtual Controller, establish an association, obtain its configuration and consider itself provisioned.

At adoption, an access point solicits and receives adoption responses from Virtual Controllers available on the network.

To define an access point's Virtual Controller configuration or apply an override to an existing parameter:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

3 Select **Device Overrides**.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Device Overrides** from the Device menu to expand it into sub menu options.

6 Select **Adoption**.

A screen displays where an access point's Virtual Controller group, VLAN and network address information can be defined or overridden for the preferred Virtual Controller resource.

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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

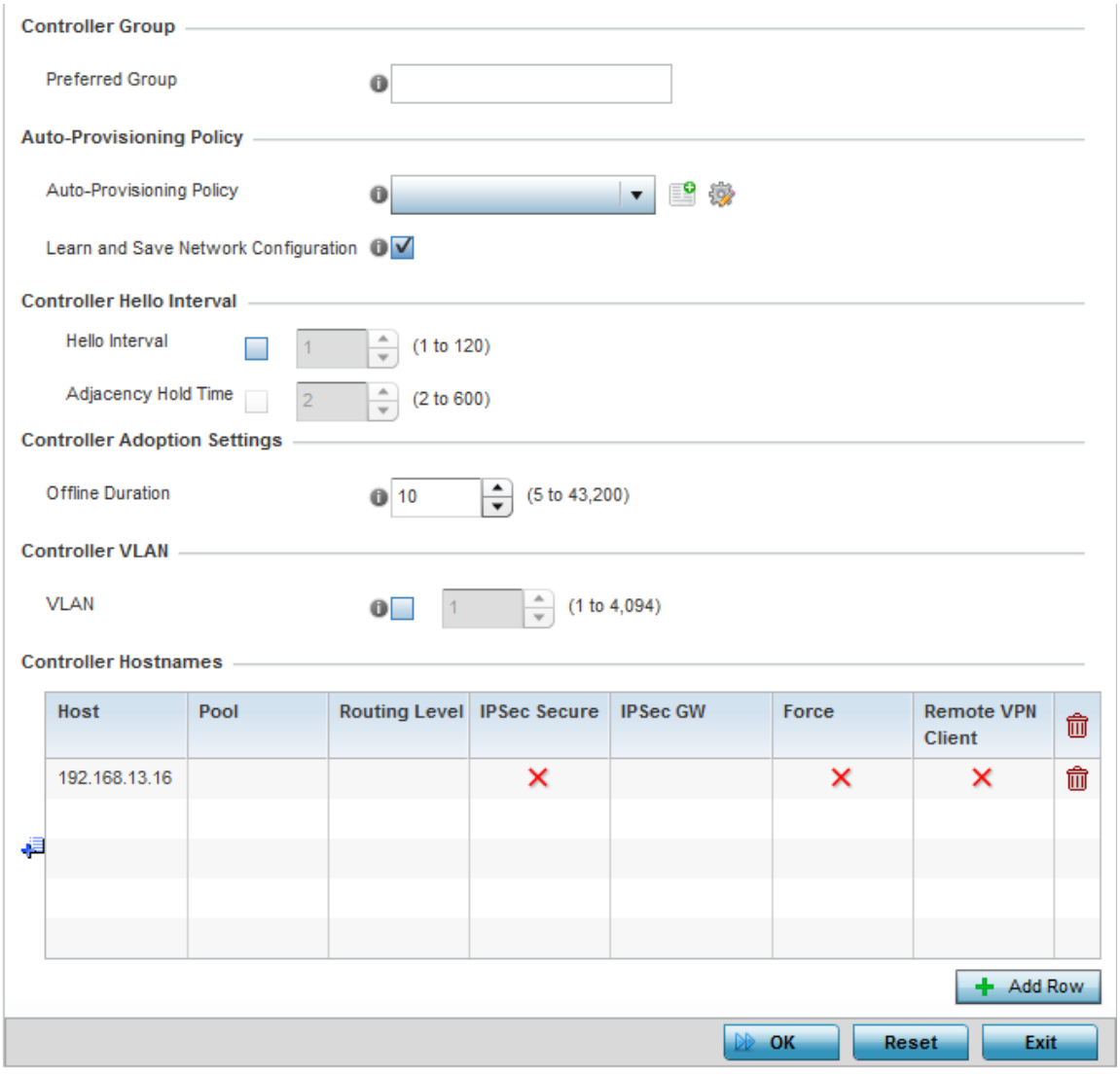


Figure 153: Device Overrides - Adoption screen

7 Define a 64 character maximum **Preferred Group**.

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

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

Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.
Learn and Save Network Configuration	Select this option to learn and save the configuration of any device requesting adoption. This setting is enabled by default.

9 Define the **Hello Interval** value for this device. This is the interval between hello keep alive messages exchanged with the wireless controller that has adopted this access point. These messages serve as a connection validation mechanism to keep the access point adopted to its wireless controller. Set a value from 1-120 seconds.

10 Define the **Adjacency Hold Time** value for this device. This is the amount of time before the preferred controller group is considered down and unavailable to provide services. Set a value from 2-600 seconds.

11 Define the **Offline Duration** for this device. This is the time duration in minutes after which an unadopted device generates an offline event.

12 Use the spinner control to set the **Controller VLAN**.

This is the VLAN the Virtual Controller is reachable on. Select from 1 - 4094. There is no default value for this setting.

13 Use the **+ Add Row** button to populate the **Controller Hostnames** table with the following host, pool and routing parameters for defining the preferred adoption resource.

Host	Use the drop-down menu to specify whether the controller 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 controller to set a pool of either 1 or 2. This is the pool the target Virtual Controller belongs to. The default setting is 1.
Routing Level	Use the spinner controller to set the routing level for the Virtual Controller link. The default setting is 1.
IPSec Support	Select to enable secure communication between the access point and the wireless controllers.
IPSec GW	Use the drop-down menu to specify if the IPSec Gateway 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.
Force	Select to enable the link to the adopting controller or the controller group to be created even when not required.
Remote VPN Client	Select to indicate whether a secure controller link must be established using a remote VPN client.

14 Select **OK** to save the changes and overrides made to the access point adoption configuration. Select **Reset** to revert to the last saved configuration.

Profile Interface Override Configuration

"Device Overrides"

An access point requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each connected VLAN ID.

An interface configuration can have overrides applied to customize the configuration to a unique deployment objective. For more information, refer to the following:

- "Ethernet Port Override Configuration"
- "Virtual Interface Override Configuration"
- "Port Channel Override Configuration"
- "Radio Override Configuration"
- "WAN Backhaul Overrides"
- "PPPoE Configuration"
- "Bluetooth Configuration"

Ethernet Port Override Configuration

"Profile Interface Override Configuration"

Use an Ethernet Port override to change (modify) parameters of an access point's Ethernet Port configuration.

The following ports are available on supported access point models:

- AP6521 - GE1/POE (LAN)
- AP6522/AP6522*M* - GE1/POE (LAN)
- AP6532 - GE1/POE (LAN)
- AP6562 - GE1/POE (LAN)
- AP7161 - GE1/POE (LAN), GE2 (WAN)
- AP7181 - GE1/POE (LAN), GE2 (WAN)
- AP7502 – GE1, fe1, fe2, fe3
- AP7522 – GE1/POE (LAN), GE2 (WAN)
- AP7532 – GE1/POE (LAN), GE2 (WAN)
- AP8122/AP8132/AP8232/AP8163 - GE1/POE (LAN), GE2 (WAN)
- AP8232 – GE1/POE (LAN), GE2 (WAN)

To define an Ethernet port configuration override:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**.

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Interface** to expand its sub menu options.

6 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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

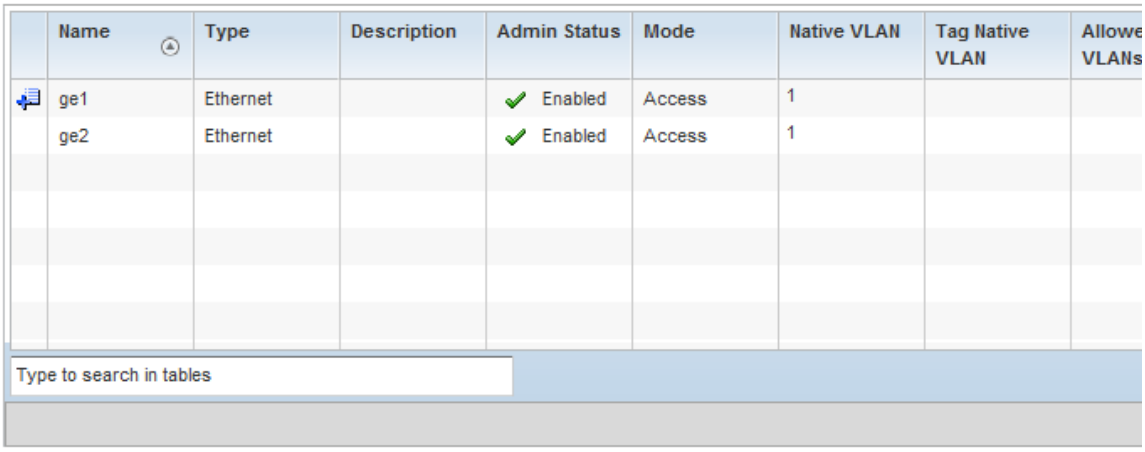


Figure 154: Device Overrides - Interface Ethernet Port screen

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

Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on the supported models.
Type	Displays the physical port type. Copper 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 access point port.
Admin Status	A green check mark 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 required.

Mode	Displays the profile's current switching mode as 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 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 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 the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to *Trunk*.
Overrides	Click the *Clear* to clear overrides made to this interface. This field is blank if there are no overrides for this configuration.

8 To edit (or override) 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.

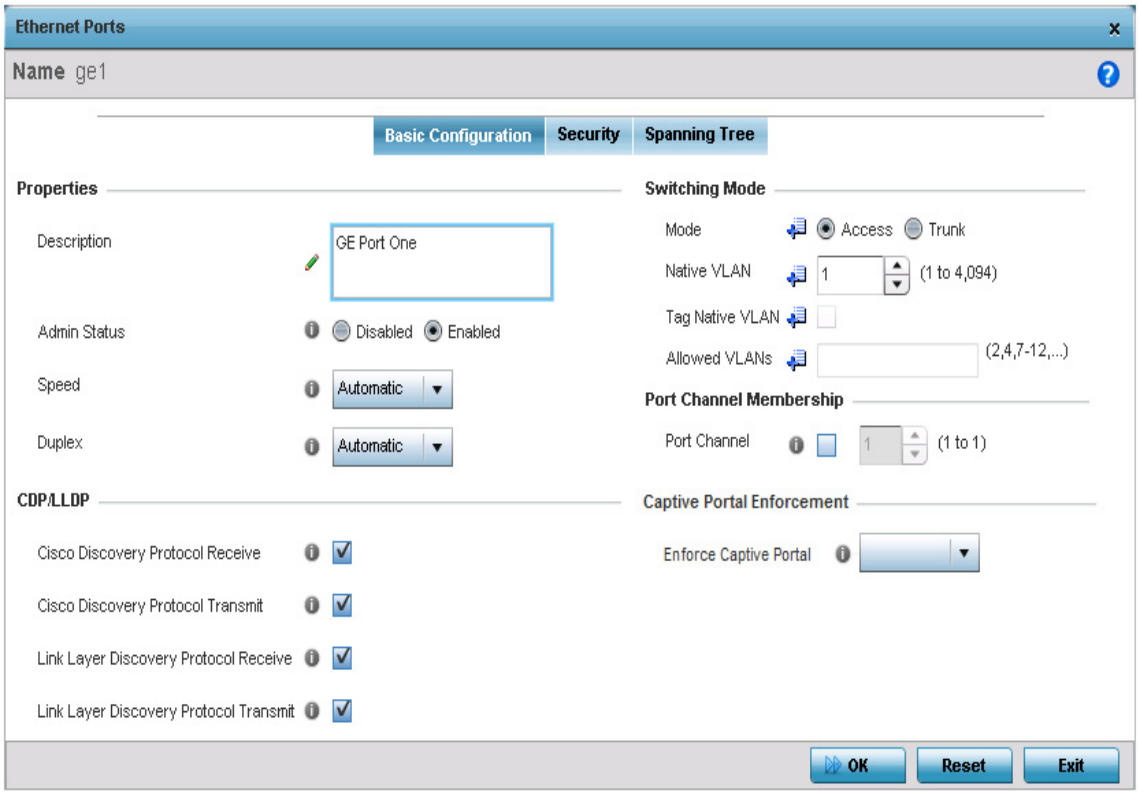


Figure 155: Ethernet Ports - Basic Configuration screen

9 Set (or override) the following Ethernet port **Properties** and **CDP/LLDP** settings:

Description	Provide a brief description for the access point's port (64 characters maximum).
Admin Status	Select the *Enabled* radio button to define this port as active to the 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	Set the speed at which the port 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 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 port at the same time. Using full duplex, the port can send data while receiving data as well. Select Automatic to enable to the access point to dynamically duplex as port performance needs dictate. Automatic is the default setting.
Cisco Discover 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 Discover 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.

10 Set (or override) 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 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 which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.
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.
Allowed VLANs	Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the listed port.

11 Select **Enforce Captive Portal** to automatically apply captive portal access permission rules to data transmitted over this specific Ethernet port. Select *None* to prevent access permission rules to be enforced. Select *Authentication Failure* to apply access permission rules only when user authentication fails. Select *Always* to enforce access permissions at all times.

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. For information on configuring a captive portal policy, see "Configuring Captive Portal Policies" on page 759.

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.

12 Optionally select the **Port Channel Membership** option and define (or override) a setting from 1 - 8 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.

14 Select the **Security** tab.

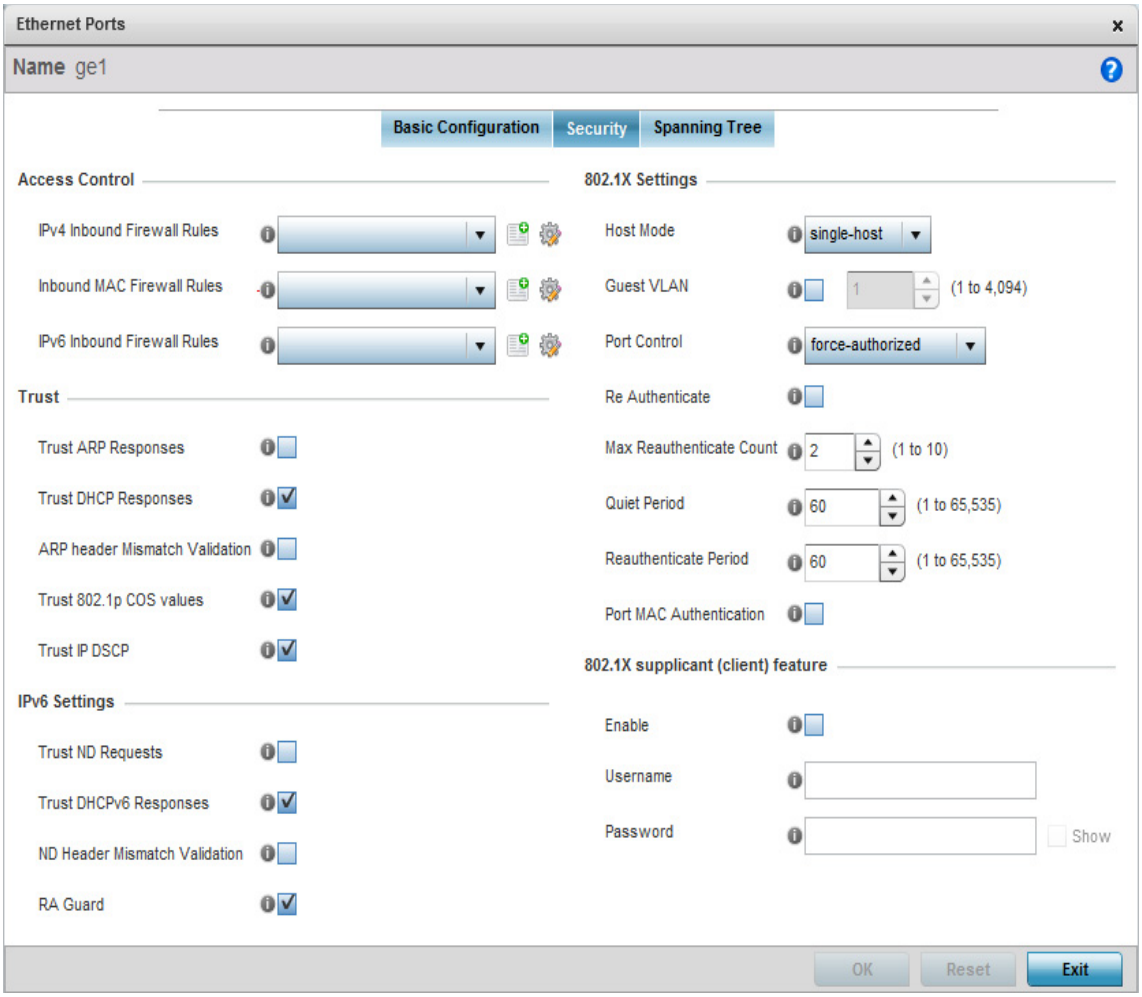


Figure 156: Ethernet Ports - Security screen

15 Refer to the **Access Control** field. As part of the port's security configuration, Inbound IP and MAC address firewall rules are required. The configuration can be optionally overridden if needed.

Use the **Inbound MAC 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.

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. For more information on creating IPv4 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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* (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.

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 on creating IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

16 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 709.

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



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.

Trust ARP Responses	Select this option 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 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. 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 enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this port. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this port. The default value is enabled.

18 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 setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the 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 setting 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 setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This setting is disabled by default.

19 Refer to the **802.1X Settings** field to define the following:

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.
Guest VLAN	Set the Guest VLAN on which traffic is bridged from a wired port when the selected port is considered unauthorized.
Port Control	Set how 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.
Re Authenticate	Select to *enable* or *disable* reauthentication. Reauthentication is primarily used to refresh the current state of the selected port. When enabled the device is forced to reauthenticate. When this happens, the port is still considered authenticated. If reauthentication fails, the port is considered unauthorized and devices using the port are denied access.
Max Reauthenticate Count	Set the number of reauthentication attempts when a port tries to reauthenticate and fails. Once this count exceeds, the port is considered unauthorized.
Quiet Period	Set the duration in seconds where no attempt is made to reauthenticate a controlled port. Set a value from 0 - 65535 seconds.
Reauthenticate Period	Set the duration after which a controlled port is forced to reauthenticate. Set a value from 0 - 65535 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 RFS4000, RFS6000 model controllers and NX4500, NX6500 and NX9000 series service platforms. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

20 Select the **Enable** option within the **802.1x supplicant (client) feature** field to enable a username and password pair used when authenticating users on this port. Select **Show** to expose the characters comprising the password in the **Password** field.

21 Select the **Spanning Tree** tab.

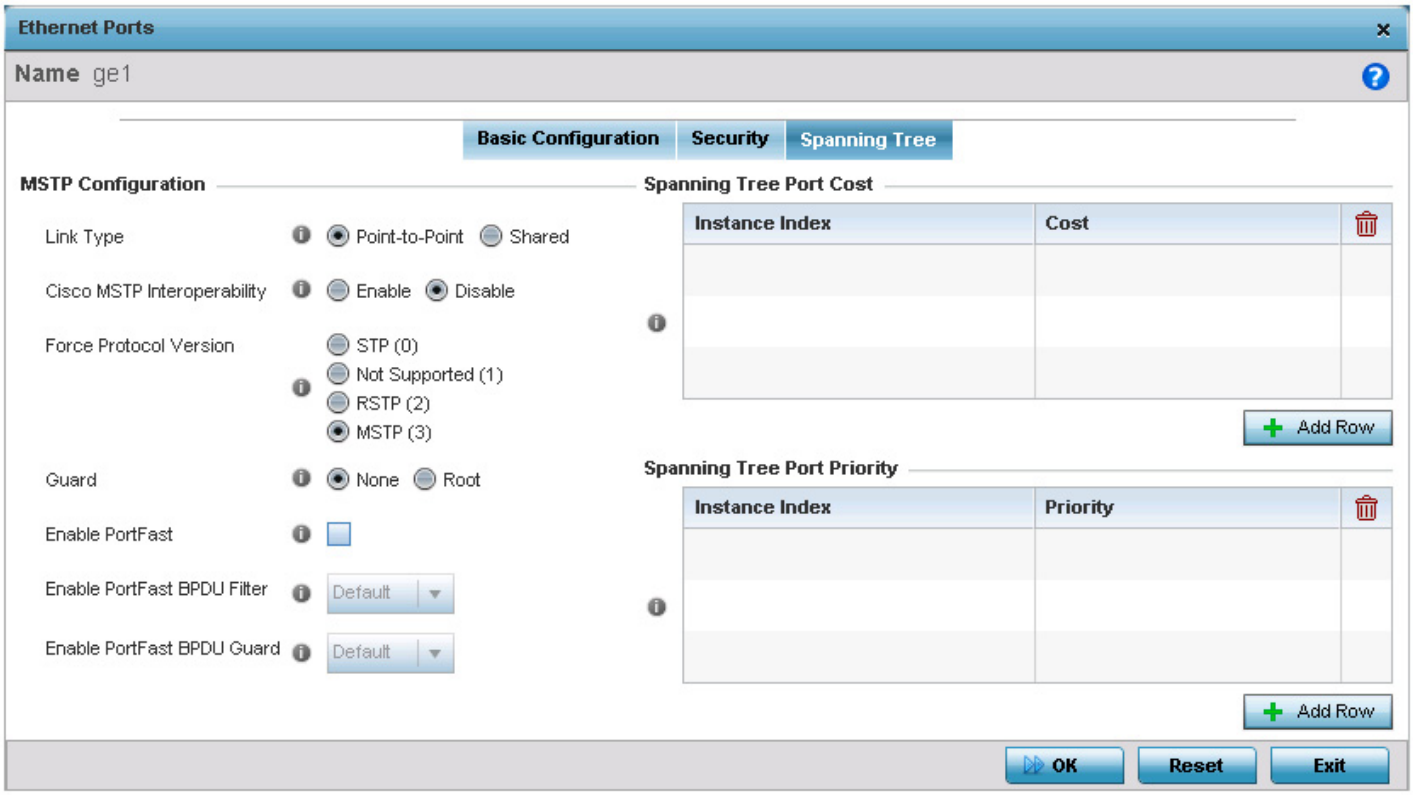


Figure 157: Ethernet Ports – Spanning Tree Configuration

Spanning Tree Protocol (STP) (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.

STP calculation happens when a port comes up. As the port comes up and STP calculation happen, 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. Once the STP calculation is complete, the port's state is changed to Forwarding and traffic is allowed.

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w standard) is a evolution over the standard STP where the primary aim was 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.

Multiple Spanning Tree Protocol (MSTP) 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 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 MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. 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.

22 Select either the **Point-to-Point** or **Shared** radio button for the **Link Type** field. When Point-to-Point is selected, it indicates that the port should be treated as connected to a point-to-point link. Selecting Shared indicates that the port is shared between multiple devices. An example for Shared connection would be when the port is connected to a hub. Similarly, an example for a Point-to-Point connection would be when the port is connected to an access point.

23 Select either the **Enable** or **Disable** radio button for the **CISCO MSTP Interoperability** field. This enables or disables inter operability with CISCO's implementation of the *Multiple Spanning Tree Protocol* (MSTP) which is incompatible with the standard MSTP implementation.

24 Select one of the available choices for **Force Protocol Version** field. 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.

25 Select either the **None** or **Root** radio button for the **Guard field**. Root guard is a mechanism to prevent election of roots other than those designated as roots in a network. When this port receives a better (superior) BPDU, the port state becomes Blocked. It retains this state till the port no longer receives the better (superior) BPDU and then the state is changed to Forwarding. Select *Root* to enable this feature. Select *None* to disable.

26 Select the **Enable Port Fast** option to enable or disable PortFast. PortFast enables reducing the time taken for a port to complete the MSTP state changes from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller which are directly connected to a Server/Workstation and not to another hub or controller. PortFast can be left unconfigured on an access point.

27 Set the **Enable PortFast BPDU Filter** value from the drop-down list. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports do not transmit BPDU messages. When set to *Default* sets the PortFast BPDU Filter value to the bridge's BPDU filter value. Select *Disable* to disable this feature.

28 Set the **Enable PortFast BPDU Guard** value from the drop-down list. MSTP BPDUs are messages that are exchanged when controllers gather information about the network topology. When enabled, PortFast enabled ports are forced to shut down when they receive BPDU messages. When set to *Default* sets the PortFast BPDU Guard value to the bridge's BPDU guard value. Select *Disable* to disable this feature.

29 Configure the **Spanning Tree Port Cost** value. Select the **+ Add Row** button to add a row to the table. Configure an **Instance Index** value and its corresponding cost in the **Cost** column. This is the cost for a packet to traverse the current network segment. The cost of a path is the sum of all costs of traversal from the source to the destination. The default rule for the cost of a network segment is, the faster the media, the lower the cost.

30 Configure the **Spanning Tree Port Priority** value. Select the **+ Add Row** to add a row to the table. Configure an **Instance Index** value and its corresponding priority in the **Priority** column. This is the priority for this port becoming a designated root. The default rule is, the lower this value, the higher the chance that the port is assigned as a designated root.

31 Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration if you do not wish to commit the overrides.

Virtual Interface Override Configuration

"Profile Interface Override Configuration"

A *Virtual Interface* is required for layer 3 (IP) access or provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each 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 existing Virtual Interface configurations and either create a new Virtual Interface configuration, modify (override) an existing configuration or delete an existing configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

5 Select **Interface** to expand its sub menu options.

6 Select **Virtual Interfaces**.

NOTE

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove a device's override, go to the *Basic Configuration* screen's **Device Overrides** field and select **Clear Overrides**.

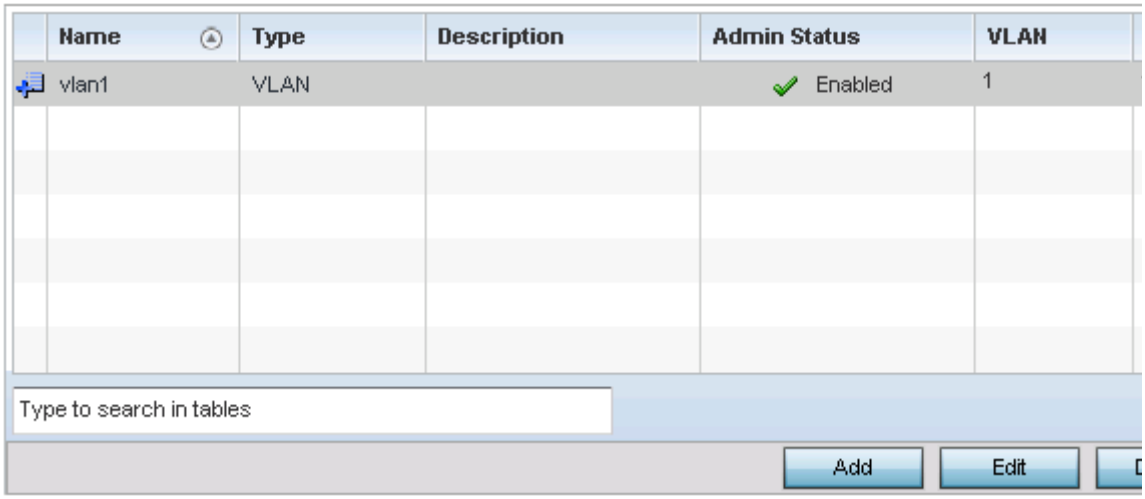


Figure 158: Device Overrides - Virtual Interfaces screen

7 Review the following parameters unique to each Virtual Interface configuration to determine whether a parameter override is warranted:

Name	Displays the name of each listed Virtual Interface assigned when it was created. The name is from 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 check mark 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.

Once the configurations of existing Virtual Interfaces have been reviewed, determine whether a new interface requires creation, or an existing Virtual Interface requires edit (override) or deletion.

8 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.

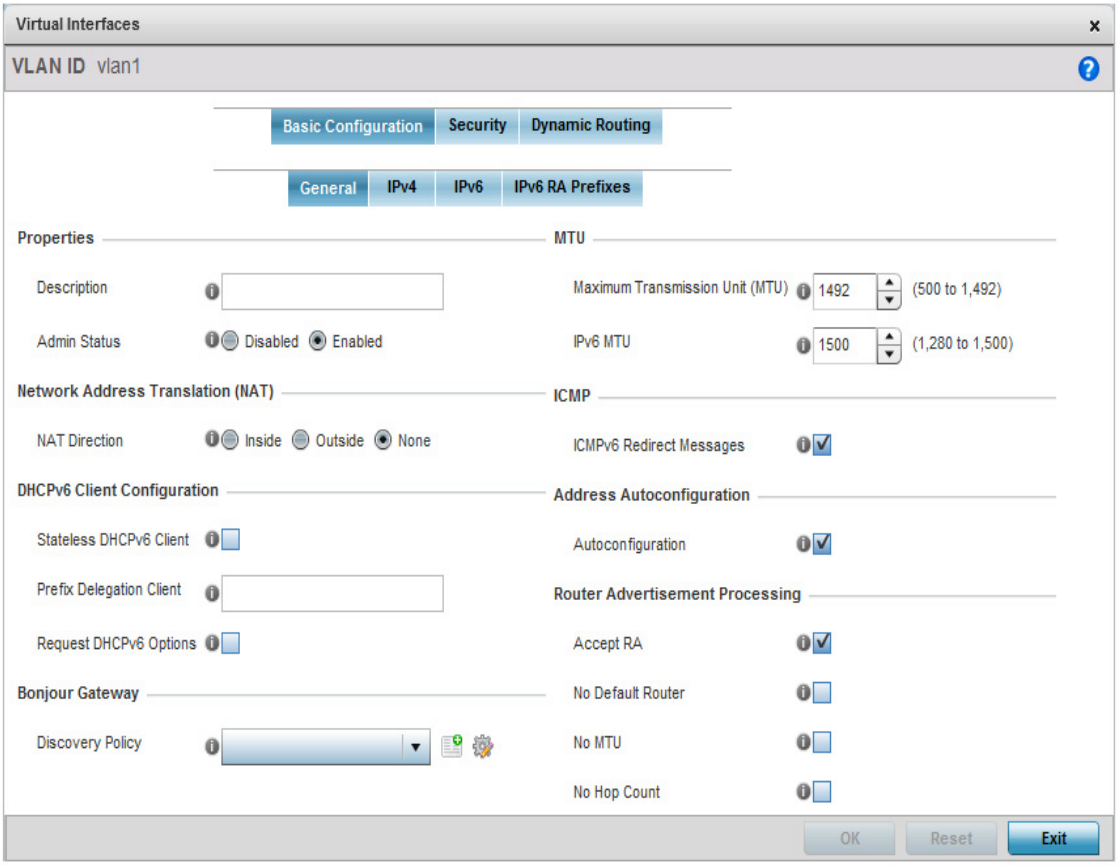


Figure 159: Device Overrides - Virtual Interfaces - Basic Configuration screen

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.

9 If creating a new Virtual Interface, use the spinner control to define a numeric ID from 1 - 4094.

10 Define or override 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.

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

Select either the *Inside*, *Outside* or *None* radio buttons.

- *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 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 239 for instructions on creating a profile's NAT configuration.

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

13 Set the following **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 drop-down, select the Bonjour Gateway discover policy. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

14 Set the following MTU settings for the virtual interface:

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.
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.

15 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.

16 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.

17 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 Router Advertisement	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.

18 Select **OK** button to save the changes and overrides to the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.

19 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

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

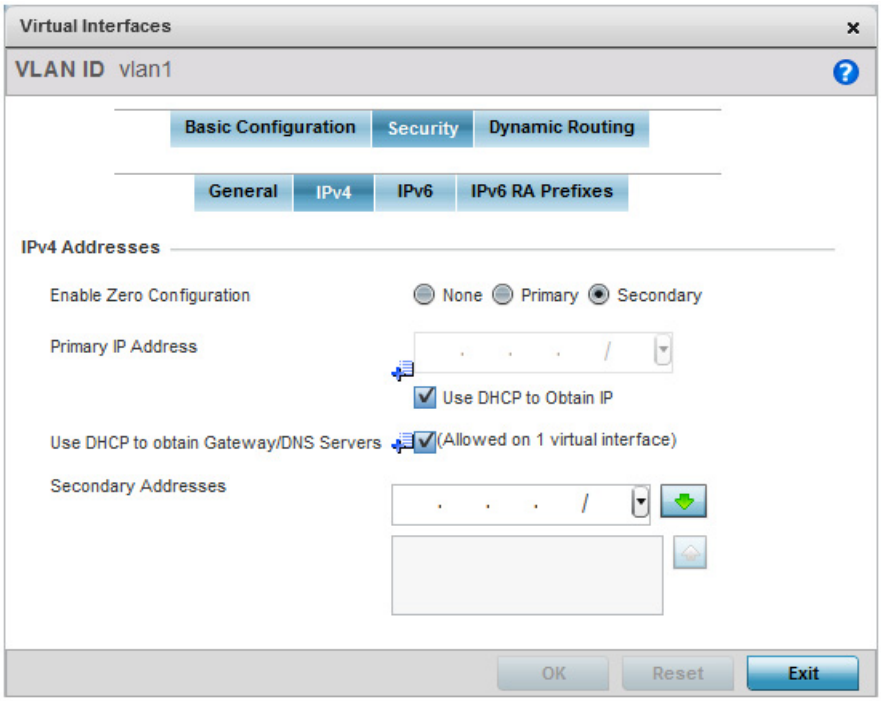


Figure 160: Device Overrides - Virtual Interfaces - Basic Configuration screen - IPv4 tab

20 Set the following network information from within 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 the *Secondary Addresses* 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.

21 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

22 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

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. 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

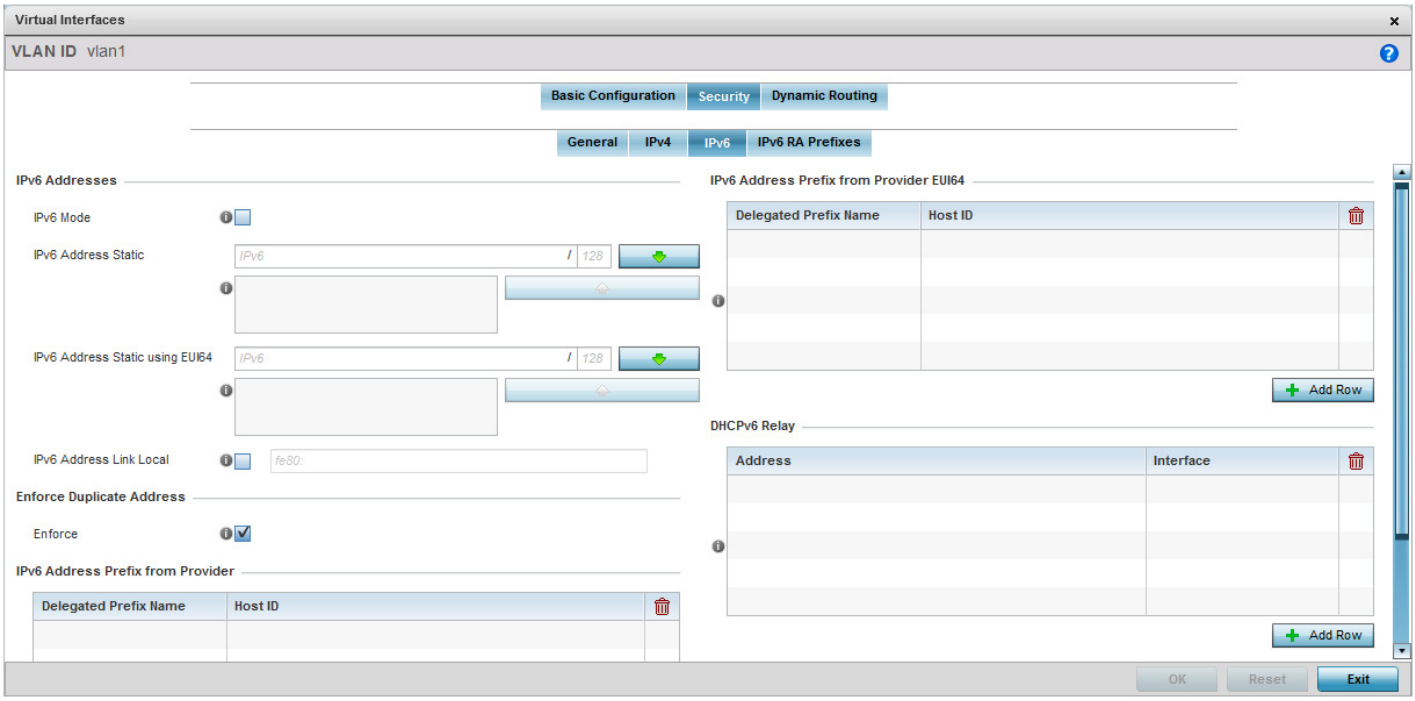


Figure 161: Device Overrides - Virtual Interfaces - Basic Configuration screen - IPv6 tab

23 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.

24 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.

25 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 sub screen wherein a new delegated prefix name and host ID can be defined.

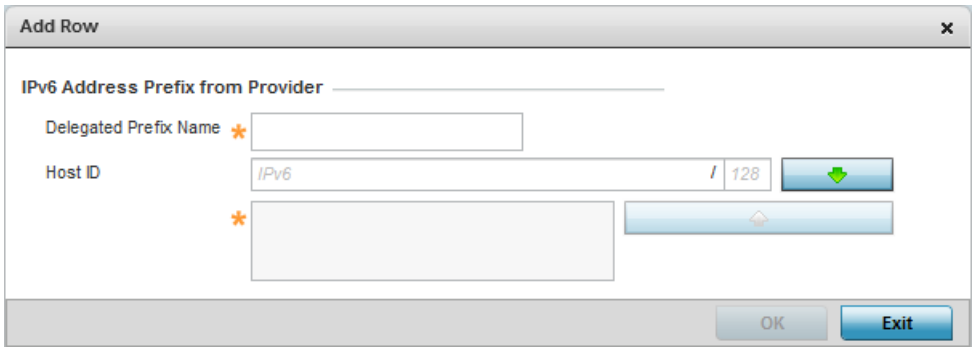


Figure 162: Device Overrides - Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider

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.

Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

26 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 sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

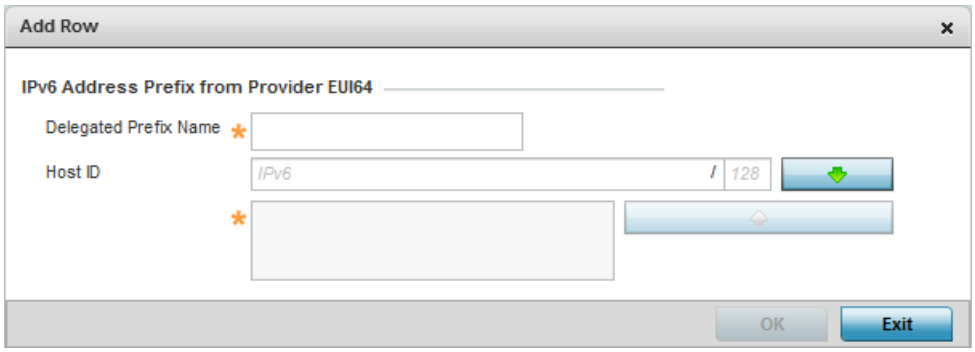


Figure 163: Device Overrides - Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64

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.

27 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

28 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 sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

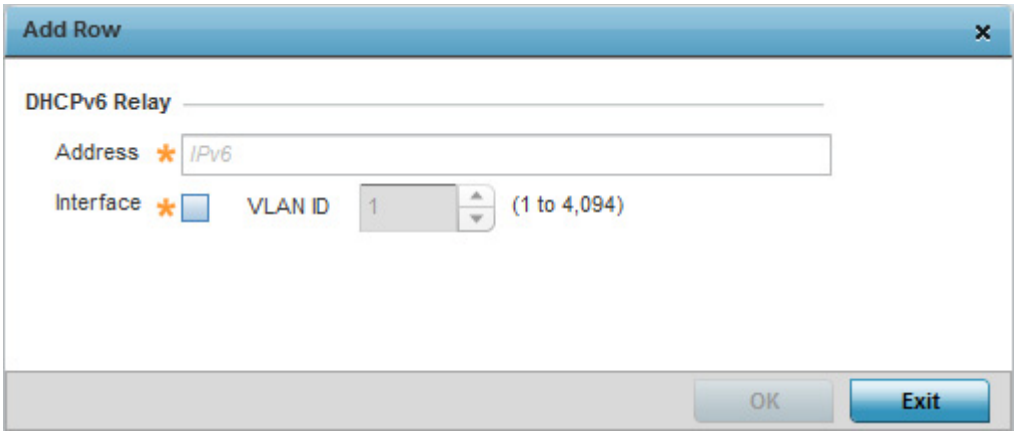


Figure 164: Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add DHCPv6 Relay

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.

Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

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

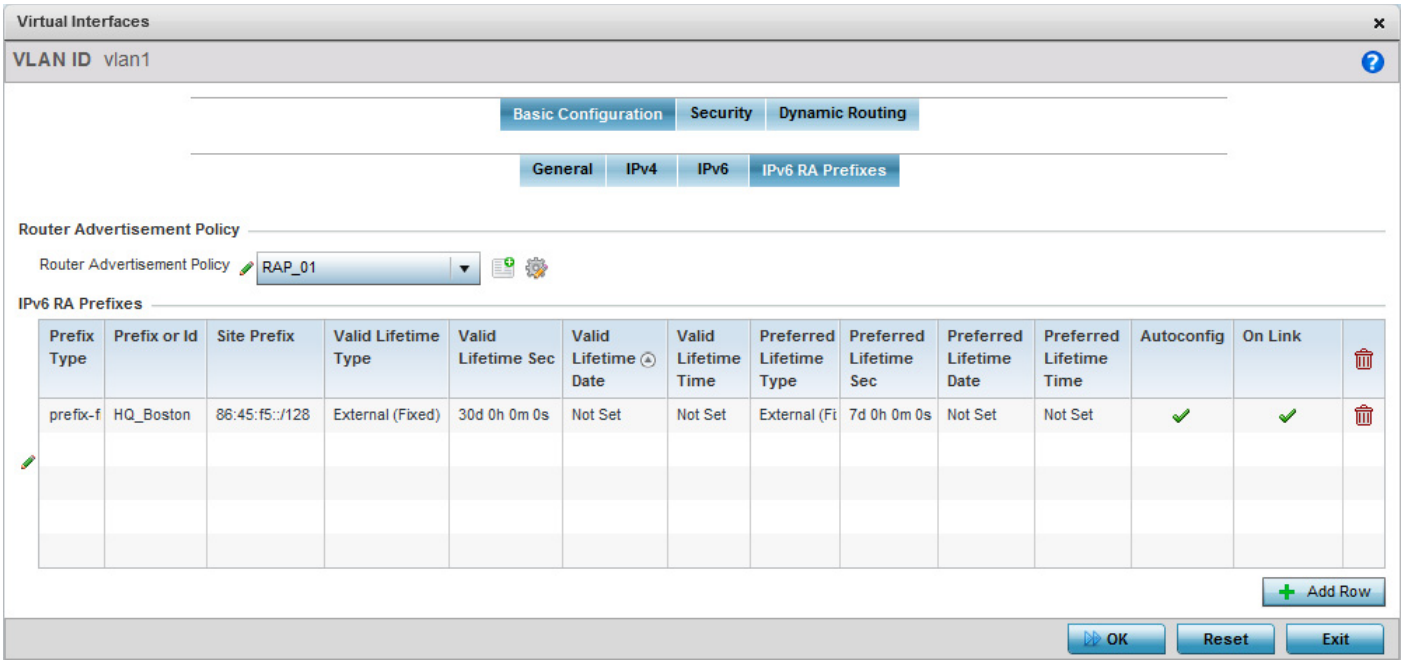


Figure 165: Device Overrides - Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab

30 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.

31 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

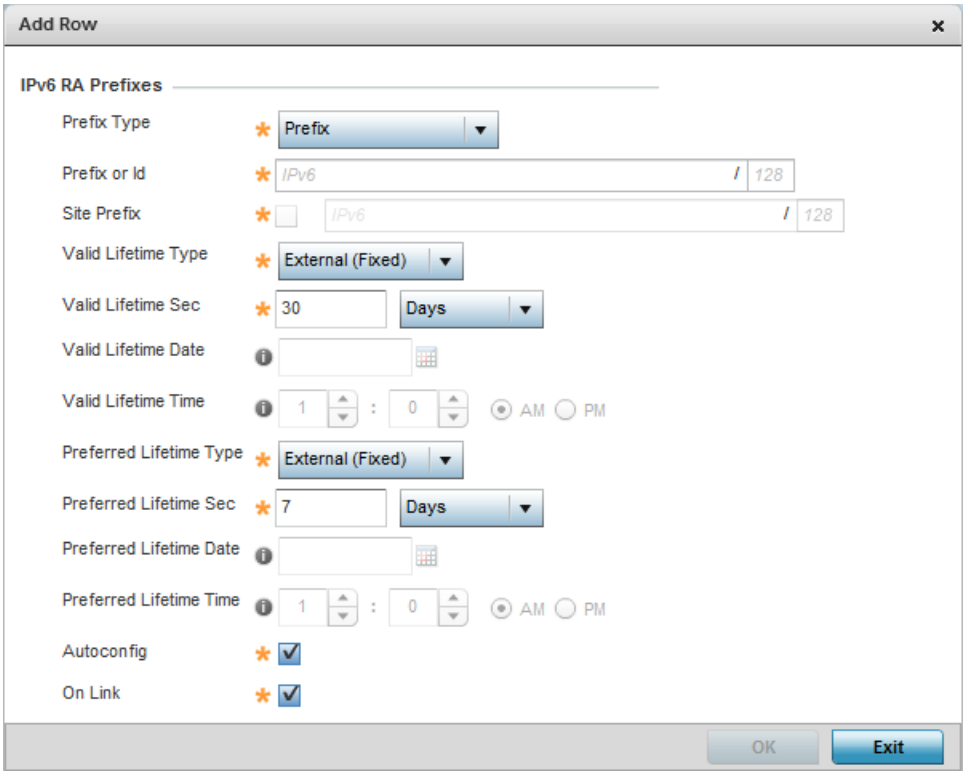


Figure 166: Device Overrides - Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix

32 Set 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 *Internet Service Provider* (ISP) 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 measurement 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.

33 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

34 Select the **OK** button to save the changes and overrides to the basic configuration. Select **Reset** to revert to the last saved configuration.

35 Select the **Security** tab.

The firewall inspects and packet traffic to and from connected clients.

If a firewall rule does not exist suiting 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 709.

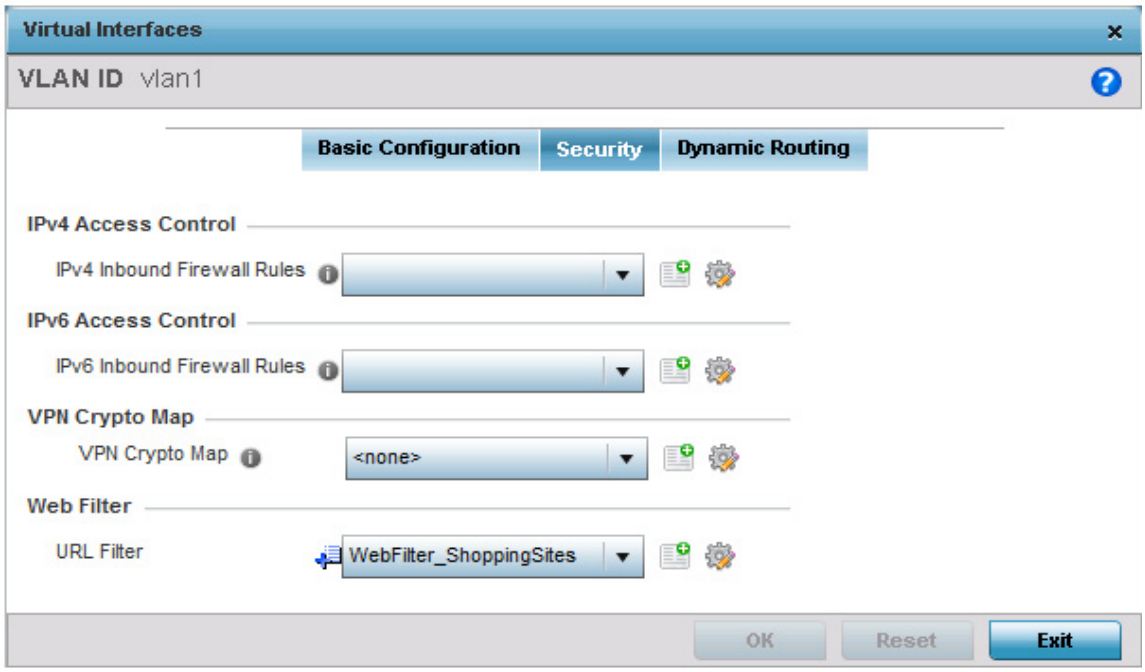


Figure 167: Device Overrides - Virtual Interfaces Security screen

36 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). For more information on creating IPv4 firewall rules, see "Configuring IP Firewall Rules" on page 724.

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.

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* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. For more information on creating IPv6 firewall rules, see "Configuring IP Firewall Rules" on page 724.

37 Use the **VPN Crypto Map** drop-down menu to define the cryptography map to use with this virtual interface. The VPN Crypto Map entry defines the type of VPN connection and

its parameters. For more information see “Defining Profile VPN Settings” on page 218.

38 Use the **Web Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

Web filtering is used to restrict access to resources on the Internet.

39 Select the **Dynamic Routing** tab.

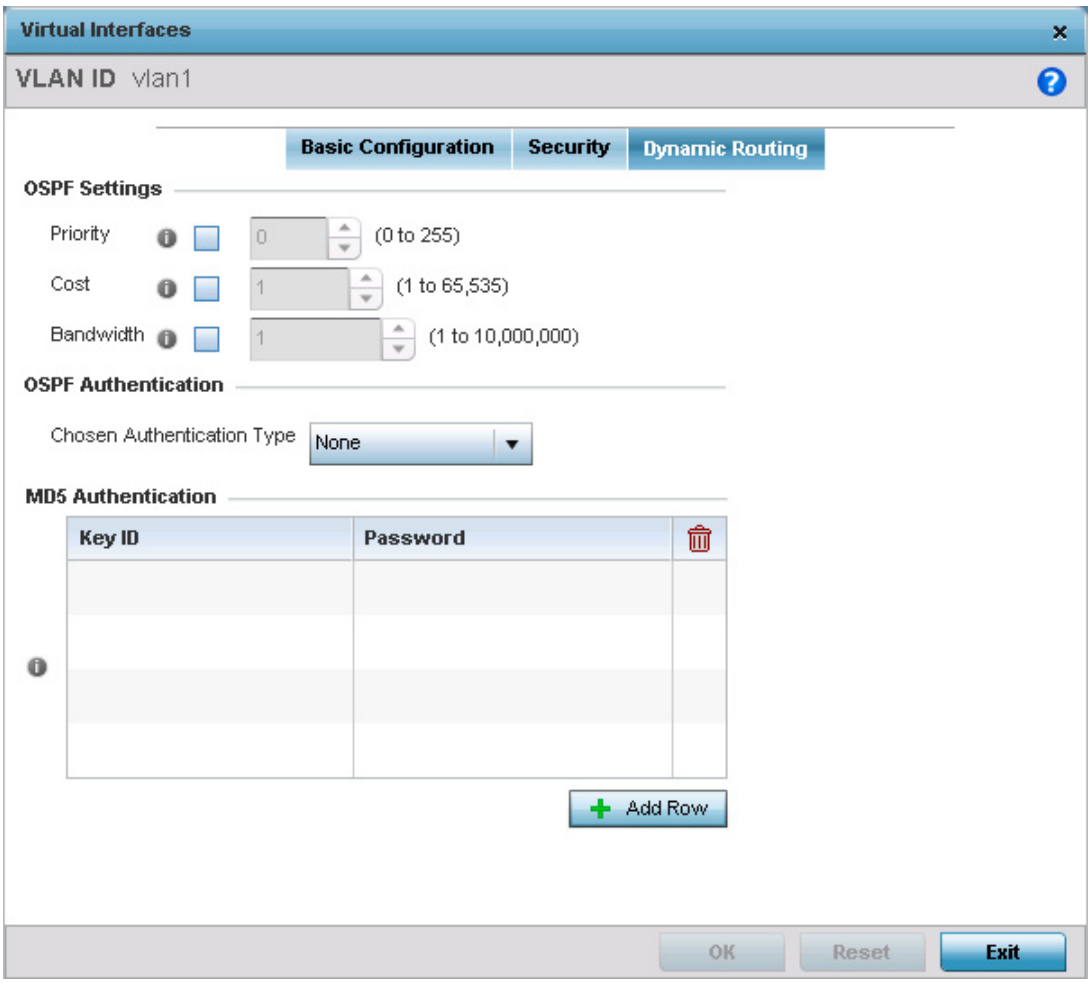


Figure 168: Device Overrides – Virtual Interfaces Dynamic Routing screen

40 Refer to the following to configure **OSPF Settings.**

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

41 Configure the **OSPF Authentication Type** settings by selecting from the drop-down list. The available options are *None*, *null*, *simple-password* and *message-digest*.

42 Refer the following to configure **MD5 Authentication** keys. Select the **+ Add Row** button to add a row to the table.

Key ID	Set the unique MD5 Authentication key ID. The available key ID range is 1 - 255.
Password	Set the OSPF password. This value is displayed as “asterisk” (*). Select *Show* to expose the characters comprising the password.

43 Select the **OK** button located at the bottom right of the screen to save the changes and overrides to the Security screen. Select **Reset** to revert to the last saved configuration.

Port Channel Override Configuration

“Profile Interface Override Configuration”

Access points can have their port channel configurations overridden if a portion of the configuration is no longer relevant to the access point’s deployment objective.

To override a port channel configuration for an access point profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the **Configuration** tab.

3 Select **Device Overrides**

4 Select a target device from the device browser in the lower, left-hand, side of the UI.

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

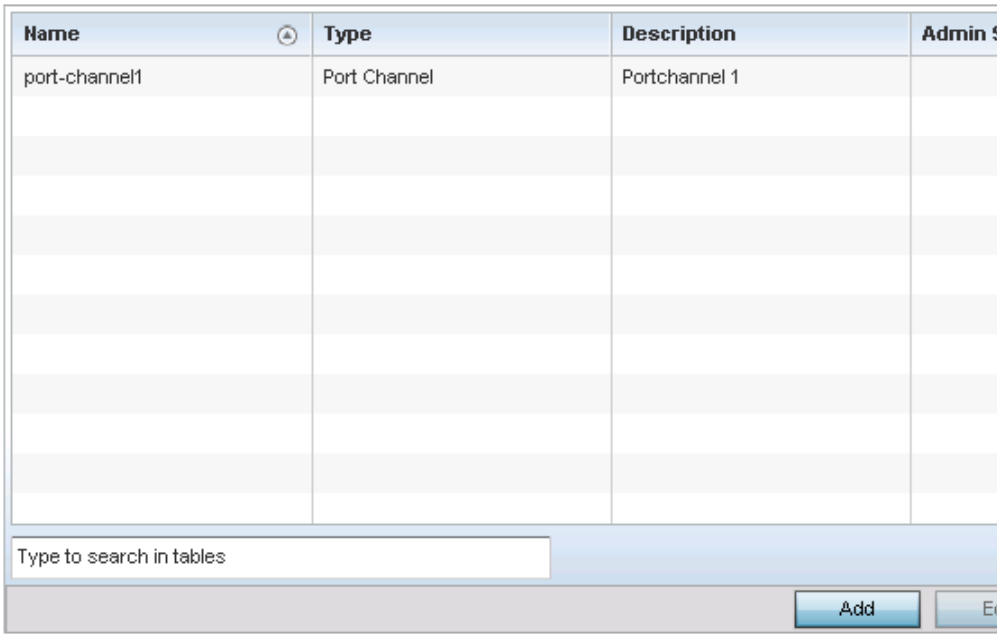


Figure 169: Device Overrides - Port Channels screen

6 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 a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed port channel as active and currently enabled with the access point's 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

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

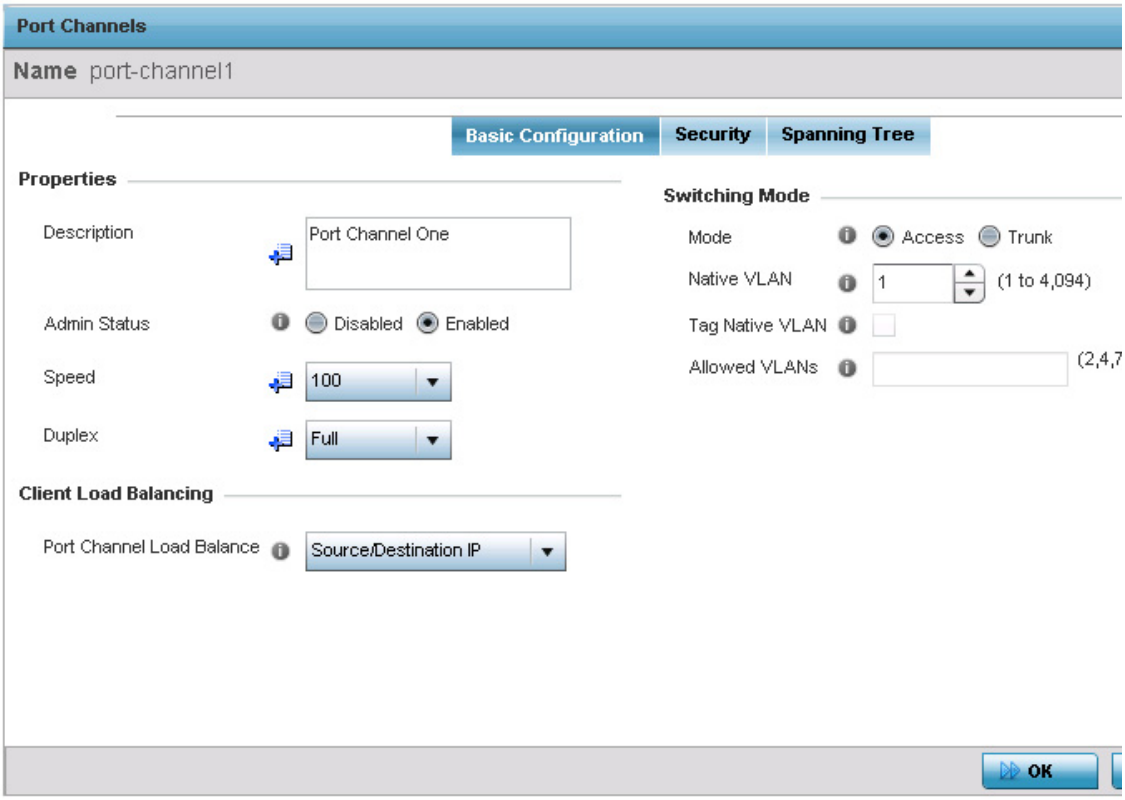


Figure 170: Device Overrides - Port Channels - Basic Configuration tab

8 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 disabled.
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 Auto 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 enable to the access point to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.

9 Use the **Port Channel Load Balance** drop-down menu within the **Client Load Balancing** field to define whether port channel load balancing is conducted using a *Source/Destination IP* or a *Source/Destination MAC* as criteria. Source/Destination IP is the default setting.

10 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 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 which 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. Access points 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.

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

12 Select the **Security** tab.

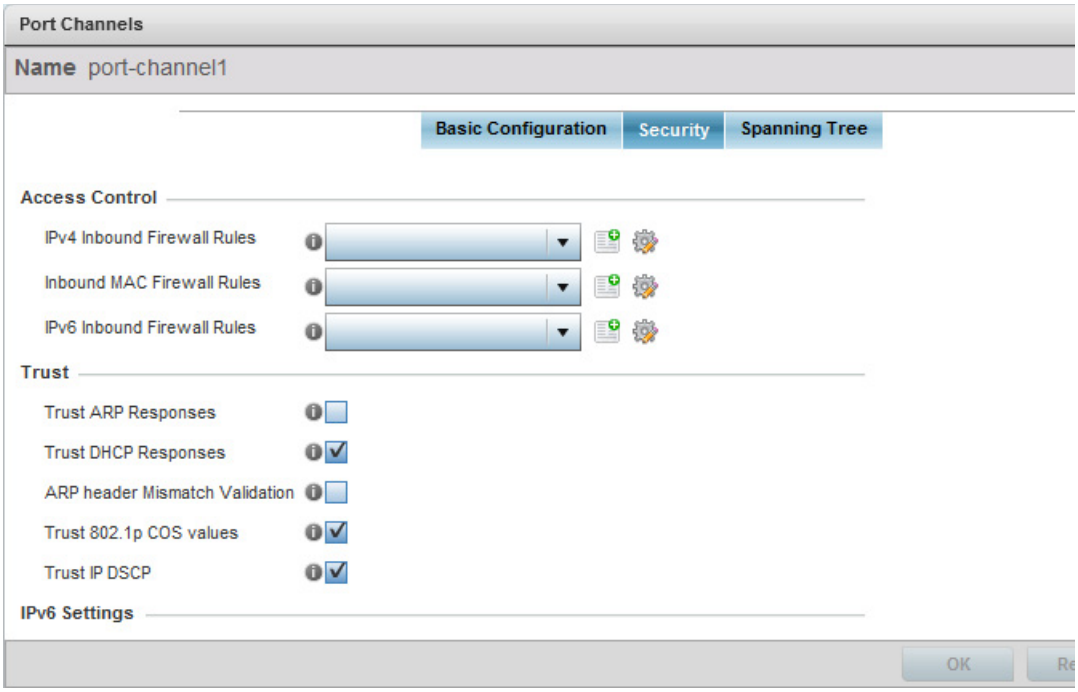


Figure 171: Device Overrides - Port Channels - Security tab

13 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 **IPv4 Inbound Firewall Rules, IPv6 Inbound Firewall Rules** and **Inbound MAC Firewall Rules** drop-down menus to select the 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

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.

Use the **IPv6 Inbound Firewall Rules** drop-down menu to select the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

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.

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

Trust ARP Responses	Select this option 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 managed network. The default value is disabled.
Trust DHCP Responses	Select this option 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 this option 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 this option to enable 802.1p COS values on this port channel. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this port channel. The default value is enabled.

15 Set the following **IPv6 Settings**:

Trust ND Requests	Select this option to enable the trust of neighbor discovery requests required on an IPv6 network. This setting is disabled by default.
Trust DHCPv6 Responses	Select this option 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 this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This setting is disabled by default.

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

17 Select the **Spanning Tree** tab.

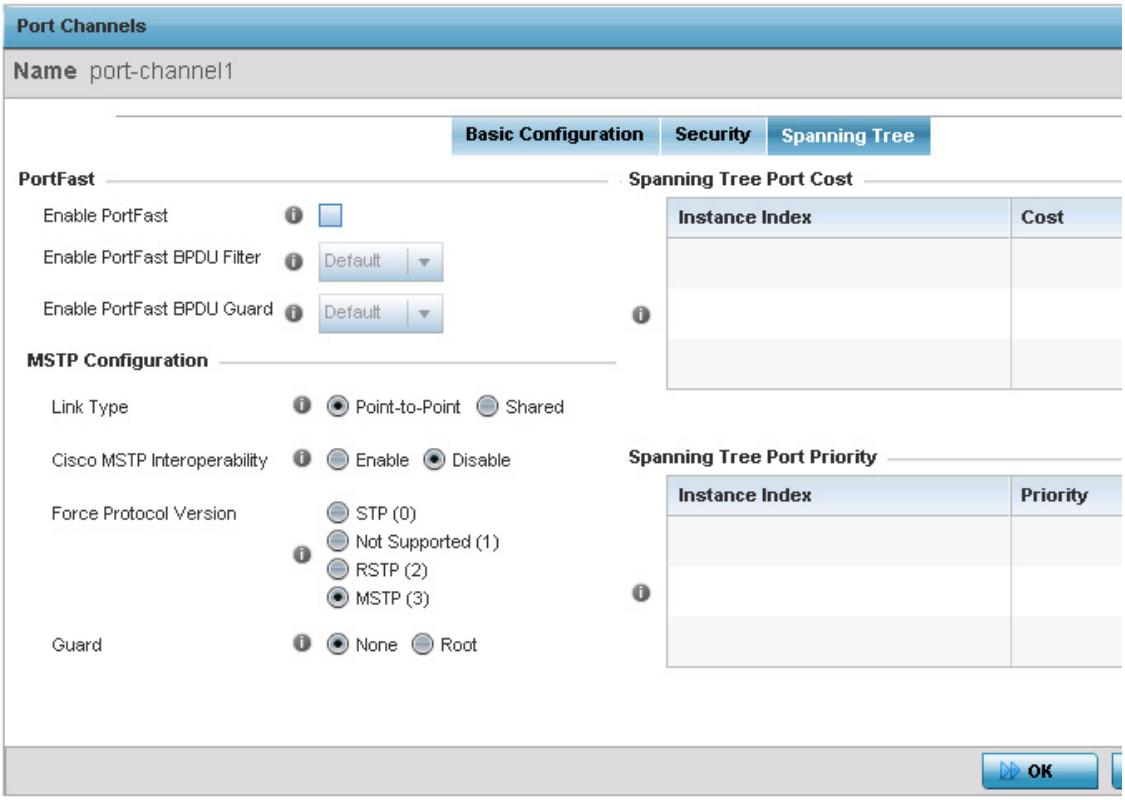


Figure 172: Port Channels - Spanning Tree tab

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

Enable PortFast	PortFast reduces the time required for a port to complete a MSTP state change from Blocked to Forward. PortFast must only be enabled on ports on the wireless controller directly connected to a server/workstation and not another hub or controller. PortFast can be left unconfigured on an access point. Select this option to enable drop-down menus for both the *Enable PortFast BPDU Filter* and *Enable PortFast BPDU Guard* options. This setting is disabled by default.
Enable PortFast BPDU Filter	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 *Default*. Select *Disable* to disable this feature.
Enable 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 *Default*. Select *Disable* to disable this feature.

19 Set the following **MSTP Configuration** parameters for the port channel:

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 means this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a access point 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.

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

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

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

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

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.

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

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

Radio Override Configuration

"Profile Interface Override Configuration"

Access points can have their radio profile configurations overridden if a portion of a profile is no longer relevant to the access point's deployment objective.

To define a radio configuration override for an access point:

1 Select the **Configuration** tab from the Web UI.

2 Select Devices from the Configuration tab.

3 Select **Device Overrides**.

4 Select a target access point from the device browser in the lower, left-hand, side of the UI.

5 Select **Interface** to expand its sub menu options.

1. Select **Radios**.

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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

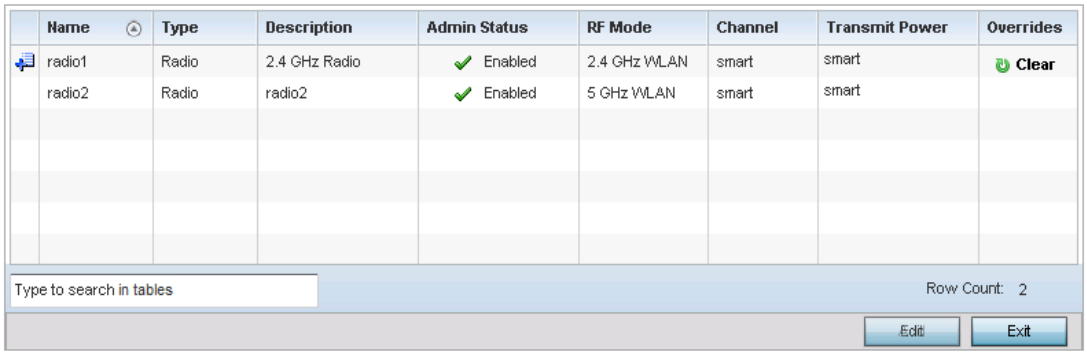


Figure 173: Device Overrides - Access Point Radios screen

6 Review the following radio configuration data to determine whether a radio configuration requires modification or override:

Name	Displays whether the reporting radio is the access point's radio1, radio2 or radio3. AP6522, AP6522M, AP6532, AP6562, AP8132, AP8232, AP7181 and AP7161 models support 2 radios and AP6521 model supports a single radio.
Type	Displays the type as either *Radio* (for typical client support) or *sensor*. If setting an AP6521 model access point to function as a sensor, the access point must be rebooted before it can begin to operate as a sensor.
Description	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
Admin Status	Defines the radio as either enabled or disabled for client or sensor support.
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 will be listed as a client bridge and does not provide typical 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 will select the channel with the lowest average power level.
Transmit Power	Lists the transmit power for each radio. Displays *smart* if Smart-RF is used to set the transmit power for this radio.
Overrides	Click the *Clear* to clear overrides made to this radio interface. This field is blank if there are no overrides for this radio.

7 If required, select a radio configuration and select the **Edit** button to modify or override portions of its configuration.

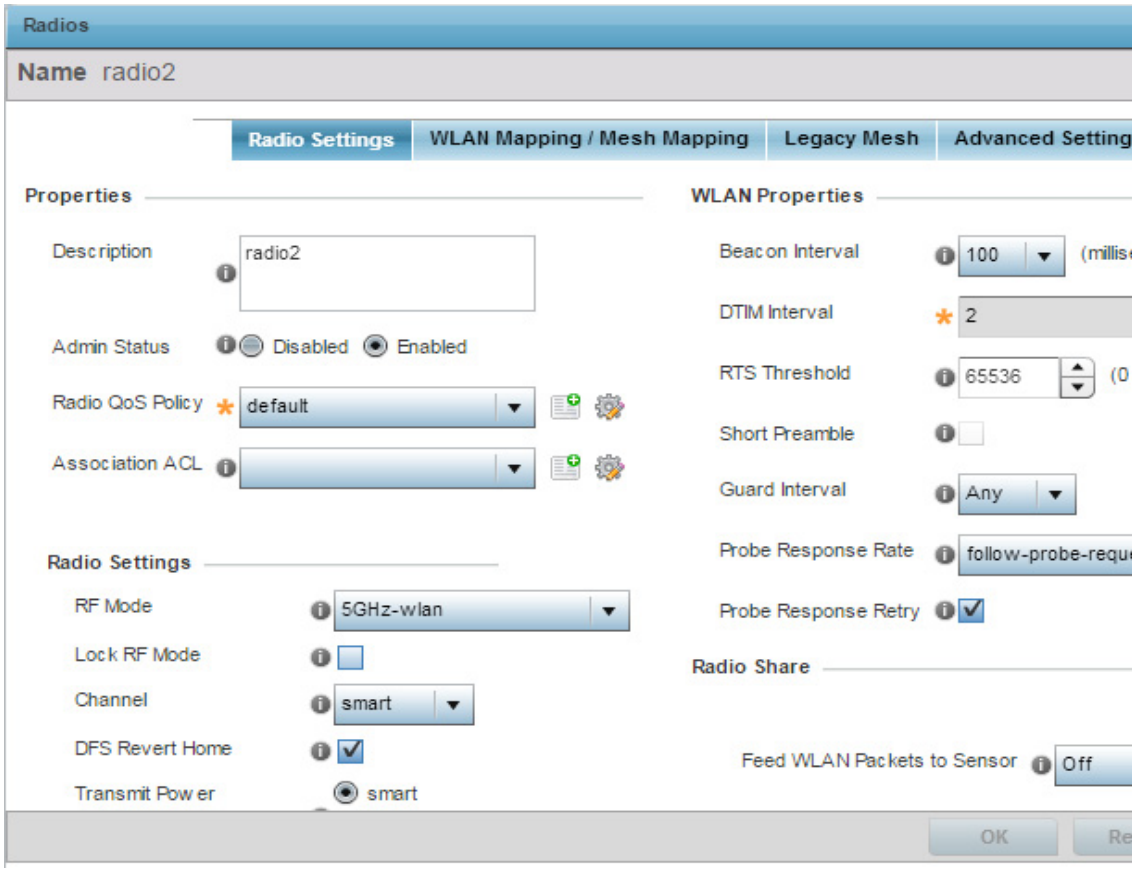


Figure 174: Device Overrides - Access Point Radio Settings tab

The **Radio Settings** tab displays by default.

8 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	Either select the *Active* or *Shutdown* radio button to define this radio's availability. When defined as Active, the access point is operational and available for client support, Shutdown renders it unavailable.
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 is no existing QoS policy suiting the radio's intended operation, select the *Create* icon.
Association ACL	Use the drop-down menu to specify an existing Association ACL policy to apply to the radio. An Association ACL is a policy-based *Access Control List* (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, the fields in the packet are compared to applied ACLs to verify the packet has the required permissions needed to be forwarded. If a packet does not meet any of the ACL criteria, the packet is dropped. Select the Create icon to define a new Association ACL.

9 Set or override the following profile **Radio Settings** for the selected radio:



NOTE

Most access point models can support up to 256 clients per access point or radio except AP6521 model access point which can only support up to 128 clients per access point or radio.

RF Mode	Set the mode to either 2.4 GHz WLAN or 5.0 GHz WLAN support depending on the radio's intended client support. Set the mode to *sensor* if using the radio for rogue device detection. Set the mode to *client-bridge* to configure the radio as a client bridge. A client bridge enables the access point to connect to a 3rd party access point and bridge frames to it.
Lock RF Mode	Select this option to lock Smart RF calibration functions for this radio. The default setting is disabled.
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 to listen for beacons from other access points. Once channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it will select 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, only appear when using an AP8232, and are unique to the 80 MHz band.
DFS Revert Home	Select this option to enable a radio to return back to its original channel. *Dynamic Frequency Selection* (DFS) 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 thirty (30) minutes. When selected, the radio can return back to its original channel of operation once the thirty minute period is over. When not selected, the radio cannot return back to its original channel of operation ever after the mandatory thirty minute evacuation period is over.
Transmit Power	Set the transmit power of the selected access point radio. If using a dual or a three radio model AP7131, each radio should be configured with a unique transmit power in respect to its intended client support function. Select *smart* to use Smart RF to determine output power. *smart* is the default value.
Antenna Gain	Set the antenna from 0.00 - 30.00 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. It is recommended that only a professional installer 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 a 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 deployed and its transmit power settings.
Enable Antenna Diversity	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.
Adaptivity Recovery	Select this option to switch channels when an access point’s radio is in adaptivity mode. In adaptivity mode, an access point monitors interference on its set channel and stops functioning when the radio’s defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.
Adaptivity Timeout	Set the adaptivity timeout from 30 to 3,600 minutes. The default setting is 90 minutes.
Wireless Client Power	Select this option to enable a spinner control for client radio power transmissions in dBm. The available range is 0 - 20 dBm.
Dynamic Chain Selection	Select this option to allow the access point radio to dynamically change the number of transmit chains. This setting is disabled by default. The radio uses a single chain/antenna for frames at non 802.11n data rates.
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. 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 5.0 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. 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). For more information on 802.11n MCS rates, see “MCS Data Rates” on page 137.
Radio Placement	Use the drop-down menu to specify whether the radio is located Indoors or Outdoors. The placement should depend on the selected country of operation and its regulatory domain requirements for radio emissions. The default setting is Indoors.
Max Clients	Use the spinner control to set the maximum permissible client connections for this radio. Set a value from 0 - 256. Most access point models can support up to 256 clients per access point or radio except AP6521 model access point which can only support up to 128 clients per access point or radio.
Rate Selection Methods	Use the drop-down menu to specify the algorithm to use for rate selection. Select *Standard* to use the standard rate selection algorithm. Select *Opportunistic* to use the Opportunistic rate selection algorithm.

10 Set or override 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. Included in a beacon is information such as the WLAN service area, the radio address, the 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 jitter-sensitive.The default value is 100 milliseconds.
DTIM Interval	Set a DTIM Interval to specify a period for *Delivery Traffic Indication Messages* (DTIM). 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 acknowledgement, 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 *Request To Send* (RTS) 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 *Clear To Send* (CTS) 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 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 option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink 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 symbols (characters) being transmitted. The guard interval eliminates *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one symbol interfere with another symbol. Adding time between transmissions allows echo's and reflections to settle before the next symbol is transmitted. A shorter guard interval results in a shorter symbol 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 this option to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

11 Use the **Feed WLAN Packets to Sensor** drop-down menu to allow the radio to send WLAN packet to the sensor radio. Options include *Off*, *Inline* and *Promiscuous*. The default setting is *Off*.

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

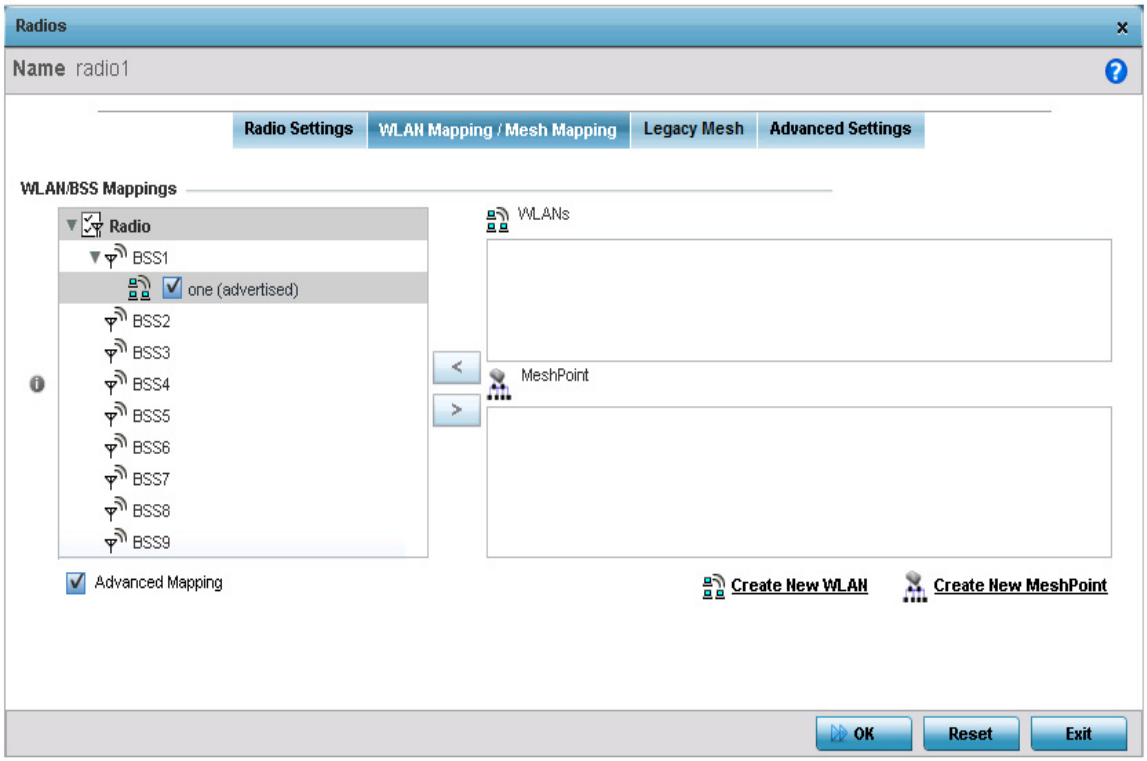


Figure 175: Device Overrides - WLAN Mapping tab

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 AP6521 access point, there are 8 BSSIDs available. If using a dual-radio AP6532, AP6522, AP6522M, AP6562, AP8132, AP7181, AP8232 or AP7161 model access point, there are 16 BSSIDs for the 802.11b/g/n radio and 16 BSSIDs for the 802.11a/n radio.

13 Select **OK** to save the changes and overrides to the WLAN Mapping. Select Reset to revert to the last saved configuration.

14 Select the **Legacy Mesh** tab.

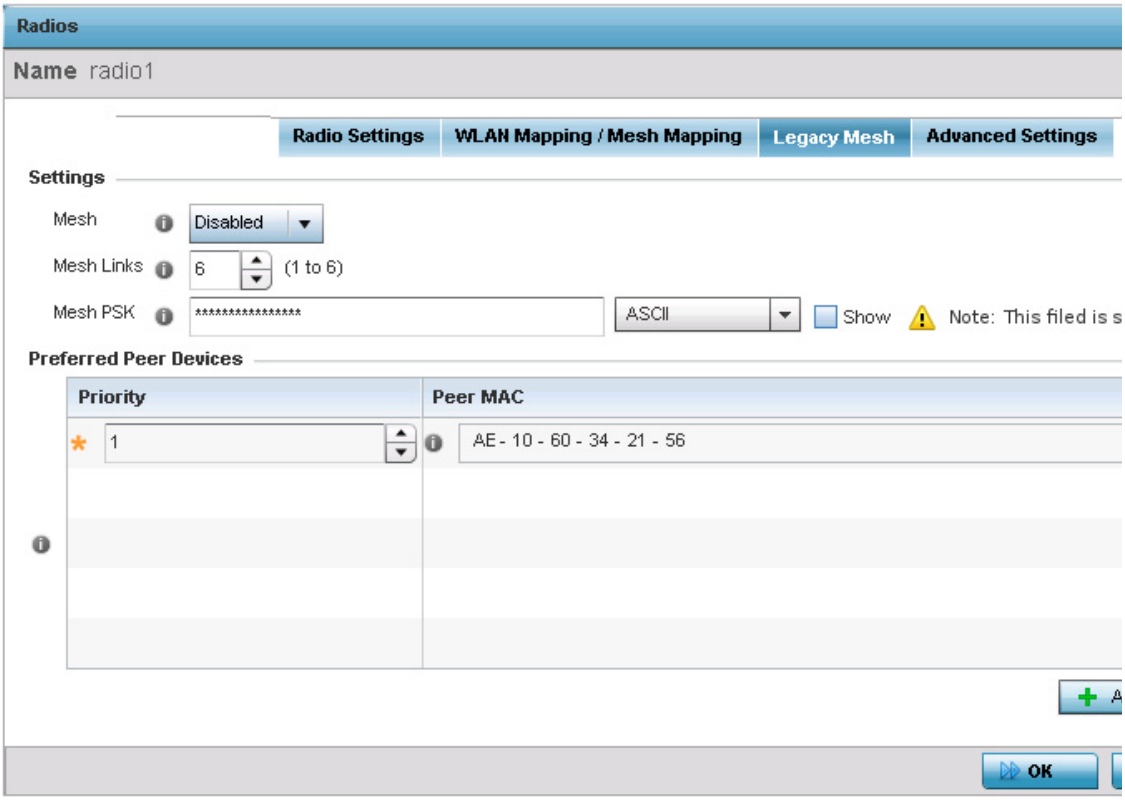


Figure 176: Device Overrides - Access Point Radio - Mesh tab

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

16 Define the following **Mesh Legacy** settings:

Mesh	Options include *Client*, *Portal* and *Disabled*. Select Client to scan for mesh portals, or nodes that have connection to portals, and connect through them. Portal operation begins beaconing immediately and accepts connections from other mesh supported nodes. In general, the portal is connected to the wired network. The default value is Disabled.
Mesh Links	Use the spinner control to define the number of mesh links (1 -6) an access point radio will attempt to create. The default settings is 3 links.
Mesh PSK	Use the field to define the shared key for mesh. From the drop-down, select the type of the key. Click *Show* to display the actual characters comprising the key.

17 Refer to the **Preferred Peer Devices** table and select **+ Add Row** to define MAC addresses representing peer devices for preferred mesh connection. Use the Priority spinner control to set a priority (1 -6) for connection preference.

18 Select the **OK** button located at the bottom right of the screen to save the changes to the Mesh configuration. Select **Reset** to revert to the last saved configuration.

19 Select the **Advanced Settings** tab.

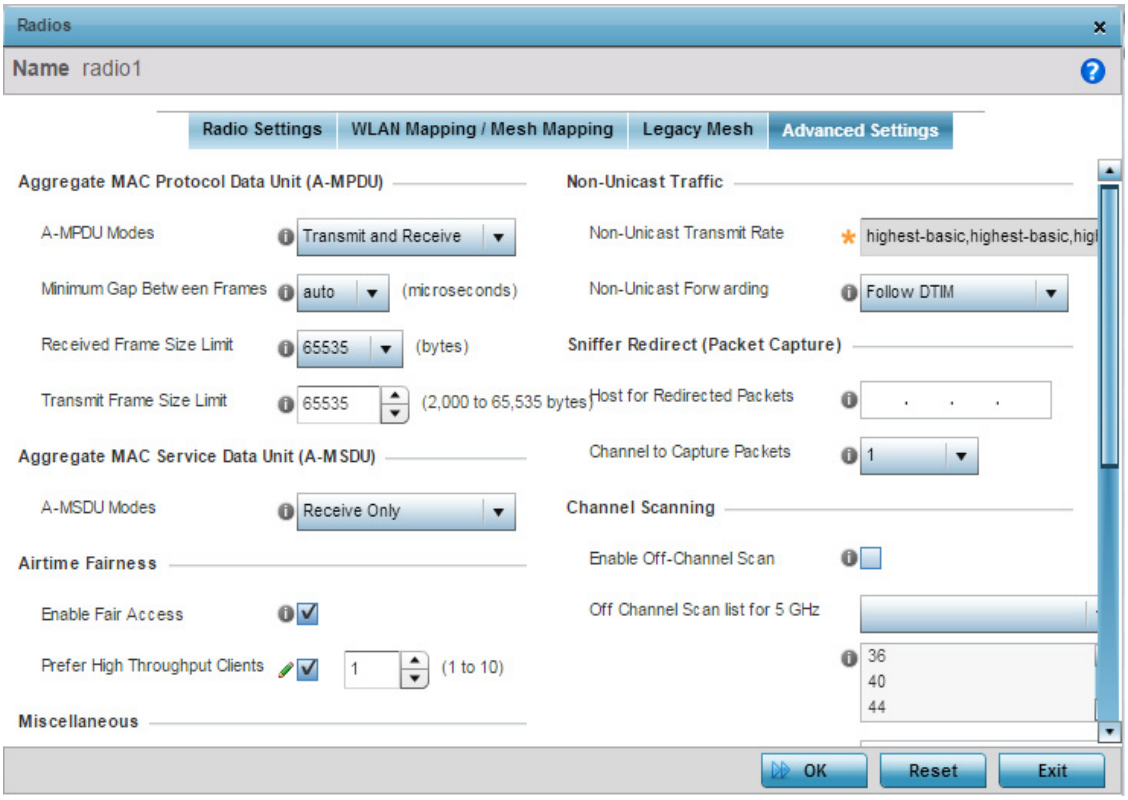


Figure 177: Device Overrides - Access Point Radio Advanced Settings tab

20 Refer to the **Aggregate MAC Protocol Data** Unit (A-MPDU) field to define or override 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. 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 the minimum gap between A-MPDU frames (in microseconds). The default value is *auto* which indicates that the minimum gap between frames is selected automatically. The other values are *0, 1, 2, 4, 8* and *16*.
Received Frame Size Limit	If a support mode is enable allowing A-MPDU frames to be received, define an advertised maximum limit for received A-MPDU aggregated frames. Options include 8191, 16383, 32767 or 65535 bytes. The default value is 65535 bytes.
Transmit Frame Size Limit	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is from 0 - 65,535 bytes). The default value is 65535 bytes.

21 Use the **Aggregate MAC Service Data Unit** (A-MSDU) drop-down menu to set or override the supported A-MSDU mode.

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

23 Use the **Airtime Fairness** fields to configure wireless access to devices based on their usage.

Select **Enable Fair Access** to enable this feature. Select **Prefer High Throughput Clients** to prefer clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients.

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

Forward	Select to enable forwarding of Aeroscout packets
MAC to be forwarded	Enter the MAC address that is incorporated in the Aeroscout packets that are forwarded.

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

Forwarding host	Provide the IP address of the host to which Ekahau packets are forwarded to.
Forwarding Port	Use the spinner to provide the Ekahau forwarding port number.
MAC to be forwarded	Enter the MAC address that is incorporated in the Ekahau packets that are forwarded.

26 Define a *Reduced Interframe Spacing* (RIFS) mode using the drop-down menu. This value determines whether interframe spacing is applied to transmissions or received packets, or both or none. The default mode is *Transmit and Receive*. Consider setting this value to *None* for high priority traffic to reduce packet delay.

27 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 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.
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.

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

29 Select the **Enable Off-Channel Scan** radio button to scan across other channels in the radio band. This setting is disabled by default.

30 Select the **Off-Channel Scan list for 5GHz** field and enter the channels on which off channel scan has to be performed for the 5.0 GHz radio. Similarly select the channels for the **Off Channel Scan list for 2.4 GHz** radio.

31 Use the **Max Multicast** spinner to set the maximum number of multicast channels on which to do off channel scan.

32 Use the **Scan Interval** spinner to set the time duration in DTIM period between 2 off channel scans.

33 Use the **Sniffer Redirect** field to provide the IP address of the device to which the captured off-channel scan packets are redirected to.

34 Select **OK** to save or override the changes to the Advanced Settings screen. Select **Reset** to revert to the last saved configuration.

WAN Backhaul Overrides

"Profile Interface Override 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. Certain AP7131N model access points have 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. For a list of supported 3G cards, see "WAN Backhaul Configuration" on page 138.

To define a WAN Backhaul configuration override for a supported access point:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the **Device** menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Interface** to expand its submenu items

5 Select **WAN Backhaul**.

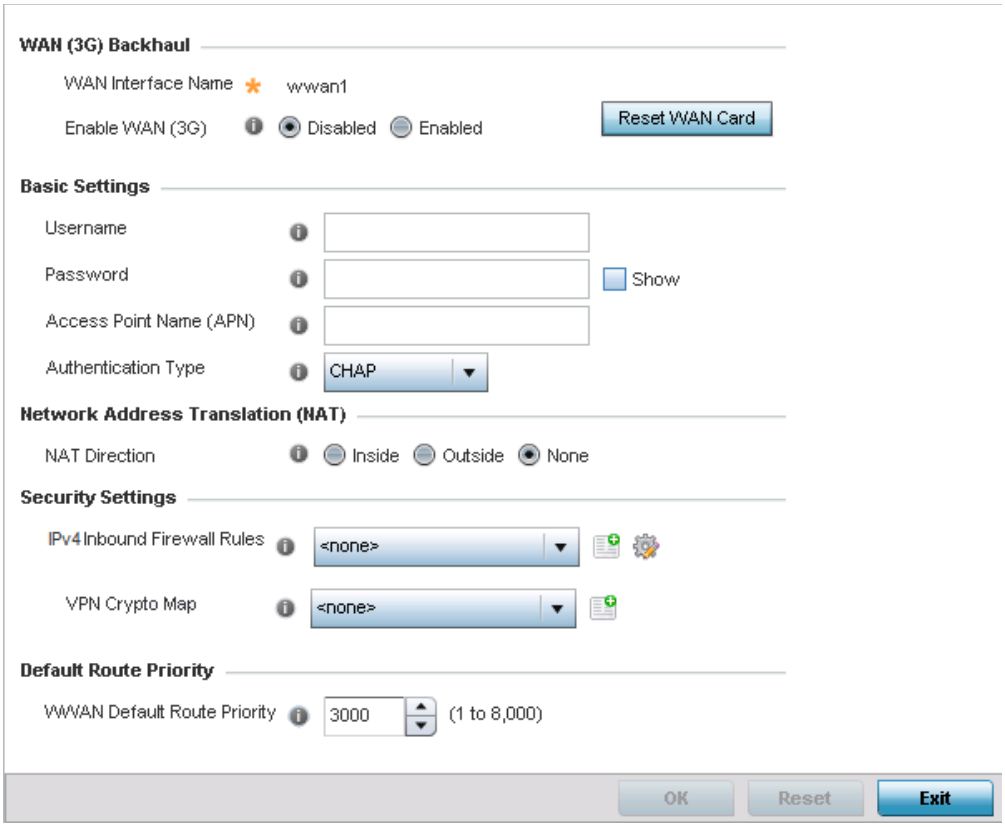


Figure 178: Device Overrides - WAN Backhaul screen

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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

6 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.
Reset WAN Card	If the WAN card becomes unresponsive or is experiencing other errors click the *Reset WAN Card* button to power cycle and reboot the WAN card.
Enable WAN (3G)	Select this option to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work.

7 Define or override the following authentication parameters from within the **Basic Settings** field:

Username	Provide your username for authentication support by your cellular data carrier.
Password	Provide your password for authentication support by your cellular data carrier.
Access Point Name (APN)	Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols such as Europe, the middle east and Asia.
Authentication Type	Use the drop-down menu to specify authentication type used by your cellular data provider. Supported authentication types are *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.

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

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

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

11 Configure the **WWAN Default Route Priority**. Use the spinner control to set the Default Route Priority for the WWAN default route. Select from 1 - 8,000. The default setting is 3,000.

12 Select **OK** to save or override the changes to the *Advanced Settings* screen. Select **Reset** to revert to the last saved configuration.

PPPoE Configuration

"Profile Interface Override Configuration"

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the access point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables WiNG supported controllers and access points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a

connection, a Wireless WAN failover is available to maintain seamless network access if the access point's Wired WAN were to fail.



NOTE

Access points 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.

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 **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Interface** to expand its submenu items

5 Select **PPPoE**.

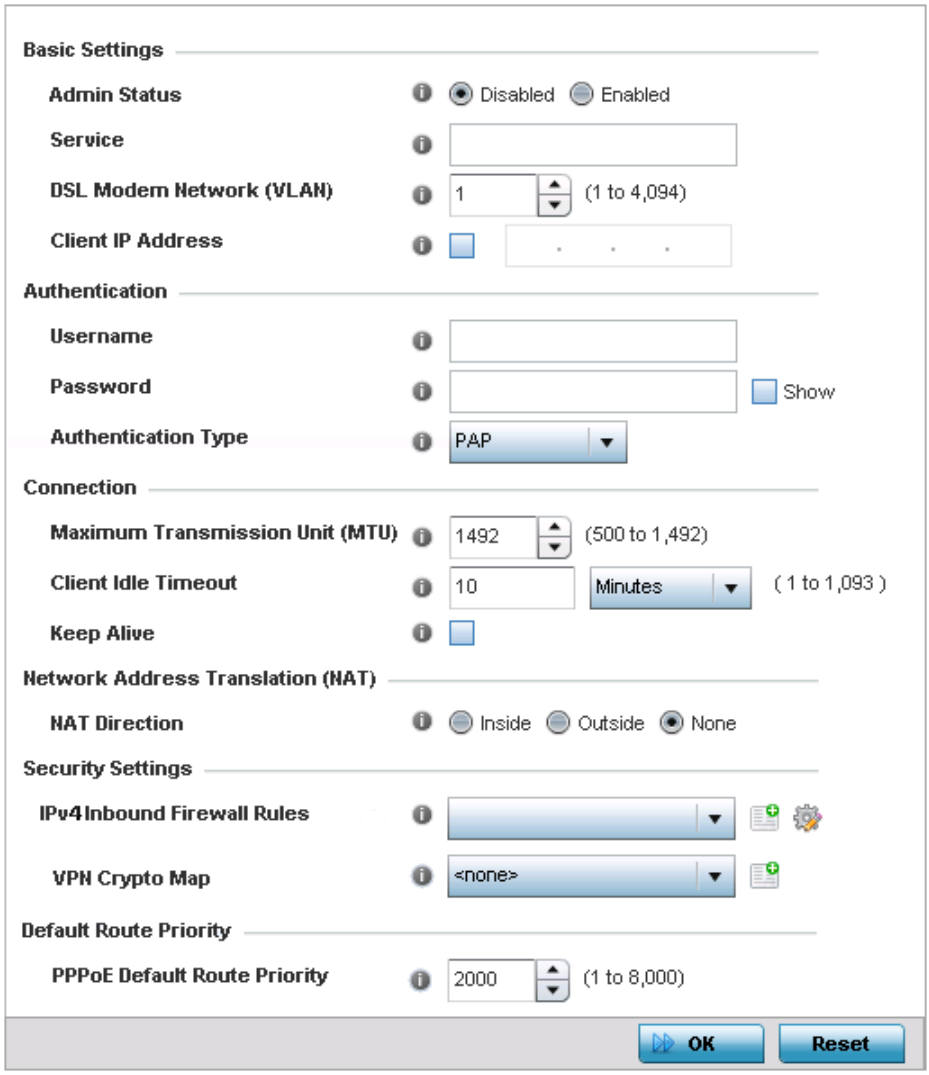


Figure 179: Device Overrides - PPPoE screen

6 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client:

Enable PPPoE	Select *Enable PPPoE* 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.

7 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. Select *Show* to display the actual characters comprising the password.
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*.

8 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 - 1,092) 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 the point-to-point connect to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

9 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

Network Address Translation (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 or outside).

10 Define the following **Security Settings** for the PPPoE configuration:

IPv4 Inbound Firewall Rules	Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the *Create* icon to define a new rule configuration or the *Edit* icon to modify an existing rule. For more information, see "Wireless Firewall" on page 709.
VPN Crypto Map	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

11 Use the spinner control to set the **PPPoE Default Route Priority** for the default route learnt using PPPoE.

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

12 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.

Bluetooth Configuration

"Profile Interface Override Configuration"

AP8432 and AP8533 model access point radios 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 can raise an alarm.



NOTE

AP8132 model access points support an external USB Bluetooth radio providing ADSP Bluetooth sensing functionality only, not the Bluetooth beaconing functionality available for AP8432 and AP8533 model access points described in this section.

AP8432 and AP8533 model access point 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 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 the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **System Profile** from the options on left-hand side of the UI.

4 Expand the **Interface** menu and select **Bluetooth**.

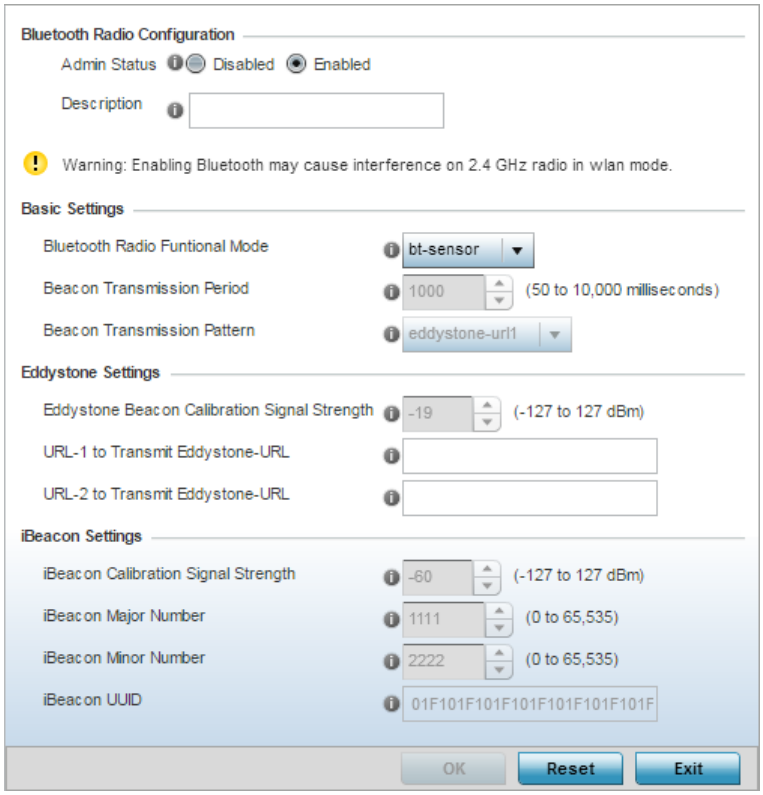


Figure 180: Profile Interface – Bluetooth screen

5 Set the following **Bluetooth Radio Configuration** parameters:

Admin Status	*Enable* or *Disable* Bluetooth support capabilities for AP8432 or AP8533 model access point Bluetooth radio transmissions. The default value is enabled.
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 may be members of the same RF Domain.

6 Set the following **Basic Settings** parameters

Bluetooth Radio Functional Mode	Set the access point's Bluetooth radio functional mode to either *bt-sensor* or *le-beacon*. • *bt-sensors* are Bluetooth classic sensors providing robust wireless connections for legacy devices. Typically these connections are not ideally suited for the newer Bluetooth low energy technology supported devices. • *le-beacons* are newer Bluetooth low energy beacons ideal for applications requiring intermittent or periodic transfers of small amounts of data. le-beacons are not designed as replacements for classic beacon sensors. le-beacon is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 50 - 10,000 milliseconds. As the defined period increases, so does the CPU processing time and the number packets incrementally transmitted (typically one per minute). The default setting is 1,000 milliseconds.
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 one of *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. If an eddystone-URL beacon broadcasts https:anysite, then clients receiving the packet can access that URL. iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). There are three data fields Apple has made 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 the Beacon Transmission Pattern has been set to either eddystone_url1 or eddystone_url2:

Eddystone Beacon Calibration Signal Strength	Set the Eddystone Beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm.
URL-1 to Transmit Eddystone-URL	Enter a 64 character maximum Eddystone-URL1. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.
URL-2 to Transmit Eddystone-URL	Enter a 64 character maximum Eddystone-URL2. The URL must be 17 characters or less once auto-encoding is applied. URL encoding is used when placing text in a query string to avoid confusion with the URL itself. It is typically used when a browser sends data to a Web server.

8 Define the following **iBeacon Settings** if the Beacon Transmission Pattern has been set to iBeacon:

iBeacon Calibration Signal Strength	Set the ibeacon measured calibration signal strength, from -127 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 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 *Universally Unique IDentifier* (UUID) classification contains 32 hexadecimal digits, split into 5 groups, separated by dashes. For example, f2468da6-5fa8-2e84-1134-bc5b71e0893e. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

9 Select **OK** to save the changes to the Bluetooth configuration. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

Overriding the Network Configuration

"Device Overrides"

Setting a network configuration is a large task comprised of numerous administration activities. Each of the configuration activities described can have an override applied to the original configuration. Applying an override differentiates the device from the profile's configuration and requires careful administration to ensure this one device still supports the deployment requirements within the network.

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

- "Overriding the DNS Configuration"
- "Overriding an ARP Configuration"
- "Overriding a L2TPv3 Profile Configuration"
- "Overriding IGMP Snooping Configuration"
- "Overriding MLD Snooping Configuration"
- "Overriding a Quality of Service (QoS) Configuration"
- "Overriding a Spanning Tree Configuration"
- "Overriding a Routing Configuration"
- "Overriding a Dynamic Routing (OSPF) Configuration"
- "Overriding a Forwarding Database Configuration"
- "Overriding a Bridge VLAN Configuration"
- "Overriding a Cisco Discovery Protocol Configuration"

- "Overriding a Link Layer Discovery Protocol Configuration"
- "Overriding Miscellaneous Network Configuration"
- "Overriding Alias Configuration"
- "Overriding IPv6 Neighbor Configuration"

Overriding the DNS Configuration

"Overriding the Network Configuration"

Domain Naming System (DNS) 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 is possible to access the resource even if the underlying machine friendly notation name changes. Without DNS you need to remember a series of numbers (123.123.123.123) instead of a domain name (www.domainname.com).

To define the DNS configuration or apply overrides to an existing configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **DNS**.

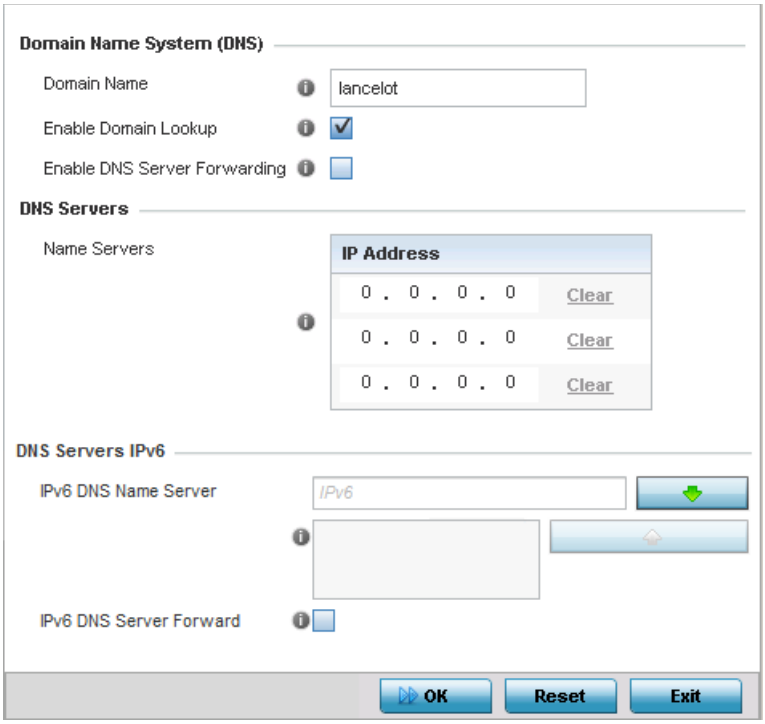


Figure 181: Device Overrides - Network DNS screen



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 screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

6 Provide or override the default Domain Name used when resolving DNS names. The name cannot exceed 64 characters.

7 Set or override the following *Domain Name System* (DNS) settings:

Enable Domain Lookup	Select this option to enable DNS on the access point. When enabled, human friendly domain names can be converted into numerical IP destination addresses. The radio button is selected by default.
Enable DNS Server Forwarding	Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by the access point's own DNS resources. This feature is disabled by default.

8 Provide a list of up to three DNS servers to forward DNS queries if 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.

9 Override the following **DNS Servers IPv6** configuration data when using IPv6:

IPv6 DNS Name Server	Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted.
IPv6 DNS Server Forward	Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default.

10 Select **OK** to save the changes and overrides made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

Overriding an ARP Configuration

"Overriding the Network Configuration"

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a hardware MAC address. ARP provides protocol rules for making this correlation and providing address conversion in both directions. This ARP assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

When an incoming packet destined for a host arrives at the access point, the access point's gateway uses ARP 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 the destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply indicating as such. 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 **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **ARP**.



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* screen's **Device Overrides** field and select **Clear Overrides**. This will remove all overrides from the device.

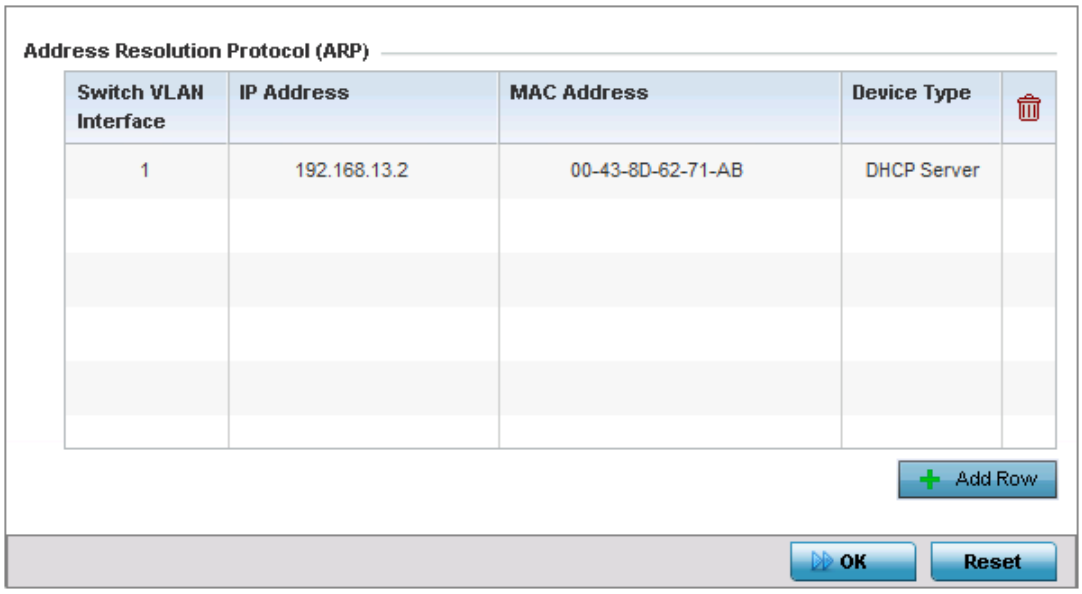


Figure 182: Device Overrides - Network ARP screen

6 Set or override the following parameters to define the ARP configuration:

Switch VLAN Interface	Use the spinner control to select a VLAN (1 - 4094) for an address requiring resolution.
IP Address	Define the IP address used to fetch a MAC address.
MAC Address	Displays the target MAC address that's subject to resolution. This is the MAC used for mapping an IP address to a MAC address that's recognized on the network.
Device Type	Specify the device type the ARP entry supports (either Host, Router or DHCP Server). Host is the default setting.

7 Select the **OK** button to save the changes and overrides to the ARP configuration. Select **Reset** to revert to the last saved configuration.

Overriding a L2TPv3 Profile Configuration

"Overriding the Network Configuration"

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and access point 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 and access points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports.

Multiple pseudowires can be created within an L2TP V3 tunnel. WING supported 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 *packet-switching network* (PSN). 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 or override an L2TPV3 configuration for an access point profile:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **L2TP V3**.



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* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

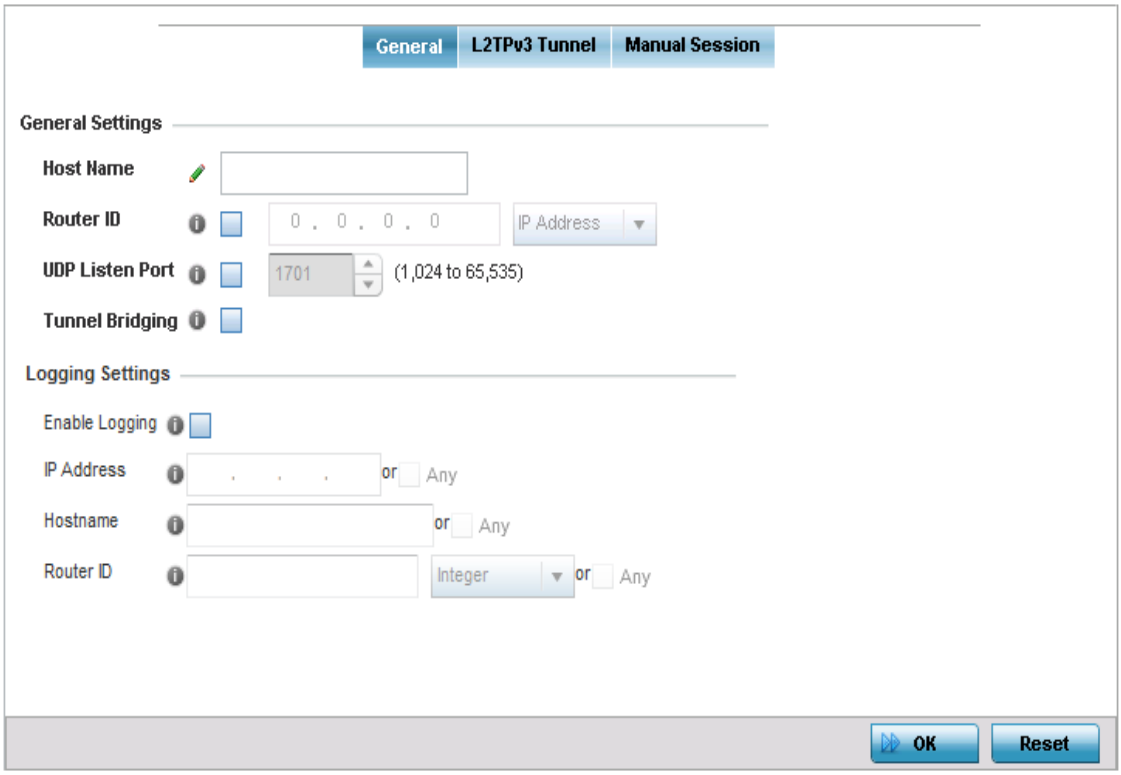


Figure 183: Device Overrides - Network - L2TPv3 screen, General tab

6 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 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.

7 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. Use *Any* to log any IP address.
Hostname	If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events. Use *Any* to log all hostnames.
Router ID	If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events. Use *Any* to log all routers.

8 Select the **L2TPv3 Tunnel** tab.

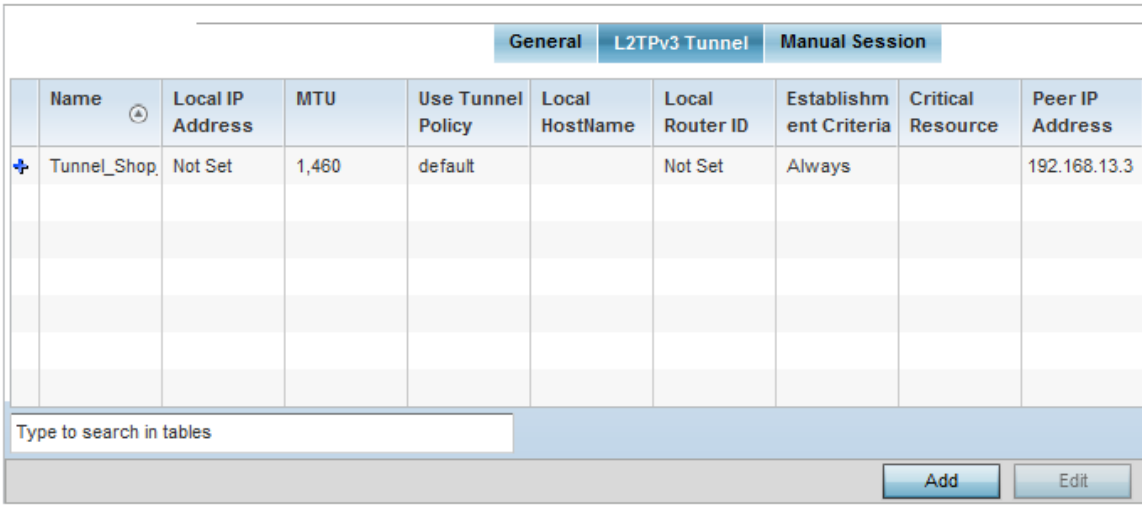


Figure 184: Device Overrides - Network - L2TPv3 screen, L2TPv3 tunnel tab

9 Set the following for an L2TPv3 profile configuration:

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 *maximum transmission unit* (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 the criteria that should be met for a tunnel between two peers to be created and maintained.
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. 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. Critical resources are pinged regularly. If there is a connectivity issue, an event is generated stating a critical resource is unavailable.
Peer IP Address	Displays the IP address of the device at the other end of the L2TPv3 tunnel.
Host Name	Specifies the administrator assigned hostname of the tunnel.

10 Either select **Add** to create a new L2TPv3 configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

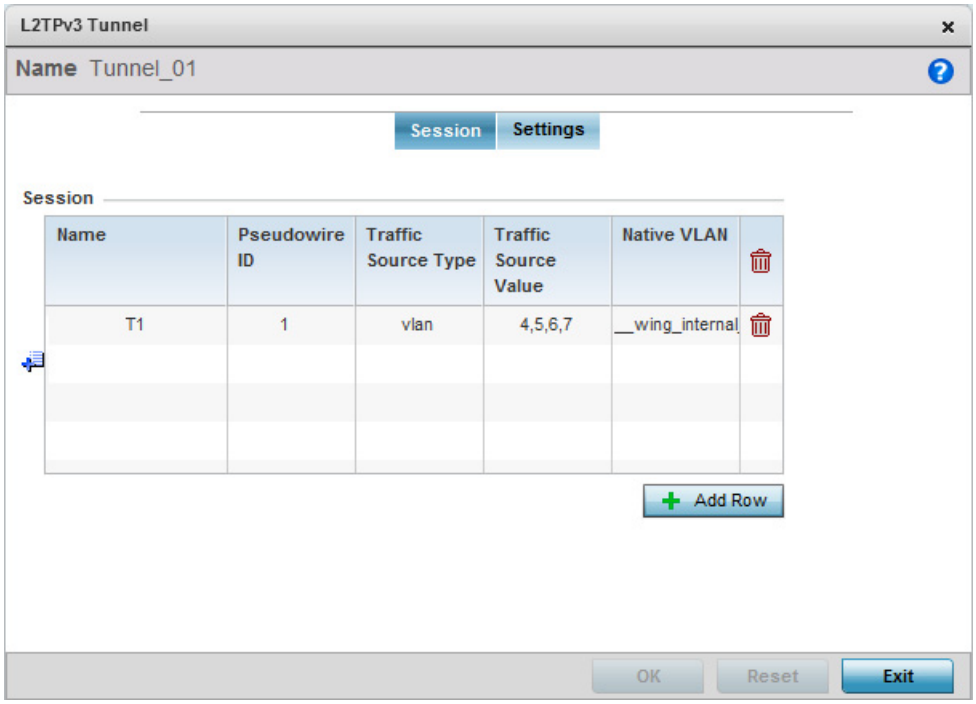


Figure 185: Device Overrides - Network - L2TPv3 screen, Add L2TPv3 Tunnel Configuration

11 If creating a new tunnel configuration, assign it a 31 character maximum **Name**.

12 Refer to the **Session** table to review the configurations of the peers available for tunnel connection.

13 Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

14 Define the following **Session** parameters:

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 *packet-switching network* (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 tunnelled 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.

15 Select the **Settings** tab.

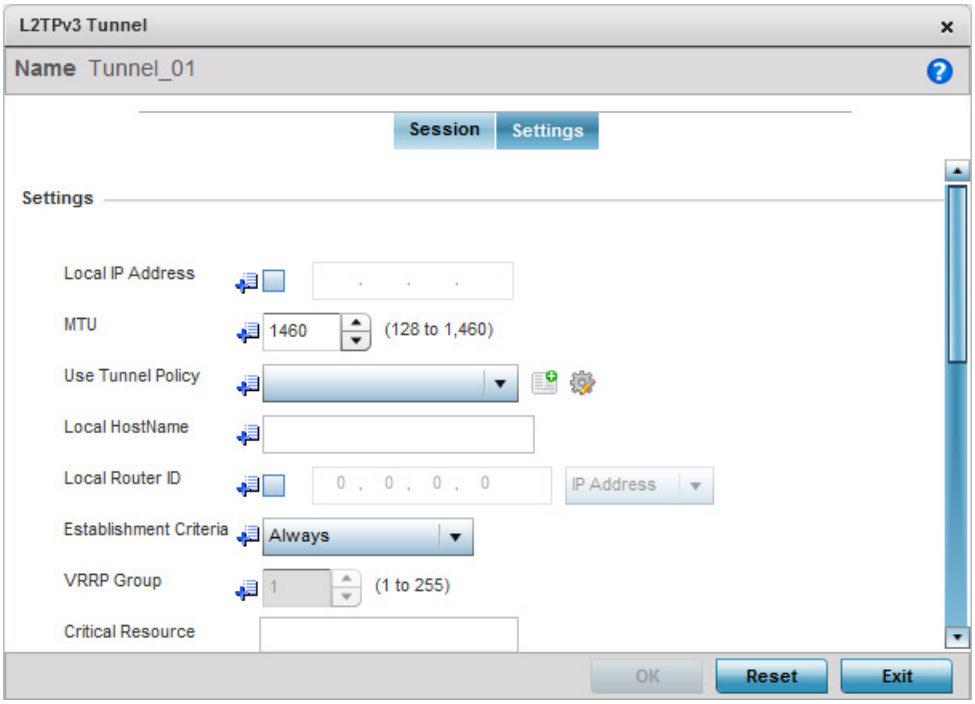


Figure 186: Device Overrides - Network - L2TPv3 screen - Add L2TPv3 Tunnel Configuration - Settings screen

16 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 *maximum transmission unit* (MTU). 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. For more information, refer to "Configuring Captive Portal Policies" on page 759.

Local Hostname	Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages.
Local Router ID	Specify the router ID sent in tunnel establishment messages with a potential peer device.
Establishment Criteria	Specify the establishment criteria for creating a tunnel. The tunnel is only created if this device is one of the following: • vrrp-master • cluster-master • rf-domain-manager The tunnel is always created if *Always* is selected. This indicates that the device need not be any one of the above three (3) to establish a tunnel.
VRRP Group	Set the VRRP group value. This is only applicable if the *Establishment Criteria* specifies *vrrp-master*.
Critical Resource	This table lists the critical resources defined for this system. The tunnel is created and maintained if the critical resources are available. The tunnel is brought down if any one of the defined critical resource goes down or is unreachable.

17 Define the following **Rate Limit** settings for the L2TP tunnel configuration. 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%.

18 Refer to the **Peer table** to review the configurations of the peers available for tunnel connection.

Select **+ Add Row** to populate the table with a maximum of two peer configurations.

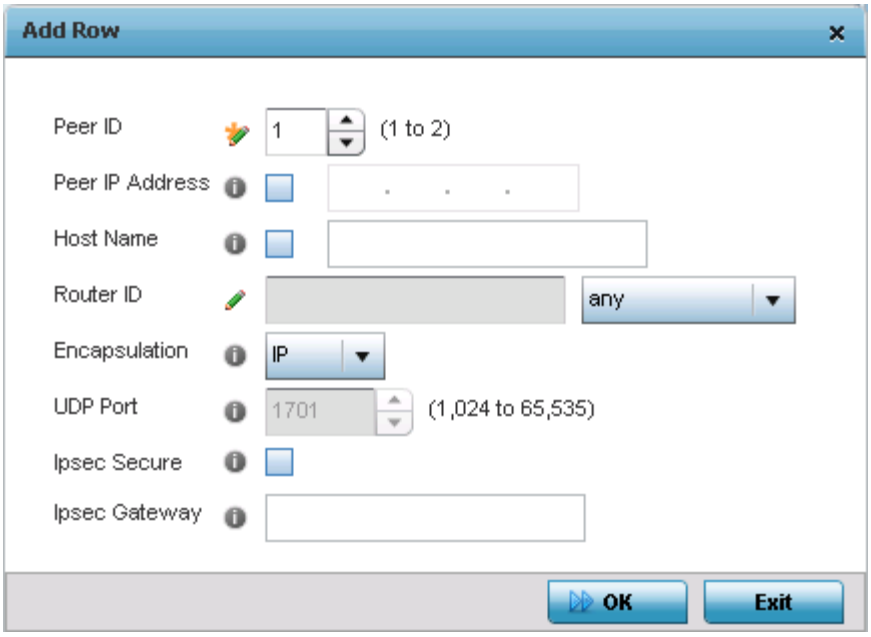


Figure 187: Device Overrides - Network - L2TPv3 screen, Add L2TP Peer Configuration

19 Define the following **Peer** parameters:

Peer ID	Define the primary peer ID used to set the primary and secondary peer for tunnel failover. 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.
Peer IP Address	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment.
Host Name	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process.
Router ID	Specify the router ID sent in tunnel establishment messages with this specific peer.
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.
IPSec Secure	Enables or disable IPSec security for the tunnel.
IPSec Gateway	If *IPSec Secure* is enabled, provide the IPSec gateway device's IP address.

20 Select **OK** to save the peer configuration and overrides.

21 From the **L2TPv3 Tunnel** screen's **Settings** tab, configure the **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.

22 Select **OK** to save the changes and overrides to the L2TPv3 Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.

23 Select the **Manual Session** tab.

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.

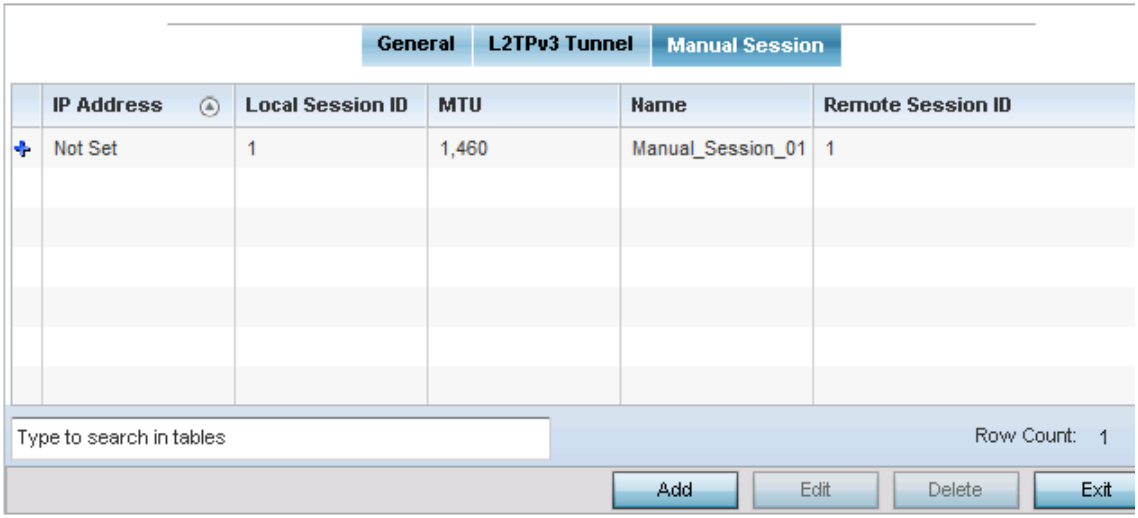


Figure 188: Device Overrides - Network - L2TPv3 screen, Manual Session tab

24 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 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 sessions's *maximum transmission unit* (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.

25 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

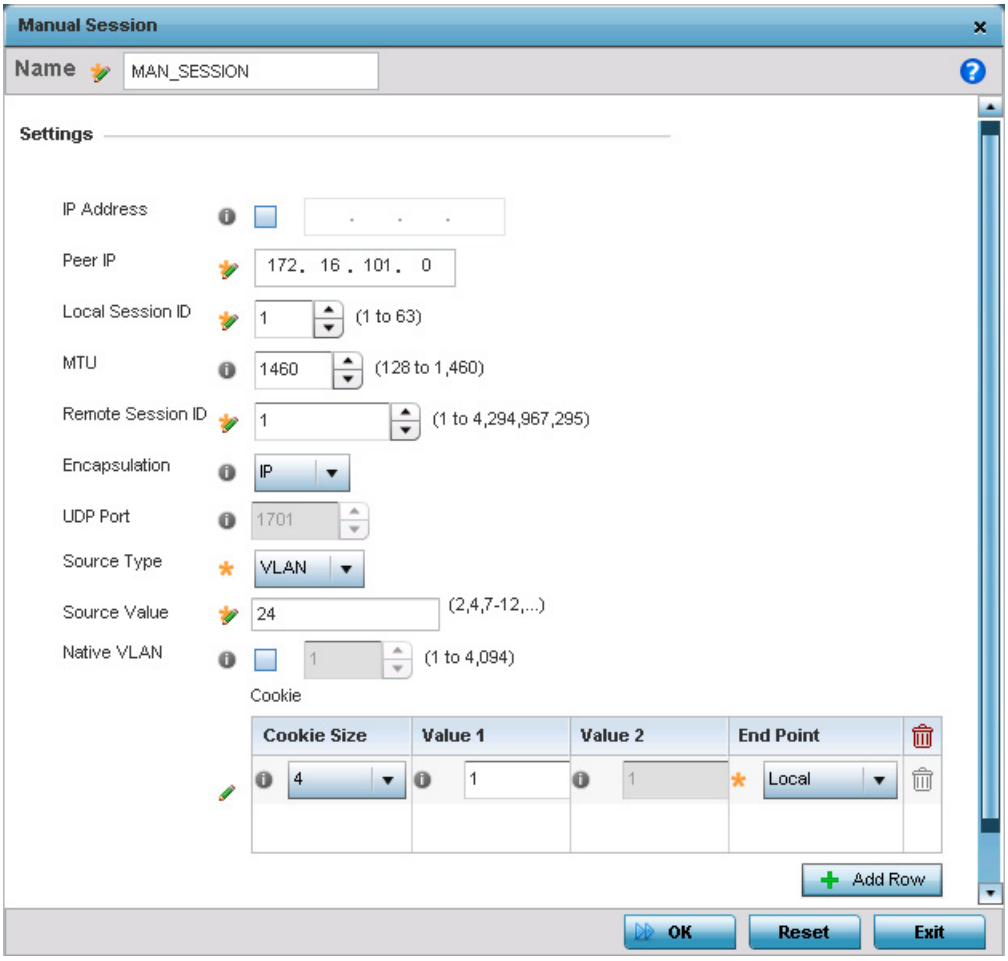


Figure 189: Device Overrides - Network - L2TPv3 screen, Add L2TPv3 Peer Configuration

26 Set the following **Manual Session** parameters:

Name	Define a 31 character maximum name of this tunnel session. After a successful tunnel connection and establishment, the session is created. Each session name represents a single data stream.
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 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 *maximum transmission unit* (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 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 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

27 Select the **+ Add Row** button 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.

28 Select **OK** to save the changes and overrides to the session configuration. Select **Reset** to revert to the last saved configuration.

Overriding IGMP Snooping Configuration

▸ "Overriding the Network Configuration"

Internet Group Management Protocol (IGMP) is a protocol to establish and maintain multicast group memberships to interested members. Multicasting allows a computer on a network to send content to multiple computers who have registered to receive the content. IGMP Snooping is the term for listening to IGMP traffic between an IGMP host and routers in the network to maintain a map of the links that require multicast streams. Multicast traffic is filtered out for those links which do not require them.

To configure IGMP Snooping:

1 Select the **Configuration** tab from the Web UI.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **IGMP Snooping**.

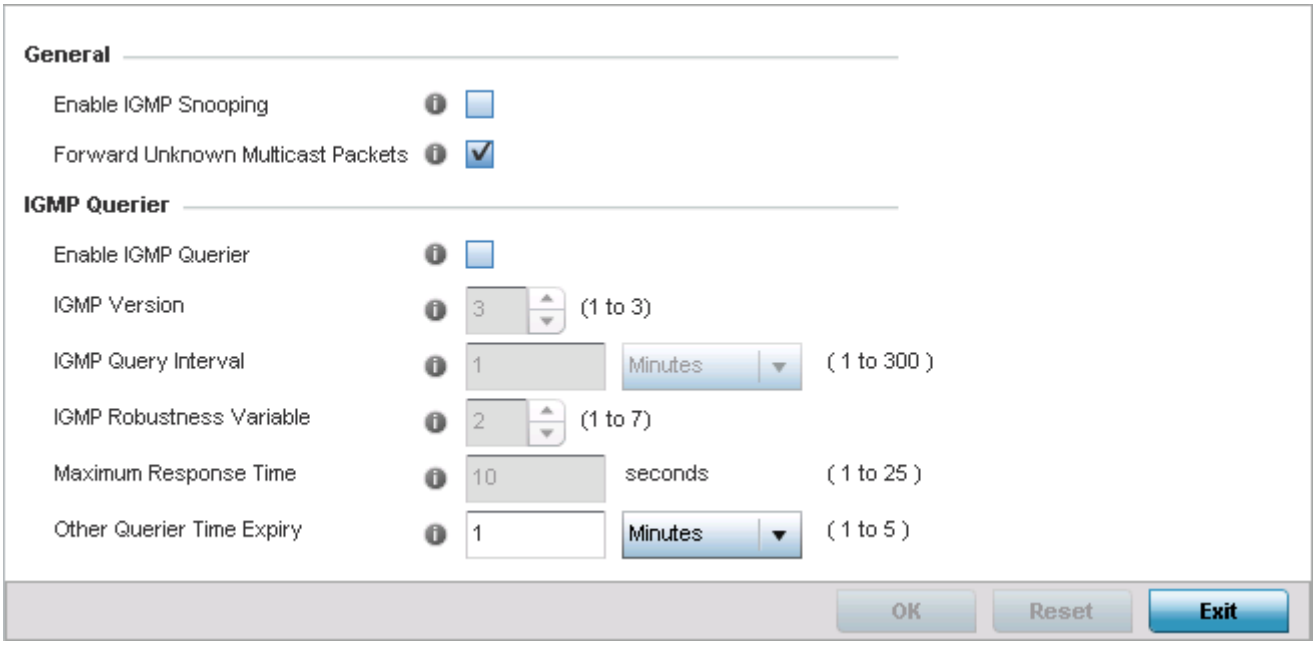


Figure 190: Device Overrides - Network - IGMP Snooping Screen

6 Set the following parameters to configure **General IGMP Snooping** values:

Enable IGMP Snooping	Select the box to enable IGMP Snooping on the access point. This feature is enabled by default.
Forward Unknown Multicast Packets	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the *Unknown Multicast Forward* feature is also disabled for the selected VLANs. This is enabled by default.

7 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 is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. 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 forwarded on that port. An AP71xx model access point can also be an IGMP querier.
IGMP Version	Use the spinner control to set the IGMP version compatibility to one of IGMP version 1,2 or 3. The default IGMP version is 3.
IGMP Query Interval	Sets the IGMP query interval. This parameter will be used only when the querier functionality is enabled. Define an interval value in *Seconds* (1 - 18,000), *Minutes* (1 - 300) or *Hours* (1 - 5) up to maximum of 5 hours. The default value is 60 seconds.
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 time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
Other Querier Time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

8 Select **OK** to save the changes and overrides to the session configuration. Select **Reset** to revert to the last saved configuration.

Overriding MLD Snooping Configuration

"Overriding the Network Configuration"

Multicast Listener Discovery (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 set an IPv6 MLD snooping configuration for the profile:

1 Select the **Configuration** tab from the Web UI.

Select **Device Overrides** from the Device menu to expand it into sub menu options.

Select a target device from the device browser in the lower, left-hand, side of the UI.

Select **Network** to expand its sub menu options.

Select **MLD Snooping**.

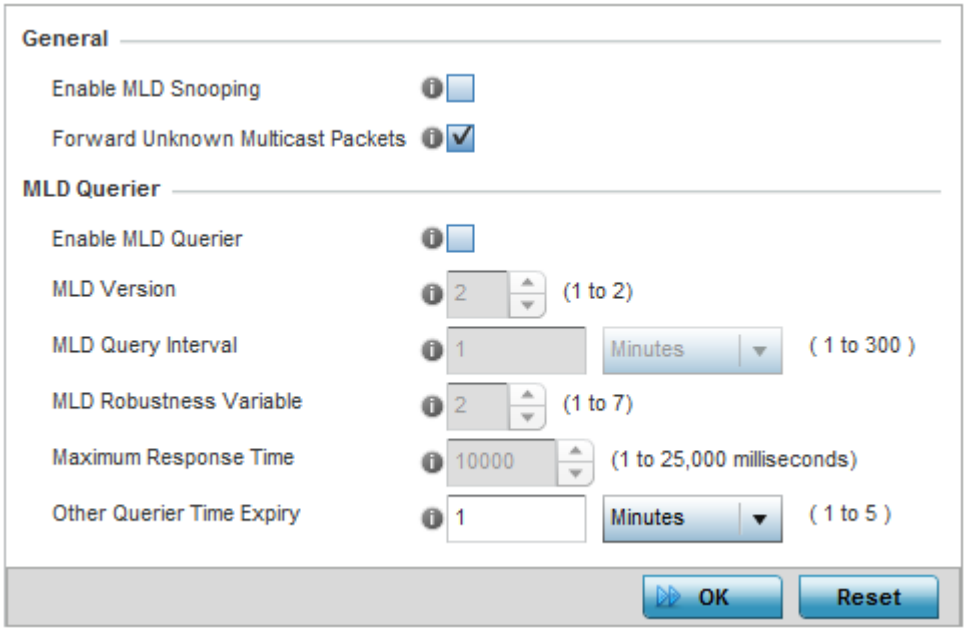


Figure 191: Profile - Network MLD Snooping screen

2 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.

3 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.

4 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

Overriding a Quality of Service (QoS) Configuration

"Overriding the Network Configuration"

QoS values are required to provide service priority to packets. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit *Differentiated Service Code Point* (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet. This QoS assignment can be overridden as needed, but removes the device configuration from the profile that may be shared with other similar access point models.

To define an QoS configuration for DSCP mappings:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Quality of Service**.

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* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

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

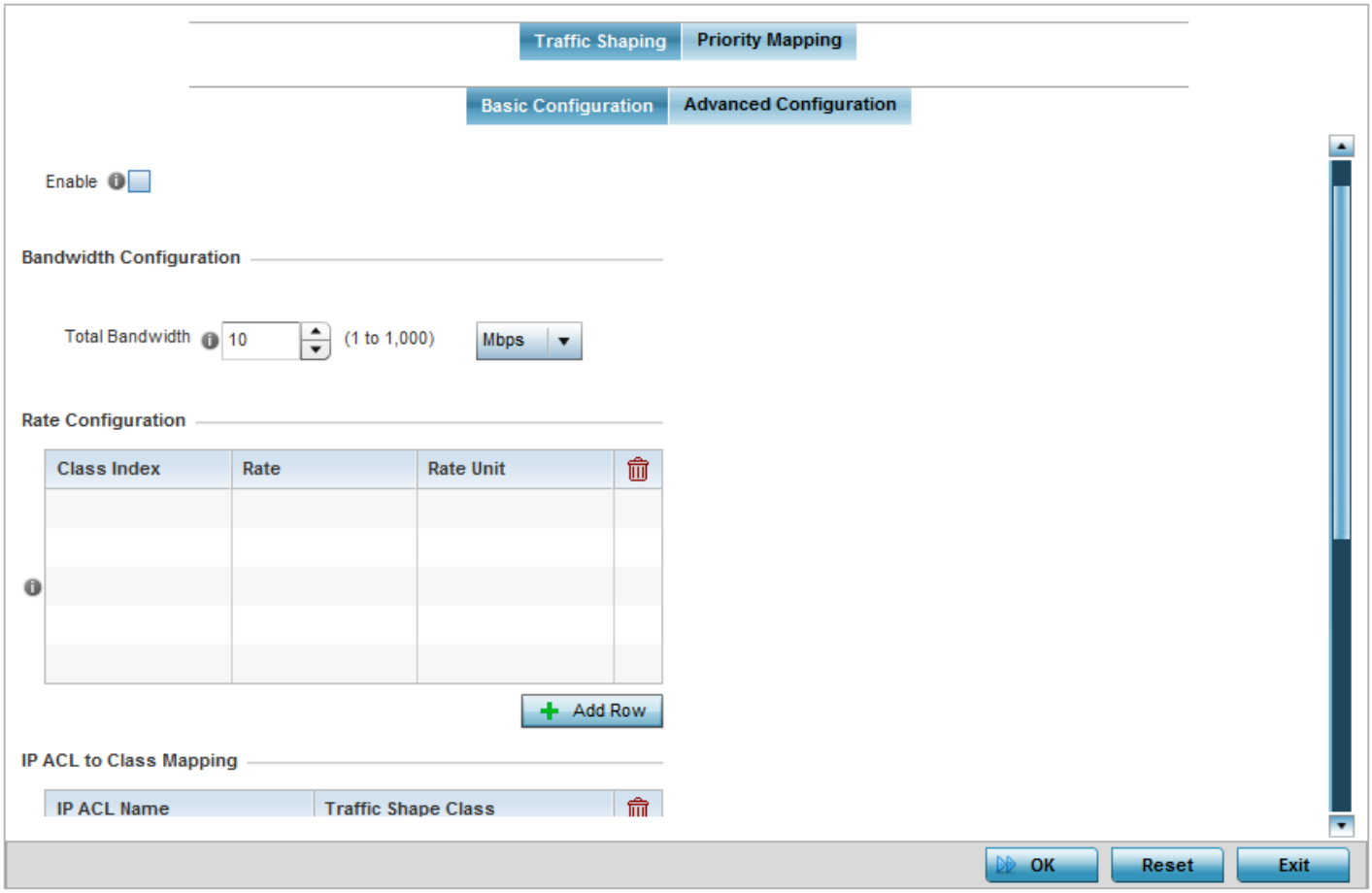


Figure 192: Profile Overrides - Network QoS Traffic Shaping Basic Configuration screen

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.

6 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

7 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.

8 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.

9 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 724 and "Setting an IPv4 or IPv6 Firewall Policy" on page 725.

10 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 724 and "Setting an IPv4 or IPv6 Firewall Policy" on page 725.

11 Select the **OK** button located to save the changes to the traffic shaping basic configuration. Select **Reset** to revert to the last saved configuration.

12 Select the **Advanced Configuration** tab.

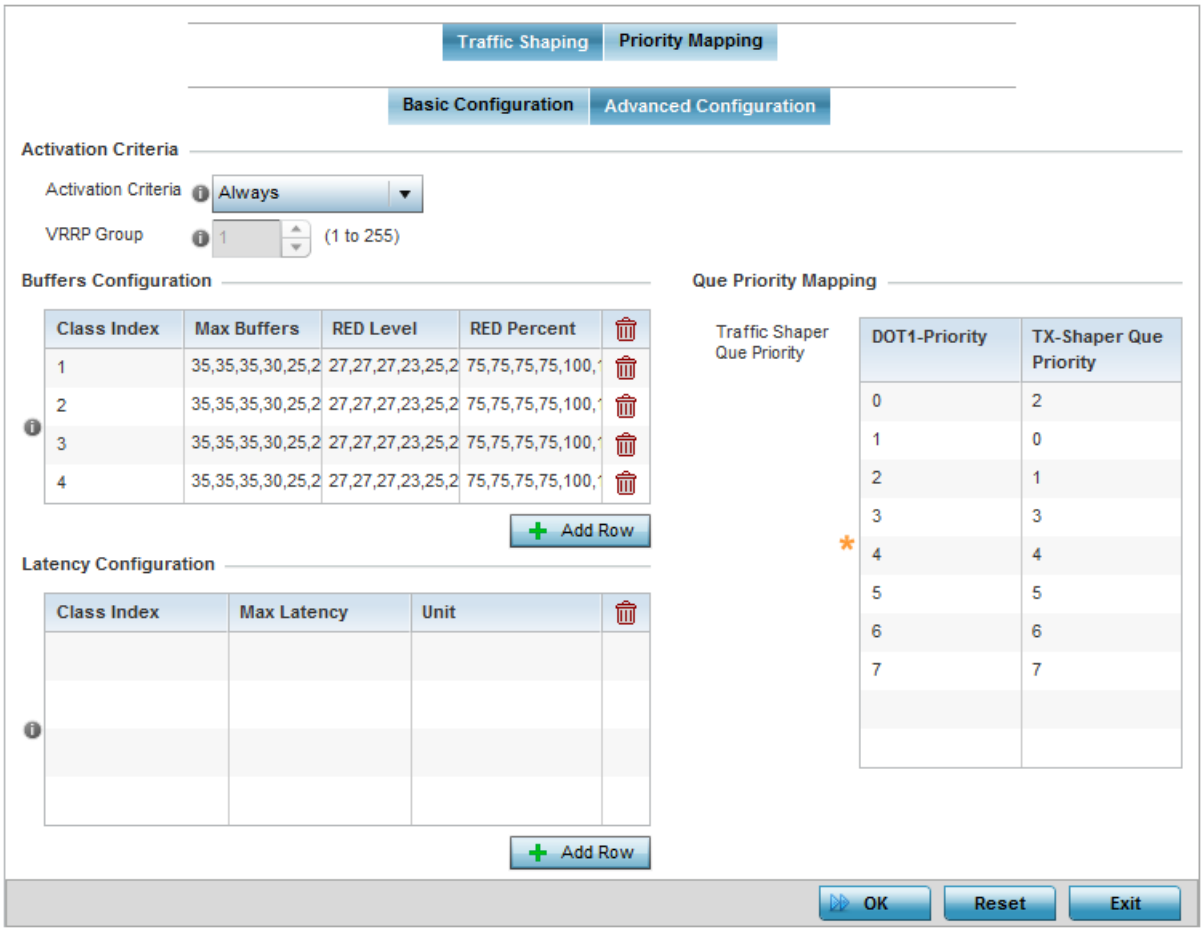


Figure 193: Profile Overrides - Network QoS Traffic Shaping Advanced Configuration screen

13 Set the following **Activation Criteria** for traffic shaper activation:

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.

14 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 *random early detection* (RED) 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.

15 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.

16 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.

17 Select the **OK** button located to save the changes to the traffic shaping advanced configuration. Select **Reset** to revert to the last saved configuration.

18 Select the **Priority Mapping** tab.

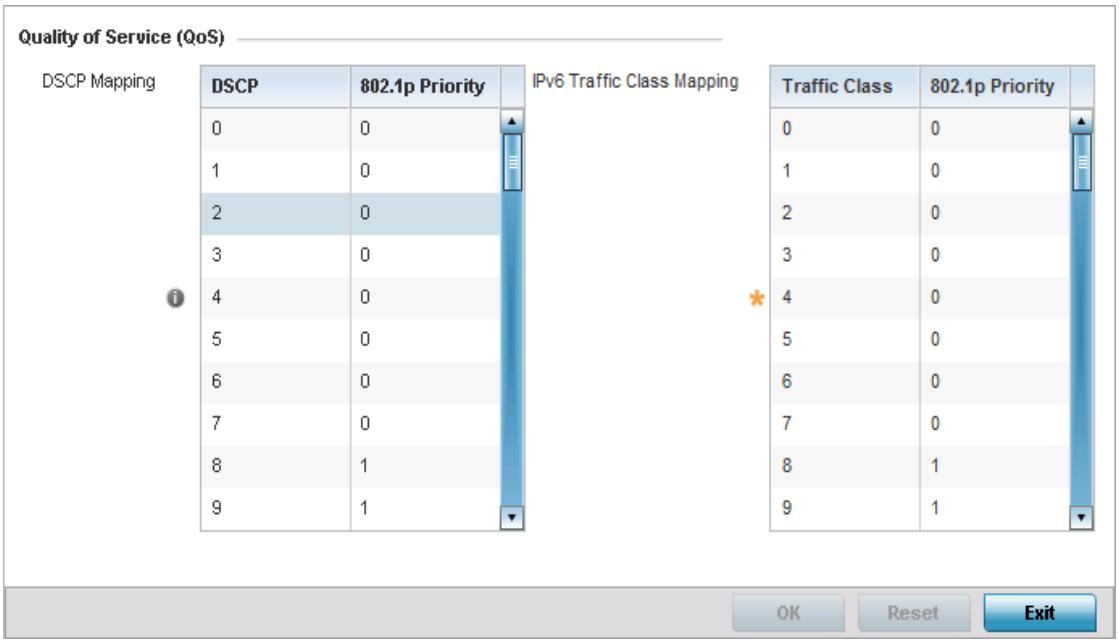


Figure 194: Device Overrides - Network QoS screen

19 Set or override the following parameters for the 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 or override the priority value.

20 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

Use the spinner controls within the 802.1p Priority field for each DSCP row to change or override the priority value.

21 Select the **OK** button located to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

Overriding a Spanning Tree Configuration

"Overriding the Network Configuration"

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness o f 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 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 *MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. 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 override a profile's spanning tree configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Spanning Tree**.

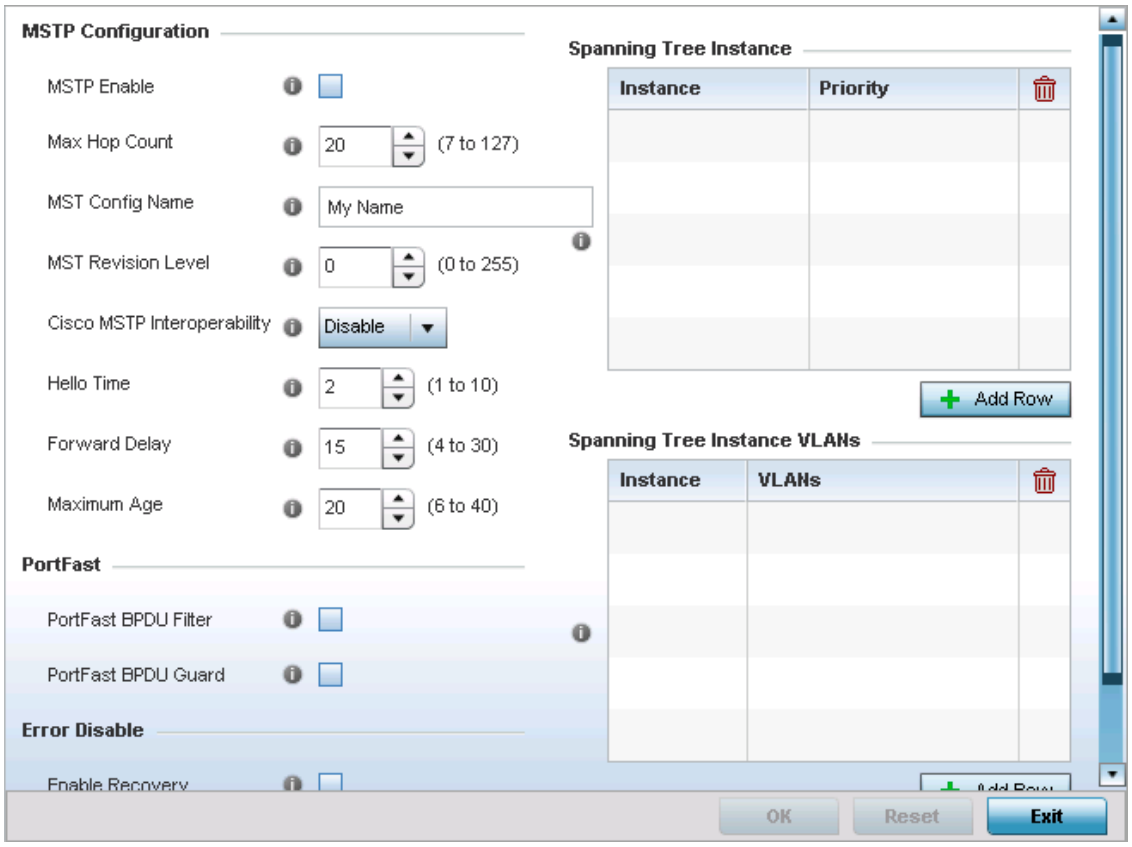


Figure 195: Device Overrides - Network - Spanning Tree screen

6 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.

7 Define the following **PortFast** 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.

8 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 Interval	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.

9 Use the **Spanning Tree Instance** table to add indexes to the spanning tree topology.

10 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.

11 Use the **Spanning Tree Instance VLANs** table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.

12 Select the **OK** button located at the bottom right of the screen to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

Overriding a Routing Configuration

"Overriding the Network Configuration"

Routing is the process of selecting IP paths in a network 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.

To override a profile's route configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Routing**. The **IPv4 Routing** screen displays by default.

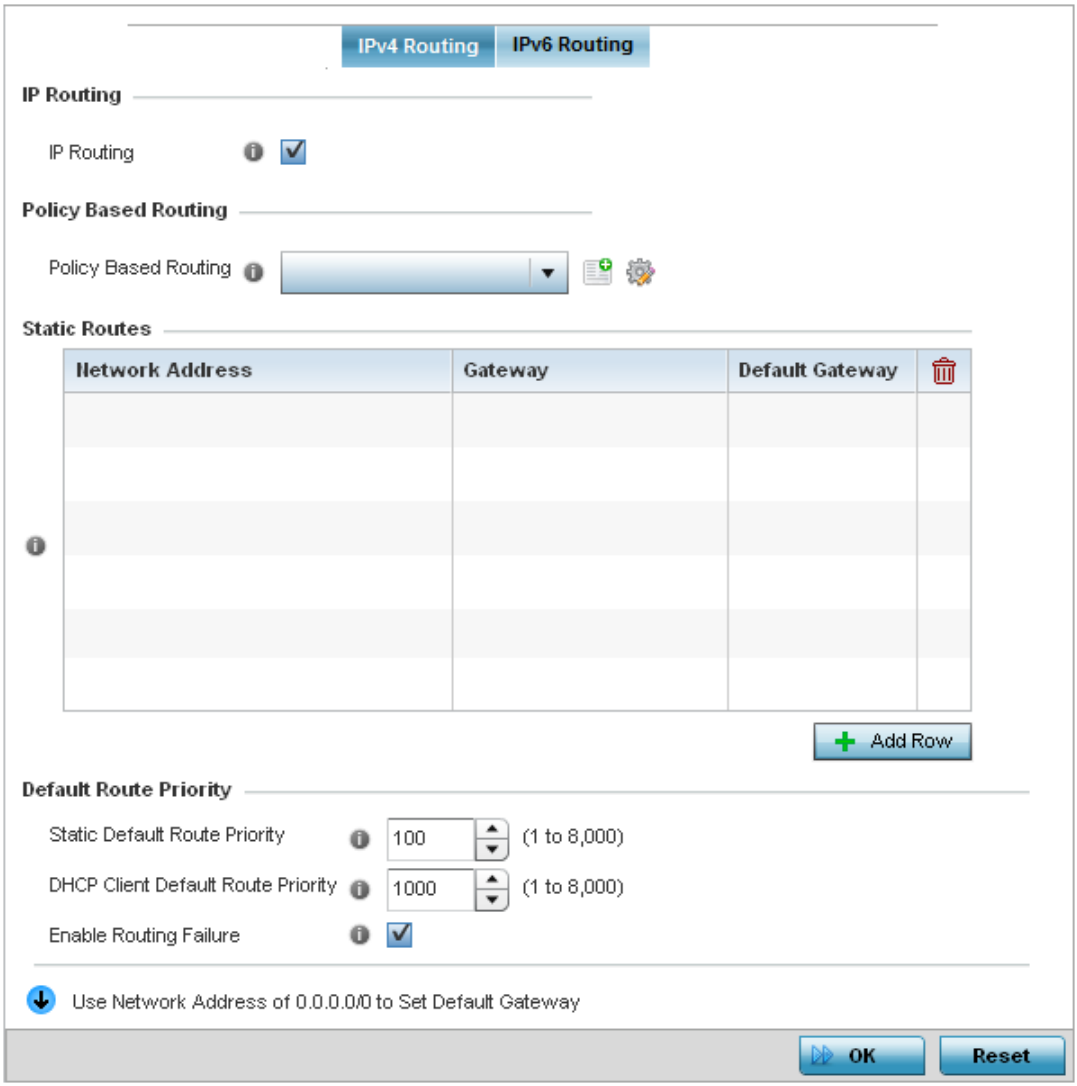


Figure 196: Device Overrides - Network - Network Routing screen

6 Select the **IP Routing** option to enable IP routing using static routes provided in the route table. This option is enabled by default.

7 Select the **Policy Based Routing** policy to apply to this profile. Click the **Create** icon to create a policy based route or click the **Edit** to edit an existing policy after selecting it in the drop-down list. For more information on policy based routing, see "Policy Based Routing (PBR)" on page 651.

8 Select **Add Row +** as needed to include single rows with in the static IPv4 route table.

9 Add IP addresses and network masks in the **Network** column.

10 Provide the **Gateway** used to route traffic.

11 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. 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.

12 Select the **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

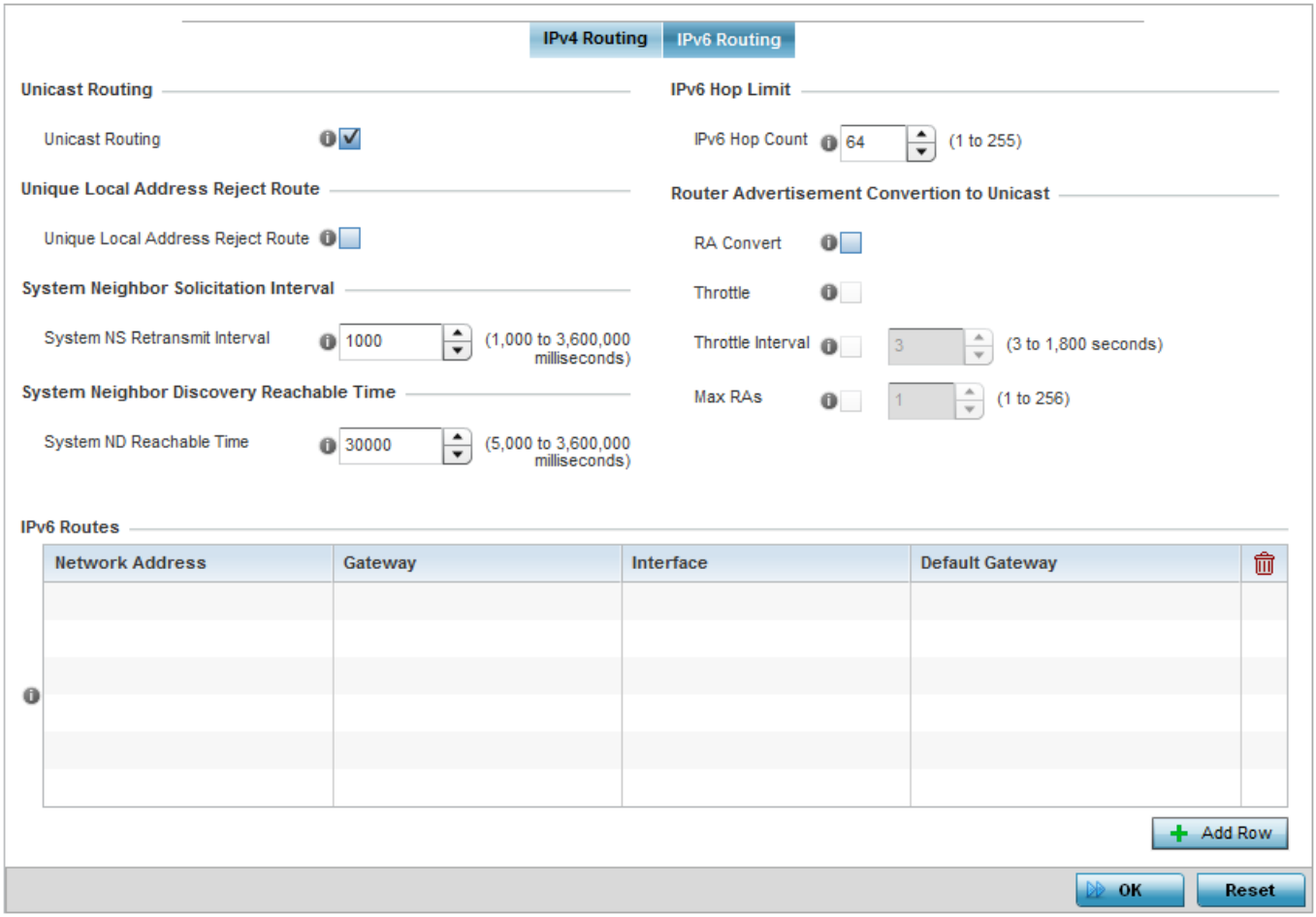


Figure 197: Device Overrides -Static Routes screen, IPv6 Routing tab

13 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.

14 Select **Unique Local Address Reject Route** to reject *Unique Local Address* (ULA). ULA is an IPv6 address block
(fc00::/7) that is an approximate IPv6 counterpart to IPv4 private addresses. When

selected, a reject entry is added to the IPv6 routing table to reject packets with Unique Local Address.

15 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.

16 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.

17 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.

18 Set the **Router Advertisement Conversion to Unicast** settings:

RA Convert	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.

19 Select **+ Add Row** as needed within the **IPv6 Routes** table to add an additional 256 IPv6 route resources.

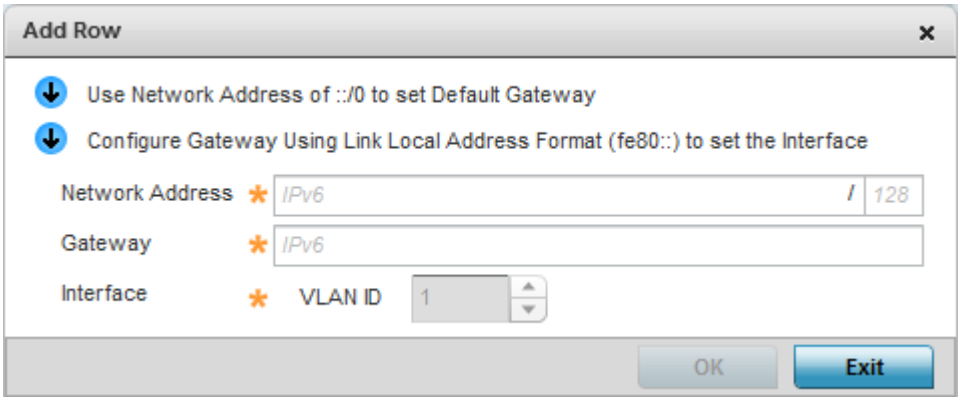


Figure 198: Device Overrides -Static Routes screen, Add IPv6 Route

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. Use a network address of ::/0 to set the default gateway.
Interface	If using a link local address, set the VLAN (1 - 4,094) used a virtual routing interface for the local address.

20 Select the **OK** button located at the bottom right of the screen to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

Overriding a Dynamic Routing (OSPF) Configuration

"Overriding the Network Configuration"

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. that is, The only way for traffic to get routed outside of the area is. A default route is the only way to route traffic outside of the area. When there is only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.
- *non-stub* - An area that 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* - This 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.

NOTE

OSPF is available on the following access points: AP8432, AP8533, AP7522, AP7532, AP7562, AP82XX, AP81XX.

To override a profile's dynamic routing configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **OSPF**.

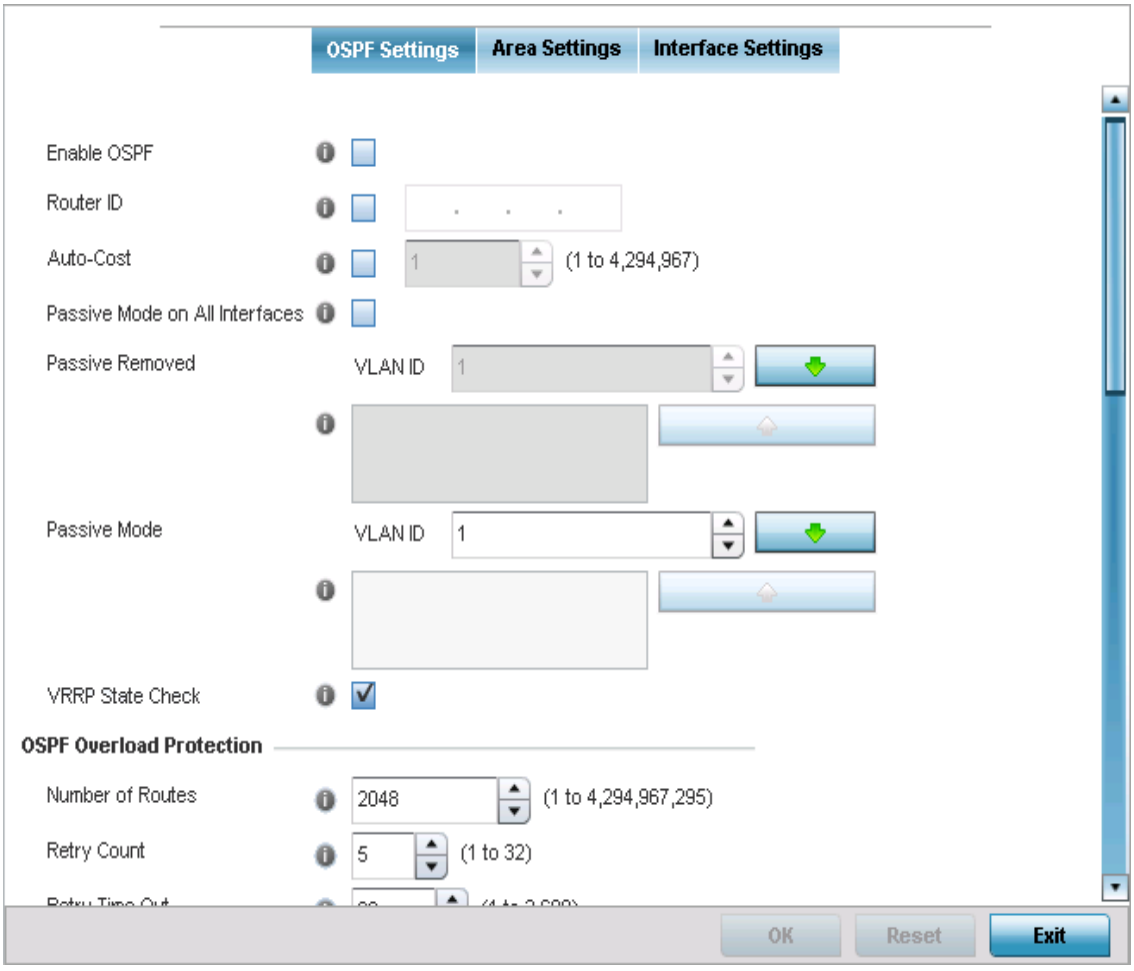


Figure 199: Device Overrides - Network - OSPF Settings screen

6 Enable/disable OSPF and provide the following dynamic routing settings:

Enable OSPF	Select this option to enable OSPF for this access point. OSPF is disabled by default.
Router ID	Select this option to define a router ID (numeric IP address) for this access point. 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 Mode Check	Select this option to enable checking VRRP state. If the interface's VRRP state is not *Backup*, then the interface is published via OSPF.

7 Set the following **OSPF Overload Protection** settings:

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 OSPS 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.

8 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 is defined by the speed (bandwidth) of the interface supporting given route.

9 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*, *kernel*, *static* and *bgp*.

10 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.

11 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.

12 Click the **Clear** button next to the **Clear OSPF Process** field to clear all OSPF routing entries.

13 Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route learnt from OSPF.

14 Select the **Area Settings** tab.

An OSPF Area contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.

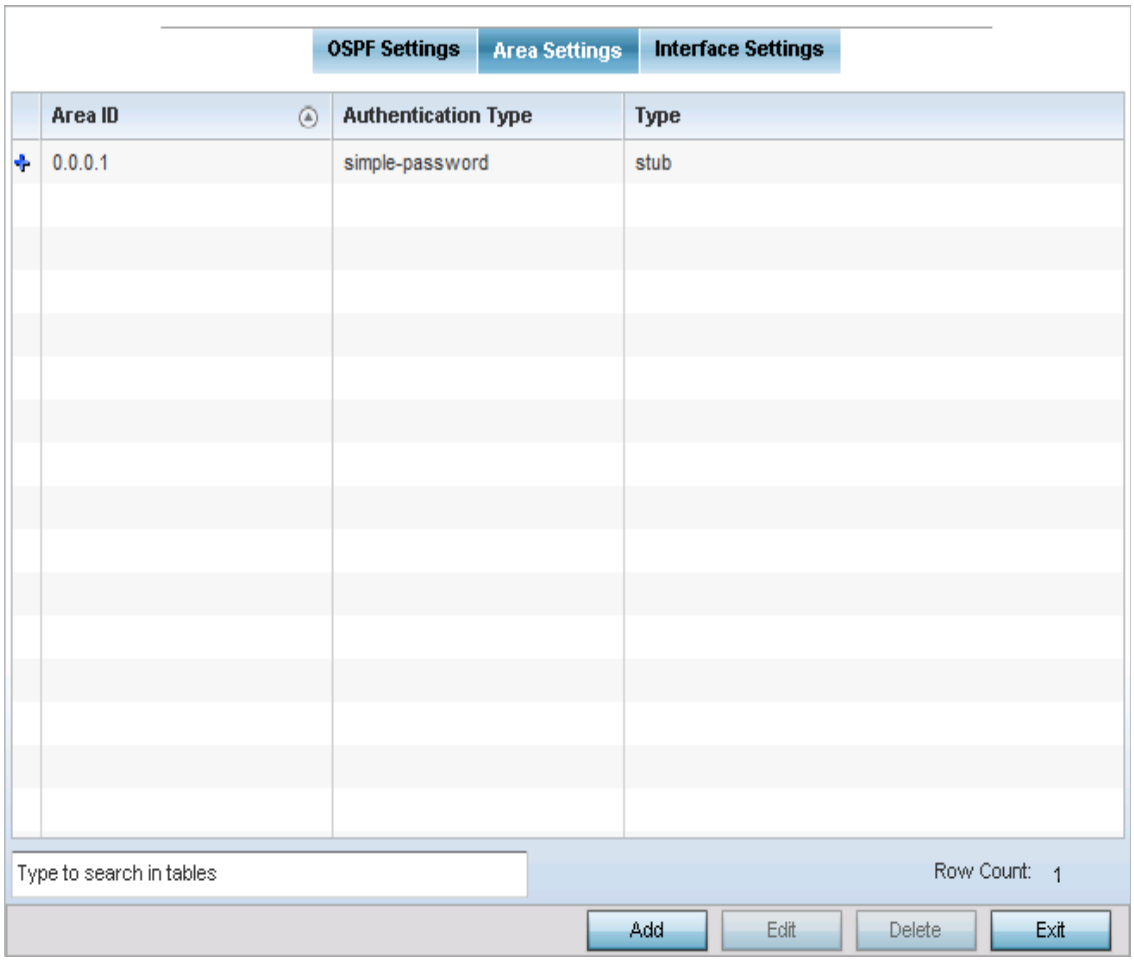


Figure 200: Device Overrides - Network - OSPF Area Settings screen

15 Review existing **Area Settings** configurations using:

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.

16 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

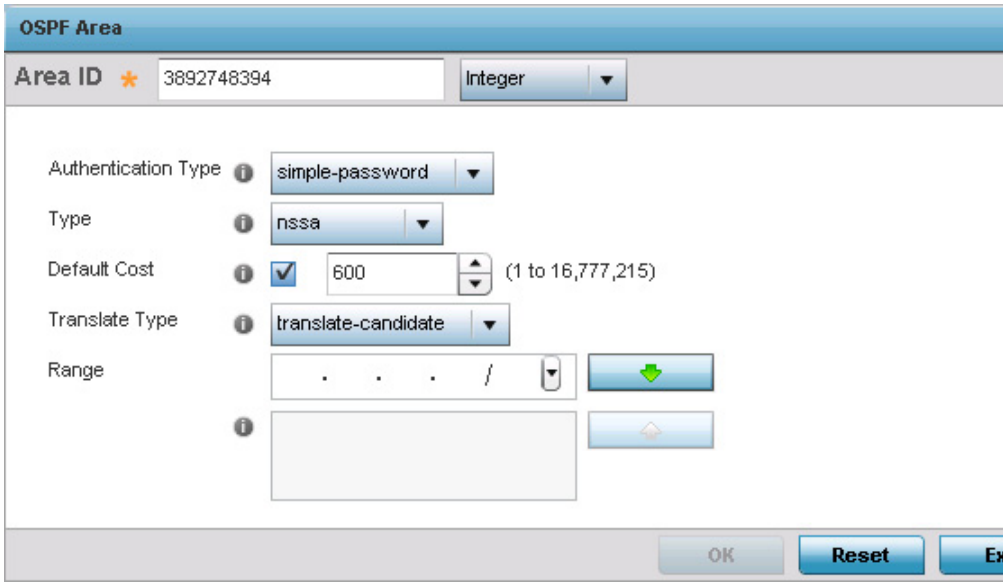


Figure 201: Device Overrides - Network - OSPF Area Configuration screen

17 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.

18 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

19 Select the **Interface Settings** tab.

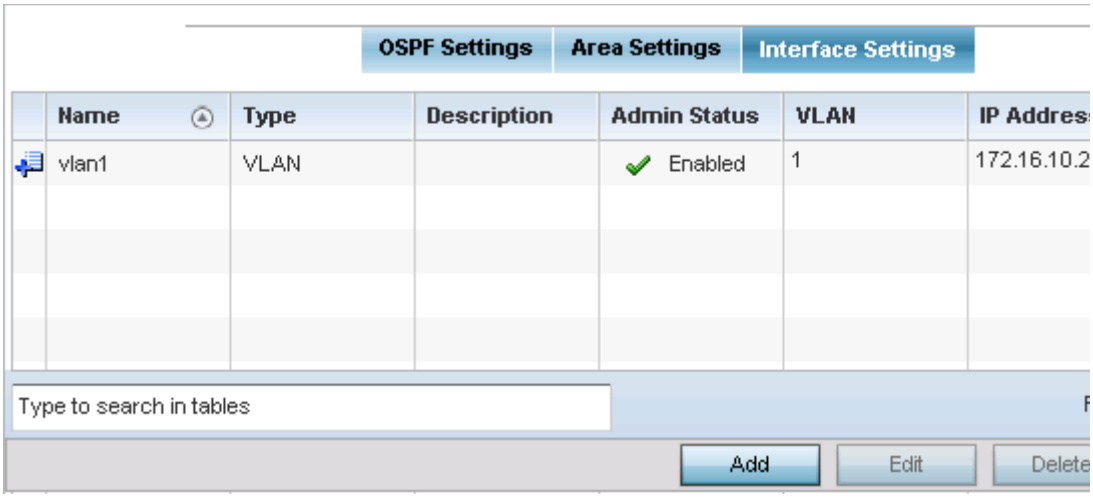


Figure 202: Device Overrides - Network - OSPF Interface Settings screen

20 Review existing **Interface Settings** using:

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 provided.

21 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.

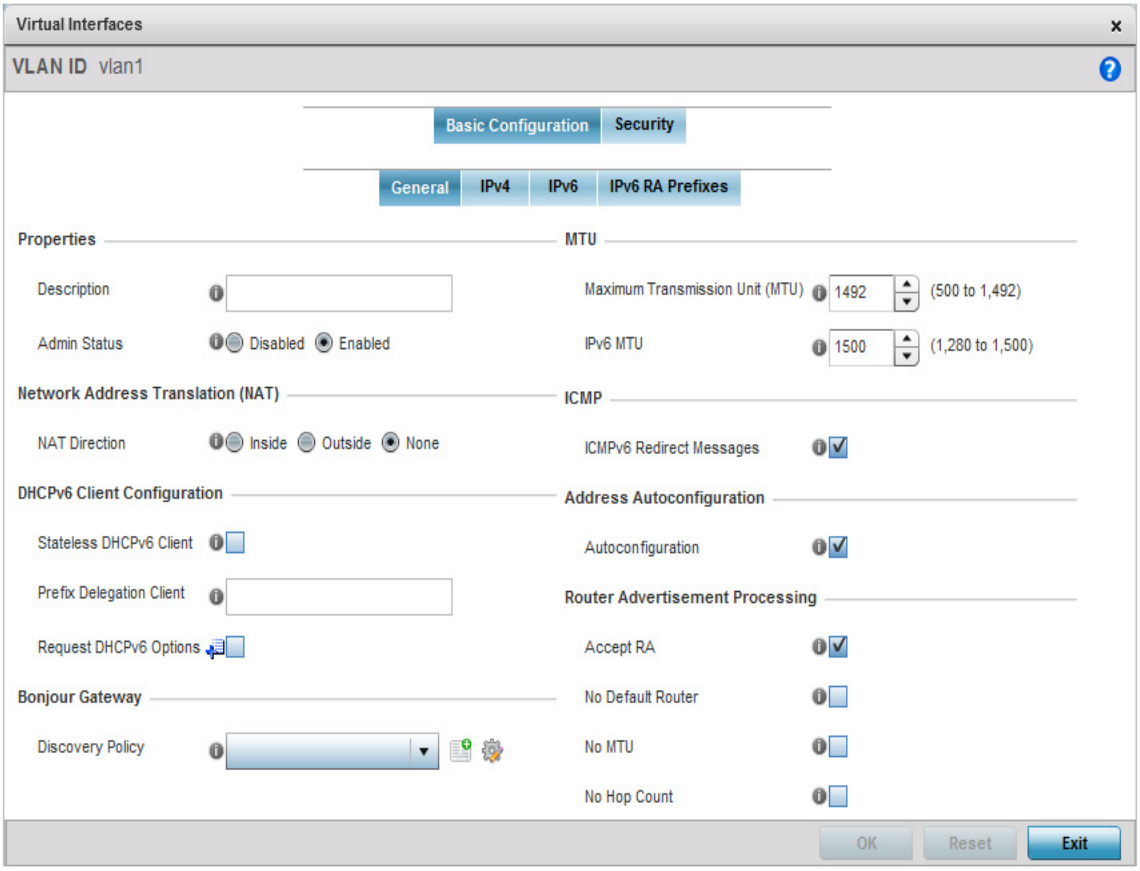


Figure 203: Device Overrides - Network - OSPF Virtual Interface - Basic Configuration screen

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.

22 If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID from 1 - 4094.

23 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.

24 Define the **Network Address Translation** (NAT) direction.

Select either the *Inside*, *Outside* or *None* radio buttons.

- *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.

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

26 Set the following **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 drop-down, select the Bonjour Gateway discover policy. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

27 Set the following **MTU** settings for the virtual interface:

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.
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.

28 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.

29 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.

30 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.

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

32 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

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

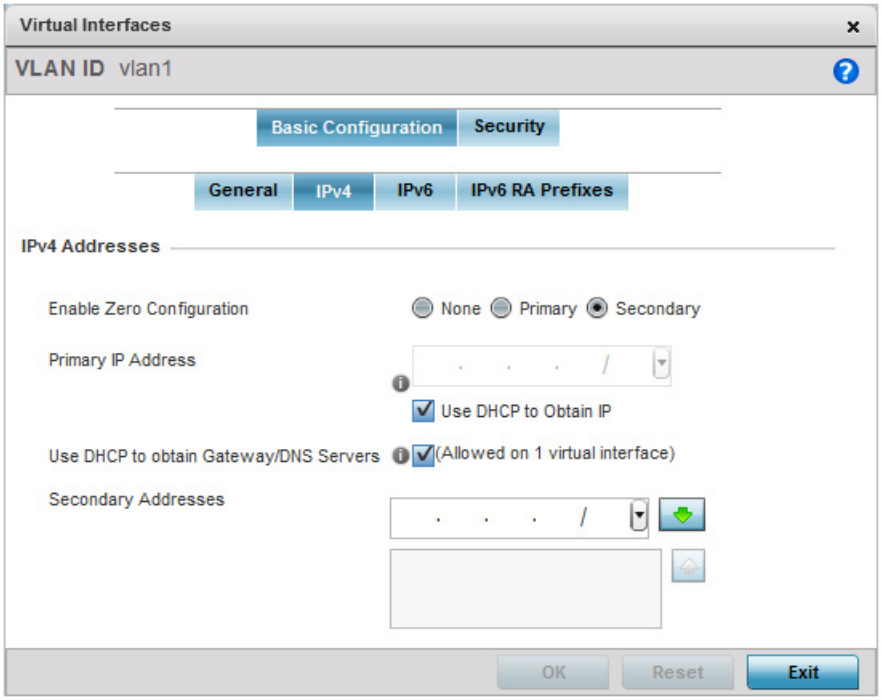


Figure 204: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv4 tab

33 Set the following network information from within 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 the *Secondary Addresses* 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.

34 Select OK to save the changes to the IPv4 configuration. Select Reset to revert to the last saved configuration.

35 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

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. 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.

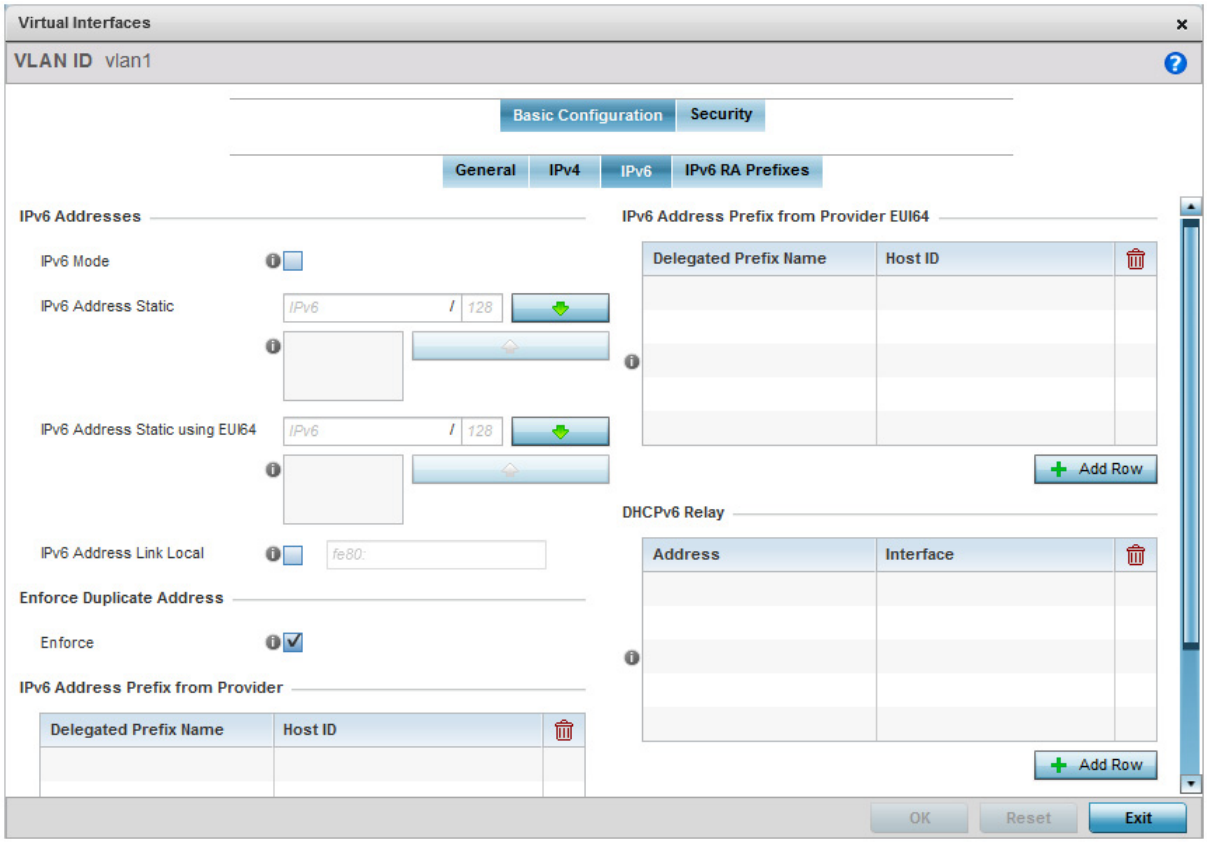


Figure 205: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab

36 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.

37 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.

38 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 sub screen wherein a new delegated prefix name and host ID can be defined.

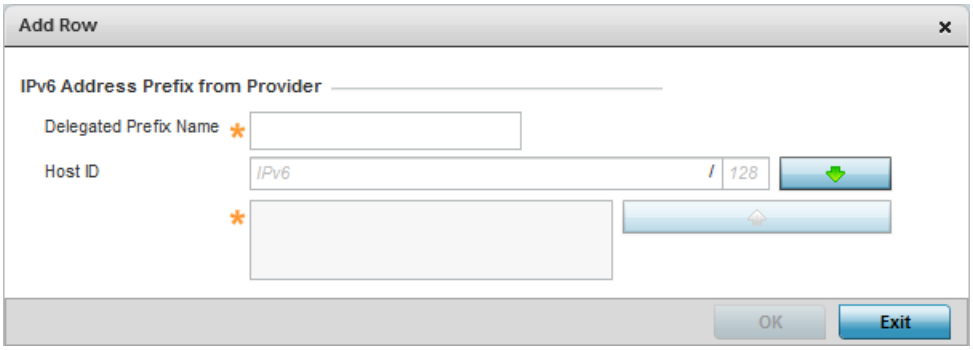


Figure 206: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider

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.

Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

39 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 sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

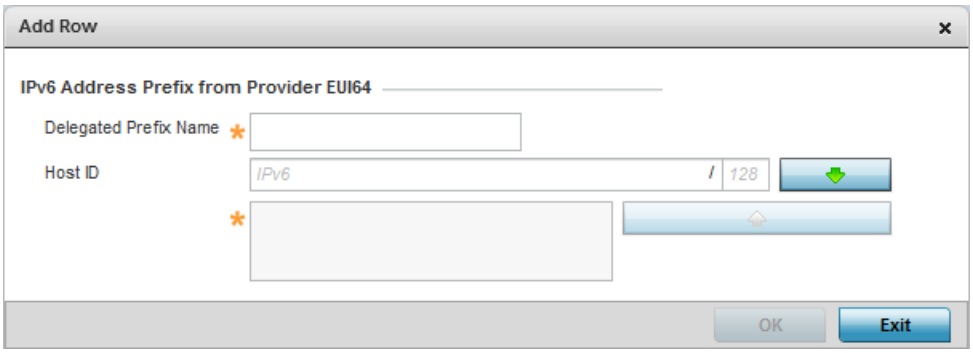


Figure 207: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64

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.

Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

40 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 sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.



Figure 208: Device Overrides - Network - OSPF 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.

Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

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

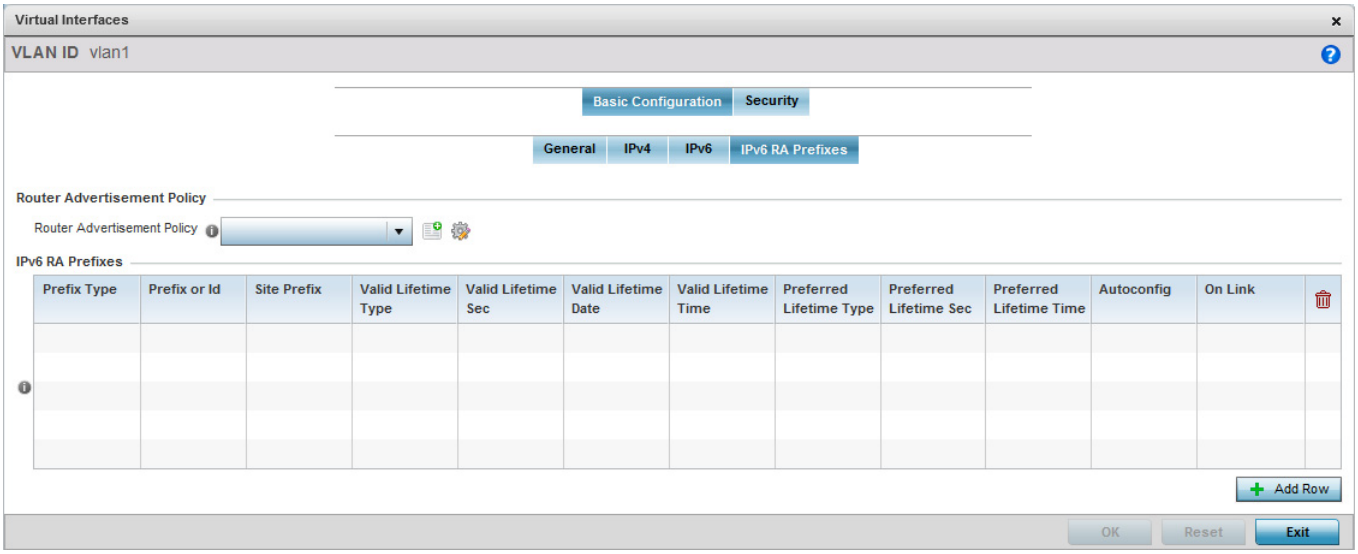


Figure 209: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab

42 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.

43 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

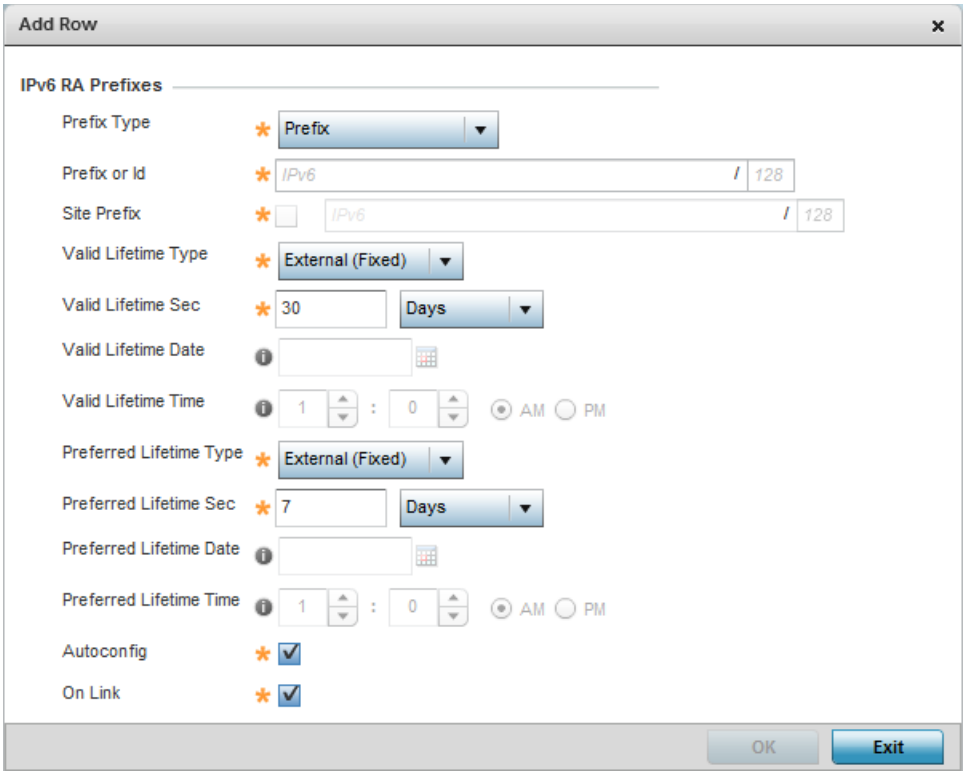


Figure 210: Device Overrides - Network - OSPF Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix

44 Set 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 *Internet Service Provider* (ISP) 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 end of 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 measurement 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.

45 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

46 Select the **OK** button to save the changes and overrides to the basic configuration. Select **Reset** to revert to the last saved configuration.

47 Select the **Security** tab.

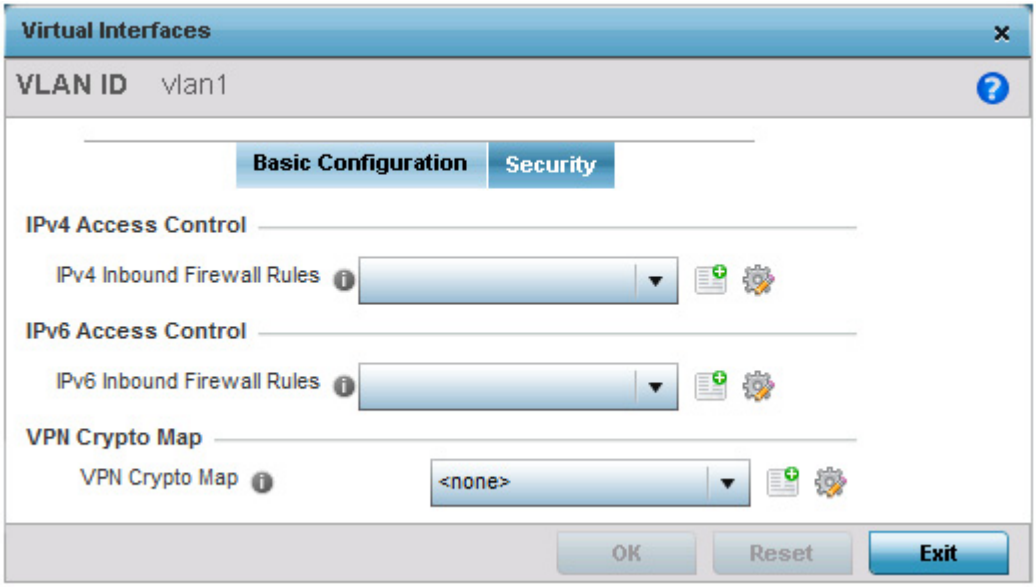


Figure 211: Device Overrides - Network - OSPF Virtual Interface - Security screen

48 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.

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* (IP) replacing IPv4. IPv6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

49 Select the **VPN Crypto Map** to use with this VLAN configuration. Use the drop-down menu to apply an existing crypto map configuration to this VLAN interface. Use the **Create** icon to create a new VPN Crypto Map or use the **Edit** icon to edit an existing VPN Crypto Map configuration before applying it to this VLAN.

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.

50 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

51 Select the **Dynamic Routing** tab.

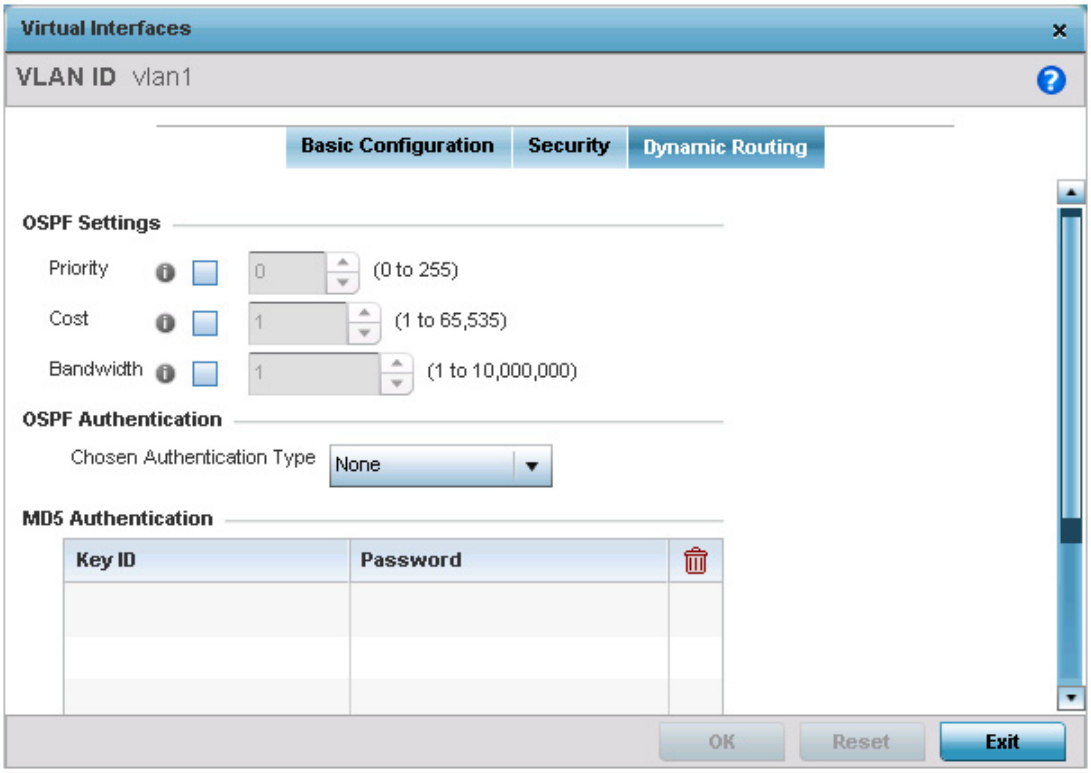


Figure 212: OSPF Virtual Interface - Dynamic Routing screen

52 Refer to the following to configure **OSPF Settings:**

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

53 Configure the **OSPF Authentication Type** settings by selecting from the drop-down list. The available options are *None*, *Null*, *simple-password* and *message-digest*.

54 Refer the following to configure **MD5 Authentication** keys. Click the **+ Add Row** button to add a row to the table.

Key ID	Set the unique MD5 Authentication key ID. The available key ID range is 1-255.
Password	Set the OSPF password. This value is displayed as “asterisk” (*). Select *Show* to display the actual characters comprising the password.

55 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

Overriding a Forwarding Database Configuration

“Overriding the Network Configuration”

A *Forwarding Database* is used by a bridge to forward or filter packets. The bridge reads the packet’s destination MAC address and 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 decide to filter or forward the packet.

This forwarding database assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

To define or override a forwarding database configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Forwarding Database**.



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* screen’s Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

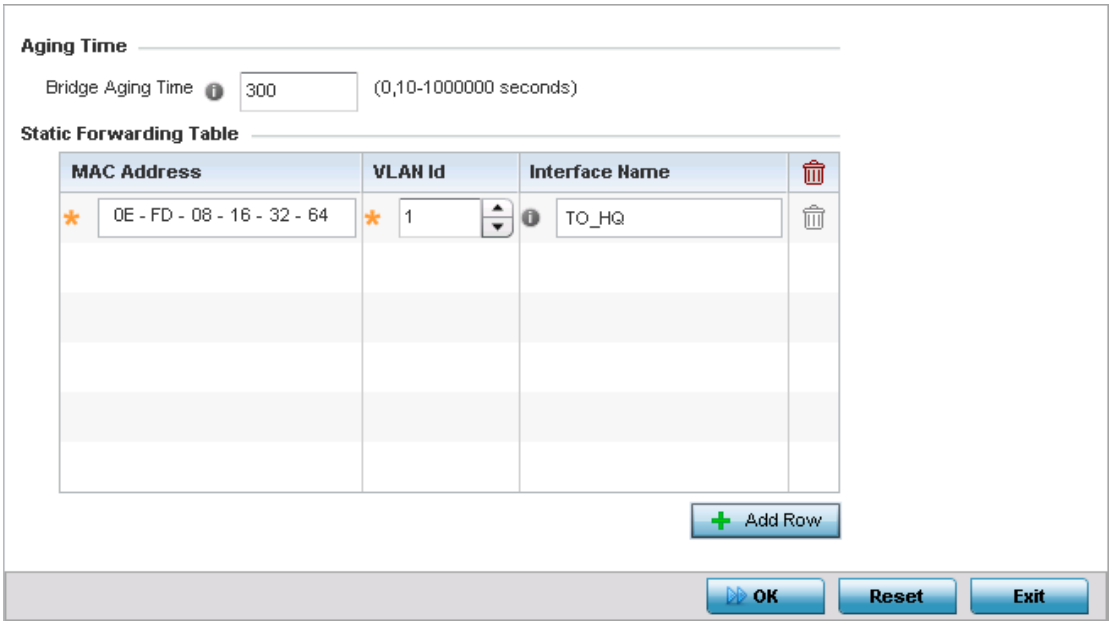


Figure 213: Device Overrides - Network Forwarding Database screen

6 Define or override 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 a bridge's forwarding table before being 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.

7 Use the **+ Add Row** button to create a new row within the **Static Forwarding Table**.

8 Set or override 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 is 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).

9 Define or override the target VLAN ID if the destination MAC is on a different network segment.

10 Provide an **Interface Name** used as the target destination interface for the target MAC address.

11 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

Overriding a Bridge VLAN Configuration

"Overriding the Network Configuration"

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical. VLANs are broadcast domains to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

For example, say several computers are used into conference room X and some into 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 entity, 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.

To define a Bridge VLAN configuration or override for a device profile:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Bridge VLAN**.



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* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

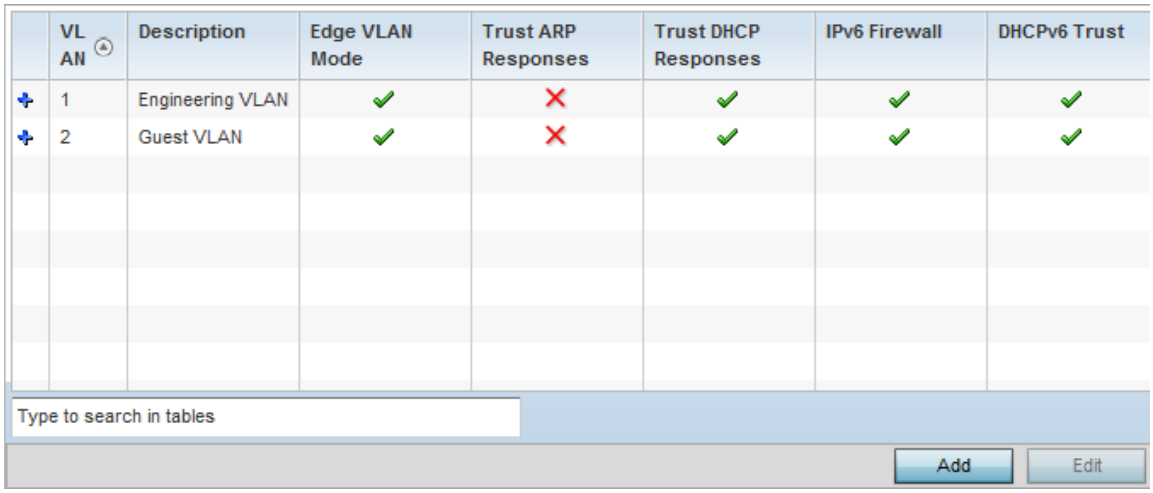


Figure 214: Device Overrides - Network Bridge VLAN screen

6 Review the following VLAN configuration parameters to determine whether an override is warranted:

VLAN	Lists the numerical identifier defined for the Bridge VLAN when it was initially created. The available range is from 1 - 4094. This value cannot be modified during the edit process.
Description	Lists a 64 character maximum 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. 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 be marked as an edge VLAN. When defining a VLAN as 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 check mark 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 check mark displays. When disabled, a red “X” displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.
IPv6 Firewall	Lists whether IPv6 is enabled on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. 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.
DHCPv6 Trust	Lists whether DHCPv6 responses are trusted on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. If enabled, only DHCPv6 responses are trusted and forwarded over the Bridge VLAN.
RA Guard	Lists whether *router advertisements* (RA) are allowed on this Bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. RAs are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

7 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify or override an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

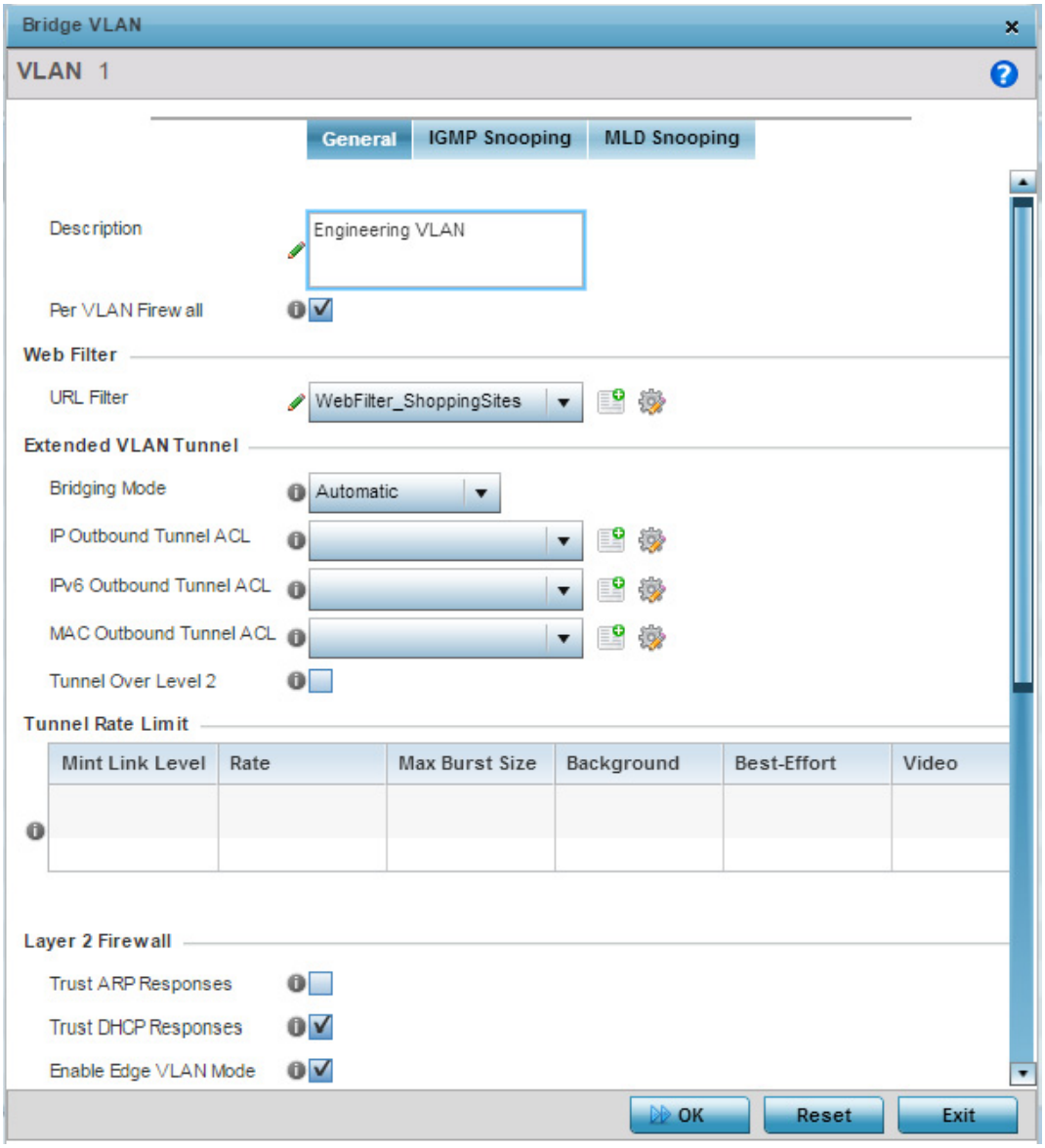


Figure 215: Device Overrides - Add Network Bridge VLAN screen

8 If adding a new Bridge VLAN configuration, use the spinner control to define or override a VLAN ID from 1 - 4094. This value must be defined and saved before the **General** tab can become enabled and the remainder of the settings defined.

9 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.

10 Select the **Per VLAN Firewall** option to enable firewall on this interface. Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate a large amount of flow tables that store information on the traffic allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory on the device that could be used for other critical purposes. With the Per VLAN

firewall feature enabled on an interface, flow tables are only generated for that interface, Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory that can be used for other purposes.

Firewall can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network.

11 Set or override the following **Web Filter** parameters. Web filters are used to control access to resources on the Internet.

URL Filter	Use the drop-down menu to select a URL filter to use with this Bridge VLAN.

12 Set or override the following **Extended VLAN Tunnel** parameters:



NOTE

If creating a mesh connection between two access points in Standalone AP mode, *Tunnel* must be selected as the bridging mode to successfully create the mesh link between the two access points.

Bridging Mode	Specify one of the following bridging mode for use on the VLAN: • *Automatic* - Select automatic mode to let the controller or service platform 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 traffic on the VLAN.
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.
IPv6 Outbound Tunnel ACL	Select an *IPv6 Outbound Tunnel ACL* for outbound traffic from the drop-down menu. If an appropriate outbound IPv6 ACL is not available, select the *Create* button.
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, select the *Create* button.
Tunnel Over Level 2	Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default.

13 Set the following **Tunnel Rate Limit** parameters:

Mint Link Level	Select the MINT link level from the drop-down menu.
Rate	Define a transmit 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 Bridge VLAN. 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 0 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion. The default burst size is 320 kbytes.
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%.

14 Set or override the following **Layer 2 Firewall** parameters:

Trust ARP Responses	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 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 IP address in the VLAN is not used for normal operations, as it is now designated to isolate devices and prevent connectivity. This feature is enabled by default.

15 Set the following **IPv6 Settings**:

IPv6 Firewall	Select this option to enable IPv6 on this Bridge VLAN. This setting is enabled by default.
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this Bridge VLAN. 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.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this Bridge VLAN. This setting is enabled by default.

16 Refer to the **Captive Portal** field to select an existing captive portal configuration to apply access restrictions to the Bridge VLAN configuration.

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.

If an existing captive portal does not suite the Bridge VLAN configuration, either select the **Edit** icon to modify an existing configuration or select the **Create** icon to define a new configuration that can be applied to the Bridge VLAN. For information on configuring a captive portal policy, see "Configuring Captive Portal Policies" on page 759.

17 Refer to the **Captive Portal Snoop IPv6 Subnet** field to configure the IPv6 clients to be excluded when snooping an IPv6 subnet for static wired captive portal clients. Multiple rows can be added to this field.

To add an entry to this field, select the **Add Row** button below this field

Subnet	Specify the IPv6 subnet on which to scan for wired captive portal clients.
Exclude IP	Specify the IPv6 address of the wired client to be excluded when snooping an IPv6 subnet for wired captive portal clients.

18 Click the **IGMP Snooping** tab to set or override the IGMP snooping configuration.

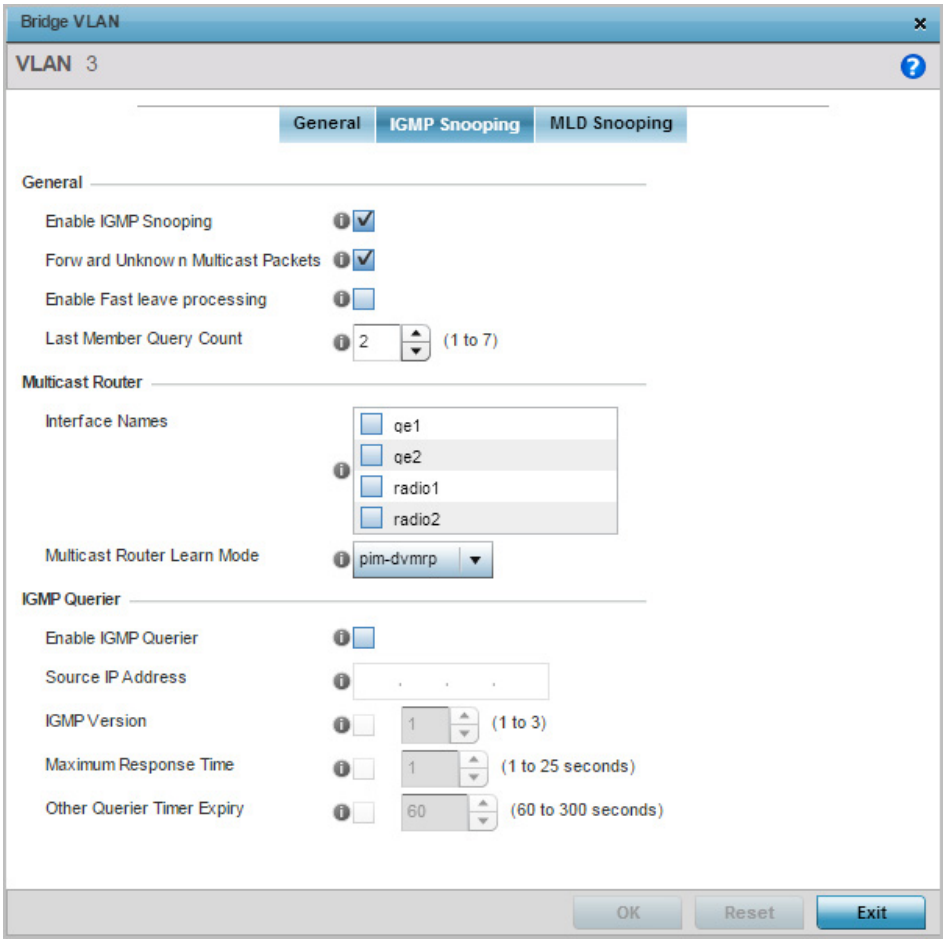


Figure 216: Device Overrides - Network Bridge VLAN - IGMP Snooping screen

19 Set the following parameters to configure **IGMP Snooping** values:

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on this Bridge VLAN is disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden.
Forward Unknown Multicast Packets	Select this option to enable the access point to forward multicast packets from unregistered multicast groups. If disabled, the *Unknown Multicast Forward* feature is also disabled for the selected VLANs. This setting is enabled by default.
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. This setting is disabled by default.
Last Member Query Count	Specify the number (1 - 7) of group specific queries sent before removing an IGMP snooping entry. The default settings is 2.

20 Set the following parameters for **Multicast Router** configuration:

Interface Name	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
Multicast Router Learn Mode	Set the learning mode to either *pim-dvmrp* or *static*. 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.

21 Set the following parameters 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 is primarily used in a network where there is a multicast streaming server and hosts subscribed to the server and no IGMP querier present. The controller can perform the IGMP querier role. 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 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 IGMP version 1, 2 or 3. The default IGMP version 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 IGMP snooping table. The access point only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller forwards these reports to the multicast router ports. The default setting is 10 seconds.
Other Querier Time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) to set a timeout interval for other querier resources. The default setting is 1 minute.

22 Select the **MLD Snooping** tab.

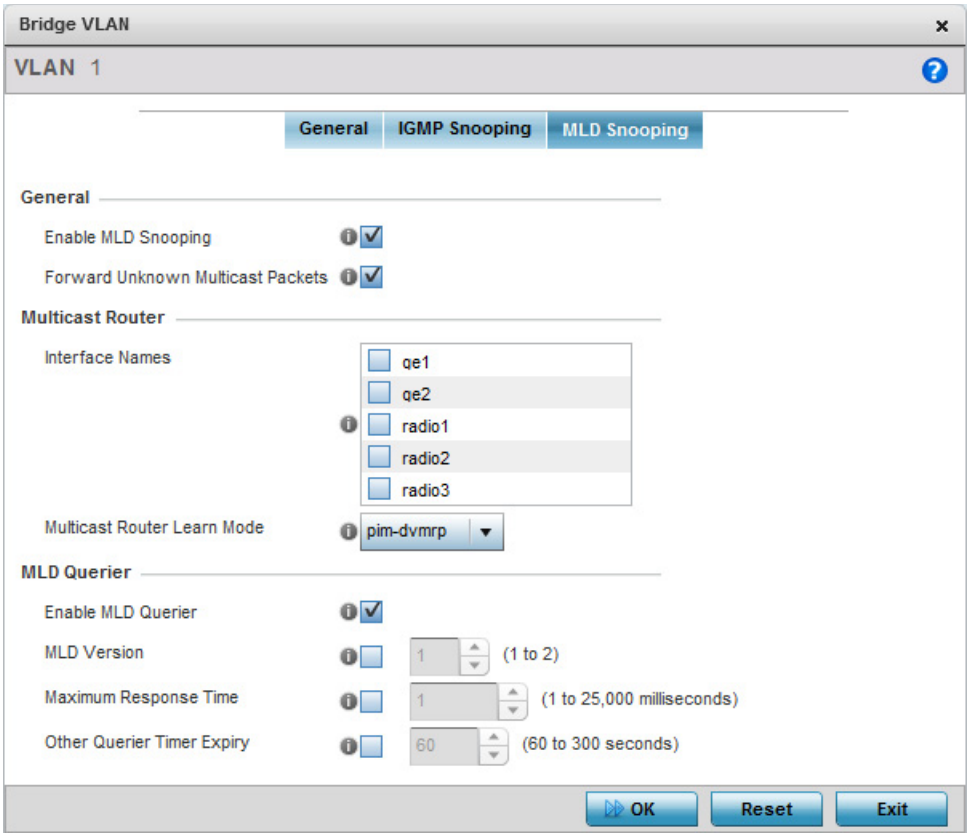


Figure 217: Device Overrides - Network Bridge VLAN screen, MLD Snooping tab

23 Define the following **General** MLD snooping parameters for the Bridge VLAN configuration:

Multicast Listener Discovery (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.

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 Multicast Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

24 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.

25 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

26 Select the **OK** button to save the changes and overrides to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

Overriding a Cisco Discovery Protocol Configuration

"Overriding the Network Configuration"

The *Cisco Discovery Protocol* (CDP) 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 configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Cisco Discovery Protocol**.

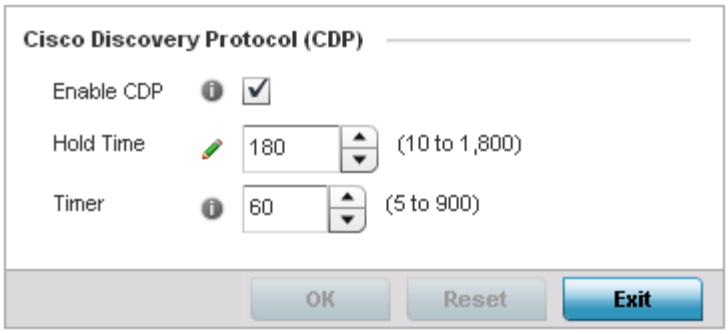


Figure 218: Cisco Discovery Protocol (CDP) screen

6 Enable/disable CDP and set the following timer settings:

Enable CDP	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default.
Hold Time	Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 180.
Timer	Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds.

7 Select the **OK** button located at the bottom right of the screen to save the changes and overrides to the CDP configuration. Select **Reset** to revert to the last saved configuration.

Overriding a Link Layer Discovery Protocol Configuration

"Overriding the Network Configuration"

The *Link Layer Discovery Protocol* (LLDP) 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 *Link Layer Discovery Protocol Data Unit* (LLDP PDU). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To override a profile's LLDP configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Link Layer Discovery Protocol**.

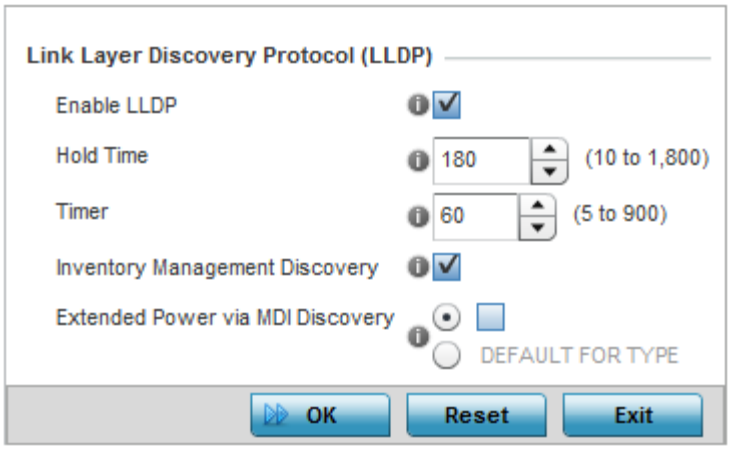


Figure 219: Link Layer Discovery Protocol (LLDP) screen

6 Set the following LLDP parameters for the profile configuration:

Enable LLDP	Select this option to enable LLDP on the access point. LLDP is enabled by default. When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them.
Hold Time	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds.
Timer	Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds.
Inventory Management Discovery	Select this option to include LLPD-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.
Extended Power via MDI Discovery	Select this option to include LLPD-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default.

7 Select the **OK** button to save the changes and overrides to the LLDP configuration. Select **Reset** to revert to the last saved configuration.

Overriding Miscellaneous Network Configuration

"Overriding the Network Configuration"

An access point profile can be configured to include a hostname in a DHCP lease for a requesting device and its profile. This helps an administrator track the leased DHCP IP address by hostname for a device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include a hostnames in DHCP request:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand side of the UI.

4 Select **Network** to expand its sub menu options.

5 Select **Miscellaneous**.

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* screen's Device Overrides field and select **Clear Overrides**. This will remove all overrides from the device.

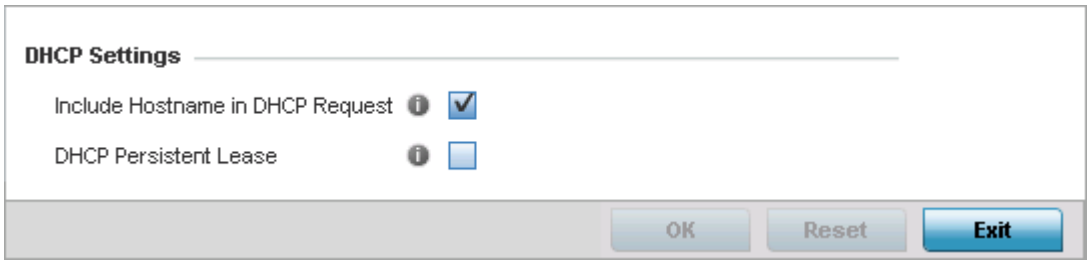


Figure 220: Device Overrides - Network Miscellaneous screen

6 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.

7 Select the **DHCP Persistent Lease** option to retain the last DHCP lease used across a reboot if the access point's designated DHCP server is unavailable. This feature is enabled by default.

8 Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

Overriding Alias Configuration

"Overriding the Network Configuration"

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

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

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

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

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

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

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

Alias can be classified as:

- "Network Basic Alias"
- "Network Group Alias"
- "Network Service Alias"

Network Basic Alias

"Overriding Alias Configuration"

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

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

To override a basic alias configuration:

1 Select **Devices** from the **Configuration** tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand side of the UI.

4 Select **Network** to expand it and display its sub menus.

5 Select the **Alias** item, the **Basic Alias** screen displays.

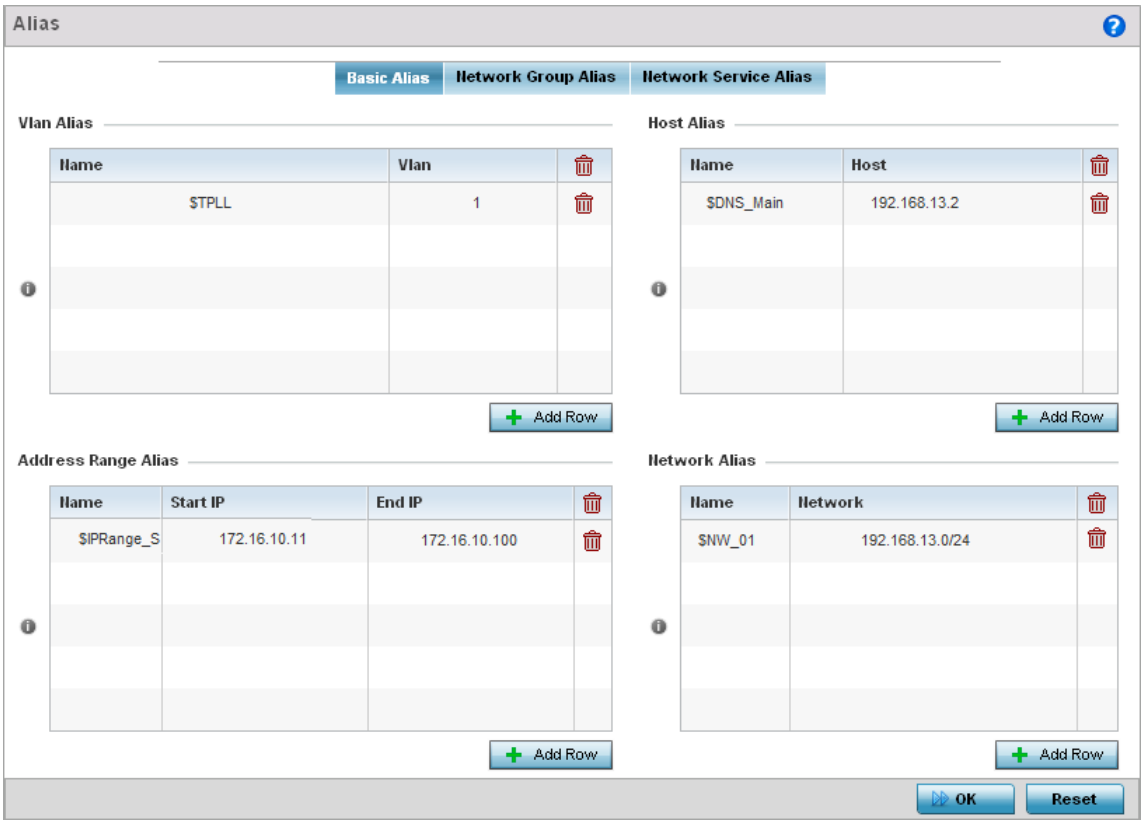


Figure 221: Device Overrides - Network - Basic Alias screen

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

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

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

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

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

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

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

- IP Firewall Rules
- DHCP

8 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 a ending IP address used with a range of addresses utilized with the address range alias.

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

9 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*.

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

- IP Firewall Rules

- DHCP

10 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 string value to use in the alias.

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

11 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

"Overriding Alias Configuration"

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

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

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

To edit or delete a network alias configuration:

1 Select **Devices** from the **Configuration** tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand side of the UI.

4 Select **Network** to expand it and display its sub menus.

5 Select the **Alias** item, the **Basic Alias** screen displays.

6 Select the **Network Group Alias** tab.

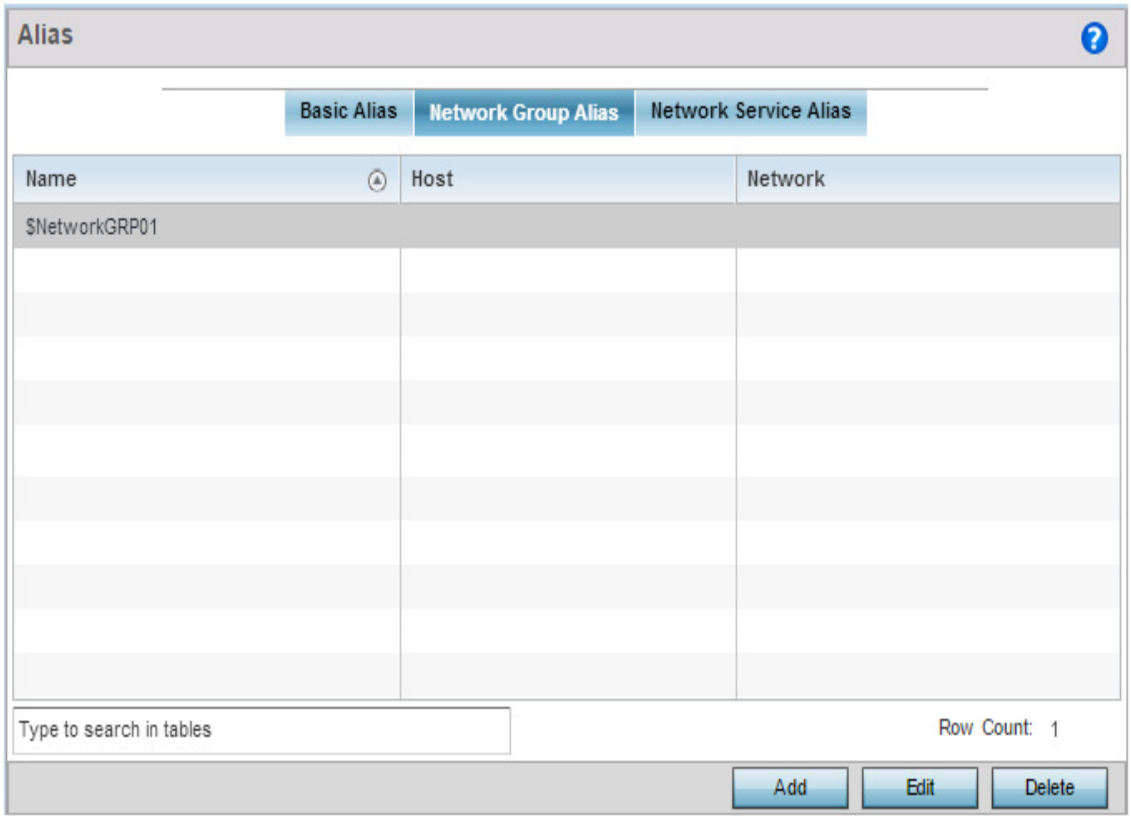


Figure 222: Device Overrides - Network - Alias - Network Group Alias screen

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

7 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Group Alias**. **Copy** to copy an existing policy or **Rename** to rename an existing policy.

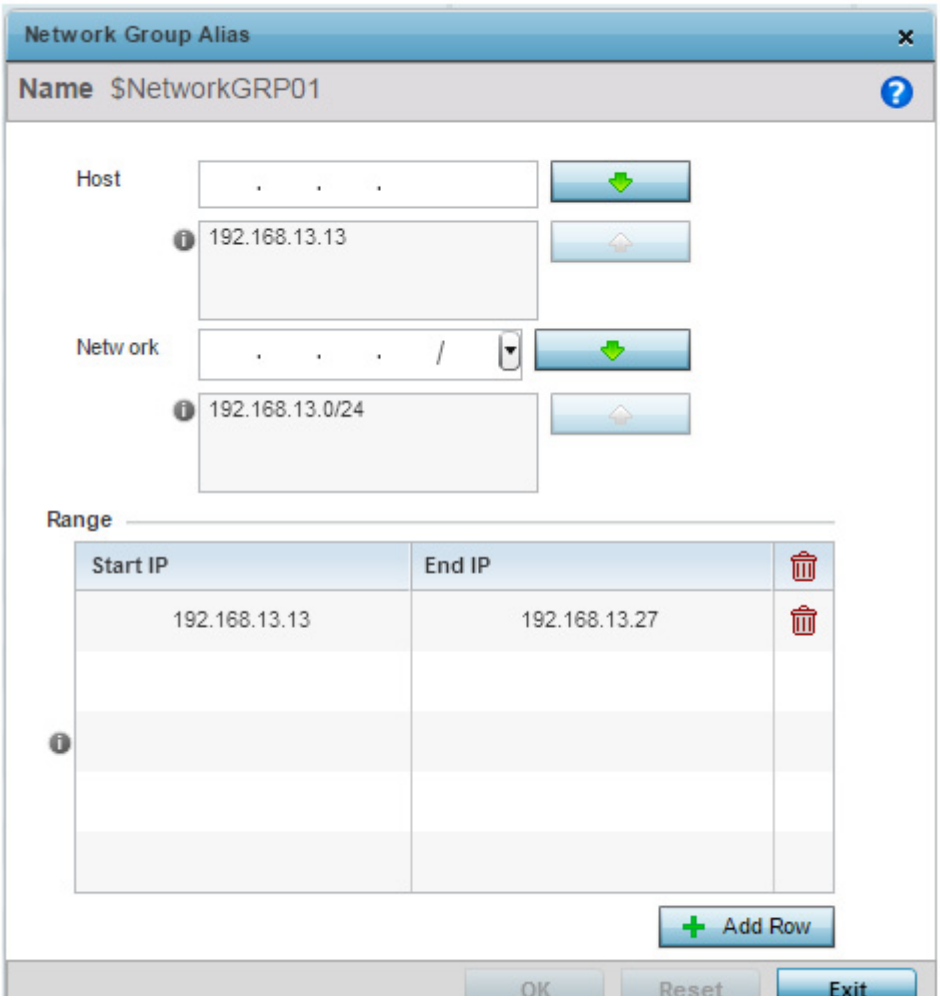


Figure 223: Device Overrides - Network - Alias - Network Group Alias Add screen

8 If adding a new **Network Group Alias**, provide it a name of up to 32 characters.

NOTE

The Network Group Alias Name always starts with a dollar sign ($).

9 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.

10 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 an alias range entry to edit it.

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

Network Service Alias

"Overriding Alias Configuration"

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.

A *network service alias* can be used in IP firewall rules to substitute protocols and ports:

To edit or delete a service alias configuration:

1 Select **Devices** from the **Configuration** tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand side of the UI.

4 Select **Network** to expand it and display its sub menus.

5 Select the **Alias** item, the **Basic Alias** screen displays.

6 Select the **Network Service Alias** tab.

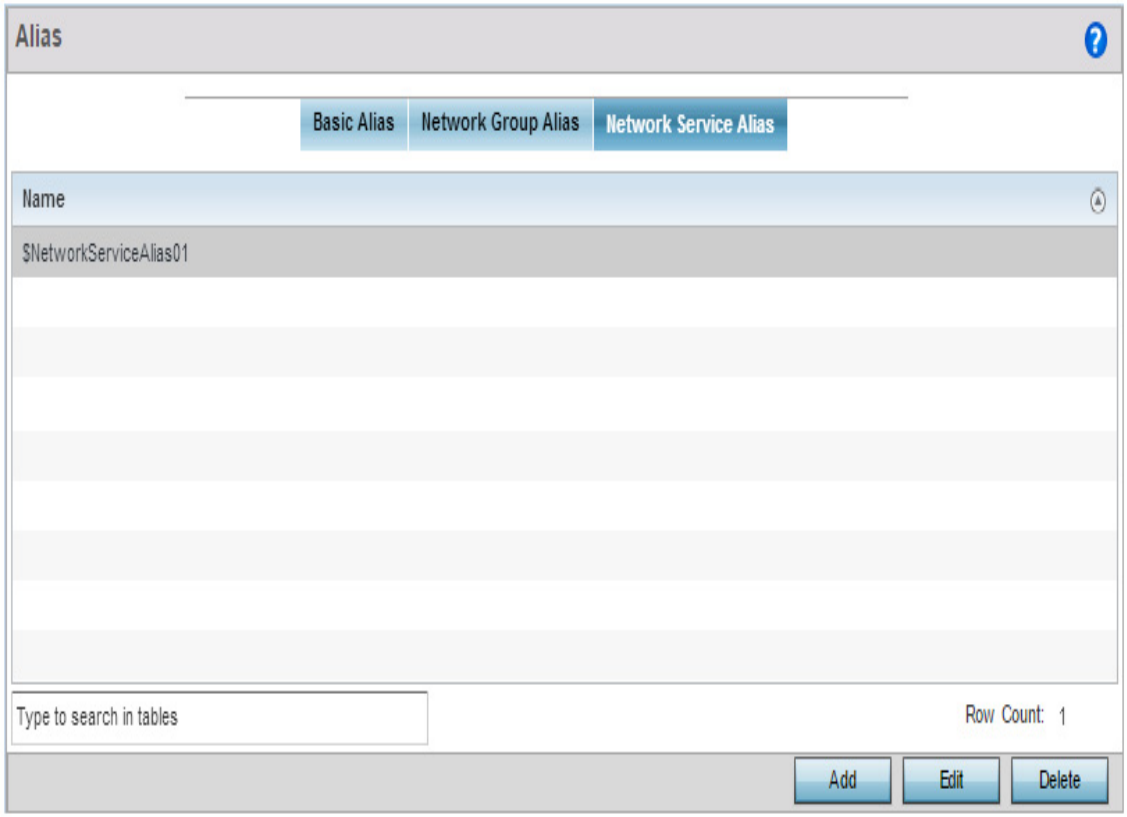


Figure 224: Device Overrides - Network - Alias - Network Service Alias screen

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

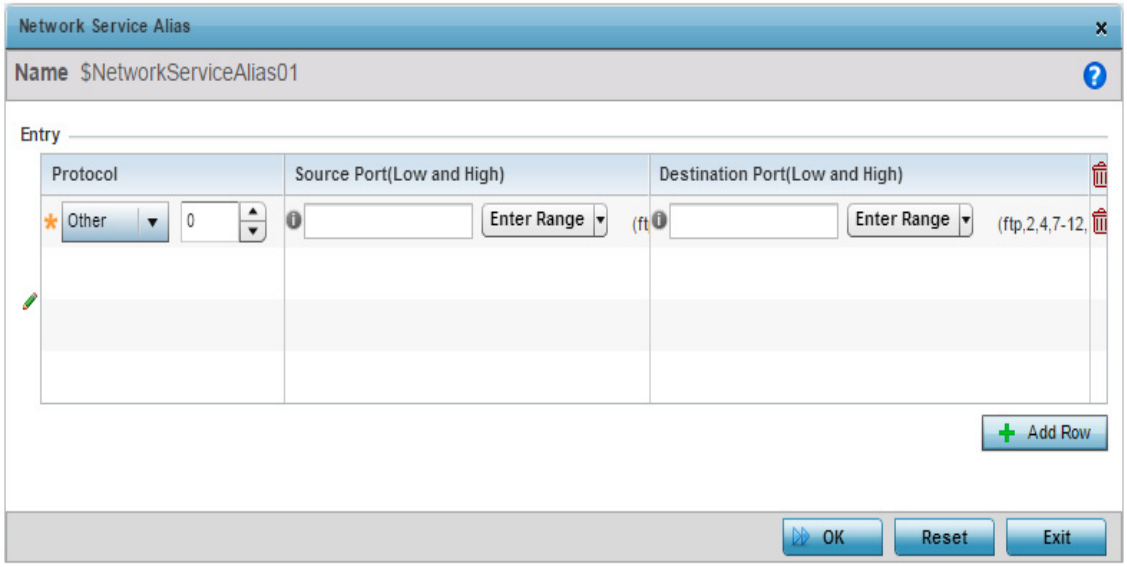


Figure 225: Device Overrides - Network - Alias - Network Service Alias Add screen

8 If adding a new **Network Service Alias**, provide it a name up to 32 characters.

NOTE

The Network Group Alias Name always starts with a dollar sign ($).

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

Protocol	Specify the protocol for which the alias has to be created. Use the drop-down 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)	Use this field only if the protocol is *tcp* or *udp*. Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	Use this field only if the protocol is *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

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

Overriding IPv6 Neighbor Configuration

"Overriding the Network 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 Select **Devices** from the **Configuration** tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand side of the UI.

4 Select **Network** to expand it and display its sub menus.

5 Select **IPv6 Neighbor**.

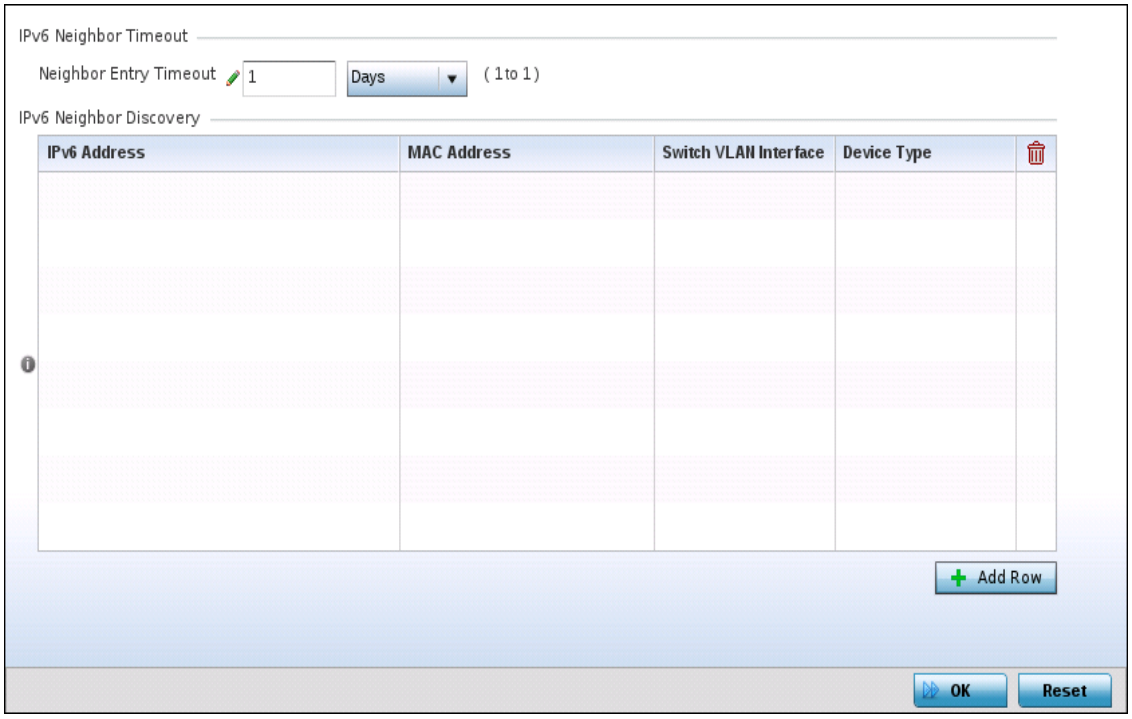


Figure 226: IPv6 Neighbor screen

6 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.

7 Select **+ Add Row** to define the configuration of **IPv6 Neighbor Discovery** configurations. A maximum of 256 neighbor entries can be defined.

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*.

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

Overriding Security Configuration

"Device Overrides"

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy applied. If an existing firewall, client role or NAT policy is unavailable create the required security policy configuration. Once created, a configuration can have an override applied as needed to meet the changing data protection requirements of a device's deployed environment. However, in doing so this device must now be managed separately from the profile configuration shared by other identical models within the network.

For more information on applying an override to an existing device profile, refer to the following sections:

- "Overriding VPN Configuration using Wizards"
- "Overriding Auto IPSec Tunnel Settings"
- "Overriding General Security Settings"
- "Overriding a Certificate Revocation List (CRL) Configuration"
- "Overriding RADIUS Trustpoint Configuration"
- "Overriding NAT Configuration"
- "Overriding the Profile's Bridge NAT Configuration"
- "Overriding a Profile's Application Visibility Settings"

Overriding VPN Configuration using Wizards

"Overriding Security Configuration"

VPN can be overridden by using either the inbuilt wizards or by manually configuring the required parameters. This section describes how to use the inbuilt wizards to override the VPN parameters. The user interface provides two (2) wizards that provide different levels of configuration.

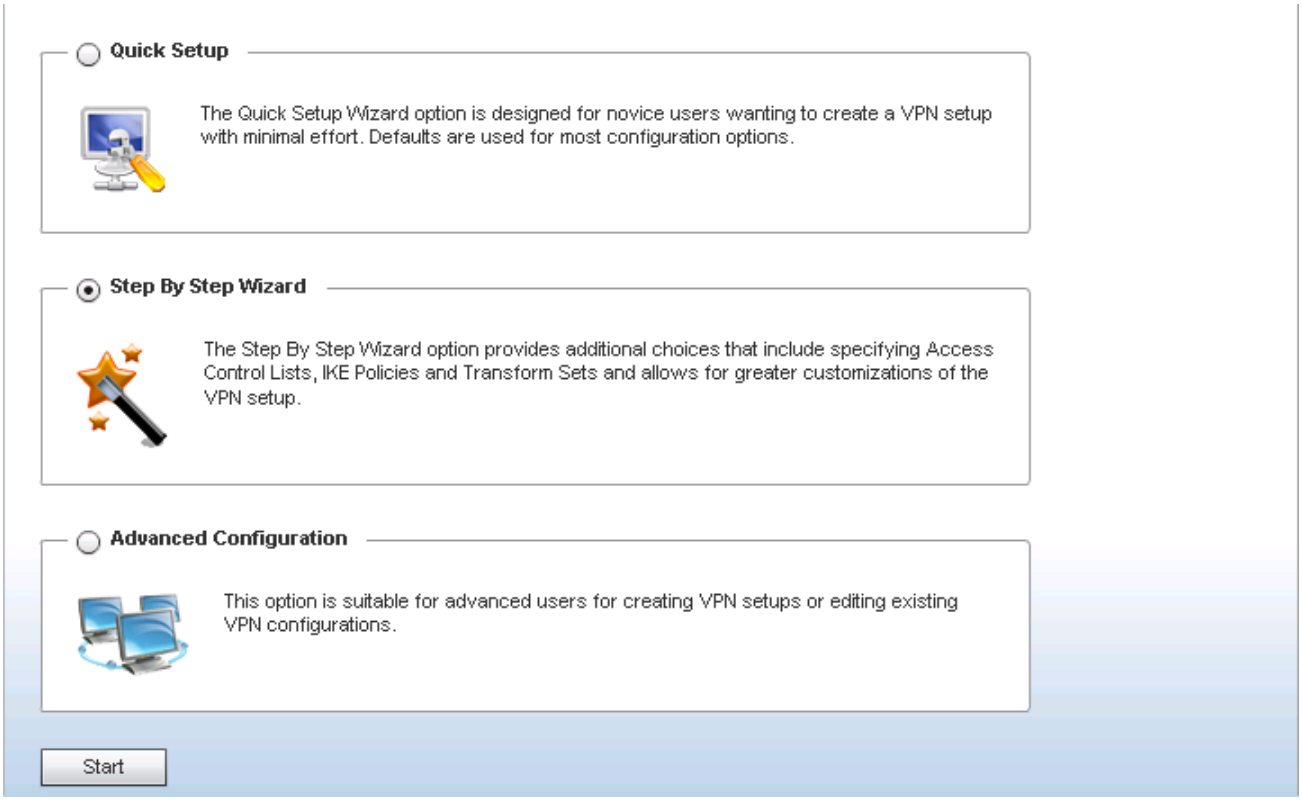


Figure 227: Security Configuration Wizard screen

The following options are available:

- "Quick Setup Wizard" – Use this wizard to setup basic VPN Tunnel on the device. This wizard is aimed at novice users and enables them to setup a basic VPN with minimum effort. This wizard uses default values for most of the parameters.
- "Step By Step Wizard" – Use this wizard to setup a VPN Tunnel step by step. This wizard is aimed at intermediate users who require the ability to customize some of the parameters.
- Advanced Configuration – Use this option to configure the VPN parameters manually.

Click the **Start** button to display the next screen for the wizards or when **Advanced Configuration** is selected, to display the VPN screen.

Quick Setup Wizard

"Overriding General Security Settings"

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

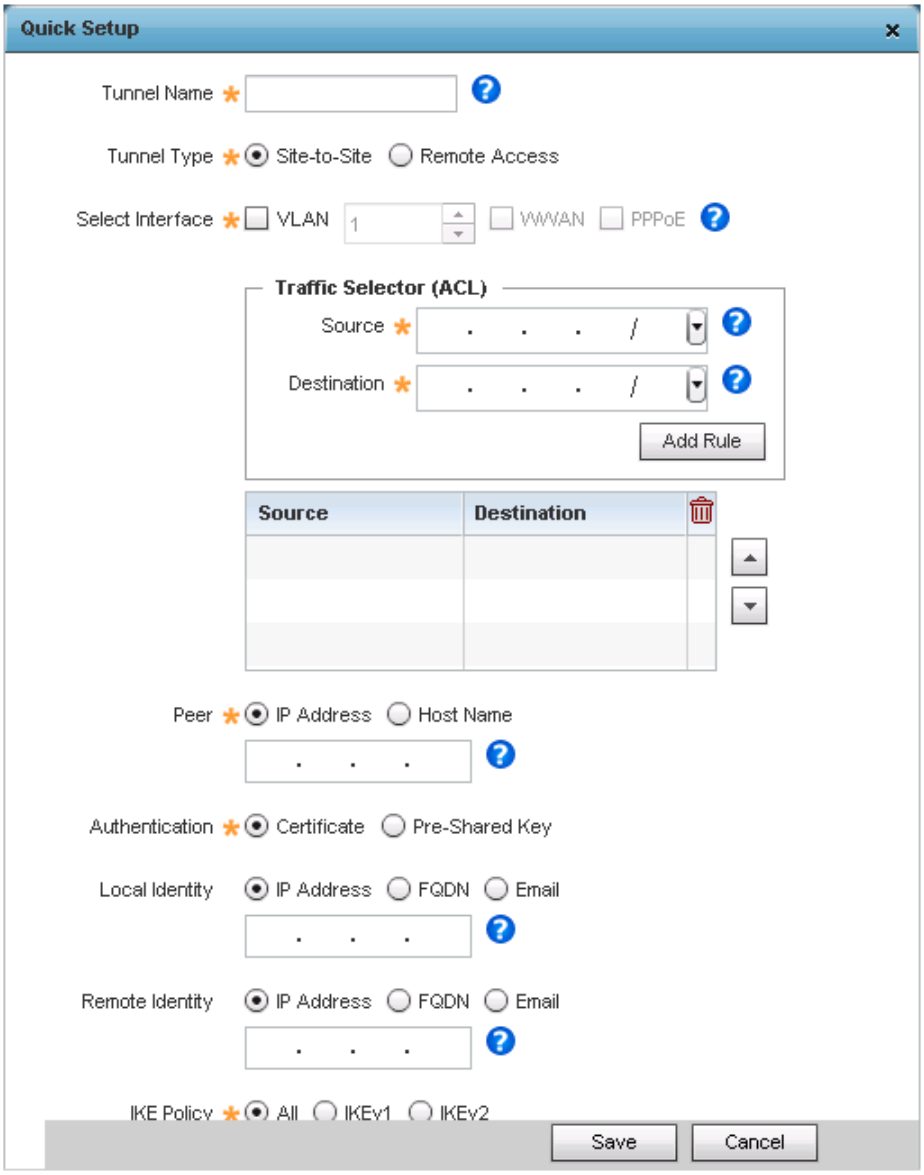


Figure 228: VPN Quick Setup Wizard

1 Provide the following information to configure a VPN tunnel:

Tunnel Name	Provide a name for the tunnel. Tunnel name must be such that it easily identifies the tunnel uniquely.
Tunnel Type	Configure the tunnel type as one of the following: • *Site-to-Site* – Provides a secured connection between two sites • *Remote Access* – Provides access to a network to remote devices.
Select Interface	Configure the interface for creating the tunnel. The following options are available: • *VLAN* – Configures the tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number. • *WWLAN* – Configures the tunnel over the WWLAN interface. • *PPPoE* – Configures the tunnel over the PPPoE interface.
Traffic Selector (ACL)	Configure ACLs that manage the traffic passing through the VPN Tunnel. • *Source* – Provide the source network along with its mask • *Destination* – Provide the destination network along with its mask.
Peer	Configures the peer for this tunnel. The peer device can be specified either by its hostname or by its IP address.
Authentication	Configure the authentication used to identify peers. The following can be configured: • *Certificate* – Use a certificate to authenticate • *Pre-Shared Key* – Use a pre-shared key to authenticate.
Local Identity	Configure the local identity used with 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 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 IKE policy to use. IKE is used to exchange authentication keys. Select from one of the following: • *All* – Uses any IKE policy. • *IKE1* – Uses IKE 1 only • *IKE2* – Uses 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 menu.

2 Click the **Save** button to save the VPN Tunnel configuration. To exit without saving, click **Cancel**.

Step By Step Wizard

"Overriding General Security Settings"

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

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 Select the **Step-By-Step Wizard** option from the VPN screen.

2 Click the **Start** button.

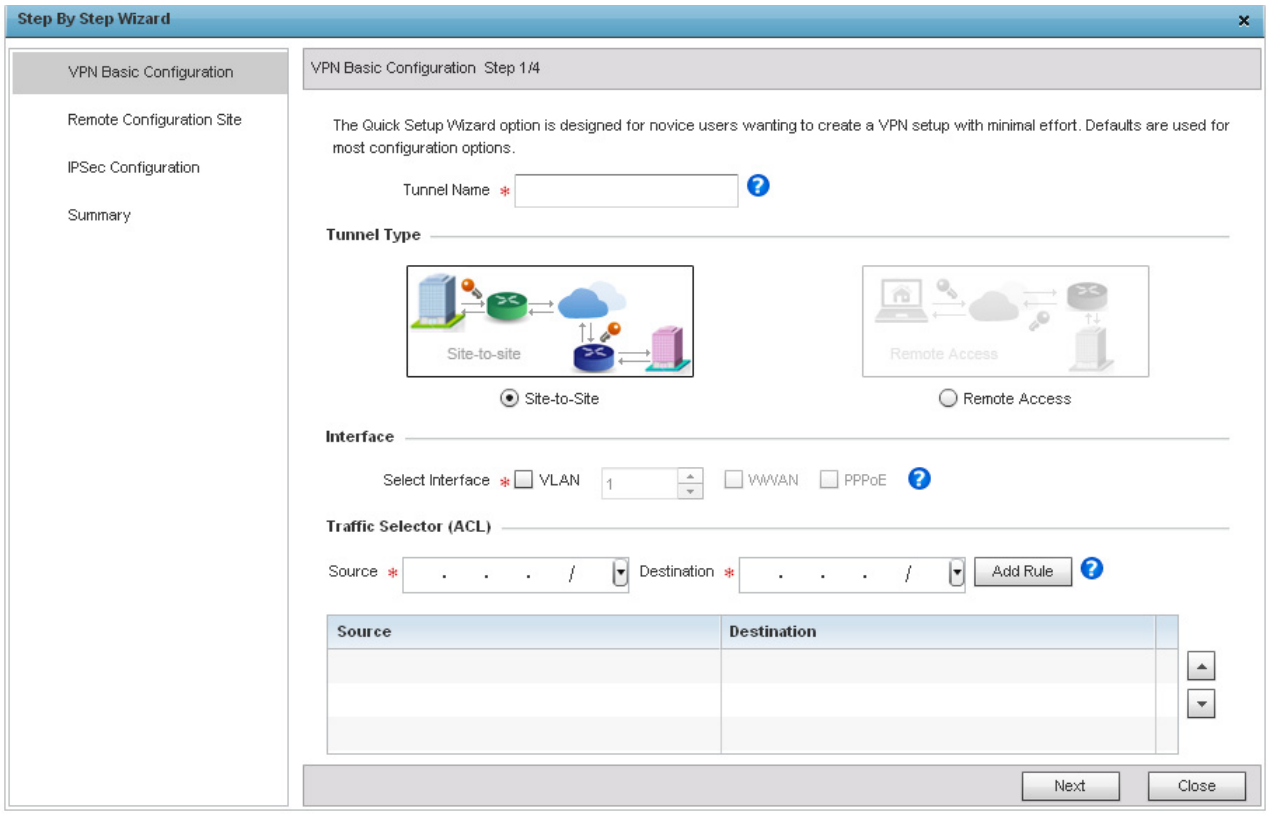


Figure 229: VPN Step-By-Step Wizard - Step 1

3 Define the following:

Tunnel Name	Provide a name for the tunnel in the *Tunnel Name* field.
Tunnel Type	Select the tunnel type being created. Two types of tunnels can be created. *Site to Site* is used to create a tunnel between two remote sites as indicated in the image. *Remote Access* is used to create a tunnel between an user device and a network as indicated in the image.
Interface	Select the interface to use. Interface can be a *Virtual LAN (VLAN)* or *WWAN* or *PPPoE* depending on the interfaces available on the device.
Traffic Selector (ACL)	This field 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 the *Add Rule* button to add the rule into the ACL.

4 Click the **Next** button to go to Step 2.

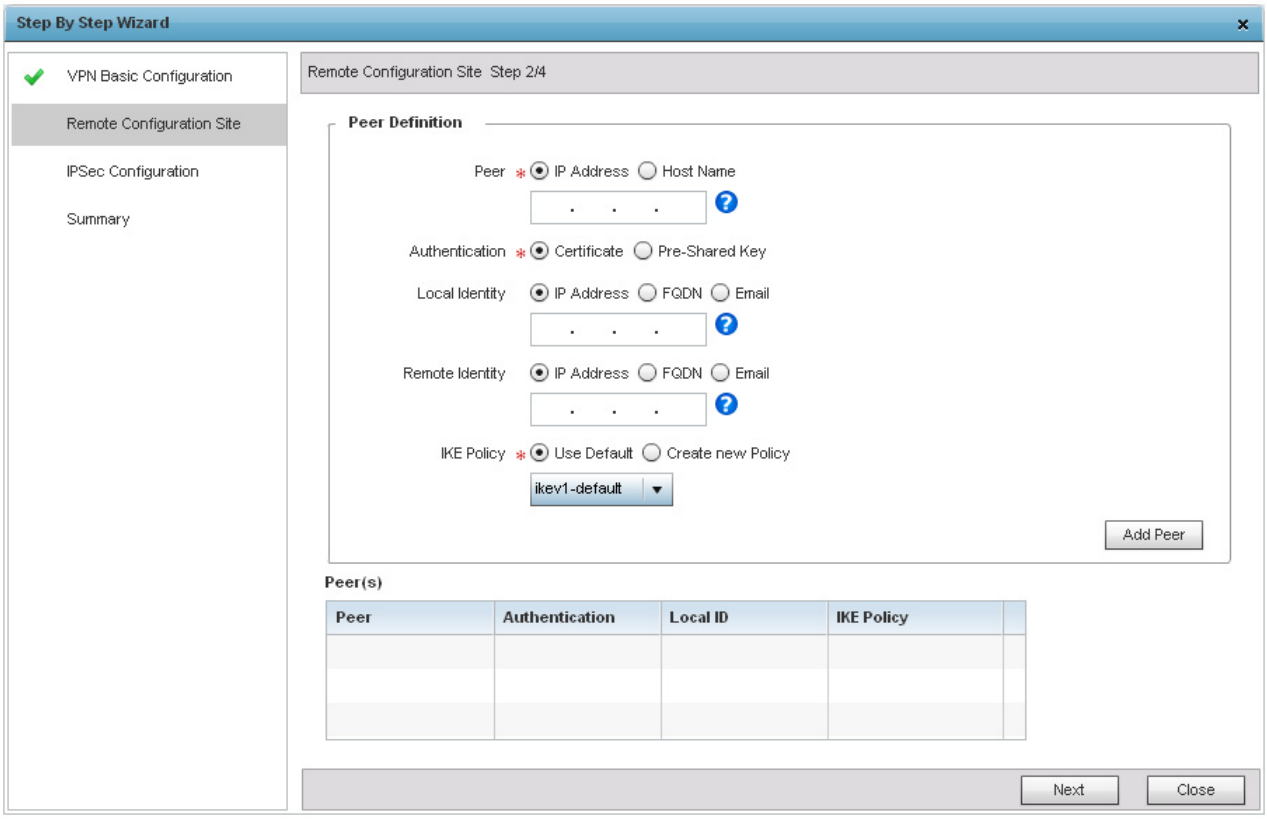


Figure 230: VPN Step-By-Step Wizard - Step 2

5 In *Step 2* screen, configure the following parameters:

Peer	Select the type of peer for this device when forming a tunnel. Peer information can be either *IP Address* or *Host Name*. Provide the IP address or the hostname of the peer device.
Authentication	Configure how the devices authenticate with each other. • *Certificate* – The devices use certificates to validate credentials. • *Pre-Shared Key* – The devices use pre-shared key to authenticate.
Local Identity	Configure the local identity for the VPN Tunnel. • *IP Address* – The local identity is an IP address. • *FQDN* – The local identity is a *Fully Qualified Domain Name* (FQDN). • *Email* – The local identity is an E-mail address.
Remote Identity	Configure the remote identity for the VPN Tunnel. • *IP Address* – The remote identity is an IP address. • *FQDN* – The remote identity is a *Fully Qualified Domain Name* (FQDN). • *Email* – The remote identity is an E-mail address.
IKE Policy	Configure the IKE policy to use when creating this VPN Tunnel. The following options are available: • *Use Default* – Click this option to use the default IKE profiles. Select one of *ike1-default* or *ike2-default*. • *Create new Policy* – Click this option to create a new IKE policy.

6 Click the **Add Peer** button to add the Tunnel peer information into the *Peer(s)* table. This table lists all the peers configured for the VPN Tunnel.

7 Click the **Next** button to go to the next configuration screen. Use the **Back** button to go to the previous step.

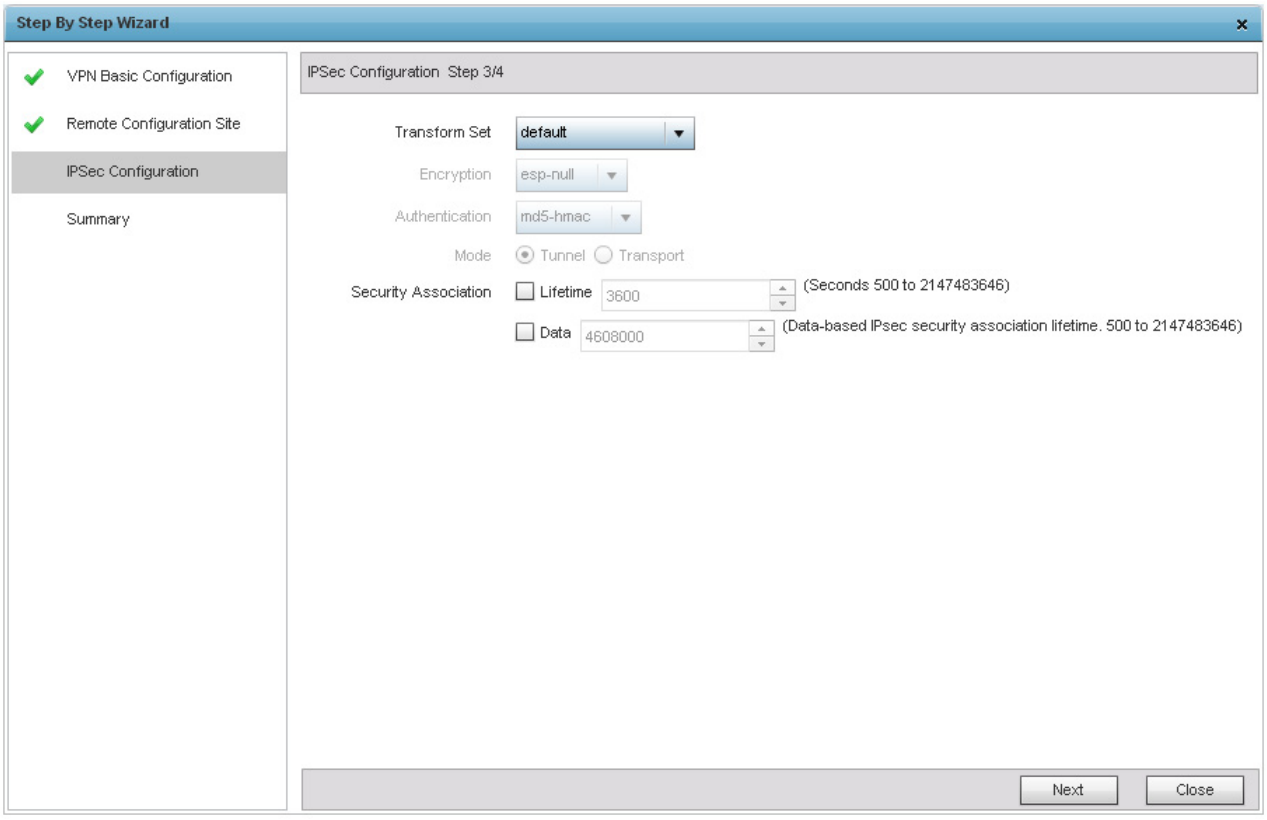


Figure 231: VPN Step-By-Step Wizard - Step 3

8 Configure the following IPSec parameters:

Transform Set	Transform set is a set of configurations exchanged for creating the VPN tunnel and impose a security policy.The transform set is comprised 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, select any pre-configured Transform Set or click the *Create New Policy* to create a new transform set.
Encryption	This field is enabled when *Create New Policy* is selected in *Transform Set* field. This is the encryption that is used on data traversing through the tunnel. Select from *esp-null*, *des, 3des, aes, aes-192* and *aes-256* algorithms.
Authentication	This field is enabled when *Create New Policy* is selected in *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 *sha256-hmac, aes-xcbc-mac, MD5* or *SHA.* The option *aes-xcbc-mac* is not available on AP7131, AP7181, AP8132, AP82XX, RFS4000, RFS6000 and RFS7000 platforms.
Mode	This field is enabled when *Create New Policy* is selected in *Transform Set* field. The mode indicates how packets are transported through the tunnel. • *Tunnel* – Use this mode when the tunnel is between two routers or servers. • *Transport* – Use this mode when the tunnel is created between a client and a server.
Security Association	Configures the lifetime of a *security association* (SA). Keys and SAs should be periodically renewed to maintain security of the tunnel. • *Lifetime* – Duration in seconds after which the keys should be changed. Set a value in from 500 - 2,147,483,646 seconds. • *Data* – The key is changed after this quantity of data has be encrypted/ decrypted. Set a value from 500 - 2,147,483,646 KBs.

9 Click the **Next** button to go to the next configuration screen. Use the **Back** button to go to the previous step.

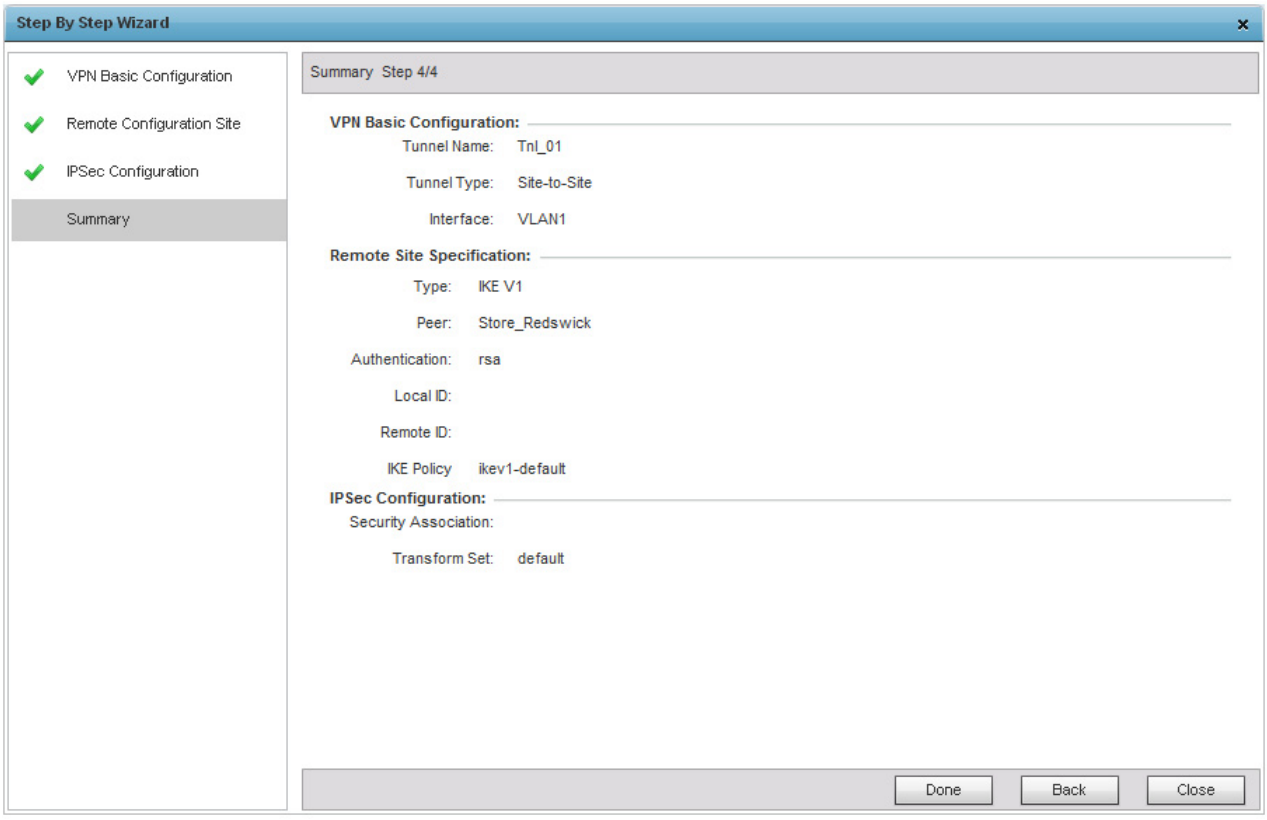


Figure 232: VPN Step-By-Step Wizard - Step 4

10 Review the configuration and click the **Done** button to create the VPN tunnel. Use the **Back** button to go back to previous screen for making modifications to the configuration. Click **Close** to close the wizard without creating a VPN Tunnel.

Overriding Auto IPSec Tunnel Settings

"Overriding Security Configuration"

IPSec tunnels are established to secure traffic, data and management traffic, from access points to remote wireless controllers. Secure tunnels must be established between access points and the wireless controller with minimum configuration pushed through DHCP option settings.

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **Auto IPSec Tunnel** to configure its parameters.

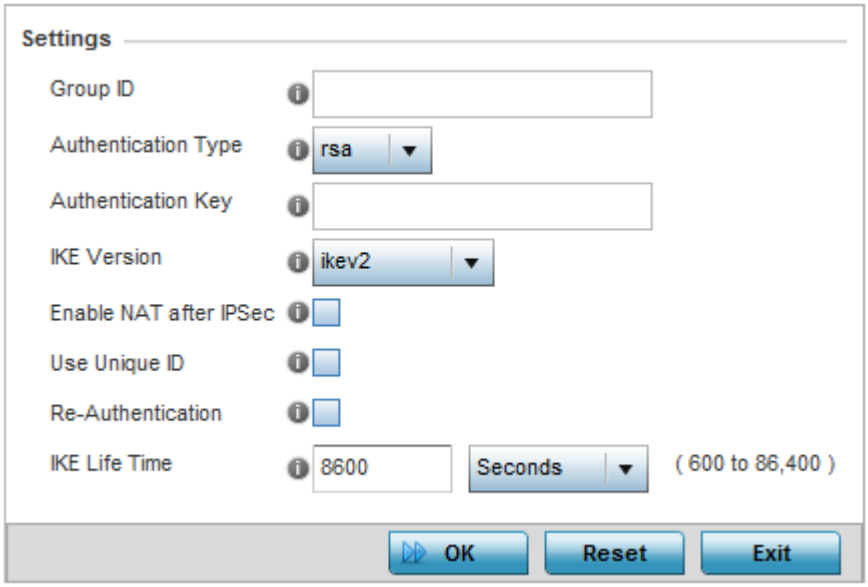


Figure 233: Device Overrides - Security – Auto IPSec Tunnel screen

6 Refer to the following table to override the Auto IPSec tunnel settings:

Group ID	Configure the ID string used for IKE authentication. String length can be between 1-64 characters
Authentication Type	Set the IPSec Authentication Type. Options include *PSK* (Pre Shared Key) or *rsa.*
Authentication Key	Set the common key for authentication between the remote tunnel peer. Key length is between 8-21 characters
IKE Version	Configure the IKE version to use. The available options are *ikev1-main*, *ikev1-aggr* and *ikev2.*
Enable NAT after IPSec	Select this option to enable NAT after IPSec. Enable this if there are NATted networks behind VPN tunnels.
Use Unique ID	In scenarios where different access points behind different NAT boxes/ routers have the same IP address, it is not possible to create a tunnel between the wireless controller and access point, as the wireless controller fails to identify the access point uniquely. When selected, each access point behind a same NAT box/router will have an unique ID which is used to create the VPN tunnel.
Re-Authentication	Select this option to re-authenticate the key on a IKE rekey. This setting is disabled by default.
IKE Life Time	Set a lifetime in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1) for IKE security association duration. The default is 8600 seconds.

7 Select **OK** to save the updates made to the **Auto IPSec Tunnel** screen. Selecting **Reset** reverts the screen to its last saved configuration.

Overriding General Security Settings

"Overriding Security Configuration"

A profile can leverage existing firewall, wireless client role and WIPS policies and configurations and apply them to the configuration. This affords a profile a truly unique combination of data protection policies. However, as deployment requirements arise, an individual access point may need some or all of its general security configuration overridden from that applied in the profile.

To define a profile's security settings and overrides:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **Settings**.

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* screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

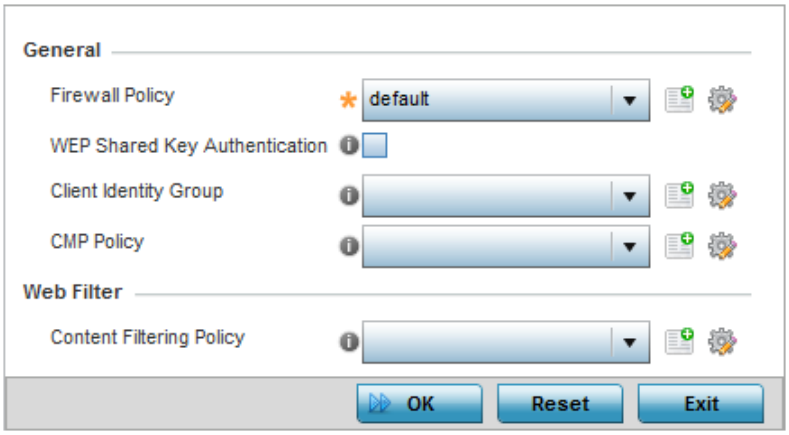


Figure 234: Device Overrides - Security Settings screen

6 Refer to the **General** field to assign or override the following:

Firewall Policy	Select the firewall policy used by devices with this profile. Use the icons next to this field to create or add new firewall policies.
WEP Shared Key Authentication	Select this option to require devices using this profile to use a WEP key to access the network using this profile. Clients without our 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 used to configure permissions and access rules for devices classes in the network. It is a collection of client identities that identify devices and applies specific permissions and restrictions on these devices. From the drop-down menu, select the client identity group to use with this security setting. For more information, see "Device Fingerprinting" on page 735.
CMP Policy	Select the CMP policy used by devices with this profile. Use the icons next to this field to create or add new CMP Policies.

7 Use the **Web Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

Web filtering is used to restrict access to resources on the Internet.

8 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

Overriding a Certificate Revocation List (CRL) Configuration

"Overriding Security Configuration"

A *certificate revocation list* (CRL) is a list of certificates 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 Certificate Revocation configuration or override:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **Certificate Revocation**.



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* screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

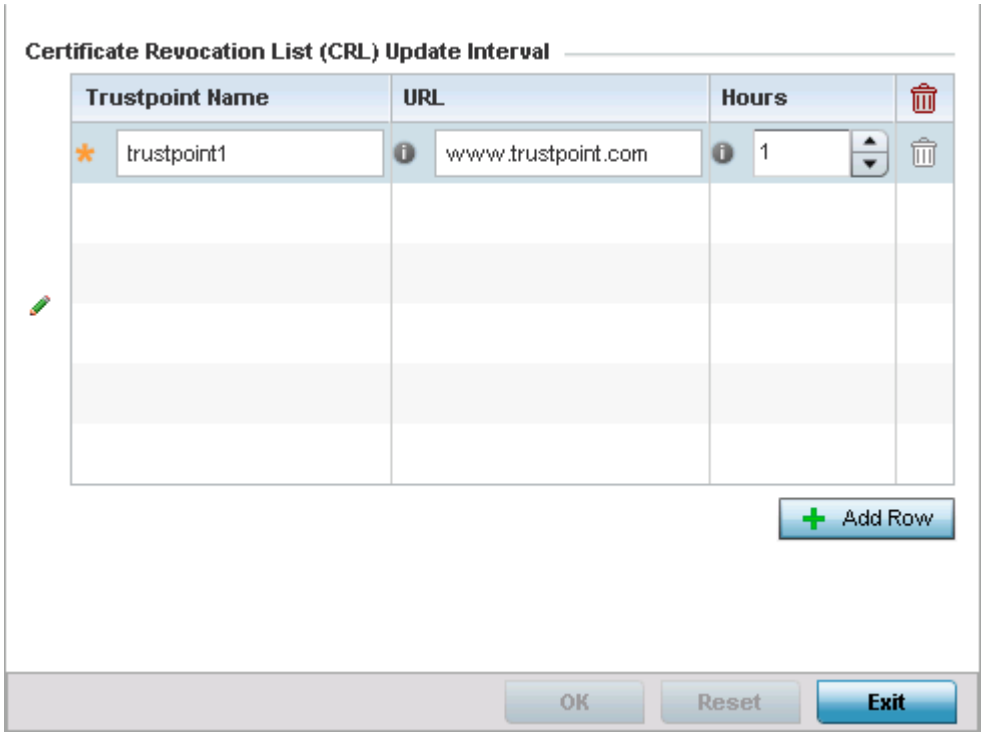


Figure 235: Device Overrides - Certificate Revocation screen

6 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.

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.

7 Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.

8 Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.

9 Use the spinner control within the **Hours** field to specify an interval (in hours) after which the access point copies a CRL file from an external server and associates it with a trustpoint.

10 Select **OK** to save the changes and overrides made within the **Certificate Revocation** screen. Select **Reset** to revert to the last saved configuration.

Overriding RADIUS Trustpoint Configuration

"Overriding Security Configuration"

A RADIUS 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.

To define a RADIUS Trustpoint configuration, utilize an existing stored trustpoint or launch the certificate manager to create a new one:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **RADIUS Trustpoints**. The following screen displays.

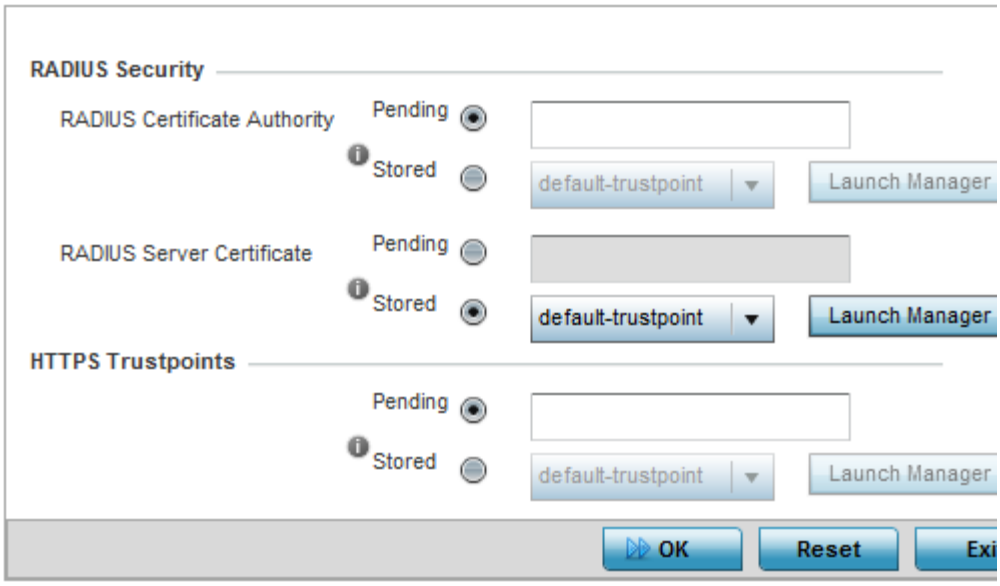


Figure 236: Device Overrides - RADIUS Trustpoint screen

6 Set the following **RADIUS Security** certificate settings:

RADIUS Certificate Authority	Select the **Pending** radio button to use a certificate that is in the process of being created or is yet to be created. As such certificates will not be listed under the **Stored** drop-down, use this method instead. Using this option is not a guarantee that the trust point will work as intended if the trust point is not loaded on to the device. The trust point can be created later, however, it must be present on the device when the device is deployed. Select the **Stored** radio button to enable a drop-down menu where an existing certificate can be leveraged or use *default-trustpoint*. To leverage an existing certificate, select the **Launch Manager** button.
RADIUS Server Certificate	Select the **Pending** radio button to use a certificate that is in the process of being created or is yet to be created. As such certificates will not be listed under the **Stored** drop-down, use this method instead. Using this option is not a guarantee that the trust point will work as intended if the trust point is not loaded on to the device. The trust point can be created later, however, it must be present on the device when the device is deployed. Select the **Stored** radio button to enable a drop-down menu where an existing certificate can be leveraged or use *default-trustpoint*. To leverage an existing certificate, select the **Launch Manager** button.

7 Set the following **HTTPS Trustpoints certificate** settings:

HTTPS Trustpoint	Either use the default trustpoint or select the **Stored** radio button to enable a drop-down menu where an existing certificate/trustpoint can be utilized. To use an existing certificate for this device, select the **Launch Manager** button. For more information, see "Manage Certificates" on page 301.

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

Overriding NAT Configuration

"Overriding Security 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 provides outbound Internet access to wired and wireless hosts. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows the access point to translate one or more private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To define a NAT configuration or override that can be applied to a profile:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **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* screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

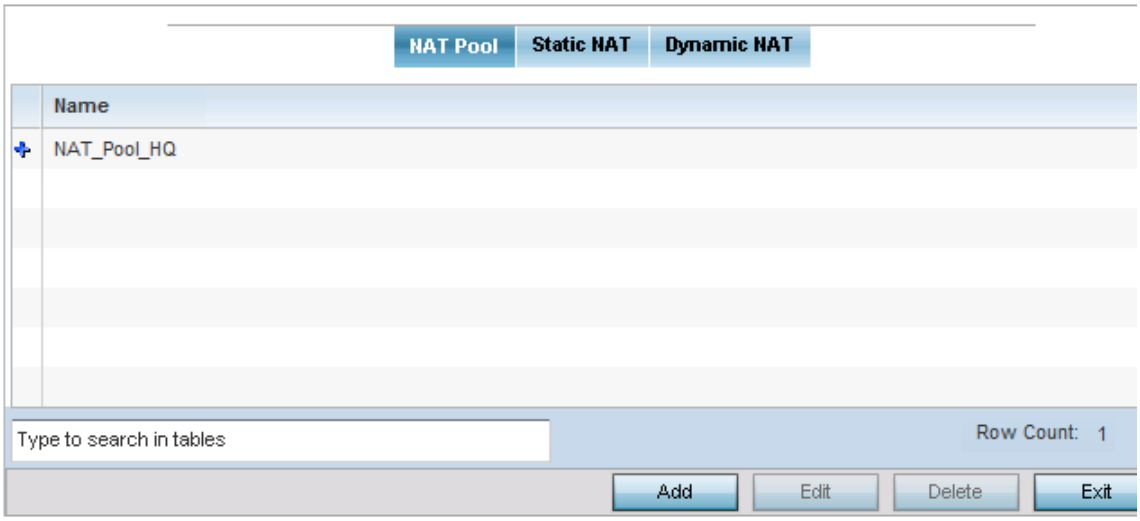


Figure 237: Device Overrides - NAT Pool screen

6 The **NAT Pool** tab 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.

7 Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify or override the attributes of a existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.

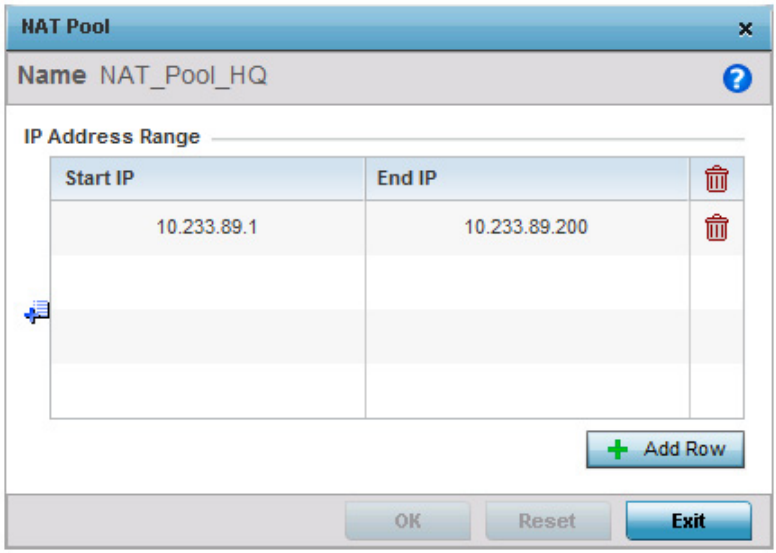


Figure 238: Device Overrides - Security - NAT Pool screen

8 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.

9 Select the **+ Add Row** button as needed to append additional rows to the IP Address Range table.

10 Select **OK** to save the changes or overrides made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.

11 Select the **Static NAT** tab. The **Source** tab displays by default.

The **Source** tab displays 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.

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.

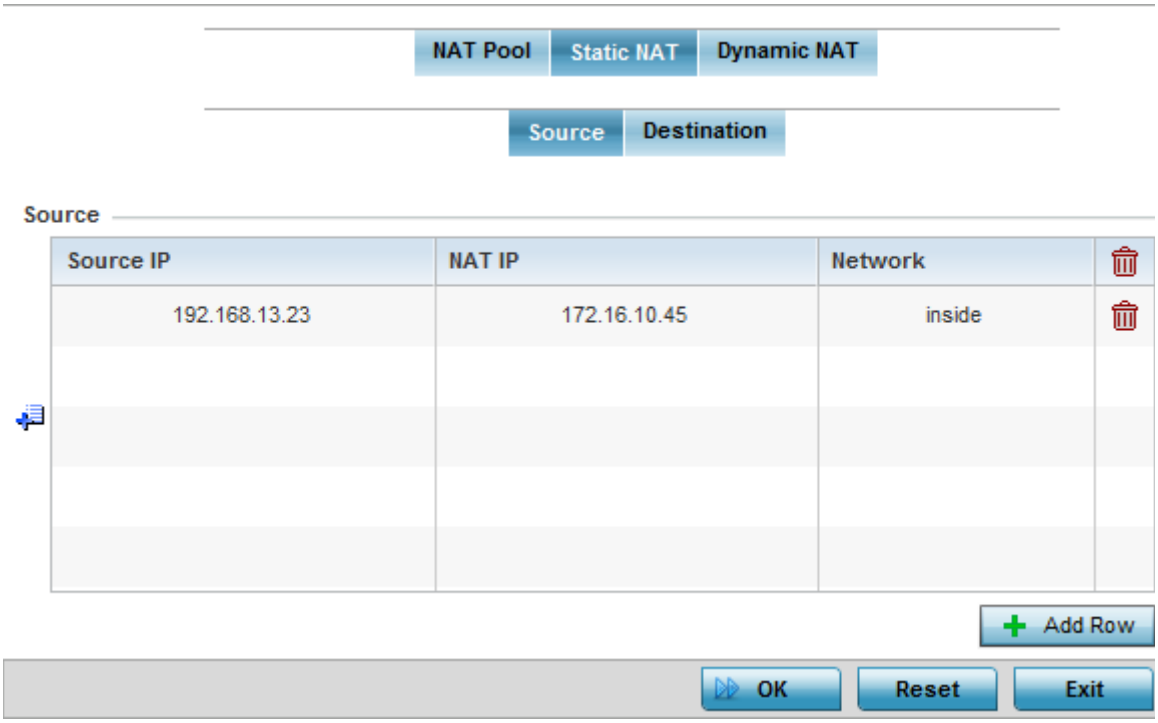


Figure 239: Device Overrides - Static NAT screen

To map a source IP address from an internal network to a NAT IP address click the **Add** button.

12 Define the following **Source NAT** parameters:

Source IP	Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either *source* or *destination* based on the direction specified.
Network	Select *Inside* or *Outside* NAT as the network direction. The default setting is Inside. 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.

13 Select the **Destination** tab to view destination NAT configurations and define packets passing through the NAT on the way back to the LAN are searched against to 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.

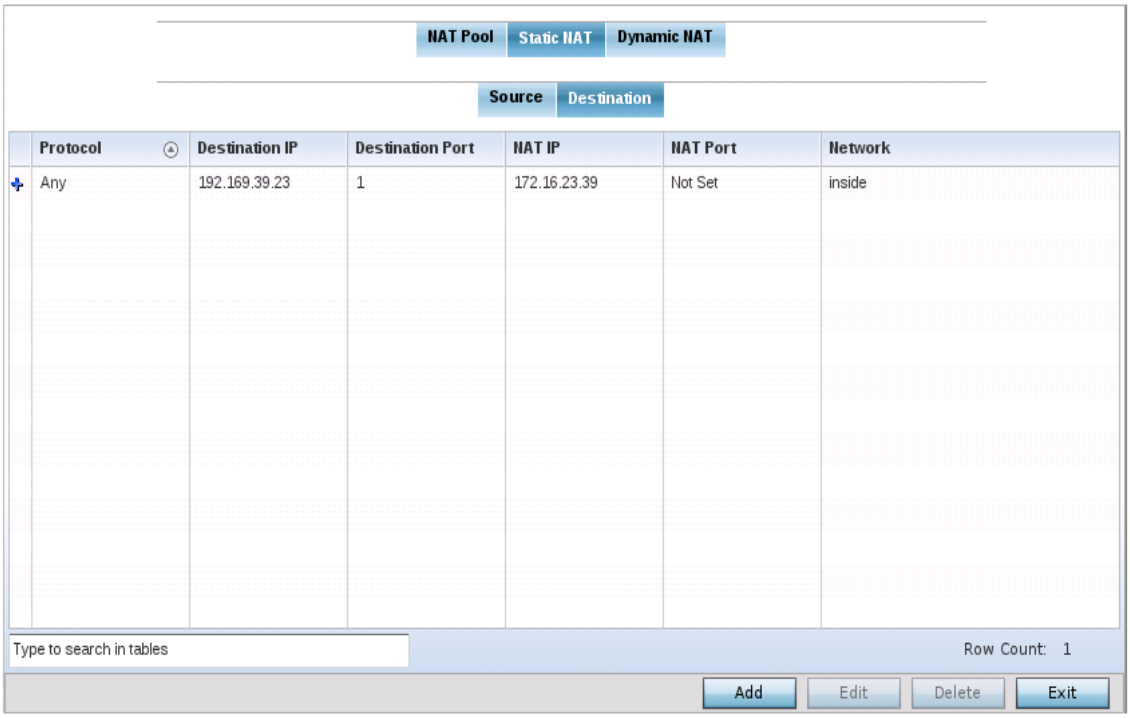


Figure 240: Device Overrides - NAT Destination screen

14 Select **Add** to create a new NAT destination configuration or **Delete** to permanently remove a NAT destination. Existing NAT destination configurations are not editable.

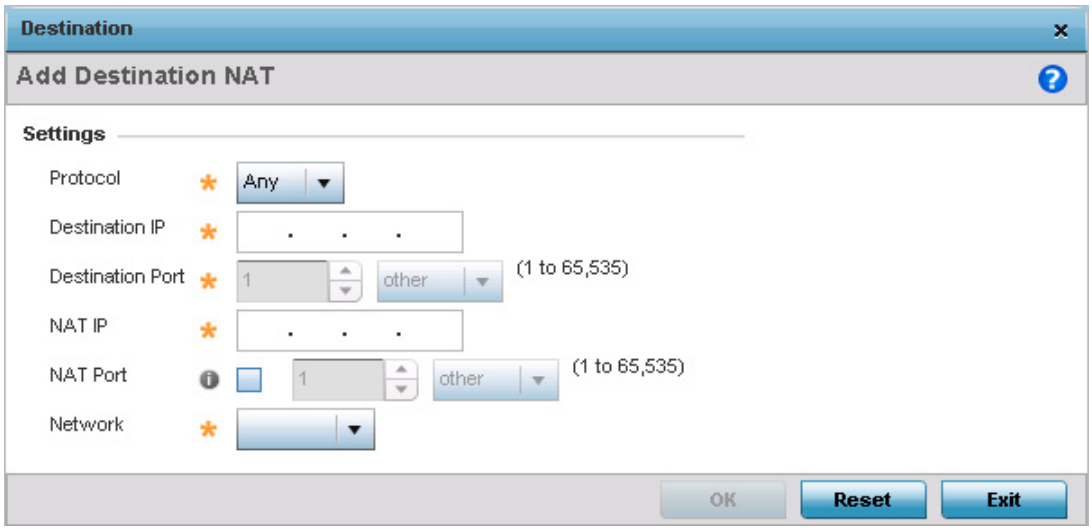


Figure 241: Device Overrides - Add Destination NAT screen

15 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. *TCP*, *UDP* and *Any* are available options. 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 *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) will 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 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	Select this option and 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. Inside is the default setting. 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.

16 Select **OK** to save the changes or overrides made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Dynamic NAT** tab.

Dynamic NAT translates 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.

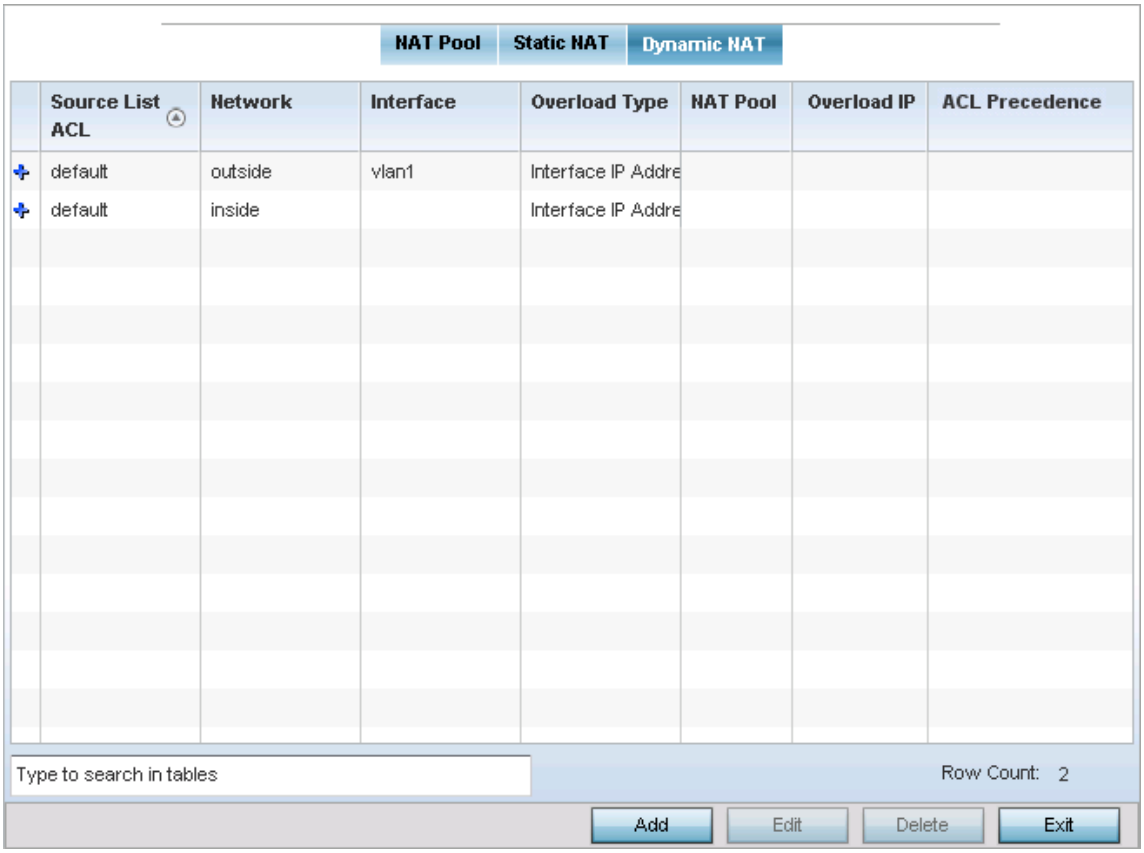


Figure 242: Device Overrides - Dynamic NAT screen

18 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

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.
Interface	Lists the VLAN (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.
Overload Type	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	If *One Global IP Address* is selected as the Overload Type, define an IP address used as a filter address for the IP ACL rule.
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.

19 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify or override an existing configuration or **Delete** to permanently remove a configuration.

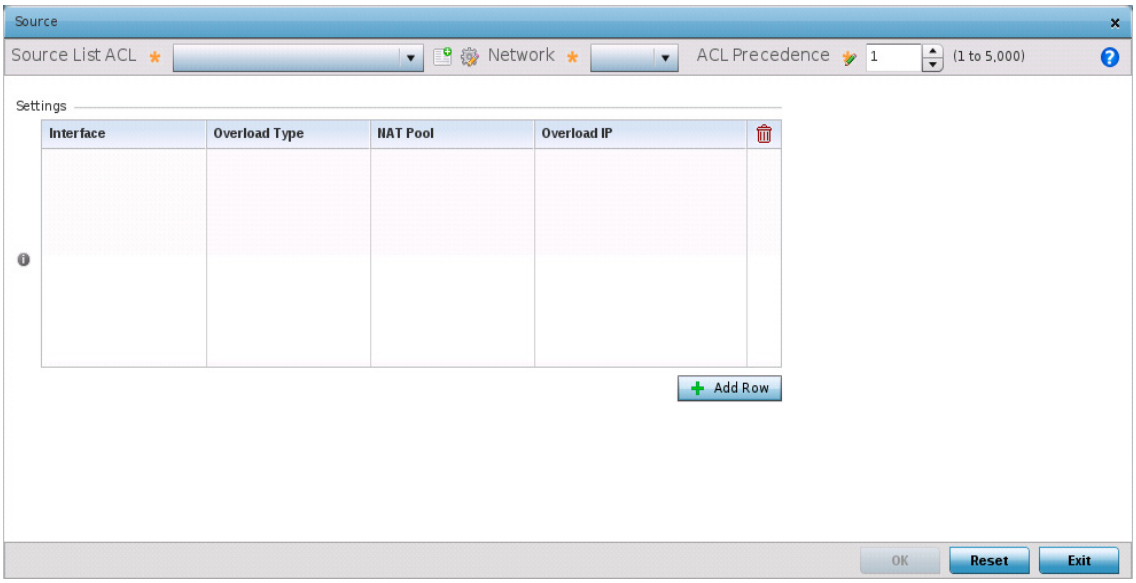


Figure 243: Device Overrides - Security - NAT - Source ACL List screen

20 Set or override 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) 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 the VLAN selected adequately supports the intended network traffic within the NAT supported configuration.
Overload Type	Define the overload type utilized 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*. 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	If *One Global IP Address* is selected as the *Overload Type*, define an IP address used a filter address for the IP ACL rule.

21 Select **OK** to save the changes or overrides made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

Overriding the Profile's Bridge NAT Configuration

"Overriding Security Configuration"

Use *Bridge NAT* to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an access point. NAT rules are applied to bridged traffic through the access point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.



NOTE

Bridge NAT supports single AP deployments only. This feature cannot be used in a branch deployment with multiple access points.

To define a Bridge NAT configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Device Overrides** from the options on left-hand side of the UI.

4 Expand the **Security** menu and select **Bridge NAT**.

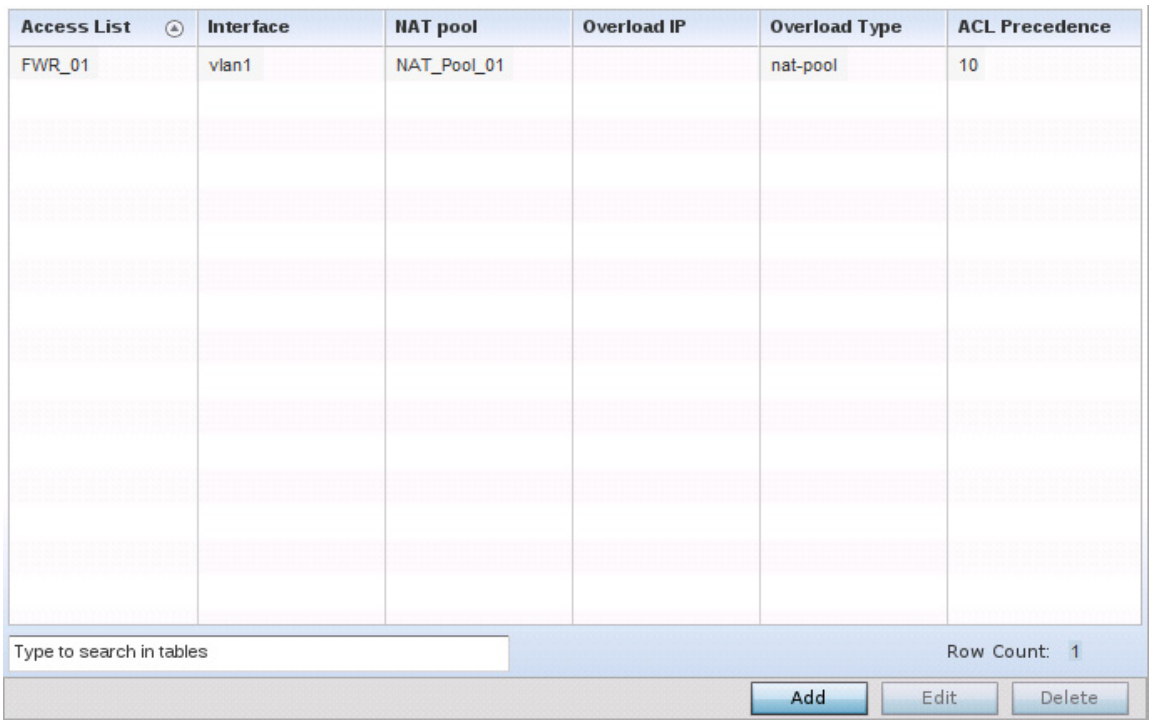


Figure 244: Profile Override - Security - Bridge NAT screen

5 Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration overridden or removed:

Access List	Lists the ACL applying IP address access/deny permission rules to the Bridge NAT configuration.
Interface	Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the access point's *pppoe1* or *w wan1* 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 local addresses for this configuration.
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 this ACL.

6 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify or override an existing configuration or **Delete** to remove a configuration.

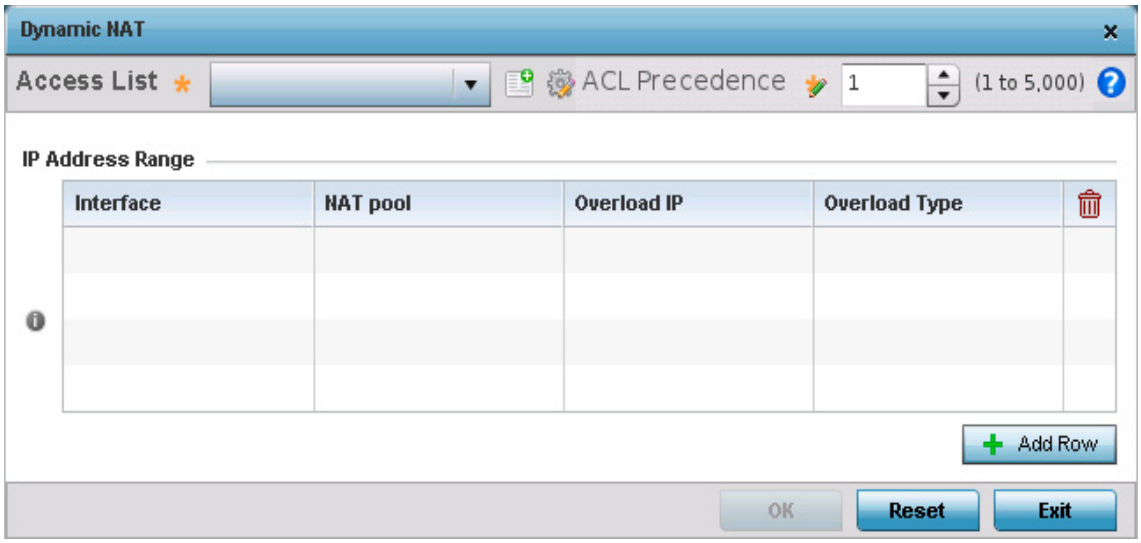


Figure 245: Profile Security - Dynamic NAT screen

7 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.

8 Use the spinner to select the **ACL Precedence**. The lower the precedence value, the higher the priority assigned to this Dynamic NAT policy rule.

9 Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the Internet.

Interface	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an access point WWAN or PPPoE interface. Traffic can also be redirected to a designated VLAN.
NAT Pool	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to NAT Pool.
Overload IP	Lists the IP address used to represent a large number local addresses for this configuration.
Overload Type	Displays the override type for this policy based forwarding rule.

10 Select **+ Add Row** to set the IP address range settings for the Bridge NAT configuration.

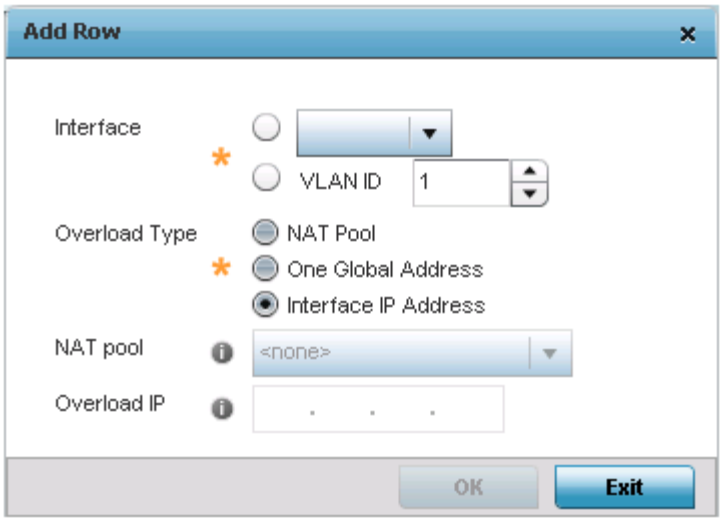


Figure 246: Profile Security - Source Dynamic NAT screen - Add Row field

11 Select **OK** to save the changes made within the **Add Row** and **Dynamic NAT** screens. Select **Reset** to revert to the last saved configuration.

Overriding a Profile's Application Visibility Settings

"Overriding Security Configuration"

Deep packet inspection (DPI) is an advanced packet filtering technique functioning at the application layer. Use DPI to find, *identify*, *classify, reroute* or *block* packets containing specific data or codes that other packet filtering techniques (examining only packet headers) cannot detect.

Enable DPI to scan data packets passing through the WiNG managed network. The contents of each packet are scanned, occasionally logged and blocked or routed to their destination. Deep packet inspection helps an ISP block the spread of viruses, illegal downloads and prioritize data transmitted by bandwidth-heavy applications (video and VoIP applications) to help prevent network congestion.

NOTE

Application Visibility is only available on AP7562, AP8432 and AP8533 access points only.

To configure a profile's application visibility settings and overrides:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Security** to expand its sub menu options.

5 Select **Application Visibility (AVC)**.

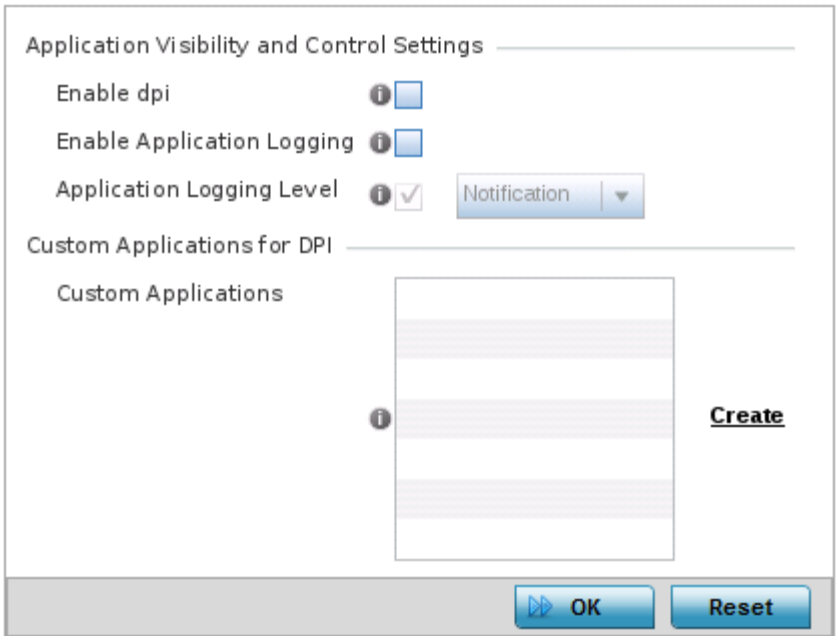


Figure 247: Profile Security - Application Visibility screen

6 Refer the following **Application Visibility and Control Settings**:

Enable dpi	Enable this setting to provide deep-packet inspection (application assurance) by inspecting every byte of each application header packet passing through the controller or service platform. When enabled, application data streams are inspected at a granular level to help prevent viruses and spyware from accessing the WiNG managed network.
Enable Applications Logging	Select this option to enable event logging for deep packet inspection application recognition. This setting is disabled by default.
Application Logging Level	If enabled, 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 of high bandwidth voice and video application data flows. The default setting is disabled.
Enable HTTP Metadata	Select this option to enable the metadata extraction of HTTP application data flows. The default setting is disabled.
Enable SSL Metadata	Select this option to enable the metadata extraction of SSL application data flows. The default setting is disabled.

7 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 704.

8 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

Overriding the Virtual Router Redundancy Protocol (VRRP) Configuration

"Device Overrides"

A default gateway is a critical resource for connectivity. However, it is prone to a single point of failure. Thus, redundancy for the default gateway is required by the access point. If WAN backhaul is available on an AP7131, 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 wireless 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.

To define the configuration of a VRRP group:

1 Select the **Configuration** tab from the Web UI.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **VRRP**.

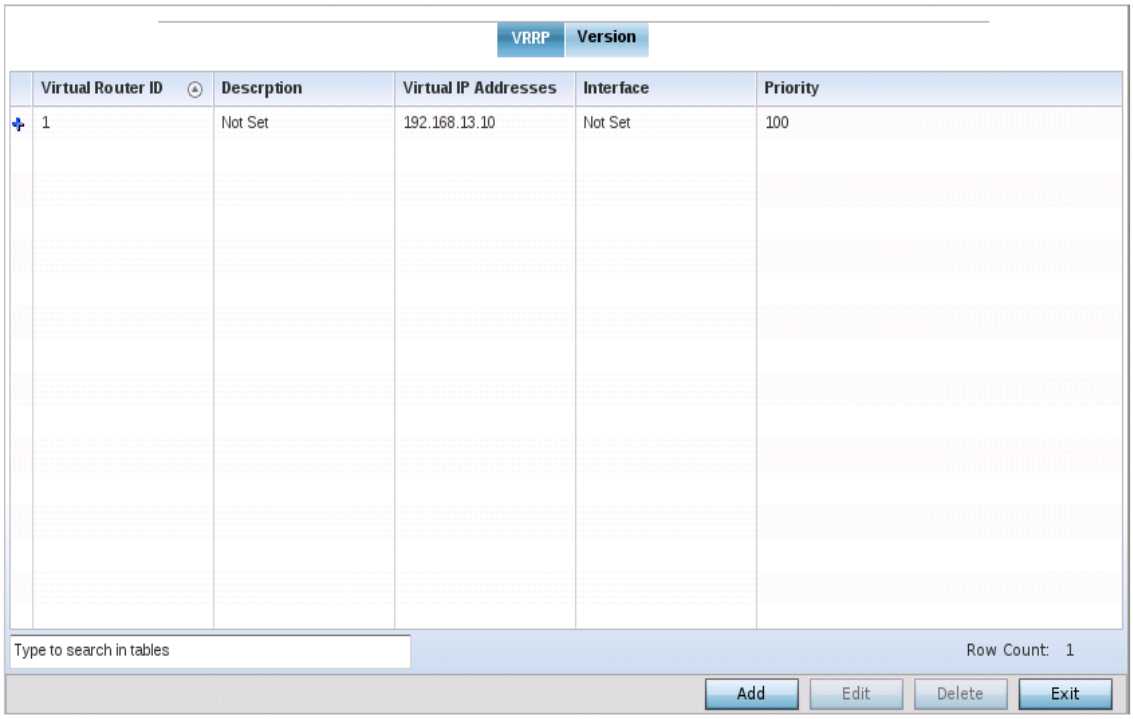


Figure 248: Device Overrides - VRRP screen - VRRP tab

5 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 (from 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 interfaces selected on the access point to supply VRRP redundancy failover support.
Priority	Lists 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 Select the **Version** tab to define the VRRP version scheme used with the configuration.

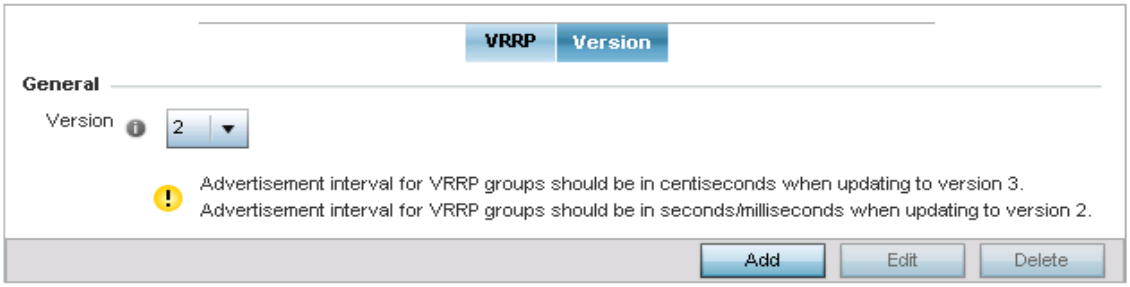


Figure 249: Device Overrides - VRRP screen - Version tab

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).

7 From within the **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**.

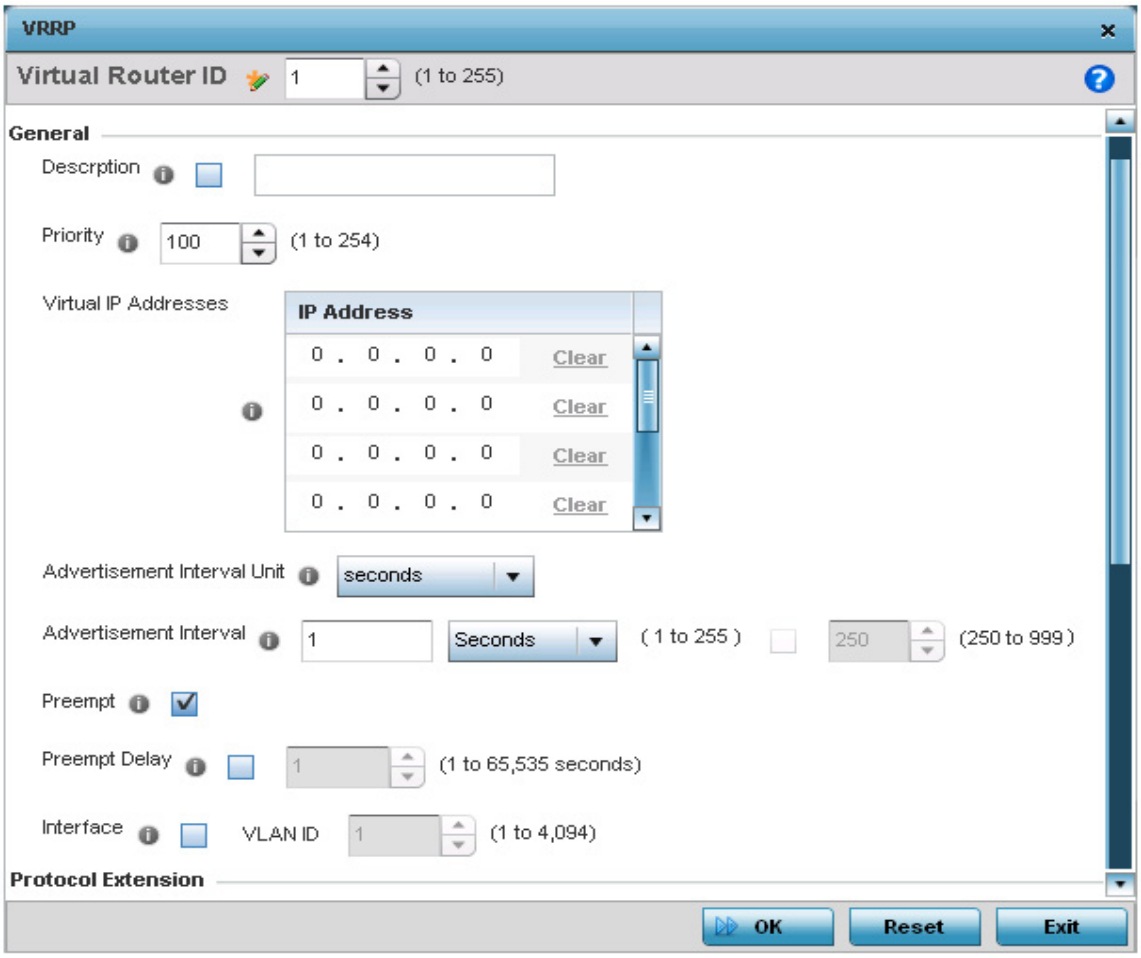


Figure 250: Device Overrides - VRRP screen

8 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.

9 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 access point 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 8 IP addresses representing the Ethernet switches, routers or security appliances defined as virtual router resources to the AP7131 access point.
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 the *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 preemption.
Interface	Select this value to enable/disable VRRP operation and define the AP7131 VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure.

10 Refer to the **Protocol Extension** field to define the following:

Sync Group	Select this 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 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 within the VRRP group.
Network Monitoring: Critical Resources	Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include *None*, *increment-priority*, and *decrement priority*.
Network Monitoring: Delta Priority	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.

11 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

Profile Critical Resources

"Device Overrides"

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're 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 the **Configuration** tab from the Web UI.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Critical Resources**.

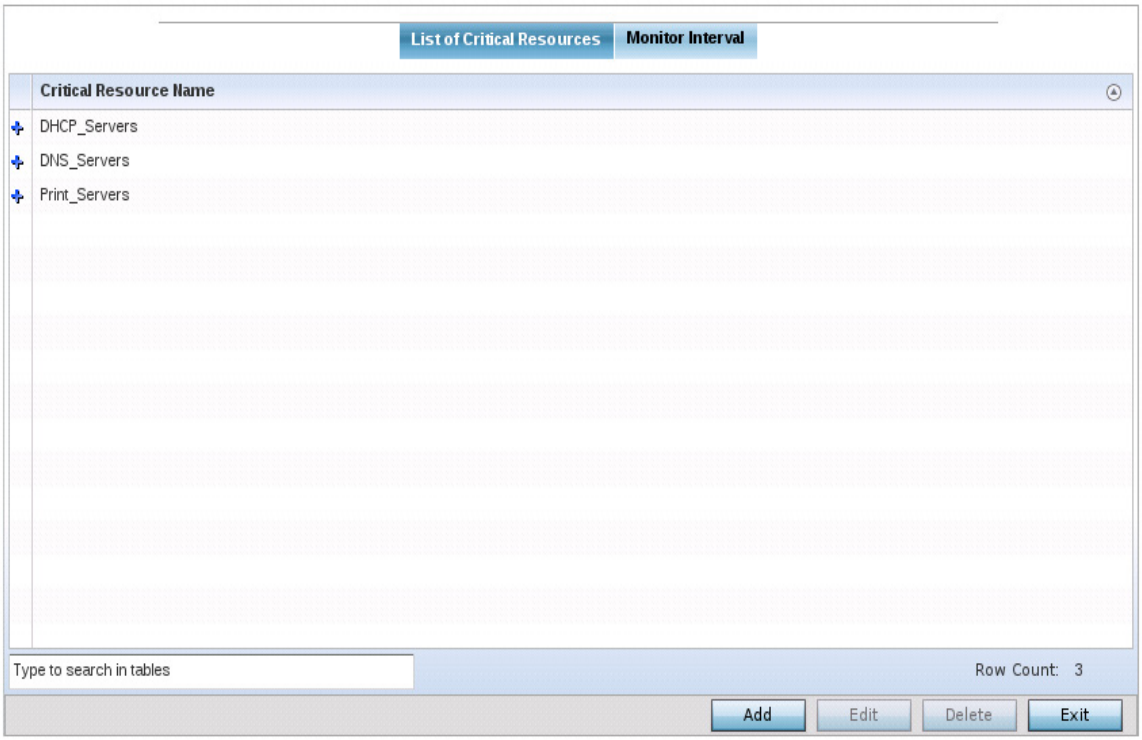


Figure 251: Device Overrides - Critical Resources screen - List of Critical Resources tab

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 access point or controller, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5 Select 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.

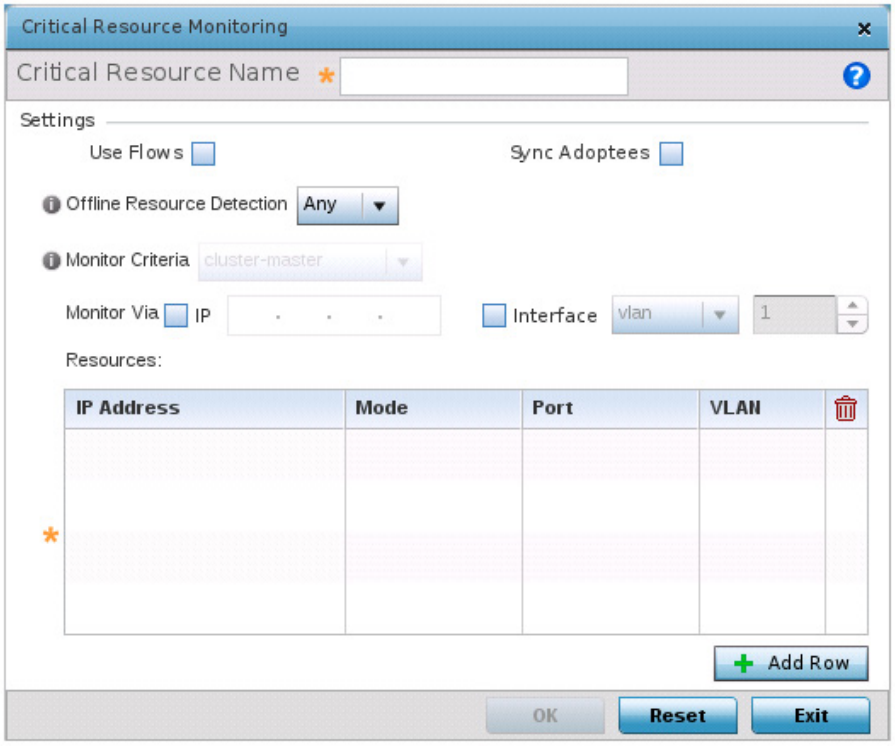


Figure 252: Device Overrides - Critical Resources screen - Adding a Critical Resource

6 Select **Use Flows** to configure the critical resource to monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets to reduce the amount of traffic on the network. Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message. These settings are disabled by default.

7 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.

8 Select the **IP** option (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.

9 Select the **Interface** option (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.

10 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 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 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 pinging the critical resource and sending control messages (device not reachable, requested service not available, etc.).
Port	Provide the port on which the critical resource is available. Use the spinner control to set the port number.
VLAN	Define the VLAN on which the critical resource is available using the spinner control.

11 Select the **Monitor Interval** tab.

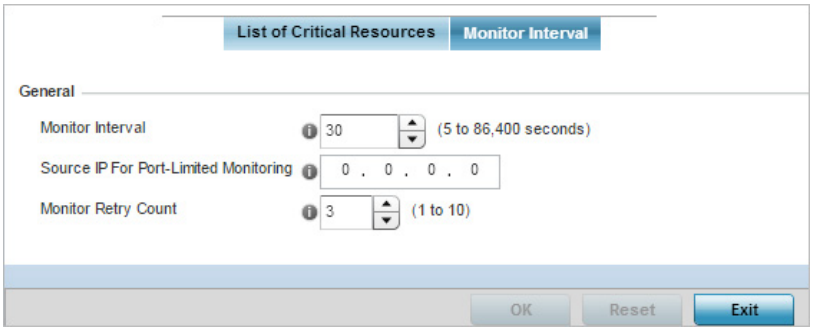


Figure 253: Device Overrides - Critical Resources screen - Monitor Interval tab

12 Set the duration between two successive pings from the access point to critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.

13 Configure the IP address for Port-Limited Monitoring in the **Source IP for Port-Limited Monitoring** field. Sets 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.

14 Set the **Monitor Retry Count** 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.

15 Select **OK** to save the changes to the critical resource configuration and monitor interval. Select **Reset** to revert to the last saved configuration.

Overriding a Services Configuration

"Device Overrides"

A profile can contain specific guest access (captive portal), DHCP server and RADIUS server configurations. 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 **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 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 screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

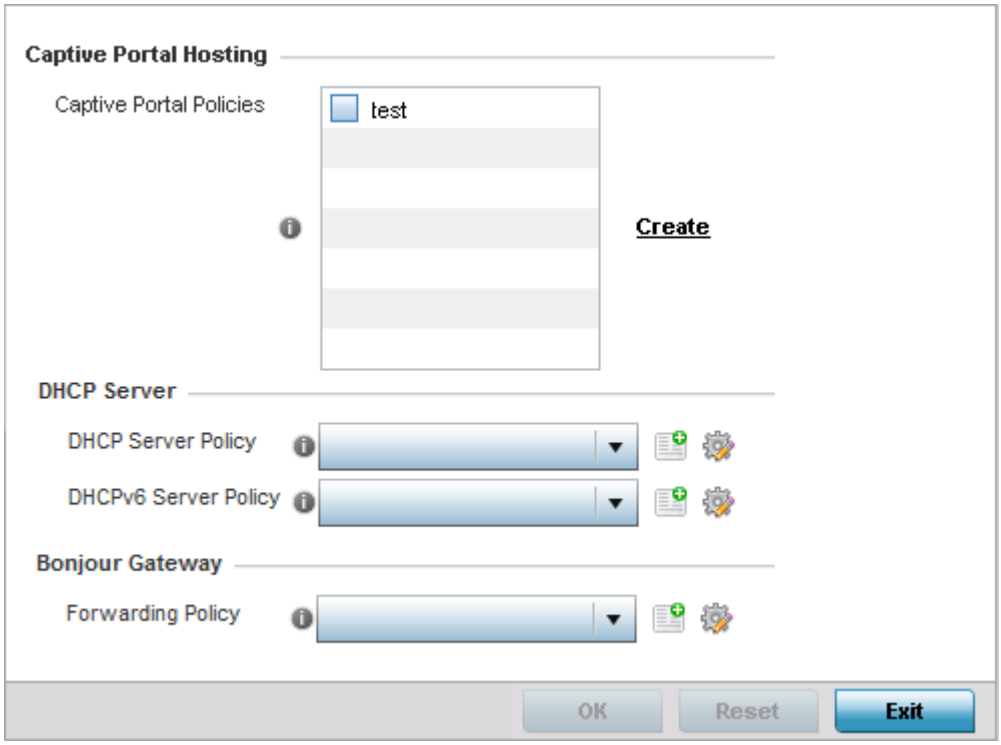


Figure 254: Device Overrides - Services screen

5 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 network. The primary means of securing such guest access is a captive portal.

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. Once logged into the captive portal, additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on the captive portal's 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 configuration that can be applied to a profile. For more information, see "Configuring Captive Portal Policies" on page 759.

6 Refer to the **DHCP Server Policy** field to select or set a DHCP server policy.

DHCP Server Policy is a configuration that defines the DHCP pool, global settings and DHCP class information for IPv4 DHCP servers.

7 Refer to the **IPv6 DHCP Server Policy** field to select or set an IPv6 DHCP server policy.

IPv6 DHCP Server Policy is a configuration that defines the DHCP pool, global settings and DHCP class information for IPv6 DHCP servers.

8 Refer to the **Bonjour Gateway** field to select or set a Bonjour Gateway **Forwarding Policy**.

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

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.

9 Select **OK** to save the changes or overrides made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

Overriding Management Configuration

"Device Overrides"

There are mechanisms to allow/deny management access to the network for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or 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 devices 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.

To define or override a profile's management configuration:

1 Select **Devices** from the Configuration tab.

2 Select **Device Overrides** from the Device menu to expand it into sub menu options.

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **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 screen's Device Overrides field and select Clear Overrides. This will remove all overrides from the device.

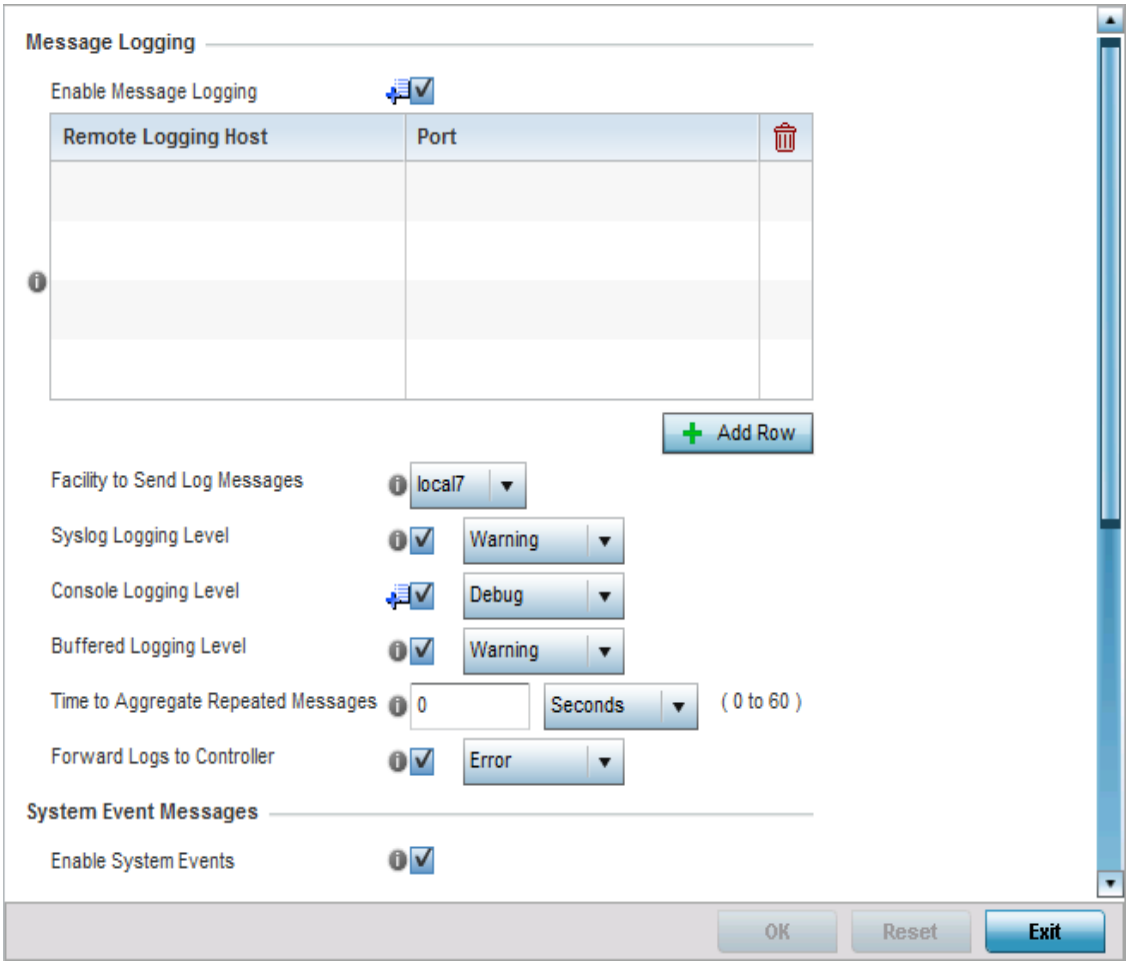


Figure 255: Device Overrides - Management Settings screen

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 may be negatively impacting performance.

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 radio button enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.
Remote Logging Host/ Port	Use this table to define numerical (non DNS) IP addresses and ports for up to four external resources where logged system events can be sent on behalf of the profile. Select the thrash icon as needed to remove an IP address from the list.
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 console 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 buffered 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 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 system messages are logged and forwarded on behalf of the profile.

Select the **Enable System Events** radio button to allow the profile to capture system events and append them to a log file. It is important to log individual events to discern an overall pattern that may be negatively impacting performance. This setting is enabled by default.

Select the **Enable System Event Forwarding** radio button to enable the forwarding of system events. This setting is enabled by default.

7 Refer to the **Events E-mail Notification** field to define or override how system event notification E-mails are sent.

SMTP Server	Specify either the *Hostname* or *IP Address* of the outgoing SMTP server where notification E-mails are originated.
Port of SMTP	If a non-standard SMTP port is used on the outgoing SMTP server select this option and specify a port from 1 - 65,535 for the outgoing SMTP server to use.
Sender E-mail Address	Specify the E-mail address that notification E-mails will be sent from. This will be the from address on notification E-mails.
Recipient's E-mail Address	Specify the E-mail address(es) of recipients for E-mail 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 E-mail 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 an username and password before sending E-mail through the server.

8 Use the **Configure** drop-down menu within the **Persist Configuration Across Reloads** field to define whether the access point saves a configuration received from a Virtual Controller AP to flash memory. The configuration would then be made available if the this access point reboots and the Virtual Controller AP is not reachable. Options include *Enabled*, *Disabled* and *secure*.

9 Use the **HTTP Analytics** section to define how data for analysis by an external engine is sent. Select **Compress** to compress the data before sending. Use the **Update Interval** field to set the duration and set the time interval in *minutes, seconds* or *hours* when the collected data is sent to the external analytics engine.

10 Select **OK** to save the changes and overrides made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.

11 Select the **Firmware** tab from the Management menu.

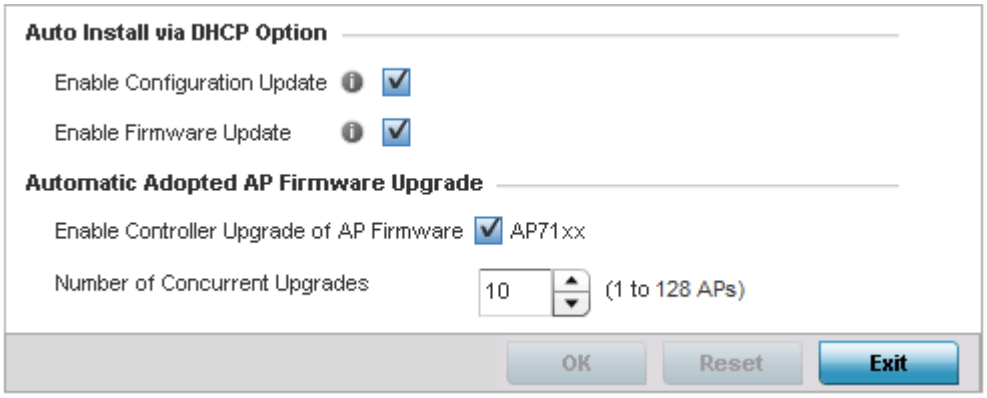


Figure 256: Device Overrides - Management Firmware screen

12 Refer to the **Auto Install via DHCP Option** field to define automatic configuration file and firmware updates.

Enable Configuration Update	Select this option to enable automatic configuration file updates for the controller profile from a location external to the access point. If enabled (the setting 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 from a user defined remote location. This value is disabled by default.

13 Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware upgrade from a controller based file.

Enable Controller Upgrade of AP Firmware	Select the access point model to upgrade using its associated Virtual Controller AP's most recent firmware file for that model. This parameter is enabled by default.
Number of Concurrent Upgrades.	Use the spinner control to define the maximum number (1 - 128) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind 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.

14 Select **OK** to save the changes and overrides made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.

15 Select **Heartbeat** from the Management menu.



Figure 257: Device Overrides - Management Heartbeat screen

16 Select the **Service Watchdog** option to implement heartbeat messages to ensure other associated devices are up and running and capable of effectively interoperating. The Service Watchdog is enabled by default.

17 Select **OK** to save the changes and overrides made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

Overriding Mesh Point Configuration

"Device Overrides"

The access point can be configured to be a part of a meshed network. A mesh network is one where each node in the network is be able to communicate with other nodes in the network and where the node can maintain more than one path to its peers. Mesh network provides robust, reliable and redundant connectivity to all the members of the network. When one of the participant node in a mesh network becomes unavailable, the other nodes

in the network are still able to communicate with each other either directly or through intermediate nodes.

Mesh Point is the name given to a device that is a part of a meshed network.

Use the *Mesh Point* screen to configure or override the parameters that set how this device behaves as a part of the mesh network.

To override Mesh Point configuration:

1 Select **Devices** from the Configuration menu.

2 Select **Device Overrides** to expand its menu items

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Mesh Point.**

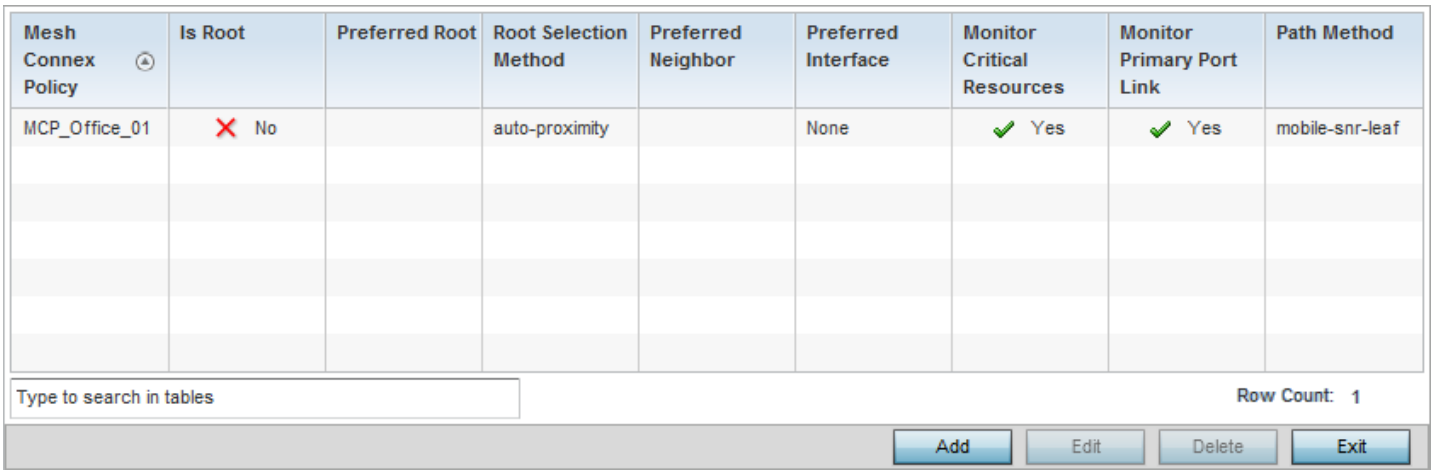


Figure 258: Device Overrides - Mesh Point screen

5 Select **Add** to create a new mesh point configuration or **Edit** to override an existing one. Select **Delete** to delete a mesh point configuration after selecting it.

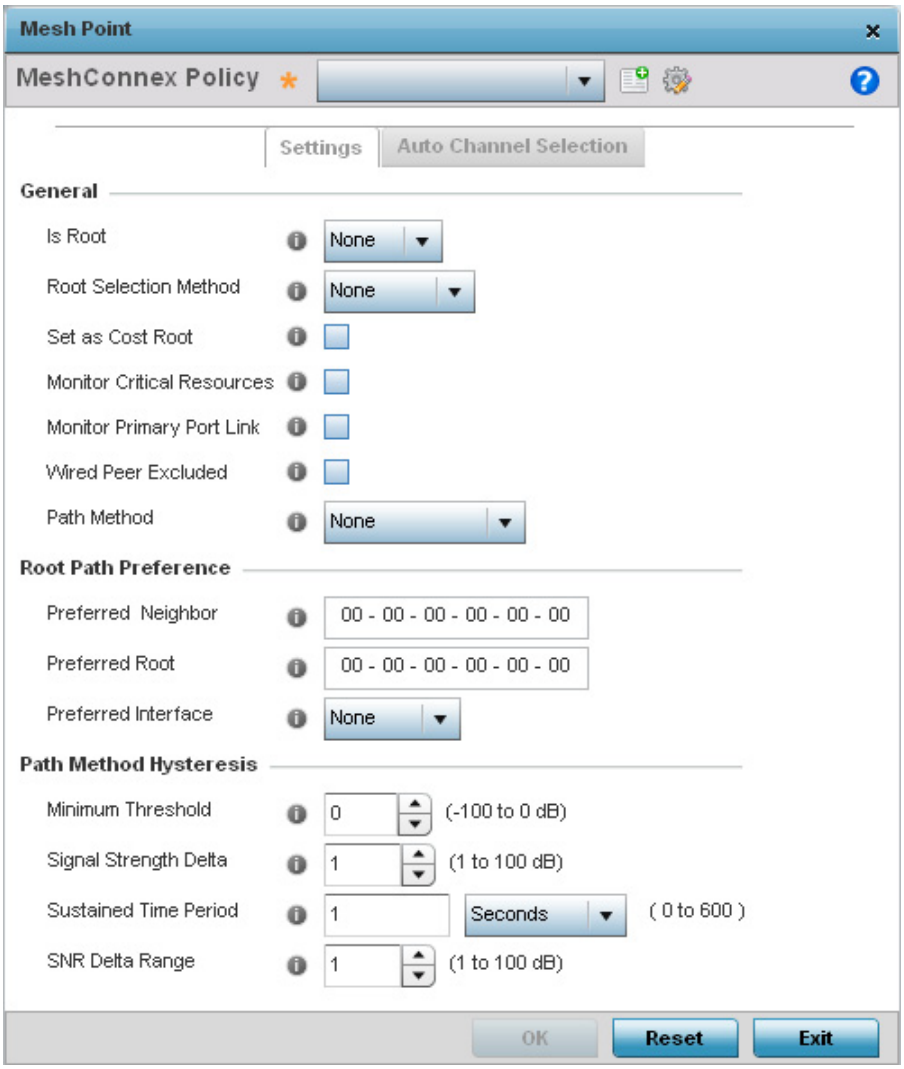


Figure 259: Device Overrides - Add Mesh Point screen

6 Refer to the following to configure **Mesh Point General** parameters:

Mesh Connex Policy	Provide a name for the Mesh Connex Policy. Use the *Create* icon to create a new Mesh Connex Policy. To edit an existing policy, select it from the drop-down and click the *Edit* icon. For more information on creating or editing a Mesh Connex Policy, see "MeshConnex Policy" on page 622.
Is Root	From the drop-down menu, select the root behavior of this access point. Select *True* to indicate this access point is a root node for this mesh network. Select *False* to indicate this access point is not a root node for this mesh network. A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network.
Root Selection Method	Use the drop-down menu to determine whether this mesh point is the root or non-root mesh point. Select either *None* (the default setting) or *auto-mint*.
Set as Cost Root	Select this option to set the mesh point as the cost root for mesh point root selection. This setting is disabled by default.
Monitor Critical Resources	Select this option to enable critical resource monitoring for this mesh point.
Monitor Primary Port Link	Select to enable monitoring of primary port link is enabled for this mesh connex policy. If the primary port link is not present and if the device is a mesh root, it is automatically changed to a non-root device. When the primary port link becomes available again, the non-root device is changed back to a root device.
Wired Peer Exclude	Select this option to exclude wired peers when creating mesh links.
Path Method	From the drop-down menu, select the method to use for path selection in a mesh network. The available options are: • *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 (AP7161 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.
Minimum Threshold	Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered. This field along with *Signal Strength Delta* and *Sustained Time Period* are used to dynamically select the next hop in a dynamic mesh network.The default setting is 0 dB.
Signal Strength Delta	Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR higher than the value configured here. This field along with the *Minimum Threshold* and *Sustained Time Period* are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB
Sustained Time Period	Enter the time duration in *seconds* (0 - 600) or *minutes* (0 - 10). This indicates the duration that a signal must sustain the constraints specified in the *Minimum Threshold* and *Signal Strength Delta* path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second.
SNR Delta Range	Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB.

7 Refer to the following to configure mesh point **Root Path Preference** parameters:



NOTE

With this release of the WiNG software, an AP7161 model access point can be deployed as a *Vehicle Mounted Modem* (VMM) 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. For VMM deployment considerations, see "Vehicle Mounted Modem (VMM) Deployment Consideration".

Preferred Neighbor	Enter the MAC address of the preferred neighbor for this mesh point.
Preferred Root	Enter the MAC address of the preferred mesh root for this mesh point.
Preferred Interface	Select the preferred Interface for this mesh point. Select *None* to set no preferences. The other interface choices are *2.4 GHz* and *5 GHz*.

8 Click the **Auto Channel Selection** tab to configure the parameters for the Mesh Connex Auto Channel Selection policy.

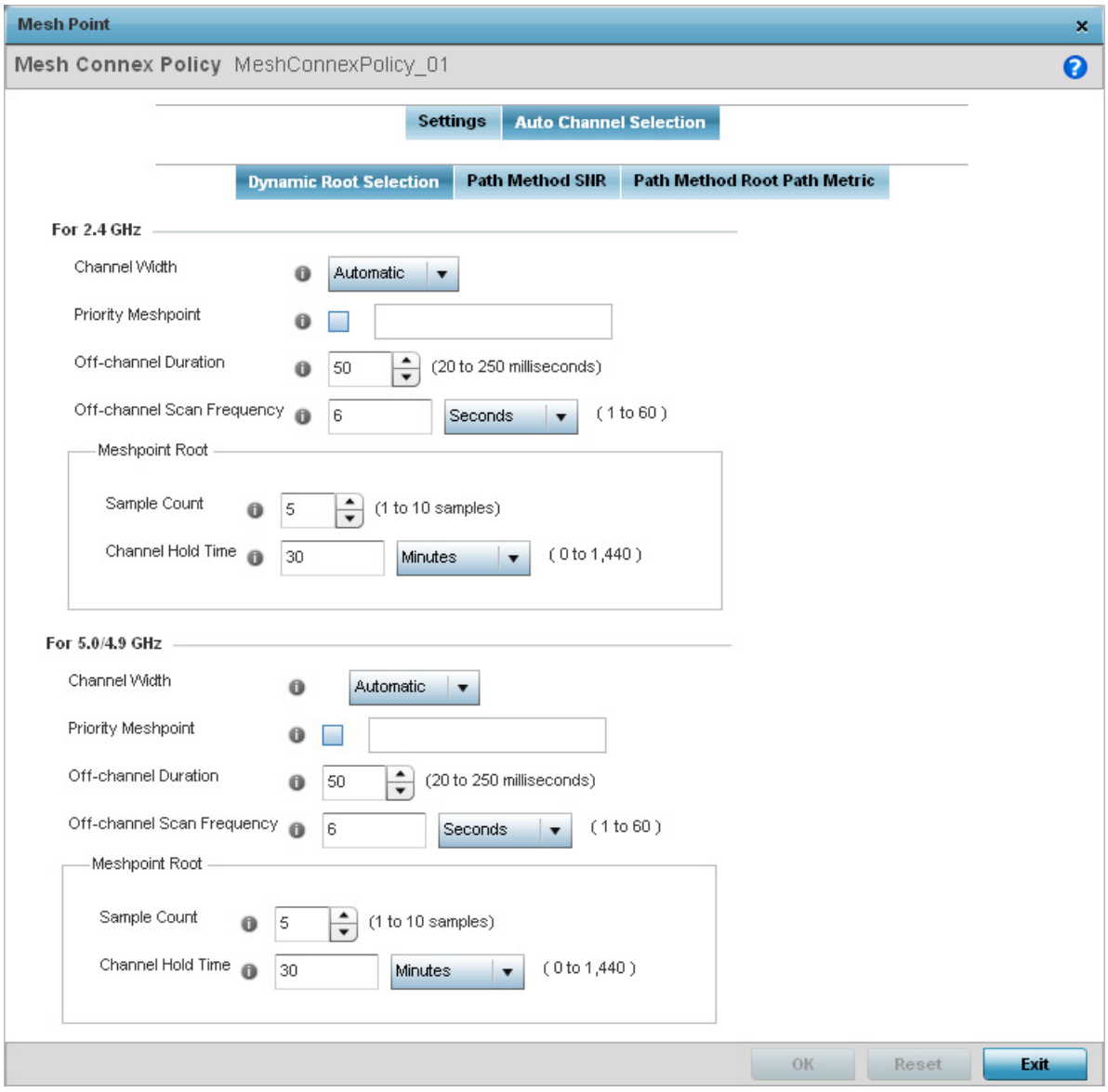


Figure 260: Mesh Point Auto Channel Selection screen

By default, the **Dynamic Root Selection** screen displays.

This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies. 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	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
Off Channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field. This is the duration that the scan dwells on each channel when performing an off channel scan.
Off Channel Scan Frequency	Configure the time duration in seconds between two consecutive Off Channel Scans. Set a duration between 1 - 60 seconds.
Meshpoint Root - Sample Count	Configure the number of scans to be performed for data collection before a mesh channel is selected. Set a value between 1 - 10 scans.
Meshpoint Root - Channel Hold Time	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

9 Select the **Path Method SNR** tab to configure the signal to noise ratio when selecting the path to the mesh point root.

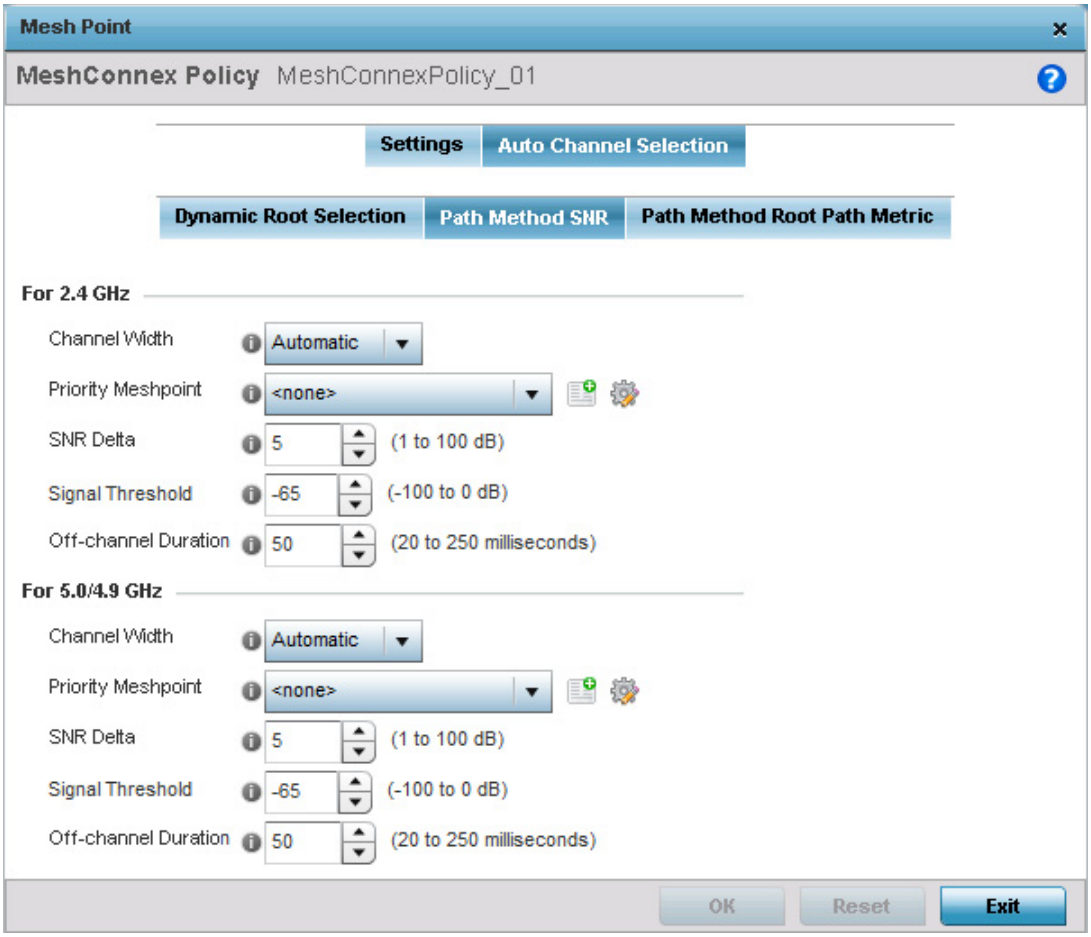


Figure 261: Mesh Point Auto Channel Selection Path Method SNR screen

Refer to the following for more information on the Path Method SNR screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

Channel Width	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected.
SNR Delta	Configure the signal to noise ratio delta value for path selection. When path selection occurs, this set value is considered 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 is 5dB
SNR Threshold	Configure the signal to noise threshold value for path selection. When the signal strength of the next hop in the mesh network goes below this value, a scan is triggered to select a better next hop. The default is -65 dB.
Off-channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field. This is the duration that the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds.

10 Select the **Path Method Root Path Metric** tab to configure the parameters controlling the calculation of the root path metrics.

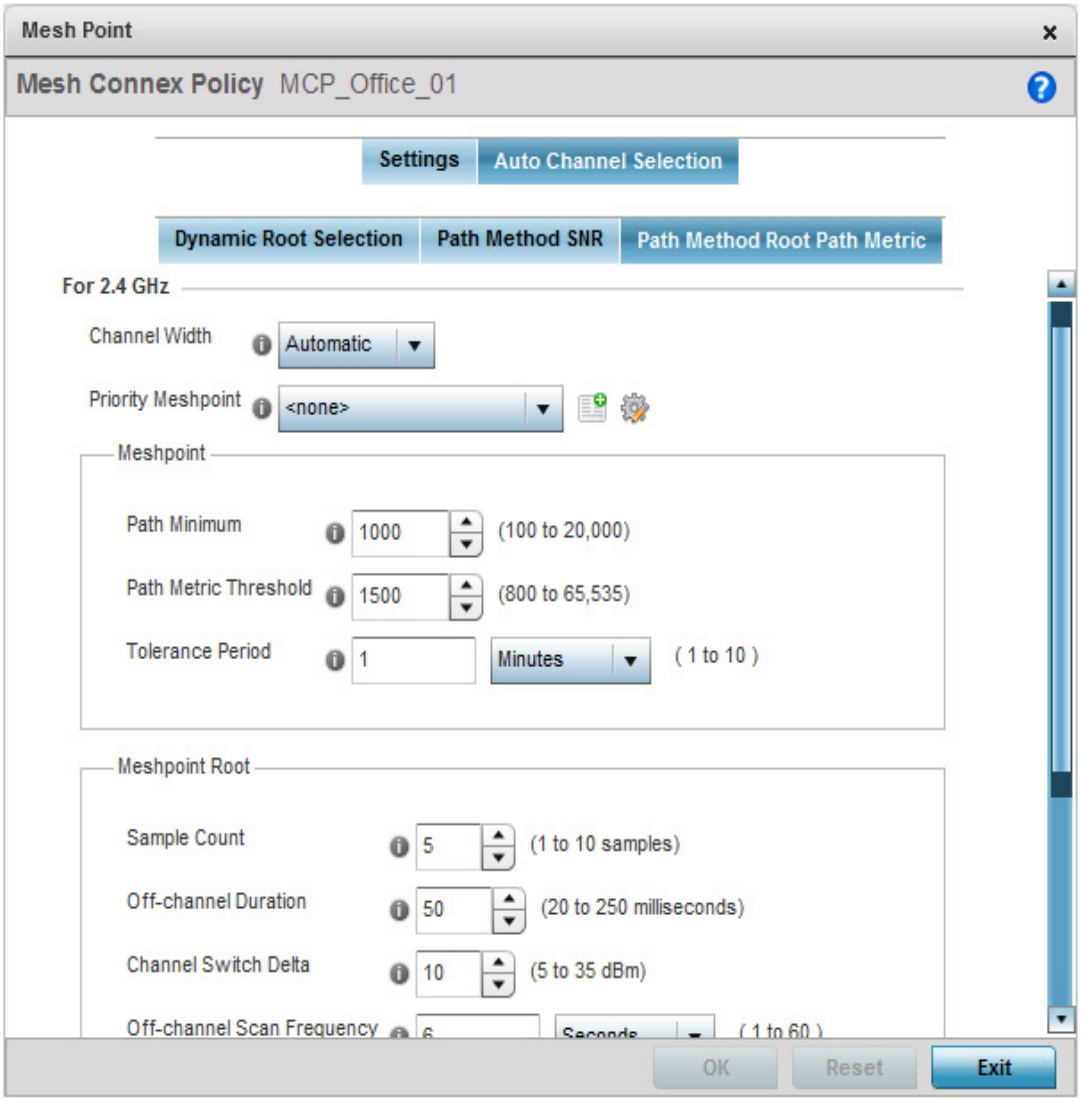


Figure 262: Mesh Point Auto Channel Selection Path Method Root Path Metric screen

11 Refer to the following for more information on the **Path Method Root Path Metric** screen. These descriptions apply to both the 2.4 GHz and 5.0/4.9 GHz frequencies.

Channel Width	Configure the channel width that mesh point automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Indicates the channel width is calculated automatically. This is the default value. • *20 MHz* – Indicates the width between two adjacent channels is 20 MHz. • *40 MHz* – Indicates the width between two adjacent channels is 40 MHz. • *80 MHz* – Indicates the width between tow adjacent channels is 80 MHz. This is only available on access points that support 802.11ac.
Priority Meshpoint	Configure the mesh point to be monitored for automatic channel scan. This is the mesh point that given priority over other available mesh points. When configured, a mesh is created with this mesh point. When not configured, a mesh point is automatically selected. The default is *<none>*.
Meshpoint: Path Minimum	Configure the minimum path metric value for a mesh connection. Set a value between 100 - 20,000.
Meshpoint: Path Metric Threshold	Configure a minimum threshold value for triggering an automatic channel selection for mesh point selection. Set a value in between 800 - 65535.
Meshpoint: Tolerance Period	Configure the time duration in seconds to wait before triggering a automatic channel selection for the next hop.
Meshpoint Root: Sample Count	Configure the number of scans to be performed for data collection before a mesh point root is selected. Set a value between 1 - 10 scans.
Meshpoint Root: Off-channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field when scanning for mesh point root. This is the duration 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 value in dBm in the range 5 - 35 dBm which when crossed triggers a mesh point root automatic channel selection.
Meshpoint Root: Off-channel Scan Frequency	Configure the duration in seconds between two consecutive Off Channel Scans for mesh point root. Set a duration between 1 - 60 seconds.
Meshpoint Root: Channel Hold Time	Configure the minimum duration to stay on a selected channel before the channel conditions are reassessed for a possible channel change for mesh point root. Set a value between 0 - 1440 minutes. Set this value to 'Zero' (0) to prevent a automatic channel selection from happening.

12 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to exit this screen.

13 Select **OK** to save the changes made to the profile's mesh point configuration. Select **Reset** to revert to the last saved configuration.

Vehicle Mounted Modem (VMM) Deployment Consideration

"Mesh Point Configuration"

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”.
- Use *Opportunistic* as the rate selection settings for the AP7161 radio The default is *Standard*. For more information on defining this setting, see “Radio Override Configuration”.
- Disable *Dynamic Chain Selection* (radio setting). The default value is enabled. This setting is disabled from the *Command Line Interface* (CLI) using the **`dynamic-chain-selection`** command, or, in the UI (refer “Radio Override Configuration”.
- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see “Radio Override Configuration”.

Overriding Environmental Sensor Configuration

“Device Overrides”



NOTE

This feature is available on the AP8132 model only.

An AP8132 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 AP8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using the *Environmental Sensor* screen.

To set an environmental sensor configuration for an AP8132 model access point:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices**.

3 Select **Device Overrides** from the options on left-hand side of the UI.

4 Select **Environmental Sensor.**

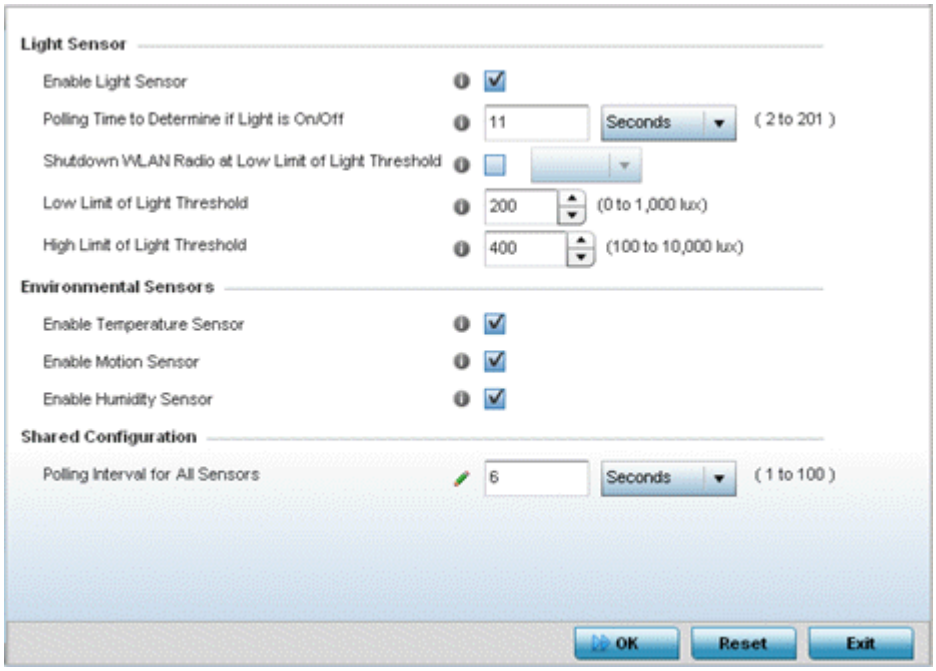


Figure 263: Profile - Environmental Sensor screen

5 Override or set the following **Light Sensor** settings for the AP8132's sensor module:.

Enable Light Sensor	Select this option to enable the light sensor on the module. This setting is enabled by default.
Polling Time to Determine if Light is On/Off	Define an interval in *Seconds* (2 - 201) or *Minutes* (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 11 seconds. Light intensity is used to determine whether the access point's deployment location is currently populated with clients.
Shutdown WLAN Radio at Low Limit of Light Threshold	Select this option to power off the AP8132's radio's if the light intensity falls below the set threshold. If enabled, select *All* (both AP8132 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 AP8132's deployment location. The default is 100.
High Limit of Light Threshold	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the AP8132's deployment location. The default is 500.

6 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 within the Statistics node. This setting is enabled by default.
Enable Motion Sensor	Select this option to enable the module's motion sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.
Enable Humidity Sensor	Select this option to enable the module's humidity sensor. Results are reported back to the access point's Environment screens within the Statistics node. This setting is enabled by default.

7 Define or override the following **Shared Configuration** setting:

Polling Interval for All Sensors	Set an interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between all environmental polling (both light and environment). The default setting is 5 seconds.

8 Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

Overriding an Advanced Configuration

"Device Overrides"

Advanced device settings sets or overrides a profile's MiNT and/or NAS configurations.

MINT secures controller profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. access point managed devices can communicate with each other exclusively over a MINT security domain. Keys can also be generated externally using any application (like openssl). These keys must be present on the managed device managing the domain for key signing to be integrated with the UI. A MAP device that needs to communicate with another first negotiates a security context with that device. The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for access points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

The profile database on the RADIUS server consists of user profiles for each connected *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.

To set or override an advanced configuration:

1 Select **Devices** from the Configuration menu.

2 Select **Device Overrides** to expand its menu items

3 Select a target device from the device browser in the lower, left-hand, side of the UI.

4 Select **Advanced** to expand its sub menu items.

5 Select **Client Load Balancing.**

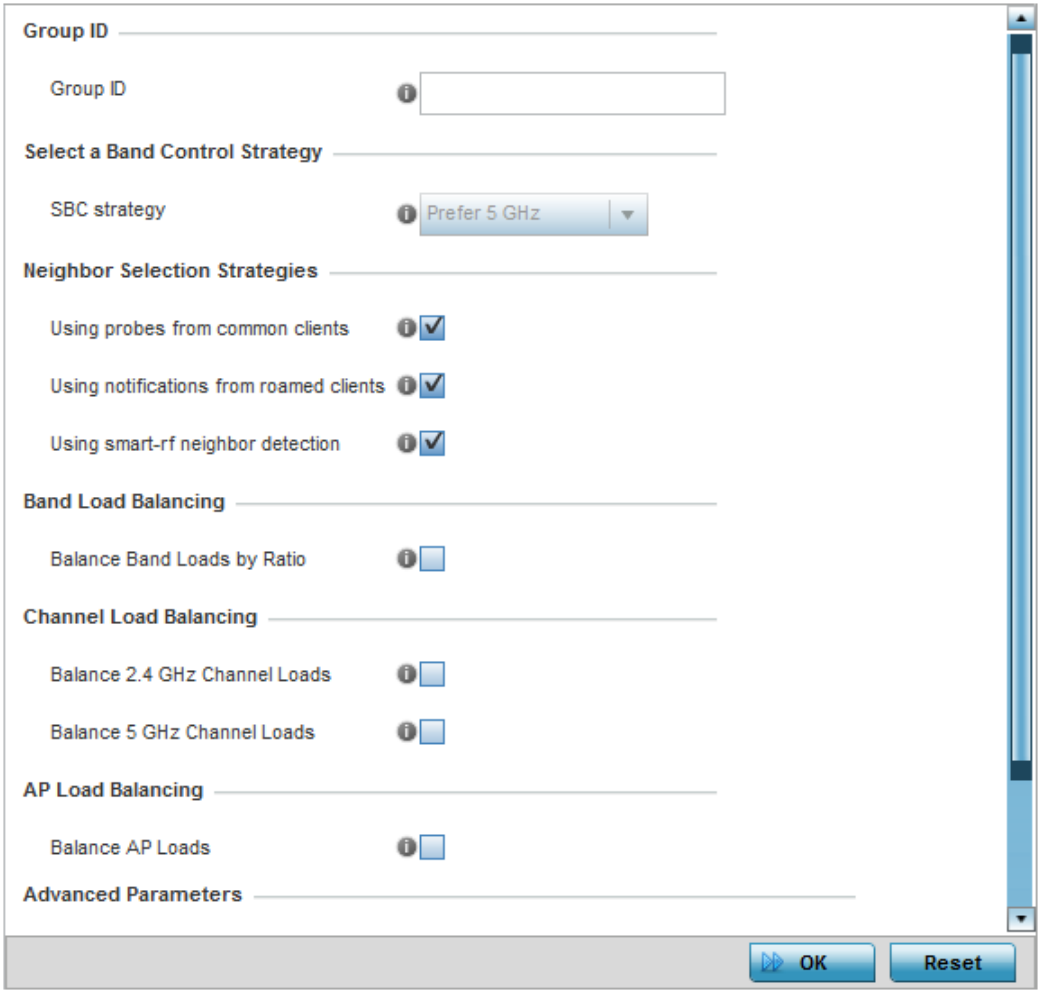


Figure 264: Device Overrides - Client Load Balancing

6 Use the **Group ID** field to define a group ID of up to 32 characters.

7 Use the drop-down to set a value for **SBC strategy**. Options include *Prefer 5GHz, Prefer 2.4 GHz*, and *distribute-by-ratio*. The default value is *Prefer 5GHz*.

8 Refer to the following **Neighbor Selection Strategies** fields to configure or override it:

Using probes from common clients	Select this option to enable neighbor selection using probe requests from common clients between the neighbor device and this device.
Using notifications from roamed clients	Select this option to enable neighbor selection using notifications from clients roamed from other devices.
Using smart-rf neighbor detection	Select this option to enable neighbor selection using Smart RF neighbor detection algorithm.

9 Select **Balance Band Loads by Ratio** to configure or override **Band Load Balancing** configuration.

10 Refer to the following **Channel Load Balancing** fields to configure or override it:

Balance 2.4 GHz Channel Loads	Select this option to balance the access point's 2.4GHz radio load across the channels supported within the country of deployment. This can prevent congestion on the 2.4GHz radio if a channel is over utilized.
Balance 5 GHz Channel Loads	Select this option to balance the access point's 5 GHz radio load across the channels supported within the country of deployment. This can prevent congestion on the 5 GHz radio if a channel is over utilized.

11 Select **Balance AP Loads** to configure or override **AP Load Balancing** configuration.

AP Loads are balance by balancing the radio load, by assigning a ratio to both the 2.4 and 5GHz bands. Balancing radio load by band ratio allows an administrator to assign a greater weight to radio traffic on either the 2.4 or 5 GHz band.

12 Refer to the following **Advanced Parameters**:

Max 2.4 GHz Load Difference Considered Equal	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points.
Min. Value to Trigger 2.4GHz Channel Balancing	Use the spinner control to define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 2.4GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%.
Weightage given to Client Count	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.

Weightage given to Throughput	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.
Max 5 GHz Load Difference Considered Equal	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 5 GHz load between APs load and load on this access point. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing load balances between access points.
Min. Value to Trigger 5 GHz Channel Balancing	Use the spinner control to define a threshold (between 1 - 100) the access point uses (when exceeded) to initiate access point load balancing in the 5GHz radio band. Set this value higher when wishing to keep radio traffic within the current access point. The default is 70%.
Weightage given to Client Count	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.
Weightage given to Throughput	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio throughput in the overall access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.

13 Refer to the following **AP Load Balancing** fields to configure or override them:

Min Value to Trigger Load Balancing	Use the spinner control to set the access point radio threshold value (from 0 - 100%) used to initiate load balancing across other access point radios. When this radio load exceeds the defined threshold, load balancing is initiated. The default is 70%.
Max. AP Load Difference Considered Equal	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing access point radio load balances. The default setting is 1%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing access point radio load balances.
Weightage given to Client Count	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize 2.4 and 5 GHz radio client count in the overall 2.4 and 5GHZ radio load calculation. Assign this value higher if this access point is intended to support numerous clients and their throughput is interpreted as secondary to maintaining client association. The default setting is 90%.
Weightage given to Throughput	Use the spinner control to assign a weight (between 0 - 100) the access point uses to prioritize throughput in the access point load calculation. Assign this value higher if throughput and radio performance are considered mission critical within the access point managed network. The default setting is 10%.

14 Refer to the following **Band Control** parameters to configure or override them:

Max. Band Load Difference Considered Equal	Use the spinner control to set a value (between 0 - 100) considered an adequate discrepancy when comparing 2.4 and 5GHz radio band load balances on this access point. The default setting is 10%. Thus, using a default setting of 1% means 1% is considered inconsequential when comparing 2.4 and 5 GHz load balances on this access point.
Band Ratio (2.4GHz)	Use the spinner control to set a loading ratio (between 0 - 10) the access point 2.4 GHz radio uses in respect to radio traffic load on the 2.4 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 2.4 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 2.4 GHz radio band. The default setting is 1.
Band Ratio (5 GHz)	Use the spinner control to set a loading ratio (between 0 - 10) the access point 5 GHz radio uses in respect to radio traffic load on the 5 GHz band. This allows an administrator to weight client traffic load if wishing to prioritize client traffic load on the 5 GHz radio band. The higher the value set, the greater the weight assigned to radio traffic load on the 5 GHz radio band. The default setting is 1.
5 GHz load which both bands enable	Use the spinner control to set a load percentage (between 0 - 100) that enables the other band (2.4 GHz) to share load with the current band.
2.4 GHz load which both bands enable	Use the spinner control to set a load percentage (between 0 - 100) that enables the other band (5 GHz) to share load with the current band.

15 Refer to the following **Neighbor Selection** parameters to configure or override them:

Minimum signal strength for common clients	Use the spinner to set the minimum signal strength require to learn about neighbors from clients that are common with the neighbor access point.
Minimum number of clients seen	Use the spinner to set the minimum number of common clients seen before the neighbor is learnt.
Max confirmed Neighbors	Use the spinner to set the maximum number of learned neighbors stored at this device.
Minimum signal strength for smart-rf neighbors	Use the spinner to set the minimum signal strength of neighbor devices that are learnt through Smart RF before being recognized as neighbors.

16 Select **MINT Protocol.** The MINT Protocol screen displays the **Settings** tab by default.

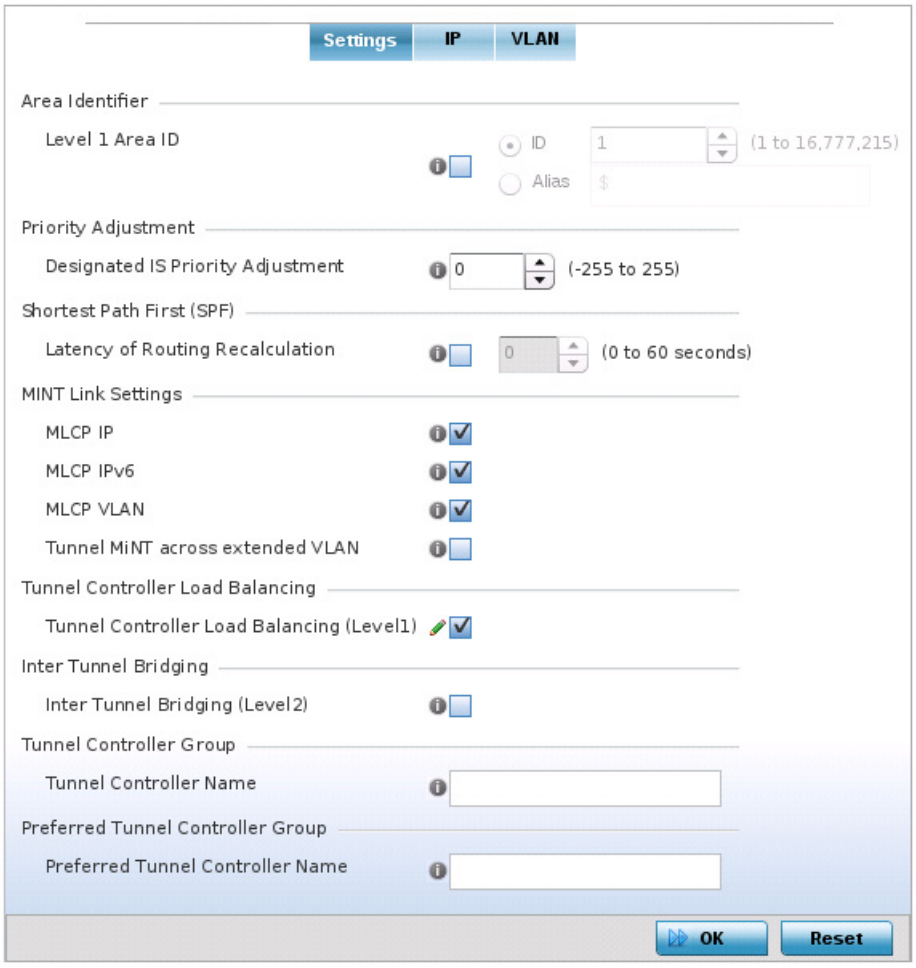


Figure 265: Device Overrides - Advanced Profile Overrides MINT screen - Settings tab

17 Refer to the **Area Identifier** field to define or override the Level 1 and Level 2 Area IDs used by the profile's MINT configuration.

Level 1 Area ID	Select this option to enable a spinner control for setting the Level 1 Area ID from 1 - 16,777,215. The default value is disabled. Alternatively provide an Alias by selecting the *Alias* option and adding the alias name to this field.

18 Define or override the following **Priority Adjustment** settings:

Designated IS Priority Adjustment	Use the spinner control to set a *Designated IS Priority Adjustment* setting from -255 - +255. This is the value added to the base level DIS priority to influence the *Designated IS* (DIS) election. A value of +1 or greater increases DISiness. The default setting is 0.

19 Select the **Latency of Routing Recalculation** option (within the *Shortest Path First* (SPF) field) to enable the spinner control used for defining or overriding a latency period from 0 - 60 seconds. The default setting has the option disabled.

20 Define or override the following **MINT Link Settings**:

MLCP IP	Select this option to enable *MINT Link Creation Protocol* (MLCP) by IP Address. MINT Link Creation Protocol is used to create one UDP/IP link from the device to a neighbor. That neighboring device can be another AP.
MLCP IPv6	Select this option to enable *MINT Link Creation Protocol* (MLCP) by IPv6 Address. MLCP by IPv6 is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a Virtual Controller, it can be an standalone access point.
MLCP VLAN	Select this option to enable MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. That neighboring device can be another AP.
Tunnel MiNT across extended VLAN	Select this option to enable tunneling MiNT protocol packets across extended VLANs.

21 Select the **Tunnel Controller Load Balancing (Level1)** option to enable load balancing on the tunnel controller.

22 Define the group name of clustered tunnel controllers in the **Preferred Tunnel Controller Name** field.

23 Use the **Re-elect Tunnel Controller for this AP** button to re-elect a different tunnel controller. This is specific for this access point only.

24 Select **OK** to save the changes and overrides made to the Settings tab. Select **Reset** to revert to the last saved configuration.

25 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MINT configuration.

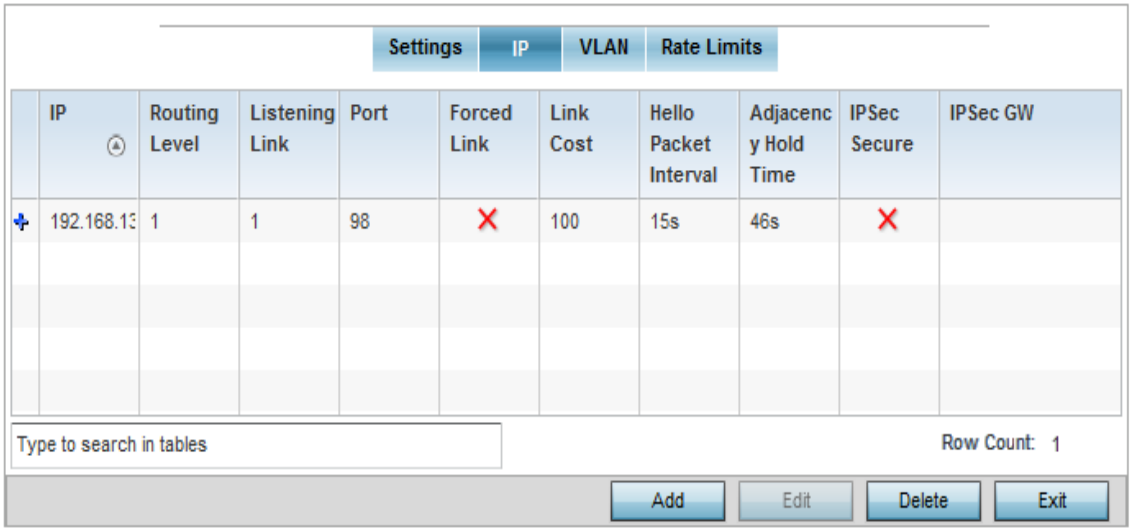


Figure 266: Device Overrides - Advanced Profile MINT screen - IP tab

The IP tab displays the *IP address*, *Routing Level*, *Listening Link*, *Port*, *Forced Link*, *Link Cost*, *Hello Packet Interval, Adjacency Hold Time, IPSec Secure* and *IPSec GW* information that managed devices use to securely communicate amongst one another.

26 Select **Add** to create a new Link IP configuration or **Edit** to override an existing MINT configuration.

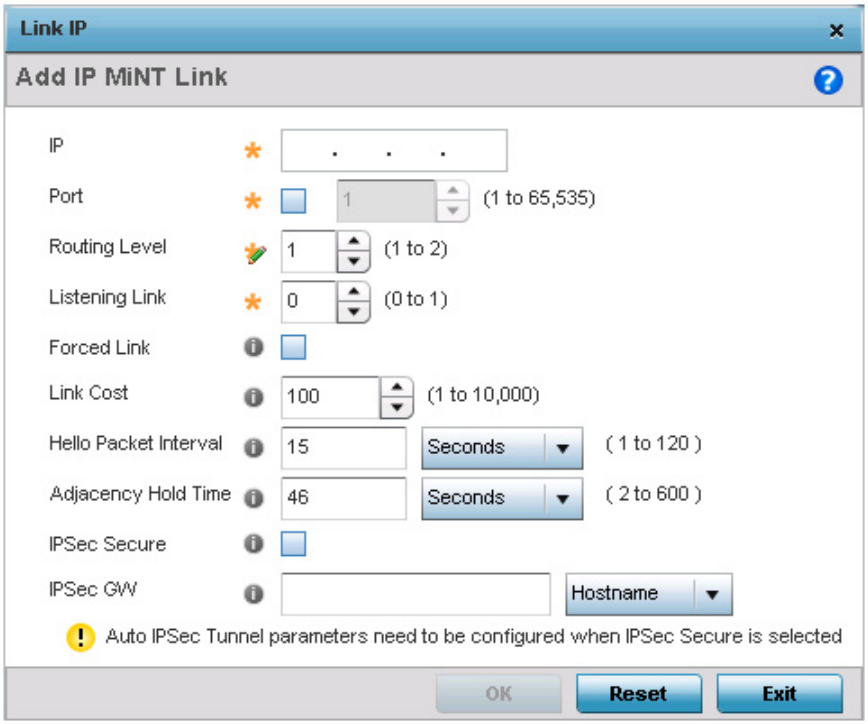


Figure 267: Device Overrides - Advanced Profile MINT screen - IP (Add)

27 Set the following **Link IP** parameters to complete the MINT network address configuration:

IP	Define or override the IP address used by peer access points for interoperation when supporting the MINT protocol.
Port	To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number from 1 - 65,535.
Routing Level	Use the spinner control to define or override a routing level of either 1 or 2.
Listening Link	Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and 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	Select this option to specify the MiNT link as a forced link. This setting is disabled by default.

Link Cost	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
Hello Packet Interval	Set or override an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
Adjacency Hold Time	Set or override a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.
IPSec Secure	Select this option to use a secure link for IPSec traffic. This setting is disabled by default. When enabled, both the header and the traffic payload are encrypted.
IPSec GW	Define either an IP address or hostname for the IPSec gateway.

28 Select **OK** to save the changes and overrides made to MINT protocol's network address configuration. Select **Reset** to revert to the last saved configuration.

29 Select the **VLAN** tab to display the link IP VLAN information shared by the access points managed by the MINT configuration.

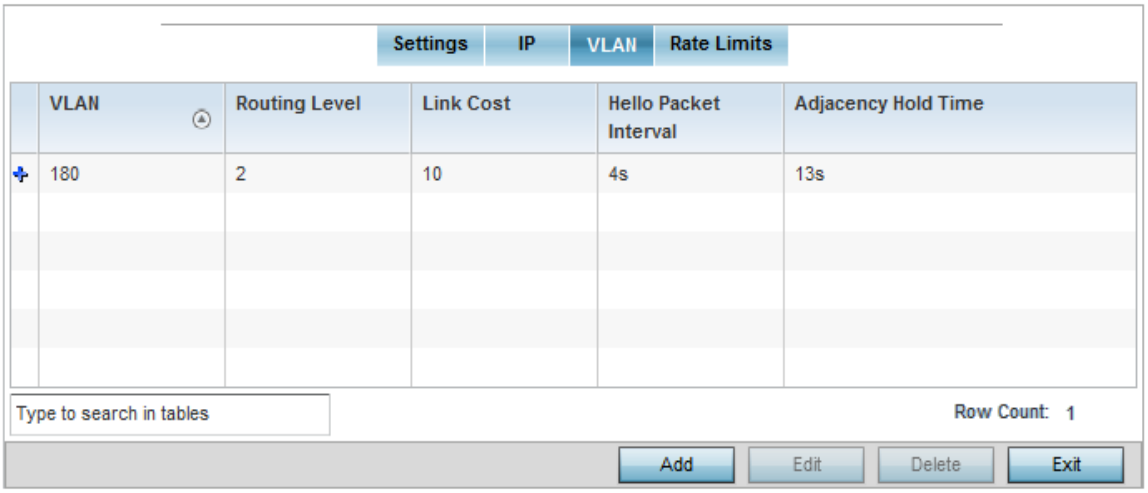


Figure 268: Device Overrides - Advanced Profile MINT screen - VLAN tab

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.

30 Select **Add** to create a new VLAN link configuration or **Edit** to override an existing MINT configuration.

NOTE

If creating a mesh link between two access points in Standalone AP mode, you'll need to ensure a VLAN is available to provide the necessary MINT link between the two Standalone APs.

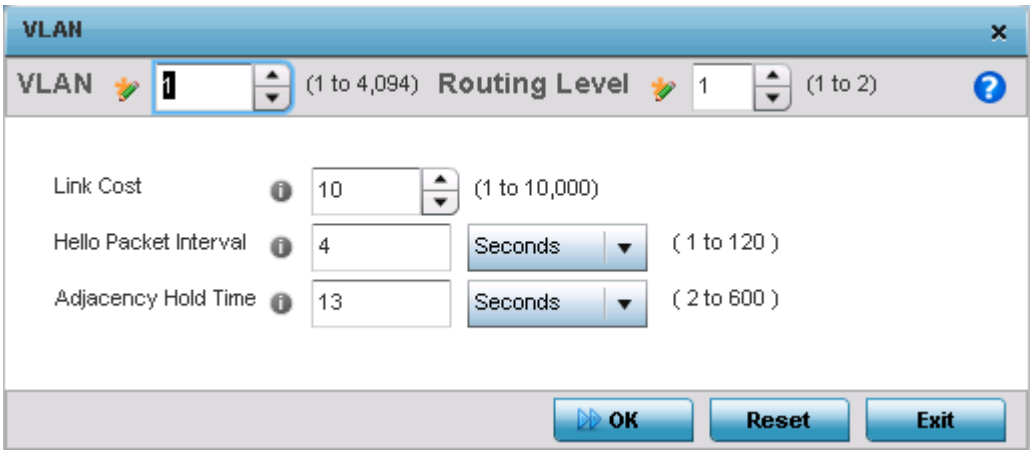


Figure 269: Device Overrides - Advanced Profile MINT screen - Add VLAN screen

31 Set the following VLAN parameters to complete the MINT configuration:

VLAN	Define a VLAN ID from 1 - 4,094 used by peer controllers for interoperation when supporting the MINT protocol.
Routing Level	Use the spinner control to define or override a routing level of either 1 or 2.
Link Cost	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 10.
Hello Packet Interval	Set or override an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 4 seconds.
Adjacency Hold Time	Set or override a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 13 seconds.

32 Select **OK** to save the updates and overrides to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

33 Select the **Rate Limits** tab.

34 The Rate Limits tab displays the **Protocol, Level, Link Type, VLAN**, **IP**, **Port**, **Rate**, **Max Burst Size**, **Background**, **Best-Effort**, **Video** and **Voice rate limiting** parameters for each of the configured devices. Select Add to create a new rate limiting configuration or Edit to override an existing MINT rate limiting configuration.

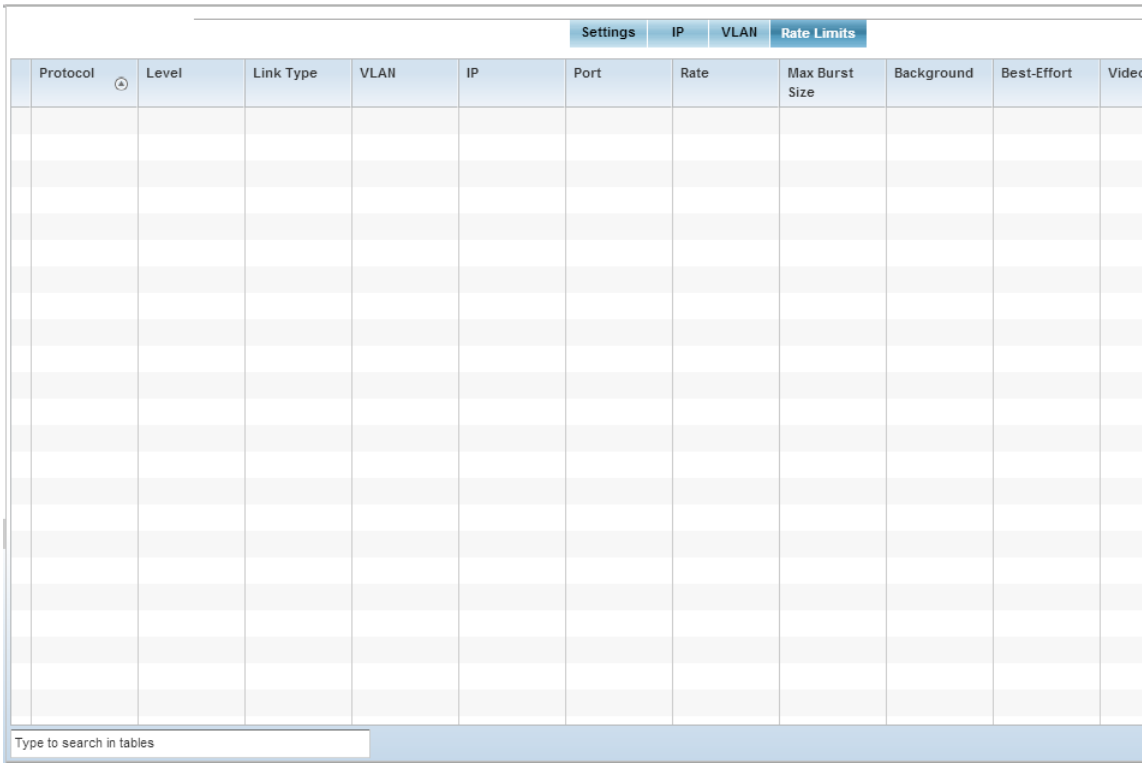


Figure 270: Device Overrides - Advanced Profile MINT screen - Rate Limits screen

35 Select the Rate Limits tab to display data rate limits configured on extended VLANs and optionally add or edit rate limit configurations. Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or access point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream). Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

36 Select **Add** to create a new rate limit configuration or **Edit** to update the configuration of an existing configuration.

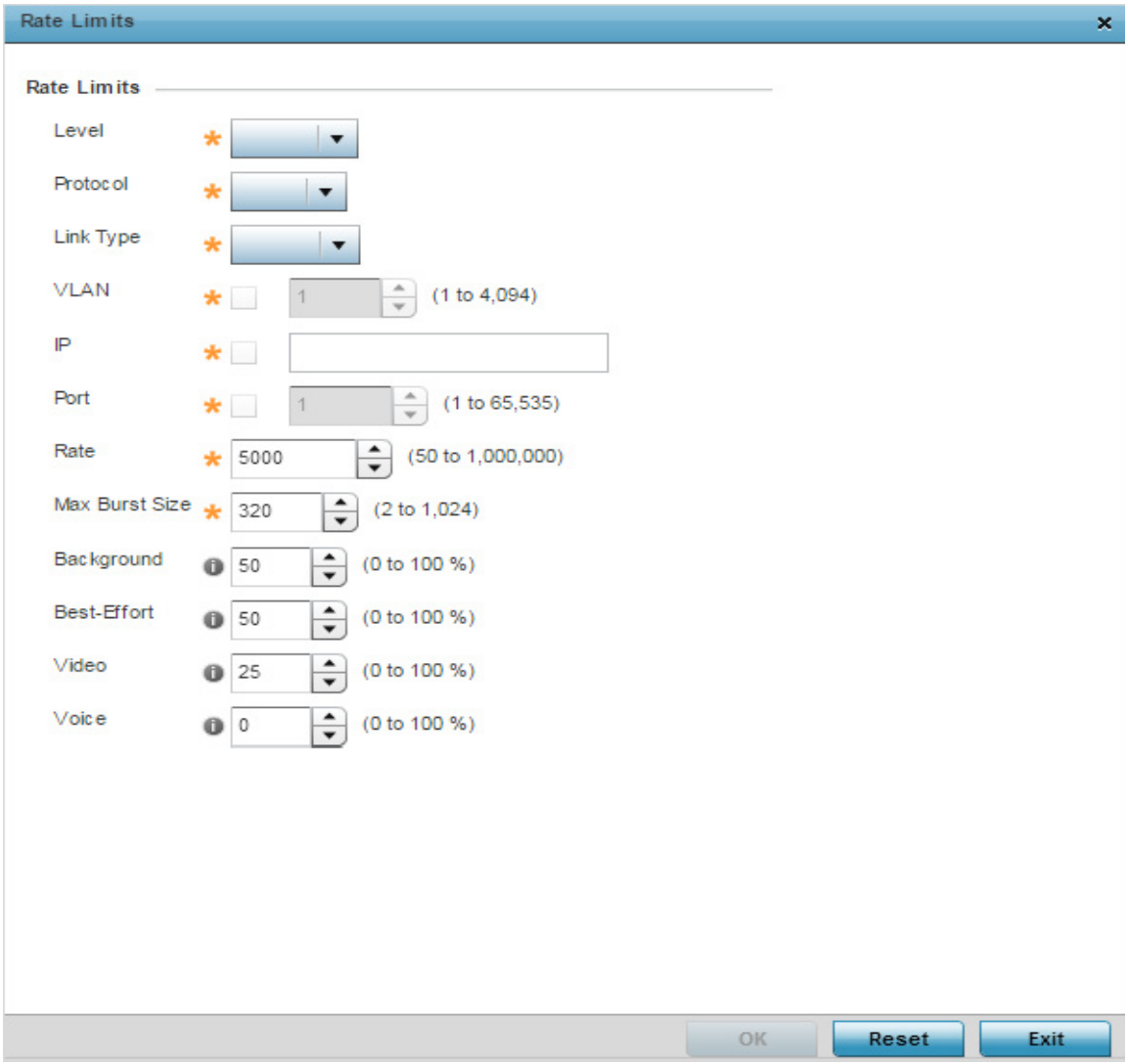


Figure 271: Device Overrides - Advanced Profile MINT screen - Add Rate Limits screen

37 Set the following **Rate Limits** to complete the MINT configuration:

Level	Select *level2* to apply rate limiting for all links on level2.
Protocol	Select either *mlcp* or link as this configuration's rate limit protocol. *Mint Link Creation* Protocol (MLCP) creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an access point with a path to the controller or service platform. Select *link* to rate limit using statically configured MiNT links.
Link Type	Select either *VLAN*, to configure a rate limit configuration on a specific virtual LAN, or *IP* to set rate limits on a static IP address/Port configuration.
VLAN	When the Protocol is set to *link* and the Link Type is set to *VLAN,* use the spinner control to select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN.
IP	When the Protocol is set to *link* and the Link Type is set to *VLAN*, enter the IP address as the network target for rate limiting.
Port	When the Protocol is set to *link* and the Link Type is set to *VLAN*, use the spinner control to set the virtual port (1 - 65,535) used for rate limiting traffic.
Rate	Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Max Burst Size	Use the spinner to set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.
Background	Configures the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.
Best-Effort	Configures the random early detection threshold (as a percentage) for low priority best effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%.
Video	Configures the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%
Voice	Configures the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%.

38 Select **OK** to save the updates and overrides to the MINT Protocol Rate Limits configuration. Select **Reset** to revert to the last saved configuration.

39 Select the **Miscellaneous** menu item.

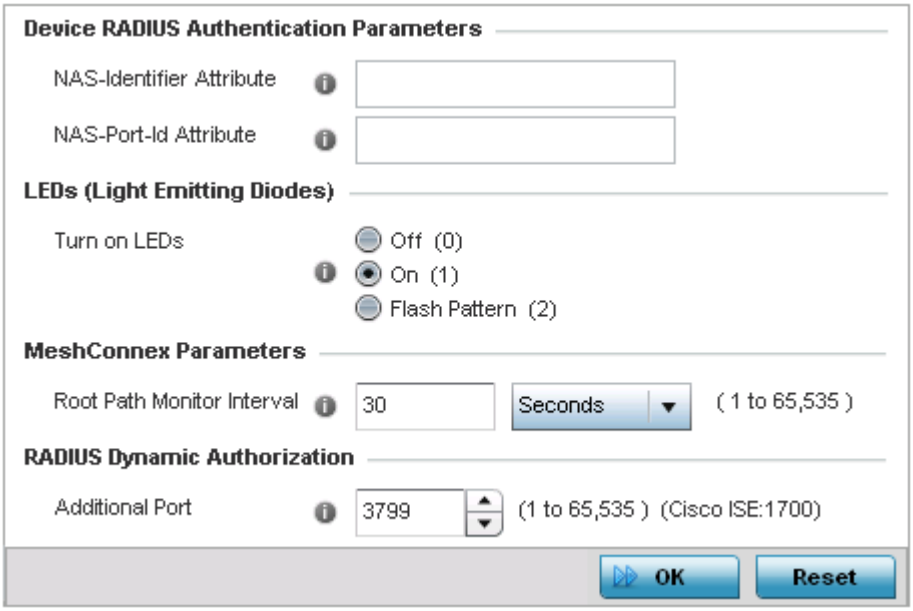


Figure 272: Device Overrides - Miscellaneous screen

40 Set a **NAS-Identifier Attribute** up to 253 characters in length. This is the RADIUS NAS-Identifier attribute that typically identifies where a RADIUS message originates

41 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

42 Refer to the **Turn on LEDs** option to enable an adopted access point's LEDs. This feature is enabled by default.

43 Select the **Flash Pattern** radio button to enable the access point to blink in a manner different from its operational LED behavior. Enabling this option allows an administrator to validate that the access point has received its configuration from its managing controller during staging. In the staging process, the administrator adopts the access point to a staging controller to get an initial configuration before the access point is deployed at its intended location. Once the access point has received its initial configuration, its LED blinks in a unique pattern to indicate the initial configuration is complete.

44 Use the drop-down menu to configure the access point's **Meshpoint Behavior**. This field configures the access point's mobility behavior. The default is *External (fixed)* and indicates that the mesh point is fixed. The value *vehicle-mounted* indicates that the mesh point is mobile. This feature is only available on an AP7161 model access point.

45 Use the **Root Path Monitor Interval** to configure the interval to monitor path to the root node.

46 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. The allowed port range is 1 to 65,535.

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.

47 Set the **Aging Time** value for **Client Bridge**. Use the spinner control to set a value in *days*, *hours*, *minutes* and *seconds*.

48 Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

Managing an Event Policy

"Device Configuration"

Event Policies enable an administrator to create specific notification mechanisms using one, some or all of the SNMP, syslog, controller forwarding or E-mail notification options available to the controller. 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, no event policy is enabled and one needs to be created and implemented.

When initially displayed, the **Event Policy** screen lists the access point interfaces. Existing policies can have their event notification configurations modified as device profile requirements warrant.

To define an access point event policy:

1 Select **Devices** from the Configuration menu.

2 Select **Event Policy**.

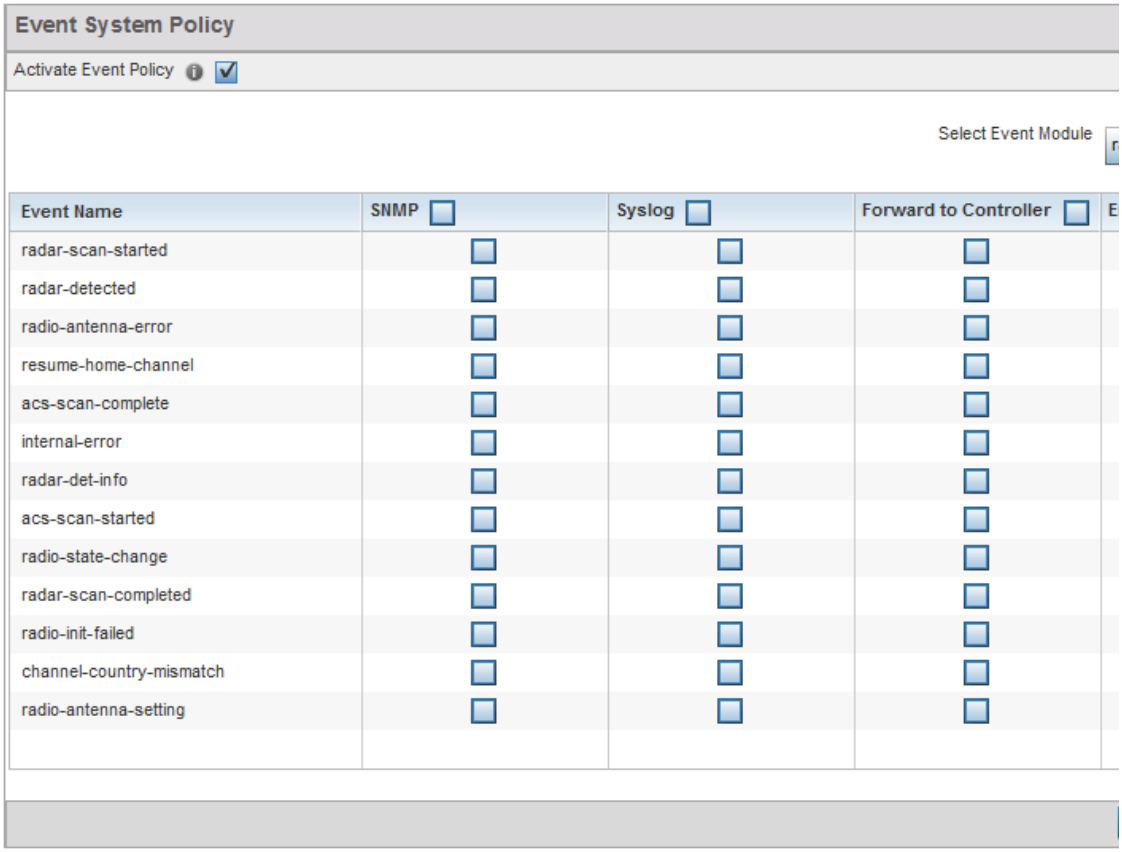


Figure 273: Event Policy screen

3 Ensure the **Activate Event Policy** option 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.

4 Refer to the **Select Event Module** drop-down menu on the top right-hand side of the screen and select an event module used to track the occurrence of each list event.

5 Review each event and select (or deselect) the *SNMP, Syslog, Forward to Controller 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.

6 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. **Delete** obsolete rows as needed.

6 Wireless Configuration

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionality of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. WLANs do not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one 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 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 provide service to specific areas of a site. For example, a guest access WLAN may only be mapped to a 2.4 GHz radio in a lobby or conference room providing limited coverage, while a data WLAN is mapped to all 2.4 GHz and 5.0 GHz radios at the branch site to provide complete coverage.

The wireless configuration is comprised of the following policies:

- "Wireless LANs"
- "WLAN QoS Policy"
- "Radio QoS Policy"
- "Association ACL"
- "SMART RF"
- "MeshConnex Policy"
- "Mesh QoS Policy"
- "Passpoint Policy"
- "Sensor Policy"

Wireless LANs

- "Wireless Configuration"

To review the attributes of existing WLANs and, if necessary, modify their configurations:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

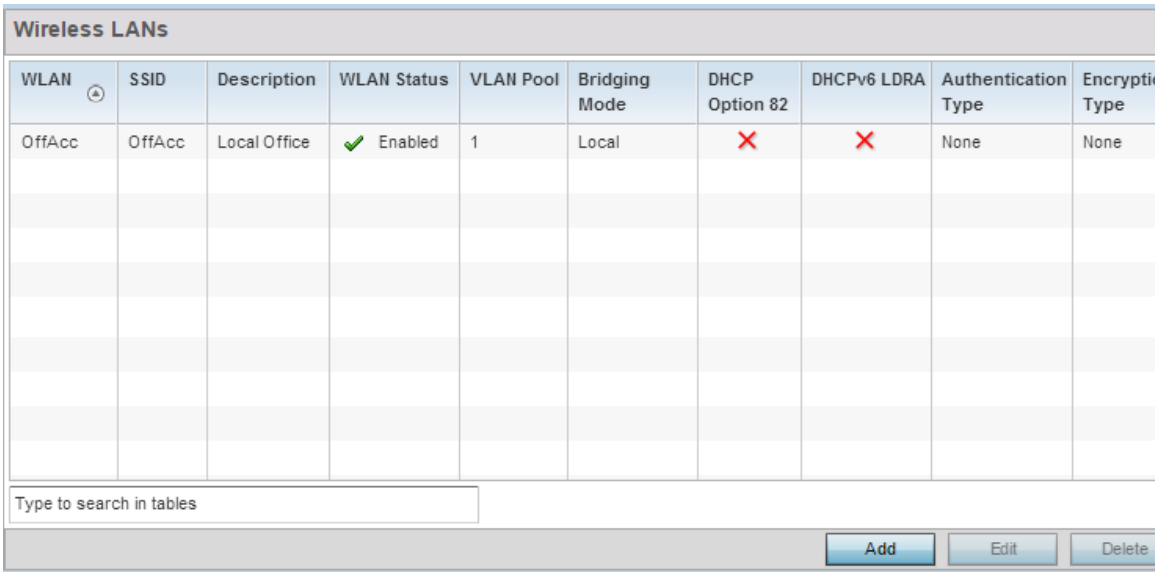


Figure 1: Wireless LANs screen

4 Refer to the following (read-only) information to assess the attributes of each available WLAN:

WLAN	Displays the name of each WLAN available to the access point. Each WLAN can be selected and its SSID and client management properties modified. Each access point can support up to 16 WLANs per radio.
SSID	Displays the name of the SSID assigned to the WLAN when it was created or last modified. Optionally, select a WLAN and select the *Edit* button to update the SSID designation.
Description	Displays the brief description assigned to each listed WLAN when it was either created or modified.
WLAN Status	Lists each WLAN's status as either *Active* or *Shutdown*. 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. When a client associates with a WLAN, the client is assigned a VLAN by means of load-balance distribution. The VLAN is picked from a pool assigned to the WLAN. 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*. Tunnel is the default mode. Local infers VLAN traffic is bridged locally, Tunnel uses a shared tunnel for bridging the WLAN's VLAN traffic.
DHCP Option 82	Displays if DHCP Option 82 is enabled or not. DHCP option 82 provides additional information on the physical attachment of a client

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 authentication scheme used by each listed WLAN to secure client transmissions. *None* is listed if authentication is not used within a WLAN. In case of no authentication, refer to the *Encryption Type* column to verify if there is some sort of data protection used with the WLAN, or risk using this WLAN with no protection at all.
Encryption Type	Displays the name of the encryption scheme used by each listed WLAN to secure client membership transmissions. *None* is listed if encryption is not used within this WLAN. In case of no encryption, refer to the *Authentication Type* column to verify if 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 wireless clients from connecting to a access point managed 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:

- "Configuring WLAN Basic Configuration"
- "Configuring WLAN Security Settings"
- "Configuring WLAN Firewall Settings"
- "Configuring WLAN Client Settings"
- "Configuring WLAN Accounting Settings"
- "Configuring WLAN Service Monitoring Settings"
- "Configuring WLAN Client Load Balancing Settings"
- "Configuring WLAN Advanced Settings"
- "Configuring Auto Shutdown Settings"

Configuring WLAN Basic Configuration

"Wireless LANs"

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 define its SSID, client behavior and VLAN assignments.

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select **Edit** to modify selected WLAN's properties. WLANs can also be removed as they become obsolete by selecting **Delete**.

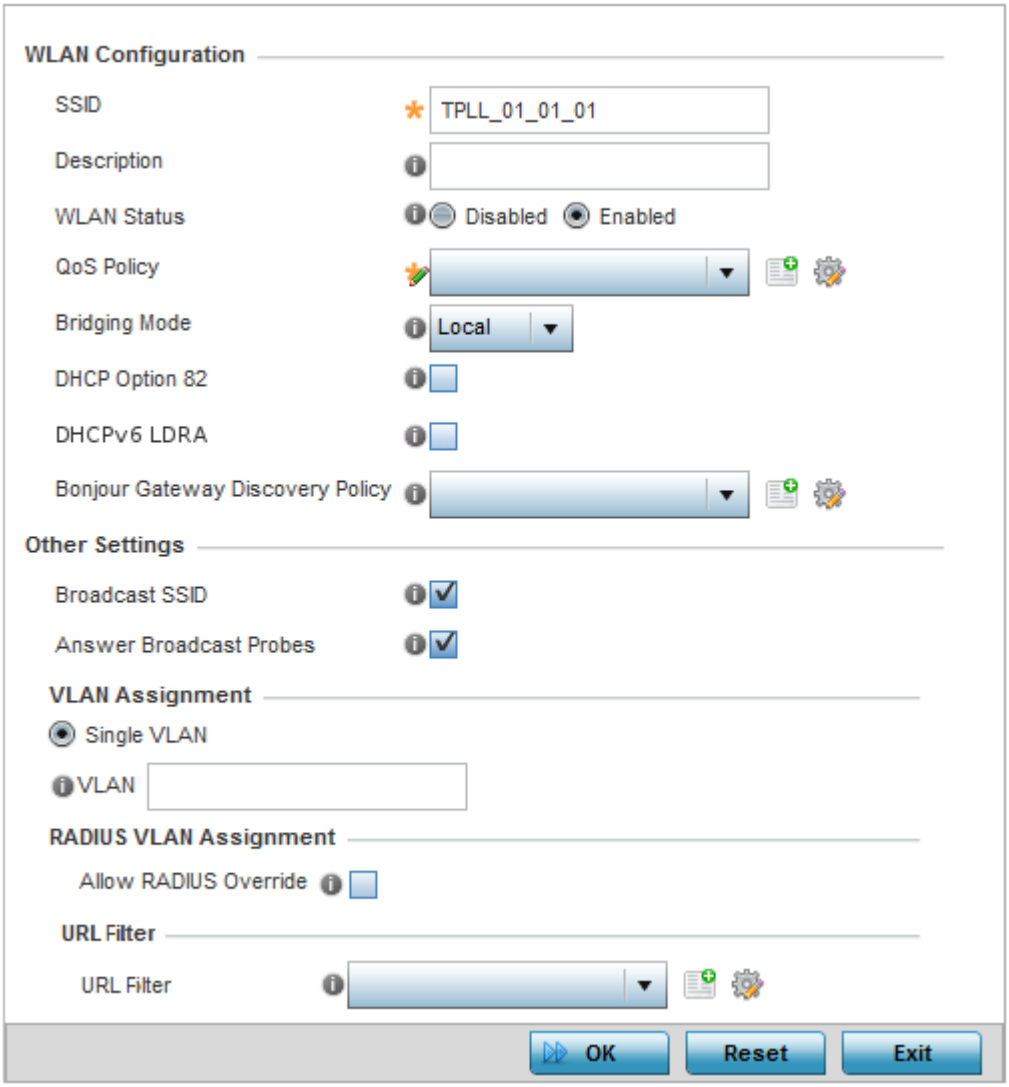


Figure 2: WLAN Basic Configuration screen

5 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 are not permitted. The name could be a logical representation of the WLAN coverage area (engineering, marketing etc.). If editing an existing WLAN, the WLAN's name appears at the top of the screen and cannot be modified. The name cannot exceed 32 characters.
SSID	Enter or modify the *Services Set Identification* (SSID) associated with the WLAN. The WLAN name is auto-generated using the SSID until changed by the user. The maximum number of characters for the SSID is 32.
Description	Provide a textual description for the WLAN to help differentiate it from others with similar configurations. A description can be up to 64 characters.
WLAN Status	Select the *Enabled* radio button to ensure this WLAN is active and available to clients on the 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.
QoS Policy	Use the drop-down menu to assign an existing QoS policy to the WLAN. If needed, select the *Create* icon to define a new QoS policy or select the *Edit* icon to modify the configuration of a 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 a WLAN, see "WLAN QoS Policy" on page 581.
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. Local is the default setting.
DHCP Option 82	Select this option to enable DHCP Option 82. DHCP option 82 provides additional information on the physical attachment of a client This setting is disabled by default
DHCPv6 LDRA	Select this option to enable the DHCPv6 relay agent. The DHCPv6 LDRA (Lightweight DHCP Relay Agent) allows for DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6.
Bonjour Gateway Discovery Policy	Use the drop-down menu to assign an existing Bonjour Gateway Discovery policy to the WLAN. 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. The Bonjour Gateway Discovery Policy configures how Bonjour services can be located on this WLAN. It configures the VLANs on which these services can be found. For more information on Bonjour Gateway Discovery Protocol, see "Setting the Bonjour Gateway Configuration" on page 790.

6 Refer to the **Other Settings** field to define broadcast behavior within this specific WLAN.

Broadcast SSID	Select this radio button to broadcast SSIDs within beacons. If a hacker tries to isolate and hack a client SSID via a client, the ESSID displays since the ESSID is in the beacon. This feature is enabled by default.
Answer Broadcast Probes	Select this radio button to associate a client with a blank SSID (regardless of which SSID the wireless controller is currently using). This feature is enabled by default.

7 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 is 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. Enter the VLAN ID that displays when the *Single VLAN* radio button is selected. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool.
VLAN Pool	Select this radio button to assign a set of VLANs to this WLAN. Use the table to configure the maximum number of clients that can use the configured VLAN. Set a value in the range 0 - 8192 clients.

8 Select **Allow RADIUS Override** to allow the access point to override the client VLAN assignment and use the VLAN assigned by a RADIUS Server instead. 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 that VLAN. If disabled, the RADIUS server returned VLAN ID is ignored and the VLAN configuration (defined in the preceding step) is used.

If RADIUS authentication fails, the VLAN defined is the VLAN assigned to the WLAN.

9 Use the **URL Filter** field to configure user access restrictions to resources in the Internet. User access is controlled by defining URL Filters. Use **URL Filter** 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.

10 Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen back to the last saved configuration.

WLAN Basic Configuration Deployment Considerations

"Configuring WLAN Basic Configuration"

Before defining a WLAN's basic configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Deploy separate VLAN for providing secure WLAN access.
- Define separate VLAN for each WLAN providing guest access.

Configuring WLAN Security Settings

"Wireless LANs"

Assign WLANs unique security configurations supporting authentication, captive portal (hotspot), self registration or encryption schemes as data protection requirements dictate.

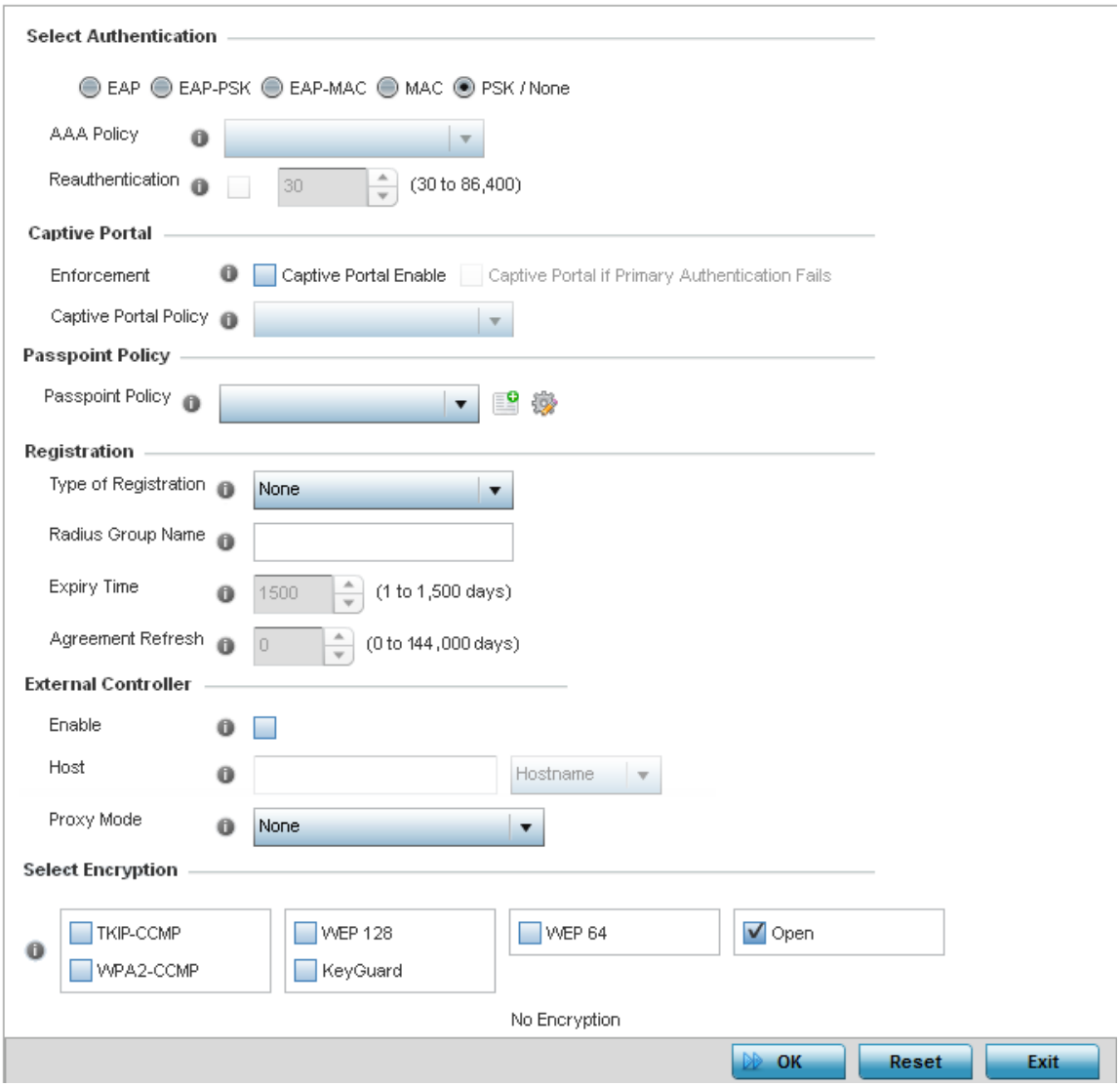


Figure 3: WLAN Security screen

Authentication ensures only known and trusted users or devices access an access point managed 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 user name, password and secret-key information.

A client must authenticate to an access point to receive resources from the network. *802.1x EAP*, *802.1x EAP-PSK*, *MAC* and *PSK/None* authentication options are supported.

Refer to the following to configure a WLAN's authentication scheme:

- "802.1x EAP, EAP-PSK and EAP MAC"
- "MAC Authentication"
- "PSK / None"

Secure guest access to the network is referred to as captive portal. A captive portal is guest access policy for providing temporary and restrictive access to the access point managed

wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

A captive portal policy provides secure authenticated access using a standard Web browser. A captive portal provides authenticated access by capturing and re-directing a wireless user's Web browser session to a login page, where a user must enter valid credentials to access the network. Once logged into the captive portal, additional *Agreement*, *Welcome* and *Fail* pages provide an administrator with a number of options for the screen flow and appearance.

Refer to "Captive Portal" on page 538 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 Policy".

MAC Registration enables returning captive portal users faster authentication and access to the captive portal service. When the user connects to the captive portal for the first time, the MAC address of the user is recorded once the authentication is successful. The next time the device is used to access the captive portal, MAC Registration allows the device and the user to be authenticated faster.

Refer to "MAC Registration" on page 539 for information on enabling and configuring MAC Registration.

Encryption is essential 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 scheme for securing a WLAN. WEP is typically used with WLAN deployments supporting legacy clients. New 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 a WLAN's encryption scheme:

- "TKIP-CCMP"
- "WPA2-CCMP"
- "WEP 64"
- "WEP 128"
- "Keyguard"

802.1x EAP, EAP-PSK and EAP MAC

"Configuring WLAN Security Settings"

The *Extensible Authentication Protocol* (EAP) 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 wireless controller managed 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 a 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 resides externally to the access point. User account creation and maintenance can be provided centrally using RFMS or individually maintained on each device. If an external RADIUS server is used, EAP authentication requests are forwarded.

When using PSK with EAP, packets are sent requesting a secure link using a pre-shared key. The access point and authenticating device must use the same authenticating algorithm and passcode. 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 the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its security properties.

5 Select **Security**.

6 Select **EAP**, **EAP-PSK** or **EAP MAC** as the Authentication Type.

Either authentication type enables the radio buttons for various encryption options as an additional measure of security with the WLAN that can be used with EAP.

7 Either select an existing **AAA Policy** from the drop-down menu, select the **Create** icon to the right of the AAA Policy parameter to create a new AAA policy, or select the **Edit** icon to modify the selected AAA policy's 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. For information on defining a new AAA policy, see "AAA Policy" on page 663.

8 Select the **Reauthentication** check box to force EAP supported clients to reauthenticate. Use the spinner control set the number of seconds (from 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate to use the resources supported by the WLAN.

9 Select **OK** to update the WLAN's EAP configuration. Select **Reset** to revert back to the last saved configuration.

EAP, EAP-PSK and EAP MAC Deployment Considerations

"802.1x EAP, EAP-PSK and EAP MAC"

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:

- It is recommended that a valid certificate 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, ensure that the round trip delay over the WAN does not exceed 150 ms. Excessive delay over a WAN can cause authentication and roaming issues and impact wireless client performance.

MAC Authentication

"Configuring WLAN Security Settings"

MAC is a device-level authentication method used to augment other security schemes. MAC can be used open, with *WEP 64* or *WEP 128*, *KeyGuard*, *TKIP* or *CCMP*.

MAC authentication enables 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 time and date access restrictions.

MAC authentication can only identify 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 mimic a trusted device within the network.

MAC authentication is enabled per WLAN, augmented with the use of a RADIUS server to authenticate each device. A device's MAC address can be authenticated against an access

point's local RADIUS server (if supported) 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 the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify its security properties.

5 Select **Security**.

6 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.

7 Either 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. A default AAA policy is also available if configuring a WLAN for the first time and there's no existing policies. Select the **Edit** icon to modify the configuration of a selected AAA policy.

Authentication, Authorization, and Accounting (AAA) is a framework for intelligently controlling access to the wireless client managed network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows. For information on defining a new AAA policy, see "AAA Policy" on page 663.

8 Select the **Reauthentication** check box to force MAC supported clients to reauthenticate. Use the spinner control set the number of minutes (from 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate.

9 Select **OK** when completed to update the WLAN's MAC configuration. Select **Reset** to revert the screen back to the last saved configuration.

MAC Authentication Deployment Considerations

"MAC Authentication"

Before defining a MAC authentication configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- MAC authentication can only be used to identify end-user devices, not the users themselves.
- MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provision a MAC address on their device to mimic a trusted device.

PSK / None

"Configuring WLAN Security Settings"

Open-system authentication can be referred to as no authentication, since no actual authentication and user credential validation takes place. When selecting PSK/None, a client requests (and is granted) authentication with no credential exchange.



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

"Configuring WLAN Security Settings"

A *captive portal* is guest access policy that provides temporary and restrictive access to the wireless network. The primary means of securing such guest access is the use of a captive portal. For an overview of the captive portal process and information on how to define a captive portal policy that can be applied to a WLAN, see "Configuring Captive Portal Policies" on page 759.

To assign a captive portal policy to a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.

5 Select **Security**.

6 Refer to the **Captive Portal** field within the WLAN security screen.

Select the **Captive Portal Enable** option if authenticated guess access is required with the selected WLAN. This feature is disabled by default.

7 Select the **Captive Portal if Primary Authentication Fails** option to enable the captive portal policy if the primary authentication is unavailable. This option is only enabled when **Captive Portal Enable** is selected.

8 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 "Configuring Captive Portal Policies" on page 759.

9 Select **OK** when completed to update the captive portal configuration. Select **Reset** to revert the screen back to the last saved configuration.

Passpoint Policy

"Configuring WLAN Security Settings"

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.

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the Add button to create an additional WLAN, or select an existing WLAN and Edit to modify its properties.

5 Select Security.

6 Refer to the **Passpoint** field within the WLAN Policy security screen.

7 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 637.

8 Select **OK** when completed to update the Captive Portal configuration. Select **Reset** to revert the *WLAN Policy Security* screen back to the last saved configuration.

MAC Registration

"Configuring WLAN Security Settings"

The MAC Registration feature provides returning captive portal users quicker access to the captive portal.

When a user accesses the captive portal for the first time, user information is gathered and stored. This information is matched with the MAC address of the device accessing the captive portal. This information is stored on board the access point.

The next time the user accesses the captive portal service using the same device, he/she is authenticated immediately as the MAC address of the device is available in the access point's database along with the user's identification information. The user saves time as identification information is not collected again speeding the logon.

The MAC Registration feature must be enabled for each captive portal WLAN.

To enable MAC Registration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the Add button to create an additional WLAN, or select an existing WLAN and Edit to modify its properties.

5 Select Security.

6 Refer to the Registration field within the WLAN security screen.

Select the **Type of Registration** field to select the type of MAC registration to use with this WLAN.

Use *None* to disallow use of MAC Registration with this WLAN. Select *device* to register a new MAC address. If a MAC address already exists, allow access. Select *device-OTP* to register a new MAC device and send a *One Time Password* (OTP) for validation. Select *user* to register a new user by sending them a registration code to the e-mail address or mobile phone number provided by the user at login.

7 Use the **Radius Group Name** field to enter the RADIUS Group to associate with MAC registrations. When left blank, devices are not associated with a RADIUS group.

8 Select Expiry Time. This is the duration for which MAC addresses are stored on the access point's database. Once this time expires, the user information is purged from the database. The user then has to provide login credentials as well as identification information again. The default value is 1500 days.

9 Set the **Agreement Refresh** as the amount of time before the agreement page is displayed if the user has not been logged during the specified period. The default setting is 0 days.

10 Select OK when completed to update the MAC Registration configuration. Select Reset to revert the screen back to the last saved configuration.

External Controller

"Configuring WLAN Security Settings"

External controller configuration enables this WLAN to be managed by a remote wireless controller. This feature is disabled by default.

To configure the external server information:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the Add button to create an additional WLAN, or select an existing WLAN and Edit to modify its properties.

5 Select Security.

6 Refer to the **External Controller** field within the WLAN security screen.

7 Select the **Enable** option to enable this WLAN to be managed by an external controller.

8 Use the **Host** field to enter a hostname/IP address of the remote wireless controller. Use the spinner control to select the type of the remote controller.

9 Use the **Proxy Mode** drop-down to configure the proxy mode for accessing remote resources.

10 Select OK when completed to update the External Controller configuration. Select Reset to revert the screen back to the last saved configuration.

TKIP-CCMP

"Configuring WLAN Security Settings"

The encryption method is *Temporal Key Integrity Protocol* (TKIP). 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 *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result.

To configure TKIP-CCMP encryption on a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify its properties.

5 Select **Security**.

6 Select the **TKIP-CCMP** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a TKIP-CCMP configuration for the WLAN.

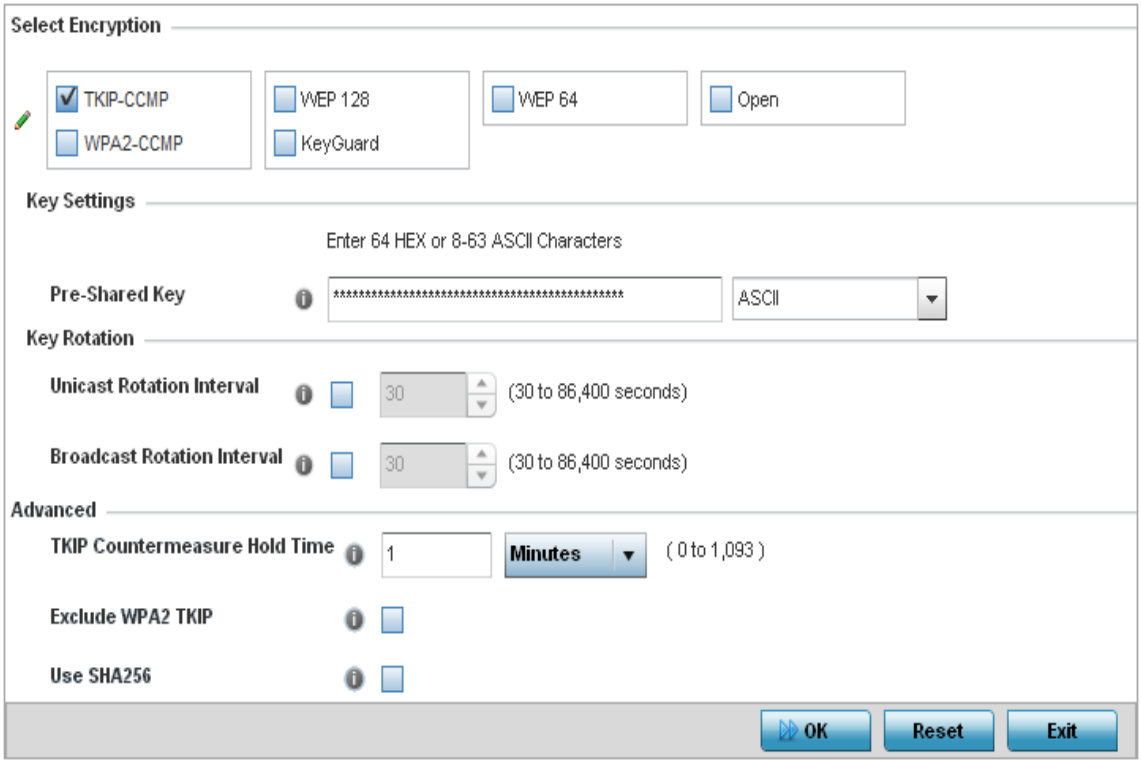


Figure 4: WLAN Security - TKIP-CCMP screen

7 Define the **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 access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

8 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 2 keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for all clients in that subnet.

Frequent rotating of these keys is recommended so that 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/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.

9 Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.



NOTE

Fast Roaming is available only when the authentication is *EAP* or *EAP-PSK* and the selected encryption is either *TKIP-CCMP* or *WPA2-CCMP.*

Using 802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, **Opportunistic Key Caching** allows multiple access points to share PMKs amongst themselves. This allows a client to roam to an access point it has

not previously visited and reuse a PMK from another access point to skip 802.1x authentication.

Pre-Authentication	Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1X authentication with other detected access points while still connected to its current access point. When a device roams to a neighboring access point, the device is already authenticated on the access point, thus providing faster re-association.
Pairwise Master Key (PMK) Caching	*Pairwise Master Key* (PMK) Caching is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1X authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated.
Opportunistic Key Caching	This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner.

10 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. It is recommended to enable this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.
Use SHA256	Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits. This feature is disabled by default.

11 Select **OK** when completed to update the WLAN's TKIP-CCMP encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

TKIP-CCMP Deployment Considerations

"TKIP-CCMP"

Before defining a WPA-TKIP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- It is recommend that TKIP only be enabled for legacy device support when WPA2-CCMP support is not available.
- Though 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. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

WPA2-CCMP

"Configuring WLAN Security Settings"

WPA2 is a newer 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the provided keys 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 for associated clients.

To configure WPA2-CCMP encryption on a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.

5 Select **Security**.

6 Select the **WPA2-CCMP** radio button from within the select **Select Encryption** field.

The screen populates with the parameters required to define a WPA2-CCMP configuration for the WLAN.

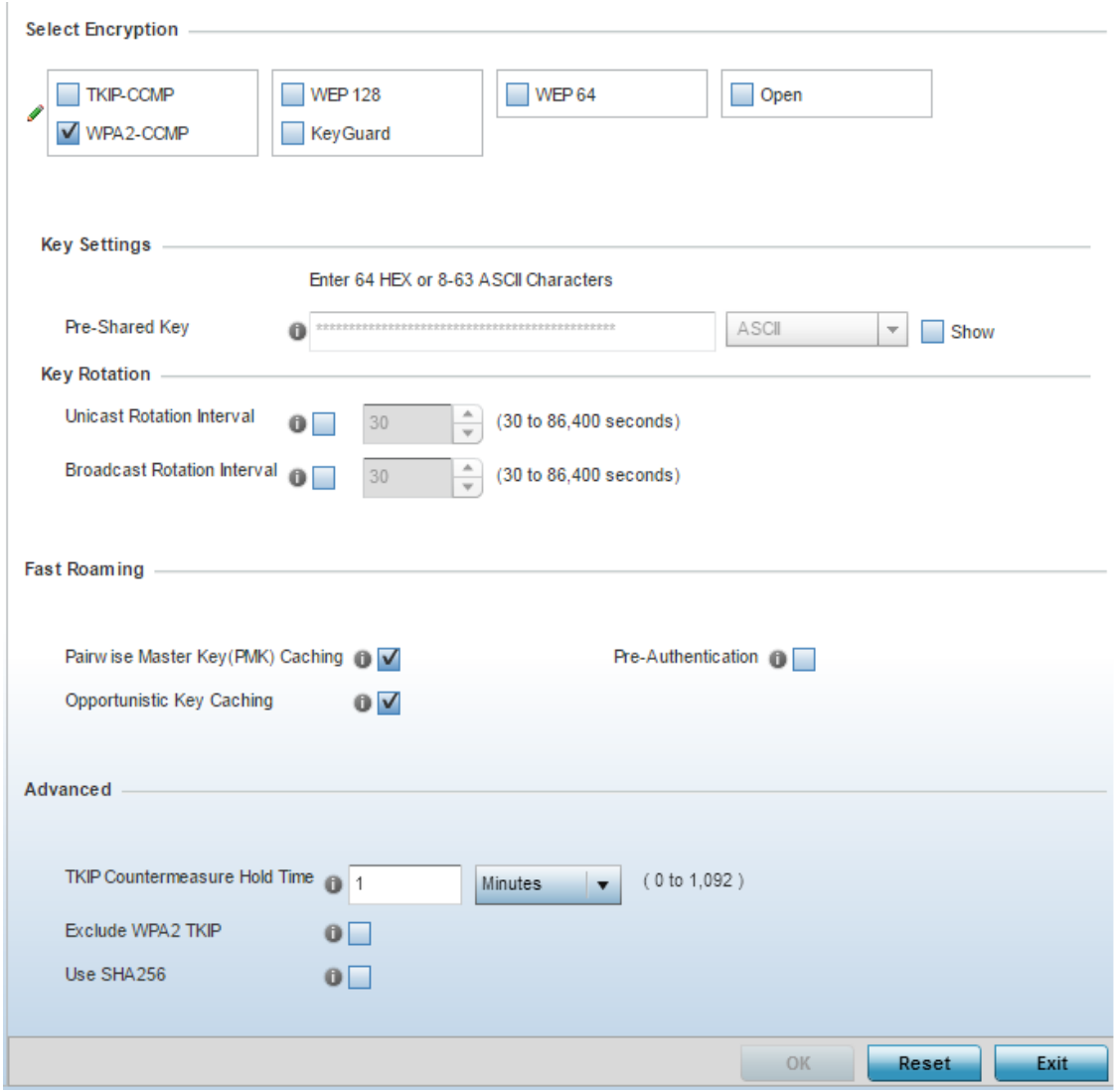


Figure 5: WLAN Security - WPA2-CCMP screen

7 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 access point converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

8 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-CCMP, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for clients in that subnet.

Frequent rotating of these keys is recommended so that a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

Unicast Rotation Interval	Define a unicast key transmission interval from 30 - 86,400 seconds. Some clients have issues using unicast key rotation, so ensure you know which clients are impacted before using unicast keys. This value is disabled by default.
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic will be 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 value is disabled by default.

9 Define the **Fast Roaming** configuration used only with 802.1x EAP-WPA/WPA2 authentication.



NOTE

Fast Roaming is available only when the authentication is *EAP* or *EAP-PSK* and the selected encryption is either *TKIP*-CCMP or *WPA2-CCMP.*

802.11i can speed up the roaming process from one access point to another. Instead of doing a complete 802.1x authentication each time a client roams between access points, 802.11i allows a client to re-use previous PMK authentication credentials and perform a four-way handshake. This speeds up the roaming process. In addition to reusing PMKs on previously visited access points, Opportunistic Key Caching allows multiple access points to share PMKs amongst themselves. This allows a client to roam to an access point it has not previously visited and reuse a PMK to skip 802.1x authentication.

Pre-Authentication	Selecting this option enables an associated client to carry out an 802.1x authentication with another access point before it roams to it. This enables a roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre-authentication, a client can perform an 802.1X authentication with other detected access points while still connected to its current access points. When a device roams to a neighboring access points, the device is already authenticated, thus providing faster re-association.
Pairwise Master Key (PMK) Caching	*Pairwise Master Key* (PMK) Caching is a technique for sidestepping the need to re-establish security each time a client roams to a different switch. Using PMK caching, clients and switches cache the results of 802.1X authentications. Therefore, access is much faster when a client roams back to a switch to which the client is already authenticated.
Opportunistic Key Caching	This option enables the access point to use a PMK derived with a client on one access point, with the same client when it roams over to another access point. Upon roaming, the client does not have to do 802.1x authentication and can start sending and receiving data sooner.

10 Set the following **Advanced** 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 minute.
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. It is recommended to enable this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.
Use SHA256	Select this option to enable SHA-256 authentication key management suite. This suite consists of a set of algorithms for key agreement, key derivation, key wrapping, and content encryption and provide a minimum cryptographic security level of 128 bits. This feature is disabled by default.

11 Select **OK** when completed to update the WLAN's WPA2-CCMP encryption configuration. Select **Reset** to revert back to its last saved configuration.

WPA2-CCMP Deployment Considerations

"WPA2-CCMP"

Before defining a WPA2-CCMP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- It is recommended that WPA2-CCMP be configured for all new (non visitor) WLANs requiring encryption, as it is supported by the majority of the hardware and client vendors using our 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

"Configuring WLAN Security Settings"

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi -Fi) 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.

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 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.

To configure WEP 64 encryption on a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select **Edit** to modify the properties of an existing wireless controller WLAN.

5 Select **Security**.

6 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 WLAN.

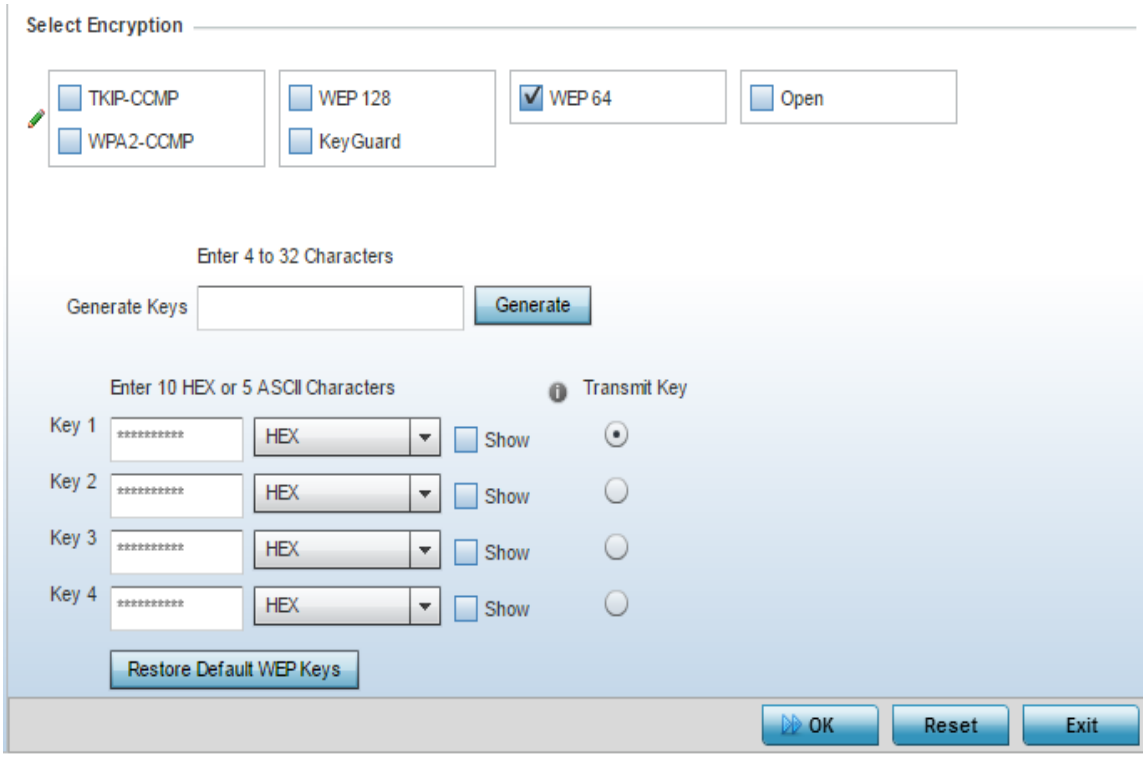


Figure 6: WLAN Security - WEP 64 screen

7 Configure the following WEP 64 settings:

Generate Keys	Specify a 4 to 32 character pass key and select the *Generate* button. The pass key can be any alphanumeric string. The wireless controller, other proprietary routers, and WiNG clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without these WiNG adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. Select one of these keys for default activation by selecting its radio button. Select *Show* to display the actual characters comprising the key.
Restore Default WEP Keys	Select this radio button to restore the WEP algorithm back to its default settings.

Default WEP 64 keys are as follows:

- Key 1 1011121314
- Key 2 2021222324
- Key 3 3031323334
- Key 4 4041424344

8 Select **OK** when completed to update the WLAN's WEP 64 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

WEP 64 Deployment Considerations

"WEP 64"

Before defining a WEP 64 supported configuration on a WLAN, refer to the following deployment guideline to ensure the configuration is optimally effective:

- It is recommended that additional layers of security (beyond WEP 64) 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 only be permitted access to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

WEP 128

"Configuring WLAN Security Settings"

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi -Fi) 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 *initialization vector* (IV) 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 only recommended if there are client devices that are 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 provide 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 the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or select **Edit** to modify the properties of an existing WLAN.

5 Select **Security**.

6 Select either 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 WLAN.

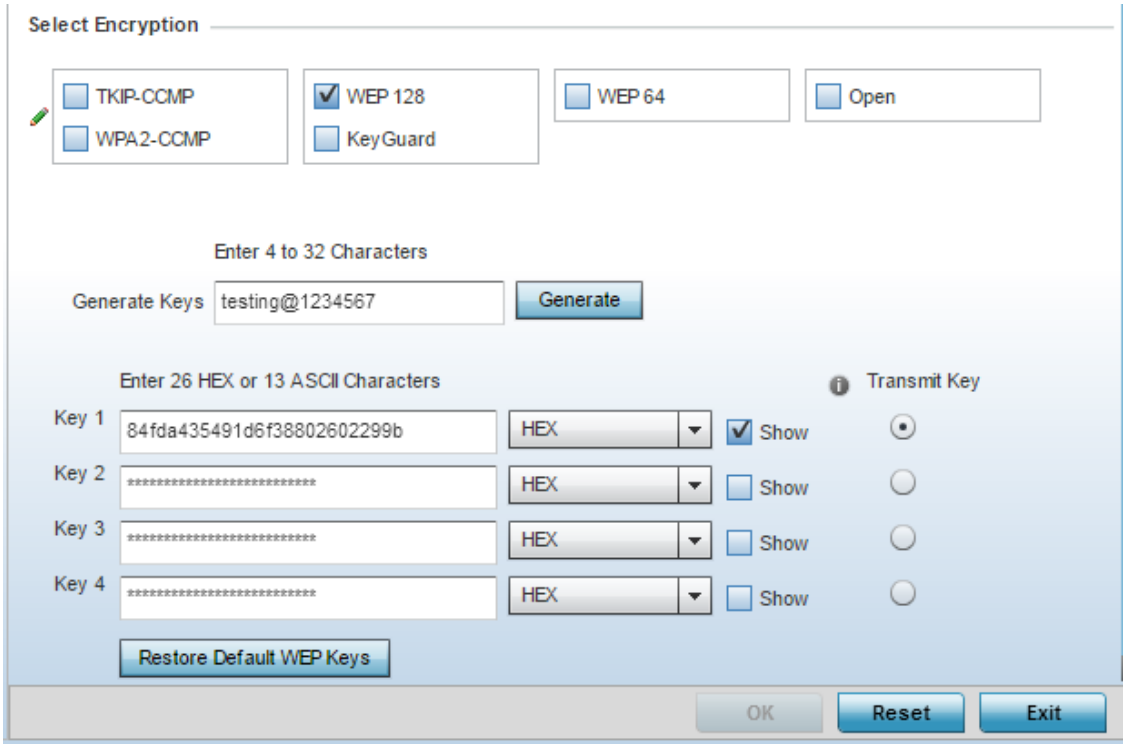


Figure 7: WLAN Security - WEP 128 screen

7 Configure the following WEP 128 settings:

Generate Keys	Specify a 4 to 32 character pass key and select the *Generate* button. The pass key can be any alphanumeric string. The access point, other proprietary routers, and WiNG clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without these WiNG adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 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 selecting its radio button. Select *Show* to display the actual characters comprising the key.
Restore Default WEP Keys	If you feel it necessary to restore the WEP algorithm back to its default settings, select the *Restore Default WEP Keys* button.

Default WEP 128 or Keyguard keys are as follows:

- Key 1 10111213141516171819 1A1B1C
- Key 2 20212223242526272829 2A2B2C
- Key 3 30313233343536373839 3A3B3C
- Key 4 40414243444546474849 4A4B4C

8 Select **OK** when completed to update the WLAN's WEP 128 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

WEP 128 Deployment Considerations

"WEP 128"

Before defining a WEP 128 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- It is recommended that additional layers of security (beyond WEP) 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 only be permitted access to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation

Keyguard

"Configuring WLAN Security Settings"

Keyguard is a form of WEP, and could be all a small business needs for the simple encryption of wireless data.

KeyGuard is an enhancement to the WEP encryption method, 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 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an WLAN.

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 WLAN.

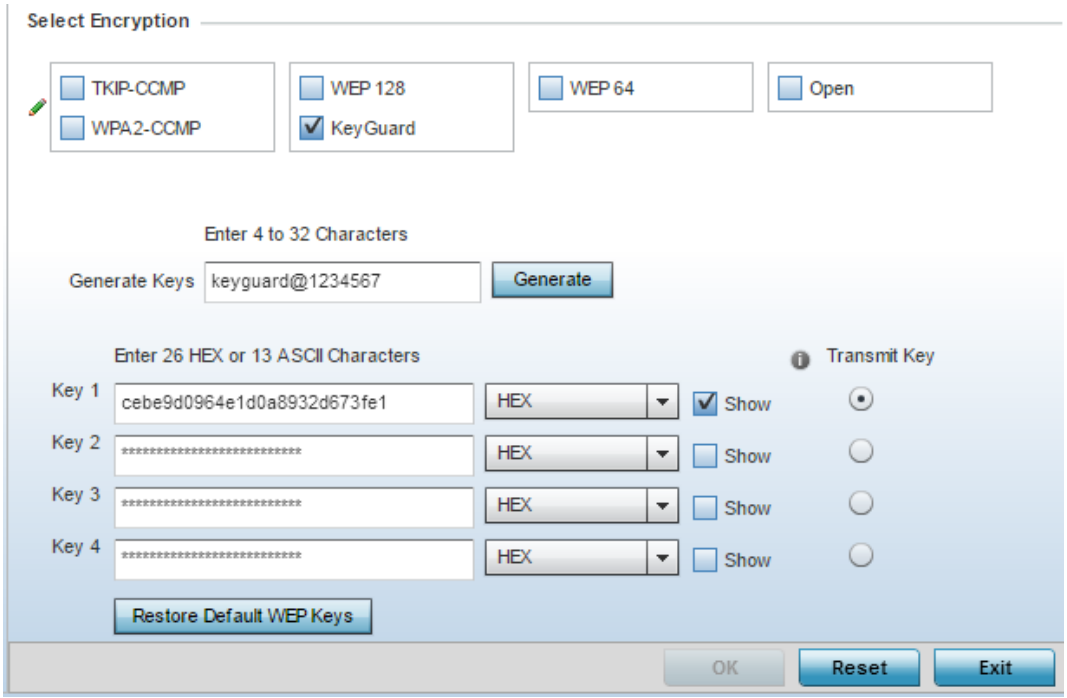


Figure 8: WLAN Security - Keyguard Screen

5 Configure the following Keyguard settings:

Generate Keys	Specify a 4 to 32 character Pass Key and click the *Generate* button. The pass key can be any alphanumeric string. WiNG clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without these WiNG adapters need to use keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 areas 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	If you feel it necessary to restore the Keyguard algorithm back to its default settings, click the *Restore Default WEP Keys* button. This may be the case 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 the screen back to its last saved configuration.

Keyguard Deployment Considerations

"Keyguard"

Before defining a Keyguard configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WiNG proprietary authentication techniques, can also be enabled on WLANs supporting other WiNG proprietary techniques, such as KeyGuard.
- A WLAN using KeyGuard to support legacy devices should also use largely limited to the support of just those legacy clients using KeyGuard.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

Configuring WLAN Firewall Settings

"Wireless LANs"

A Firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within an access point managed WLAN. The means by which this is accomplished varies, but in principle, a Firewall is a mechanism that blocks and permits data traffic. For a Firewall overview, see "Wireless Firewall" on page 709.

WLANs use Firewalls like *Access Control Lists* (ACLs) 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 *Access Control Entries* (ACEs). 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 because the access point stops testing conditions 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.

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, IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

To review existing Firewall configurations, create a new Firewall configuration or edit the properties of a WLAN's existing Firewall:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create a new WLAN or **Edit** to modify the properties of an existing wireless controller WLAN.

5 Select **Firewall** from the WLAN options.

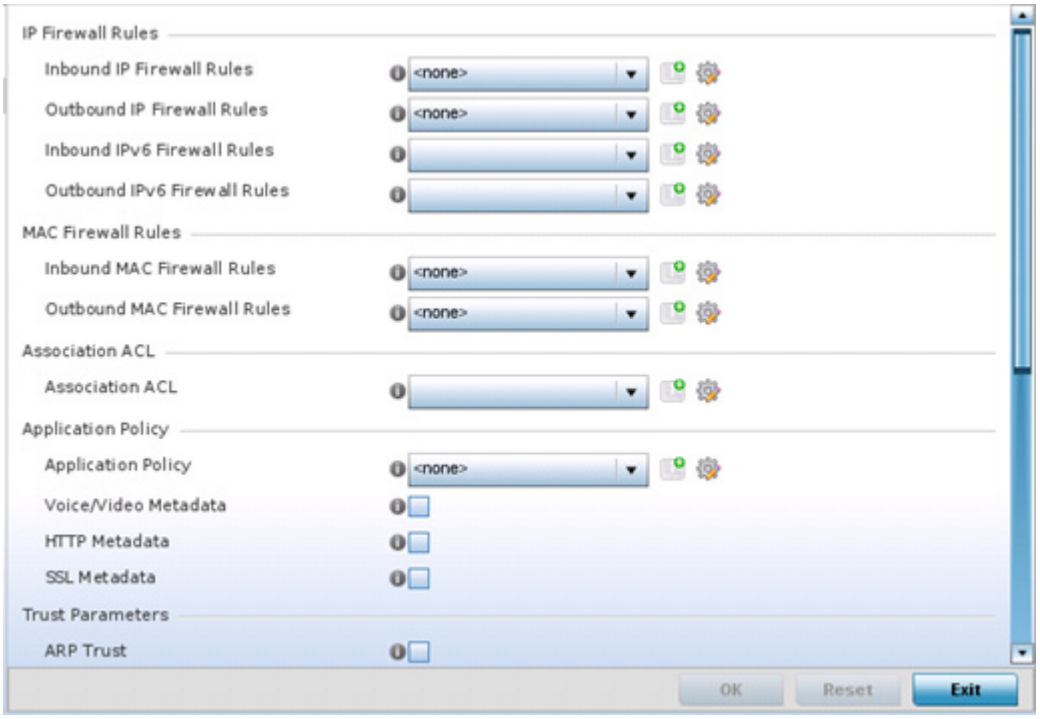


Figure 9: WLAN Security - WLAN Firewall screen

6 Select an existing **Inbound IP Firewall Rules** or **Outbound IP Firewall Rules** or **Inbound IPv6 Firewall Rules** or **Outbound IPv6 Firewall Rules** using the drop-down menu. If no rules exist, select the **Create** icon to create a new firewall rule configuration. Select the **Edit** icon to modify the configuration of a selected firewall.

If creating a new rule, provide a name up to 32 characters.

7 Select the **Add** button.

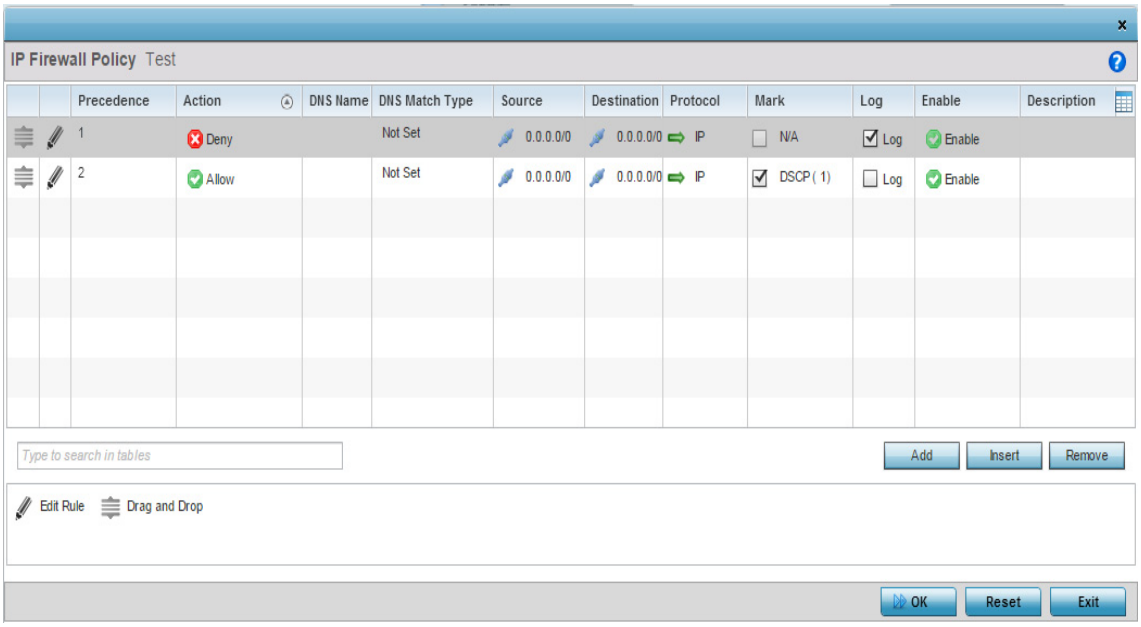


Figure 10: WLAN Security - IP Firewall Rules screen

8 IP Firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a. Select the **Edit Rule** icon to the left of a particular IP Firewall rule configuration to update its parameters collectively.

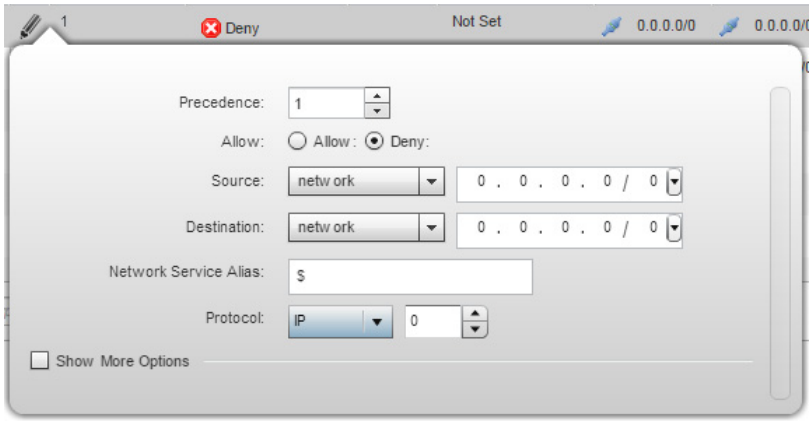


Figure 11: WLAN Security - IP Firewall Rules - Edit Rule screen

b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.

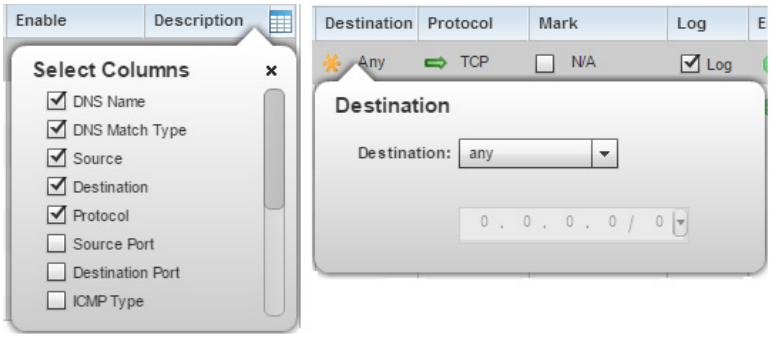


Figure 12: WLAN Security - IP Firewall Rules - IP Firewall Rules Add Criteria screen

NOTE

Only those selected IP ACL filter attributes display. Each value can have its current settings adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

9 Define the following parameters for either inbound or outbound IP firewall rules:

Precedence	Specify or modify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
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. • *Allow* - Instructs the firewall to allow a packet to proceed to its destination.
DNS Name	Specify the *DNS Name* which may be a full domain name, a portion of a domain name or a suffix. This name is used for the *DNS Match Type* criteria.
DNS Match Type	Specify the DNS matching criteria that the DNS Name can be matched against. This can be configured as an exact match for a DNS domain name, a suffix for the DNS name or a domain that contains a portion of the DNS name. If traffic matches the configured criteria in the DNS Match Type, that rule will be applied to the ACL.
Source	Select the source IP address or network group configuration used as a basis matching criteria for this IP ACL rule. Source options include: • *Any* – Indicates any host device in any network. • *Network* – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IP address. • *Alias* – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.

Destination	Select the destination IP address or network group configuration used as a basis matching criteria for this IP ACL rule. Destination options include: • *Any* – Indicates any host device in any network. • *Network* – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IP address. • *Alias* – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of ACL configuration. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.
Protocol	Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number.
Network Service Alias	The service alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $ character and containing one special character) and include the protocol as relevant. Selecting either *tcp* or *udp* displays an additional set of specific TCP/UDP source and destinations port options.
Source Port	If using either *tcp* or *udp* as the protocol, define whether the source port for incoming IP ACL rule application is *any*, *equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for *Low* and *High* numeric range settings. A source port cannot be a destination port.
Destination Port	If using either *tcp* or *udp* as the protocol, define whether the destination port for incoming IP ACL rule application is *any*, *equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for *Low* and *High* numeric range settings.
ICMP Type	Selecting *ICMP* as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric *type*. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
ICMP Code	Selecting *ICMP* as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding *code*, helpful for troubleshooting network issues (0 - Net Unreachable, 1- Host Unreachable, 2 - Protocol Unreachable etc.).
Start VLAN	Select a *Start VLAN* icon within a table row to set (apply) a start VLAN range for this IP ACL filter. 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. End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
Mark	Select this option to mark certain fields inside a packet before allowing them. Mark is only applicable for *Allow* rules. Mark sets the rule's 802.1p or *dscp* level (from 0 - 7)
Log	Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed.
Enabled	Select this option to enable or disable this particular IP Firewall rule in this rule set.
Description	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a *Select Columns* screen used to add or remove IP ACL criteria from the table.

10 The **Precedence** column sets the priority of a IP Firewall rule within its rule set. Click on this column and drag the rule to its appropriate place in the ruleset to set its precedence.

11 Select an existing **Inbound IPv6 Firewall Rule** or **Outbound IPv6 Firewall Rule** using the drop-down menu. If no rules exist, select the **Create** icon to create a new firewall rule configuration. Select the **Edit** icon to modify the configuration of a selected firewall.

If creating a new rule, provide a name up to 32 characters.

12 Select the **Add** button.

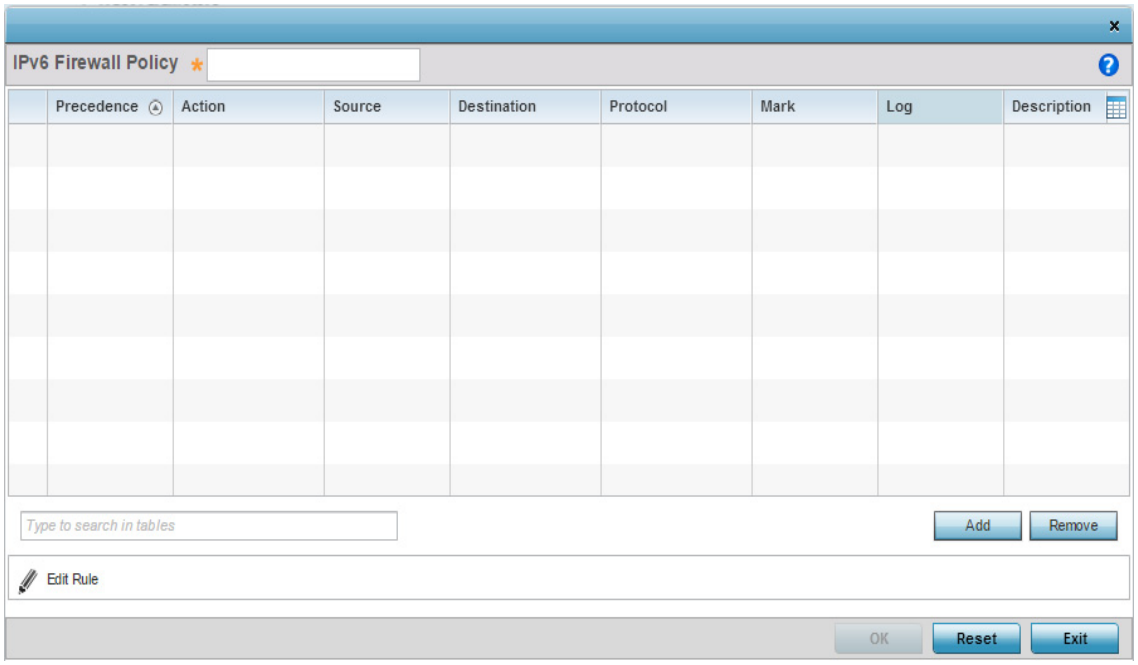


Figure 13: WLAN Security - IPv6 Firewall Rules screen

IPv6 Firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

13 Select the **Edit Rule** icon to the left of a particular IPv6 Firewall rule configuration to update its parameters collectively.

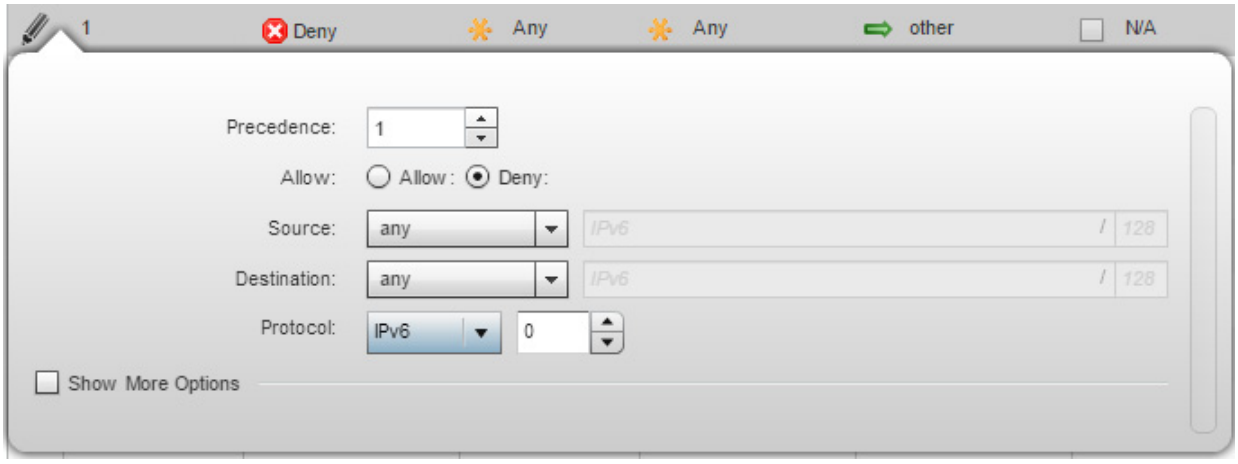


Figure 14: WLAN Security - IPv6 Firewall Rules - Edit Rule screen

14 Click the icon within the **Description** column (top right-hand side of the screen) and select IPv6 filter values as needed to add criteria into the configuration of the IPv6 ACL.

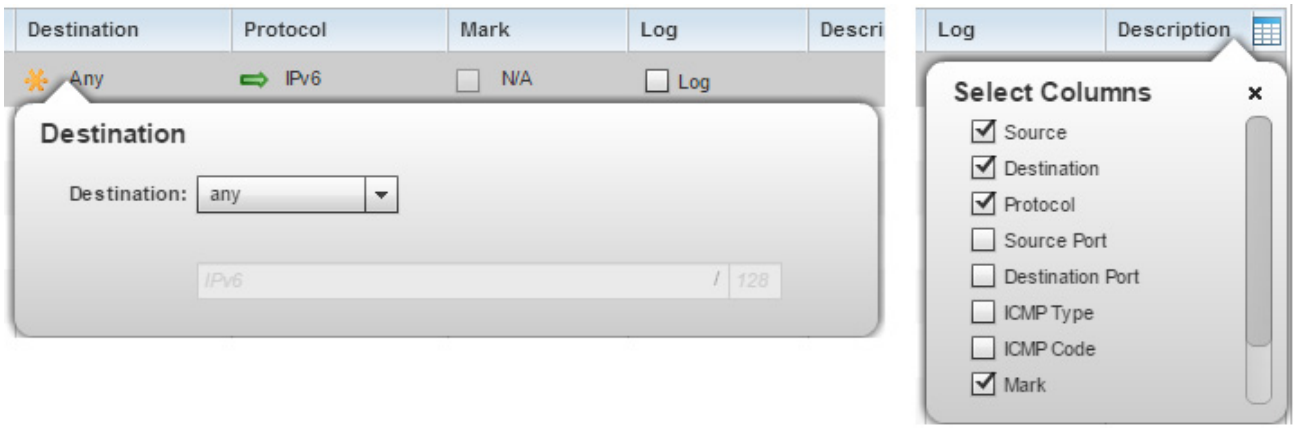


Figure 15: WLAN Security - IPv6 Firewall Rules - IPv6 Firewall Rules Add Criteria screen

15 Define the following parameters for either inbound or outbound IPv6 firewall rules:

Precedence	Specify or modify a precedence for this IPv6 policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority. The **Precedence** column sets the priority of a IPv6 Firewall rule within its rule set.
Action	Every IPv6 firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: • *Deny* - Instructs the firewall to prohibit a packet from proceeding to its destination. • *Allow* - Instructs the firewall to allow a packet to proceed to its destination.
Source	Select the source IPv6 address or network group configuration used as a basis matching criteria for this IPv6 ACL rule. Source options include: • *Any* – Indicates any host device in any network. • *Network* – Indicates all hosts in a particular IPv6 network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IPv6 address.
Destination	Select the destination IPv6 address or network group configuration used as a basis matching criteria for this IPv6 ACL rule. Destination options include: • *Any* – Indicates any host device in any IPv6 network. • *Network* – Indicates all hosts in a particular IPv6 network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IPv6 address.
Protocol	Select the protocol to filter for this IPv6 ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number.
Source Port	If using either *tcp* or *udp* as the protocol, define whether the source port for incoming IPv6 ACL rule application is *any*, *equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for *Low* and *High* numeric range settings. A source port cannot be a destination port.
Destination Port	If using either *tcp* or *udp* as the protocol, define whether the destination port for incoming IPv6 ACL rule application is *any*, *equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting equals invokes a spinner control for setting a single numeric port. Selecting range displays spinner controls for *Low* and *High* numeric range settings.

ICMP Type	Selecting *ICMP* as the protocol for the IPv6 rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric *type*. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
ICMP Code	Selecting *ICMP* as the protocol for the IPv6 rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding *code*, helpful for troubleshooting network issues (0 - Net Unreachable, 1- Host Unreachable, 2 - Protocol Unreachable etc.).
Mark	Select this option to mark certain fields inside a packet before allowing them. Mark is only applicable for *Allow* rules. Mark sets the rule's 802.1p or *dscp* level (from 0 - 7)
Log	Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed.
Description	Lists the administrator assigned description applied to the IPv6 ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a *Select Columns* screen used to add or remove IPv6 ACL criteria from the table.

16 Click the **OK** button to save all changes made to the **IPv6 Firewall Rules** dialog. Click **Exit** to close the dialog and return to the previous screen.

17 Select existing inbound or outbound **MAC Firewall Rules** using the drop-down menu. If no rules exist, select **Create** to display a screen where Firewall rules can be created.

18 Select the **+ Add Row** button.

19 Select the added row to expand it into configurable parameters.

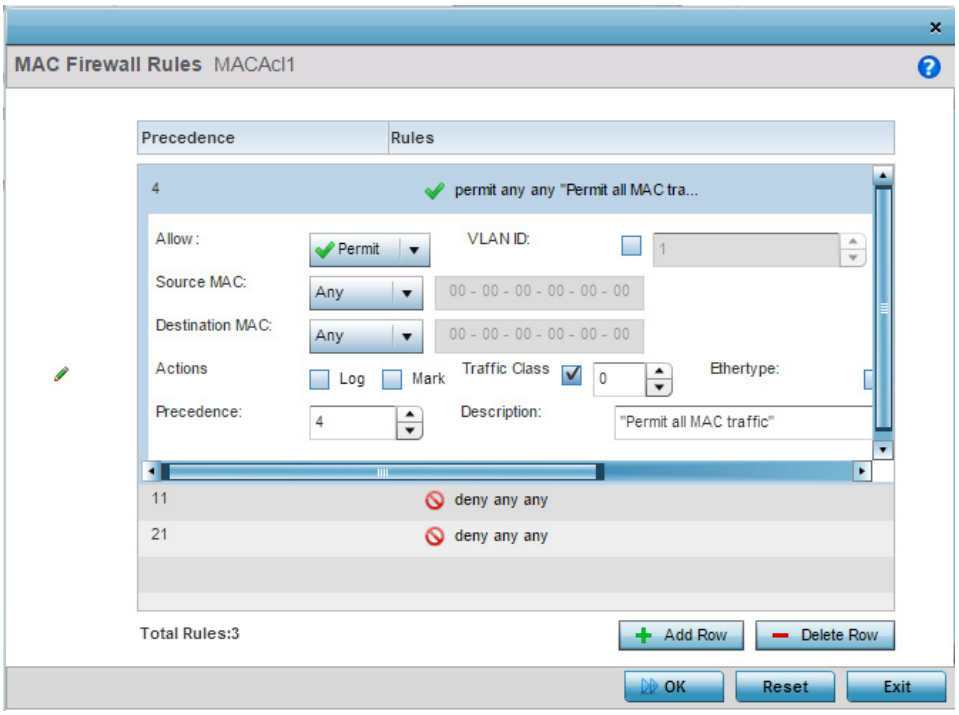


Figure 16: WLAN Security - MAC Firewall Rules screen

20 Define the following parameters for either the inbound or outbound **MAC Firewall Rules**:

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 prohibit a packet from proceeding to its destination. • *Permit* - Instructs the firewall to allow a packet to proceed to its destination.
Source and Destination MAC	Enter both *Source* and *Destination* MAC addresses. The access point uses the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.
Actions	The following actions are supported: • *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 a 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 in the range 1-10.
Precedence	Use the spinner control to specify a precedence for this MAC Firewall rule from 1-1500. Access policies with lower precedence are always applied first to packets.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the access point's local RADIUS server). Set the VLAN form 1 - 4094.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting from 0 - 7.
Ethertype	Use the drop-down menu to specify an Ethertype of either *ipv4, ipv6*, *arp*, *rarp*, *appletalk*, *aarp*, *mint*, *wisp*, *ipx*, *802.1q* or *others*. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. When *other* is selected, ethertype value can be configured manually.
Description	Provide a description (up to 64 characters) for this rule to help differentiate it from others with similar configurations.

21 Save the changes to the new MAC rule, or reset to the last saved configuration as needed.

22 Define the following parameters for Association ACL. An Association ACL defines the rules used to allow/deny association to devices for this wireless LAN. If no Association ACL exists, select the Create button to display a new window where new ACL can be created.

23 Select the + Add Row button.

24 Define the following parameters for Association ACL:

Precedence	Enter a numerical value indicating the precedence of rule execution.
Starting MAC Address	Enter a MAC address to define the start of range. This field is mandatory.
Ending MAC Address	Enter a MAC address to define the end of range.
Allow/Deny	Every Association ACL rule consists of matching criteria rules. The action defines what to do with the device if it matches the specified criteria. The following actions are supported: • *Deny* - Instructs the Firewall to not to allow the device to associate with this WLAN. • *Permit* - Instructs the Firewall to allow the device to associate with this WLAN.

25 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 Policy" on page 700.
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 NSight dashboard in manner similar to HTTP and SSL. Call quality and metrics can only be determined from calls established 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 NSight application's 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 NSight application's dashboard.This setting is disabled by default.

26 Set the following **Trust Parameters**:

ARP Trust	Select this radio button to enable ARP trust on this WLAN. ARP packets received on this WLAN are considered trusted and information from these packets is used to identify rogue devices within the network. This setting is disabled by default.
Validate ARP Header Mismatch	Select this radio button to check for a source MAC mismatch in the ARP header and Ethernet header. This setting is enabled by default.
DHCP Trust	Select this radio button to enable DHCP trust on this WLAN. This setting is disabled by default.

27 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.

28 Set the following **Wireless Client Deny** configuration:

Wireless Client Denied Traffic Threshold	If enabled, any associated client, exceeding the thresholds configured for storm traffic, is either *deauthenticated* or *blacklisted* depending on the selected action. The threshold range is from 1- 1000000 packets per second. This feature is disabled by default.
Action	If enabling a wireless client threshold, use the drop-down menu to determine whether clients are *deauthenticated* when the threshold is exceeded, or *blacklisted* from connectivity for a user-defined interval. Selecting *None* applies no consequence to an exceeded threshold.
Blacklist Duration	Select this option and define a setting from 0 - 86,400 seconds. Offending clients can reauthenticate, once this blacklist duration has been exceeded.

29 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.

30 Select **OK** when completed to update this WLAN's Firewall settings. Select **Reset** to revert the screen back to its last saved configuration.

WLAN Firewall Deployment Considerations

Before defining an access control configuration on a WLAN, refer to the following deployment guideline 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

"Wireless LANs"

Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations. AP6562, AP6532, AP6522, AP6522M, AP8132, AP8232, AP7181 and AP7161 model access points can support up to 256 clients per access point. AP6521 model can support up to 128 clients per access point. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed.

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create a new WLAN, or select an existing WLAN and **Edit** to modify its properties.

5 Select the **Client Settings** tab.

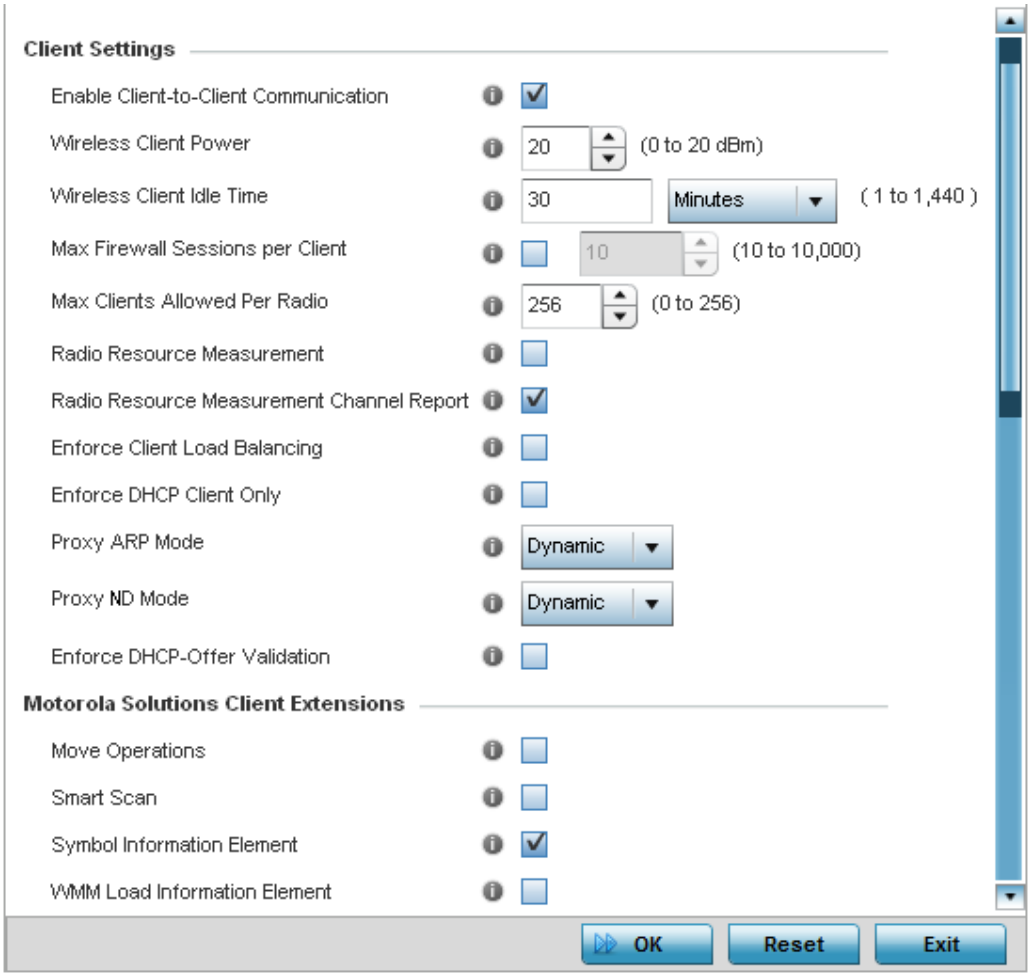


Figure 17: WLAN - Client Settings screen

6 Define the following **Client Settings** for the WLAN:

Enable Client-to-Client Communication	Select this option to allow client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. Disabling this setting does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting is disabled on the other WLAN, clients are not permitted to interoperate.
Wireless Client Power	Use this parameter to set the maximum transmit power (from 0 - 20 dBm) available to wireless clients for transmission. 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* (1 - 24) or *Days* (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 number of sessions (from 10 - 10,000 clients) over the Firewall. When enabled, this parameter limits the number of simultaneous sessions allowed by the Firewall per wireless client. This feature is disabled by default.
Max Clients Allowed Per Radio	Select this option to set the maximum number of clients (from 1- 256 clients) allowed to connect using a single radio. When enabled, this parameter limits the number of clients that are allowed to connect to a single radio. This feature is set to 256 by default.
Radio Resource Measurement	Select this option to enable radio resource measurement capabilities (IEEE 802.11k) on this WLAN. 802.11k improves how traffic is distributed. In a WLAN, each device normally connects to an access point with the strongest signal. Depending on the number and locations of the clients, this arrangement can lead to excessive demand on one access point and under utilization of 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 under utilized 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 enabled by default.

Enforce Client Load Balancing	Select this option to distribute clients evenly amongst associated access point radios. This feature is disabled by default. Client load balancing can be enforced for the WLAN as more and more WLANs are deployed. Loads are balanced by ignoring association and probe requests. Probes and association requests are not responded to forcing a client to associate with another access point.
Enforce DHCP Client Only	Select this option to enforce that the access point only allows packets from clients using 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 AP to answer ARP requests intended for another system. By faking its identity, the AP 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 *neighbor discovery* (ND) 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 this option to enforce DHCP offer validation. The default setting is disabled.

7 Define the following WING **Client Extensions** for the WLAN:

Move Operations	Select this option to enable the use of our *Fast Roaming* (HFSR) 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 this option to support the Symbol Information Element with legacy Symbol Technology clients. The default setting is enabled.
WMM Load Information Element	Select this option to support a WMM Load Information Element in radio transmissions with our 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 *fast transition* (FT) 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.

8 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.

9 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.

10 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 day.
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.

11 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.

12 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.

13 Select **OK** when completed to update the WLAN's client setting configuration. Select **Reset** to revert the screen back to the last saved configuration.

Configuring WLAN Accounting Settings

"Wireless LANs"

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. 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 managed 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 a remote location for periodic network and user permission administration.

To configure WLAN accounting settings:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.

5 Select **Accounting**.

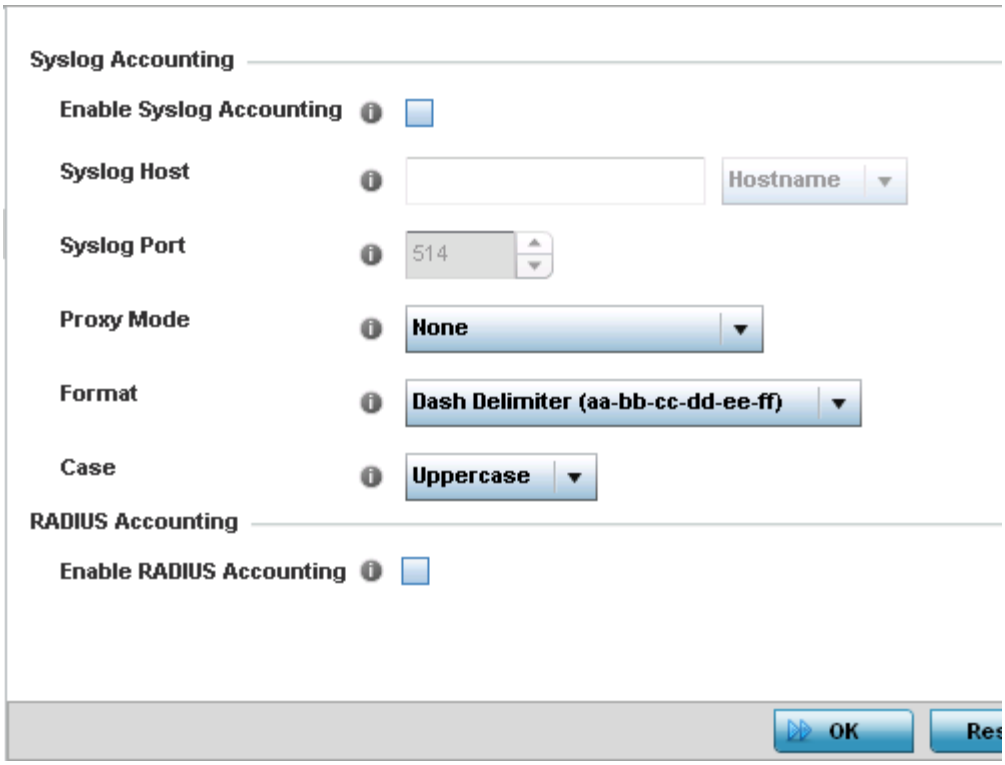


Figure 18: WLAN - Accounting screen

6 Set the following **Syslog Accounting** information:

Enable Syslog Accounting	Select this option for the access point to generate accounting records in standard syslog format (RFC 3164). The feature is disabled by default.
Syslog Host	Specify the IP address (or hostname) of the external syslog host where accounting records are routed. Use the drop-down menu to select the host type from *Hostname* or *IP Address*.
Syslog Port	Use the spinner control to set the destination UDP port of the external syslog host where accounting records are routed. The default port is 514.
Proxy Mode	Use the drop-down menu to define how syslog accounting is conducted. Options include *None, Through Wireless Controller* and *Through RF Domain Manager*. If no proxy is needed, select *None*.
Format	Select the format used to include (pack) the MAC address in a syslog request. Options include *No Delimiter (aabbccddeeff), Colon Delimiter (aa:bb:cc:dd:ee:ff), Dash Delimiter (aa-bb-cc-dd-ee-ff), Dot Delimiter per four (aabb.ccdd.eef)* and *Middle Dash Delimiter (aabbcc-ddeeff)*. The default setting is Dash Delimiter (aa-bb-cc-dd-ee-ff).
Case	Use the drop-down menu to specify whether the MAC address format supplied is specified in *upper* or *lower* case. The default setting is upper case.

7 Select **Enable RADIUS Accounting** to use an external RADIUS resource for AAA accounting. When the radio button is selected, a **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.

8 Select **OK** when completed to update this WLAN's accounting settings. Select **Reset** to revert the screen back to its last saved configuration.

Accounting Deployment Considerations

Before defining a AAA configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- When using RADIUS authentication, it is recommended that the WAN port round trip delay not exceed 150 ms. Excessive delay over a WAN can cause authentication and roaming issues. When excessive delays exist, a distributed RADIUS service should be used.
- It is recommended that authorization policies 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

"Wireless LANs"

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 the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.

5 Select **Service Monitoring**.

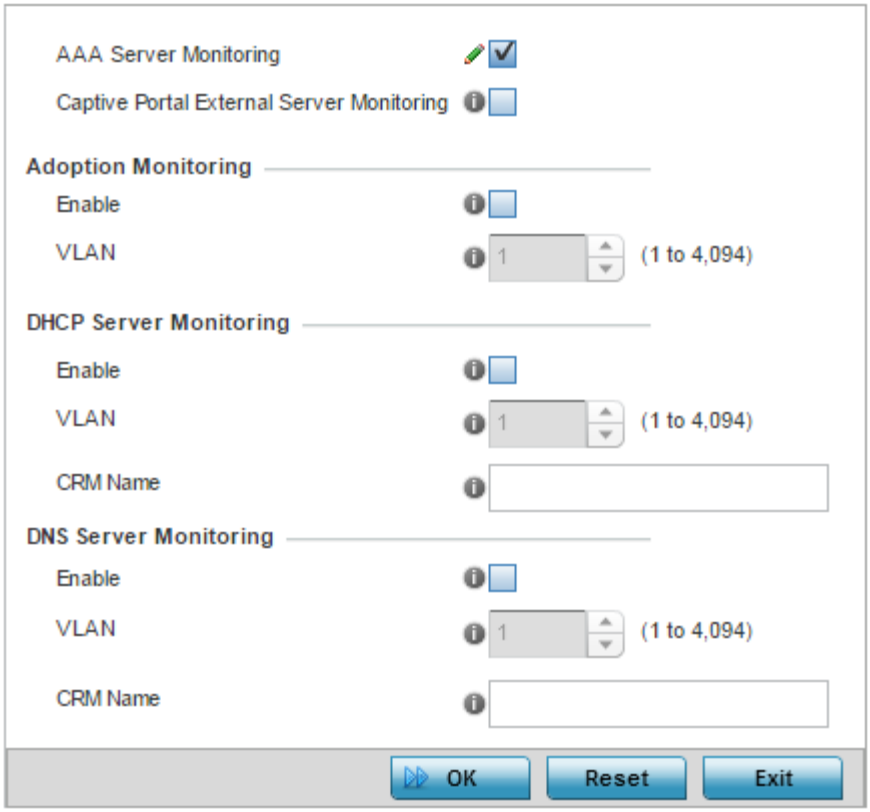


Figure 19: WLAN – Service Monitoring screen

6 Refer the following for more information on Service Monitoring fields:

AAA Server Monitoring	Select to enable monitoring of a dedicated external RADIUS server and ensure its adoption resource availability. This option is disabled by default. Configure a RADIUS server through an AAA Policy. See "AAA Policy" on page 663 for more information.
Captive Portal External Server Monitoring	Select to enable monitoring of an externally hosted captive portal activity, and temporary and restrictive user access to the controller or service platform managed network. This option is disabled by default.
Adoption Monitoring - Enable	Select this option to verify access point's adoption status to its controller or service platform. When the connection is lost, captive portal users are automatically migrated to the VLAN defined in the *Adoption Monitoring:VLAN* field. This option is disabled by default.
Adoption Monitoring - VLAN	Use the spinner control to select the VLAN that users are migrated to when as access point's connection to its adopting controller or service platform is lost.
DHCP Server Monitoring - Enable	Select to enable monitoring of the configured DHCP server. When the connection to the monitored DHCP server is lost, all captive portal are automatically migrated to the VLAN defined in the *DHCP Server Monitoring:VLAN* field.
DHCP Server Monitoring - VLAN	Use the spinner control to select the VLAN that users are migrated to when the configured DHCP becomes unavailable.
DHCP Server Monitoring - CRM Name	Configure the DHCP server to monitor. When this DHCP server becomes unavailable, the device falls back to the VLAN configured in the *DHCP Server Monitoring:VLAN* field. This VLAN has a DHCP server that provides a pool of IP addresses with a lease time lesser than the main DHCP server.
DNS Server Monitoring - Enable	Select to enable monitoring of the configured DNS server. When the connection to the DNS server is lost, captive portal users are automatically migrated a defined VLAN. The feature is disabled by default.
DNS Server Monitoring - VLAN	Use the spinner control to select the VLAN that users are migrated to when the configured DNS server resource becomes unavailable. The available range is from 1 - 4,094.
DNS Server Monitoring - CRM Name	Configure 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 till the primary DNS server becomes available.

7 Select **OK** when completed to update this WLAN's service monitoring settings. Select **Reset** to revert the screen back to its last saved configuration.

Configuring WLAN Client Load Balancing Settings

- "Wireless LANs"

Client load balance settings can be defined generically for both the 2.4 GHz and 5.0 GHz bands, and specifically for either of the 2.4 GHz or 5.0 GHz bands.

To configure client load balancing settings on an access point managed WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.

5 Select **Client Load Balancing**.

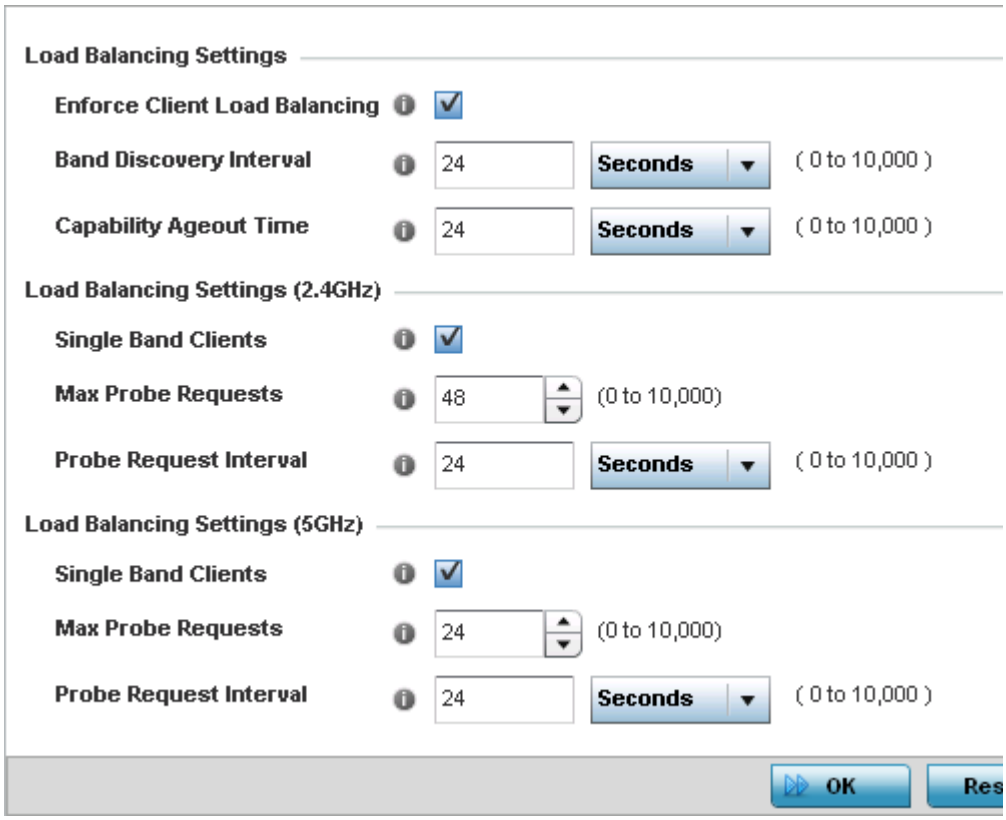


Figure 20: WLAN - Client Load Balancing screen

6 Set the following **Load Balance Settings** generic to both the 2.4 GHz and 5.0 GHz bands:

Enforce Client Load Balancing	Select this radio button to enforce a client load balance distribution on this WLAN. This setting is disabled by default. Loads are balanced by ignoring association and probe requests. Probes and association requests are not responded to, forcing a client to associate with another access point.
Band Discovery Interval	Define a value in either *Seconds* (0 - 10,000), *Minutes* (0 -166) or *Hours* (0 - 2) the access point uses to discover a client's band capabilities before associating. The default is 10 seconds.
Capability Ageout Time	Define a value in either *Seconds* (0 - 10,000), *Minutes* (0 -166) or *Hours* (0 - 2) to ageout a client's capabilities from the access point's internal table. The default is 1 hour.

7 Set the following **Load Balancing Settings (2.4 GHz)**:

Single Band Clients	Select this option to enable single band client associations on the 2.4 GHz frequency, even if load balancing is available. The option is enabled by default.
Max Probe Requests	Enter a value (from 0 - 10,000) for the maximum number of probe requests for client associations on the 2.4 GHz 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 setting is 10 seconds.

8 Set the following **Load Balancing Settings (5 GHz)**:

Single Band Clients	Select this option to enable single band client associations on the 5.0 GHz frequency, even if load balancing is available. This option is enabled by default.
Max Probe Requests	Enter a value (from 0 - 10,000) for the maximum number of probe requests for 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 set an interval for client probe requests, beyond which association is allowed for clients on the 5.0 GHz frequency. The default setting is 10 seconds.

9 Select **OK** when completed to update this WLAN's client load balance settings. Select **Reset** to revert the screen back to its last saved configuration.

Configuring WLAN Advanced Settings

"Wireless LANs"

To configure advanced RADIUS configuration and radio rate settings for a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.

5 Select **Advanced**.

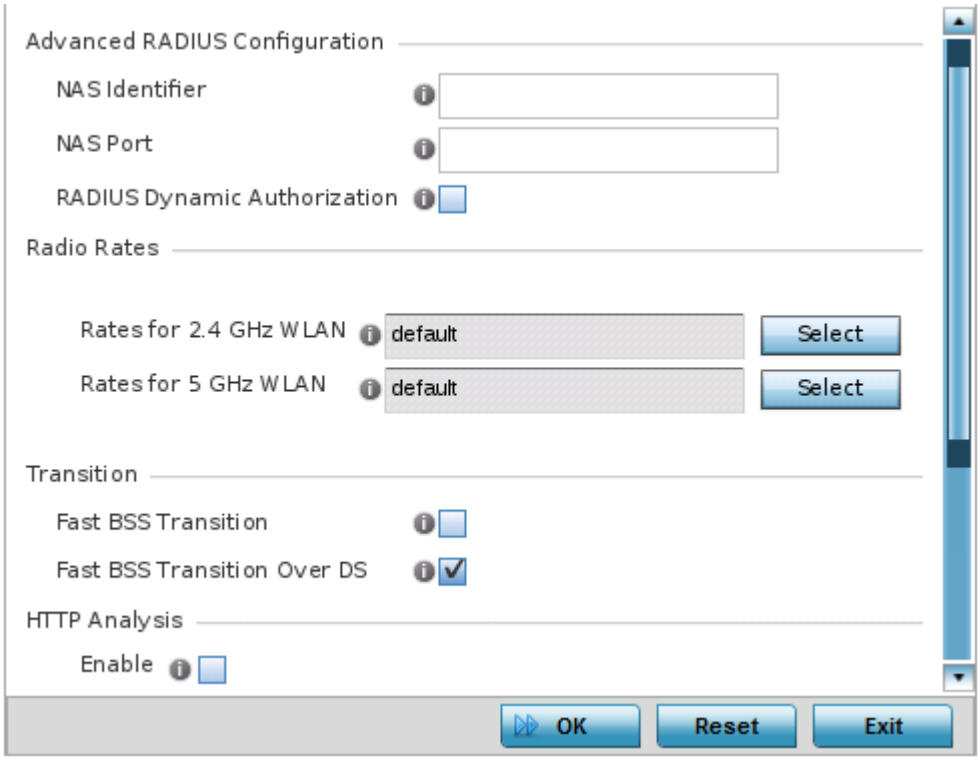


Figure 21: WLAN - Advanced Configuration screen

6 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 *network access server* (NAS) port. Each profile is matched to a user name representing a physical port. When the access point authorizes users, it queries the user profile database using a user name representative of the physical NAS port making the connection.
RADIUS Dynamic Authorization	Select this check box to enable the RADIUS protocol to support unsolicited messages sent from the RADIUS server. These messages allow administrators to issue *change of authorization* (CoA) messages, which affect session authorization, or *Disconnect Message* (DM), which cause a session to terminate immediately. This option is disabled by default.

7 Refer to the **Radio Rates** field to define selected data rates for both the 2.4 GHz and 5.0 GHz bands.

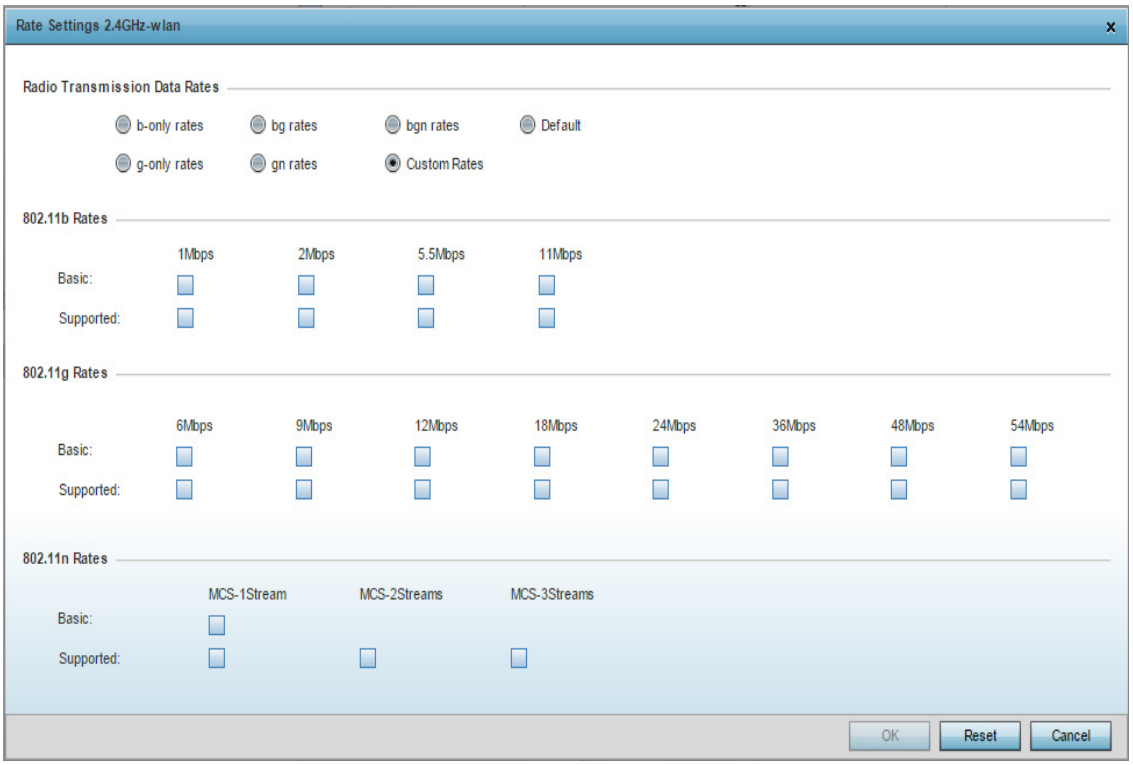


Figure 22: Advanced WLAN - Rate Settings 2.4 GHz-WLAN screen

8 For 2.4 GHz WLAN radio transmission rate settings, define the minimum *Basic* and *Supported* rates in the **802.11b Rates**, **802.11g Rates** and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set 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).

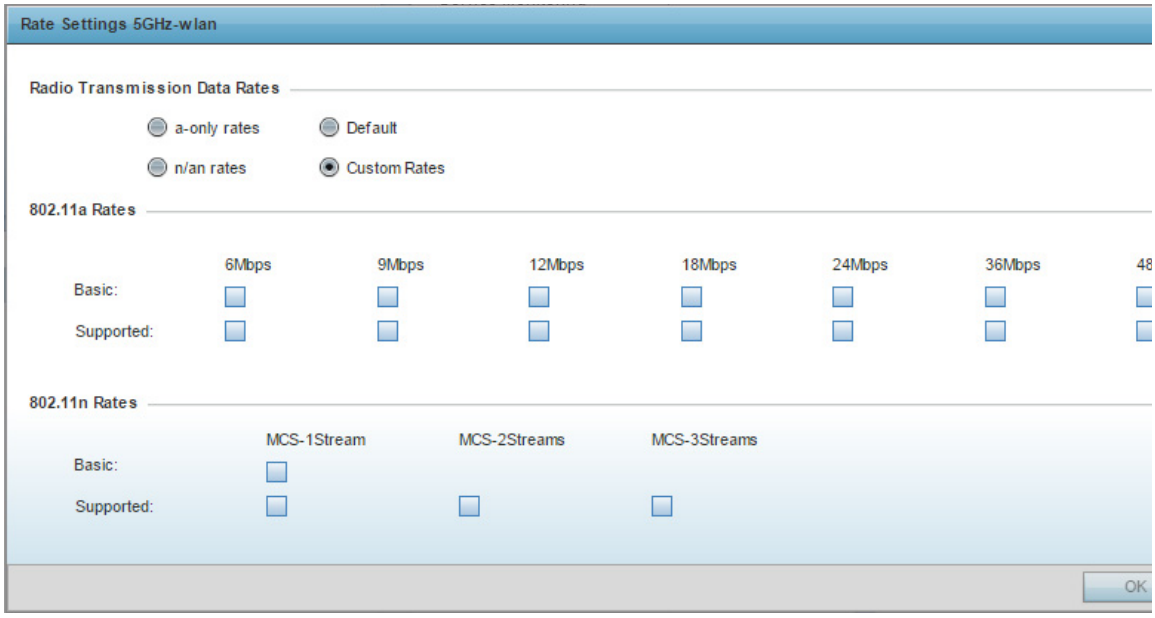


Figure 23: Advanced WLAN - Rate Settings 5 GHz-WLAN screen

9 For 5.0 GHz WLAN radio transmission rate settings, define the minimum *Basic* and *Supported* rates in the **802.11a Rates**, and **802.11n Rates** sections. These rates are applicable to client traffic associated with this WLAN only.

If supporting 802.11n, select a Supported MCS index. Set 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).

802.11n MCS rates are defined as follows both with and without *short guard intervals* (SGI):

Table 6.1 *MCS-1Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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 6.2 *MCS-2Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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 6.3 *MCS-3Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz 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 6.4 *MCS-802.11ac (theoretical throughput for single spatial streams)*

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI	80 MHz No SGI	80MHz 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

10 Set the following **Transition** options:

Fast BSS Transition	If needed, select the *Fast BSS Transition* check box 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 back 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 the *Fast BSS Transition Over DS* check box to enable 802.11r over DS fast roaming on this WLAN. This setting is enabled by default.

11 Select **Enable** to enable **HTTP Analysis** for log file analysis on this WLAN. This option is disabled by default.

12 Set the following **Filter** settings for HTTP analysis on this WLAN:

Filter Out Images	Select this check box to filter images out of this WLAN's log files. This option is disabled by default.
Filter Post	Select this check box to filter posts out of this WLAN's log files. This option is disabled by default.
Strip Query String	Select this check box to filter query strings out of this WLAN's log files. This option is disabled by default.

13 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 option is disabled by default.
Host	Provide a Hostname or IP Address of the remote syslog server. Use the drop-down menu to select the type of host address.
Port	Specify the port on which the external syslog server can be reached. 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*.

14 Select **OK** when completed to update this WLAN's Advanced settings. Select **Reset** to revert to the last saved configuration.

Configuring Auto Shutdown Settings

"Wireless LANs"

Auto shutdown provides a mechanism to regulate the availability of a WLAN based on time. WLANs can be enabled or disabled depending on the day of the week and time of day.

A WLAN can be made available during a particular time of the day to prevent misuse and reduce the vulnerability of the wireless network. WLANs can be disabled when there are no users on the network, such as after hours or during the weekends/holidays. This enables the network administrator to have more time to manage the network as the mundane task of shutting down/staring up a WLAN is automated.

You can also use the *Auto Shutdown* screen to configure network parameters, which if not met, can force the WLAN to shut down. These parameters are:

- *Shutdown on Mesh Point Loss* – If an access point is a member in a meshed network and its connection to the mesh is lost, then all WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Primary Port Link Loss* – When there is a loss of link on the primary wired link on the access point, all the WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Critical Resource Down* – If critical resource monitoring is enabled on the access point and one or all of the monitored critical resource goes down, the all WLANs on the access point that have this option enabled are shut down.
- *Shutdown on Unadoption* – If the access point is unadopted from its wireless controller, then all WLANs on the access point that have this option enabled are shut down.

To configure auto shutdown parameters for the selected WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LANs** to display a high level display of existing WLANs.

4 Select the **Add** button to create an additional WLAN, or **Edit** to modify the properties of an existing WLAN.

5 Select **Auto Shutdown**.

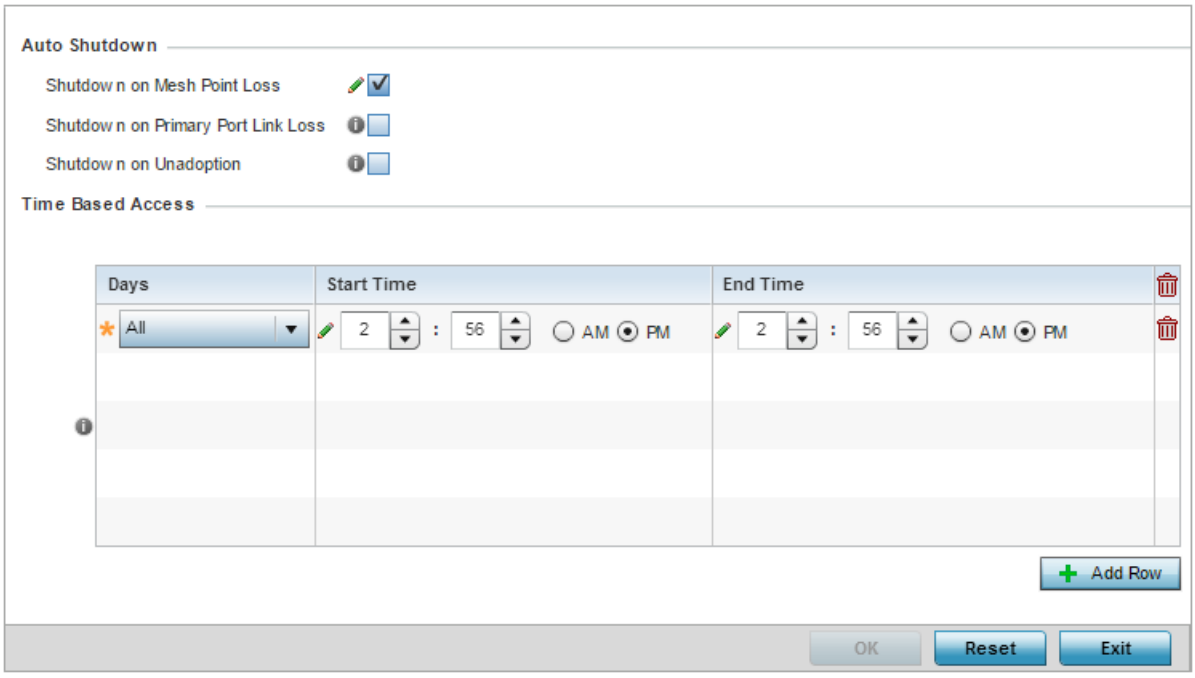


Figure 24: WLAN - Auto Shutdown screen

6 Refer to the following to configure **Auto Shutdown** parameters:

Shutdown on Mesh Point Loss	Select to enable the WLAN to shutdown if the access point's connection to the mesh network is lost. This setting is disabled by default.
Shutdown on Primary Port Link Loss	Select to enable the WLAN to shutdown if the access point's connection on its primary wired port is lost. This setting is disabled by default.
Shutdown on Unadoption	Select to enable the WLAN to shutdown if the access point is unadopted from its wireless controller. This setting is disabled by default.

7 Select the **+ Add Row** button to add time based access configuration for the WLAN.

8 Refer to the following to configure **Time Based Access** parameters:

Days	Configure the days on which the WLAN is accessible. Select from one of the following: • *All* – Select this option to make the WLAN available on all days of the week. • *Weekends* – Select this option to make the WLAN available only during weekends (Saturday and Sunday). • *Weekdays* – Select this option to make the WLAN available only during weekdays (from Monday to Friday). • *Sunday/Monday/Tuesday/Wednesday/Thursday/Friday/Saturday* – Select a week day to make the WLAN available only during that specific day.
Start Time	Configures 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	Configures the ending time of day(s) that the WLAN will be 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.*

9 Refer to the following to configure the **Critical Resource Down** parameters:

Shutdown on Critical Resource Down	Select to enable the WLAN to shutdown if the access point's connection to the selected critical resource is lost. This setting is disabled by default.
Critical Resource Name	Enter the name of the critical resource to check for.

10 Select **OK** when completed to update this WLAN's Advanced settings. Select **Reset** to revert to the last saved configuration. Select **Exit** to exit the screen.

WLAN QoS Policy

"Wireless Configuration"

QoS provides a data traffic prioritization scheme that 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. When bandwidth is shared by different users and applications, QoS provides policy

enforcement for mission-critical applications and/or users with critical bandwidth requirements.

QoS ensures each WLAN receives a fair share of the overall bandwidth, either equally or in the configured proportion. Packets directed towards clients are classified into categories such as *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 for this WLAN, select the **Add** button to create new policy. Select the radio button of an existing WLAN and select **OK** to map the QoS policy to the WLAN displayed in the banner of the screen.

Use the **WLAN Quality of Service (QoS)** screen to add a new QoS policy or edit an existing policy. Each access point model supports up to 32 WLAN QoS policies, with the exception of AP6521 model that support 16 WLAN QoS policies.

NOTE

WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients the access point's radios support.

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless QoS Policy** to display a high level display of existing WLAN QoS policies.

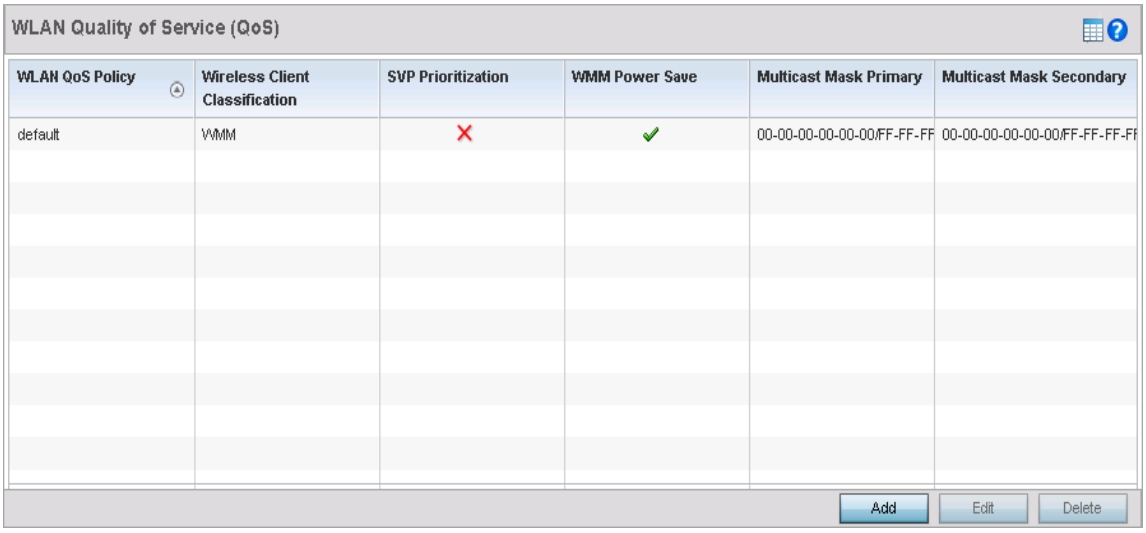


Figure 25: WLAN - WLAN Quality of Service (QoS) screen

Refer to the following read-only information to determine whether an existing policy can be used as is, an existing policy requires edit or a new policy requires creation:



NOTE

When using a wireless client classification other than WMM, only legacy rates are supported on that WLAN.

WLAN QoS Policy	Displays the name assigned to each listed WLAN QoS. The policy name cannot be edited.
Wireless Client Classification	Lists 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). The 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.
SVP Prioritization	A green check mark defines the policy as having *Spectralink Voice Prioritization* (SVP) enabled to allow the access point 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 *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by WMM capable voice devices. The default setting is enabled.
Multicast Mask Primary	Displays 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	Displays the secondary multicast mask defined for each listed QoS policy.

4 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** its configuration. Existing QoS policies can also be selected and deleted as needed.

A **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 QoS WMM Settings"
- "Configuring a WLAN's QoS Rate Limit Settings"
- "Configuring Multimedia Optimizations"

Configuring QoS WMM Settings

"WLAN QoS Policy"

Using WMM, 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 priority.

WMM's prioritization capabilities are based on four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over the access point managed WLAN. ACs were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled access points 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 a 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 should be granted the *opportunity to transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category.

- The minimum inter-frame space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- 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 the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.

4 Select the **Add** button to create a new QoS policy, or **Edit** to modify the properties of an existing WLAN QoS policy.

The **WMM** tab displays by default.

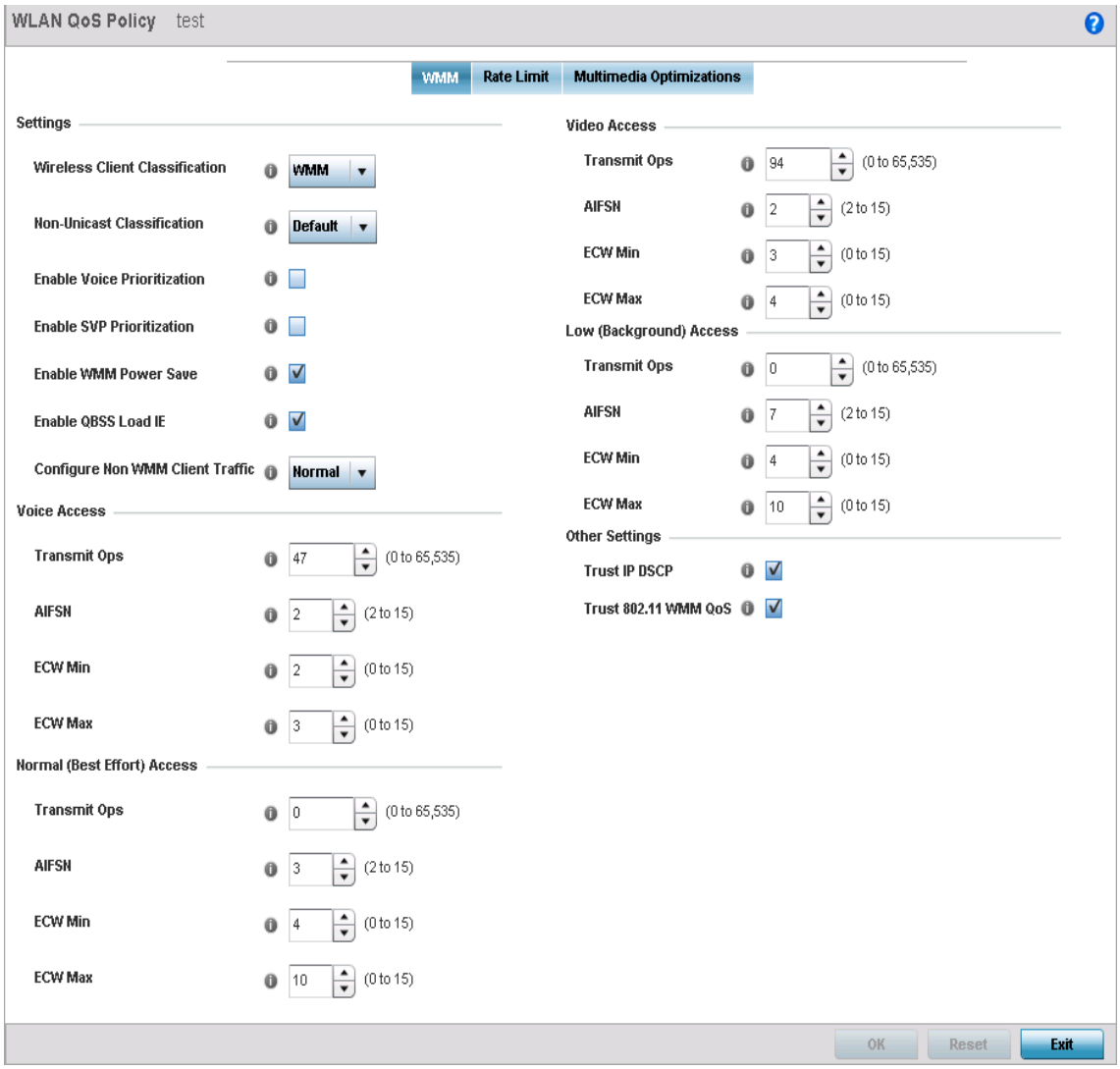


Figure 26: WLAN - WLAN QoS Policy screen - WMM tab

5 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. The Classification Categories are the different WLAN-WMM options available to the radio. The Wireless Client Classification types are: • *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). The 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 Classification	Use this drop-down menu to define how traffic matching multicast masks is classified relative to prioritization on the radio. Options include *Video, Voice, Normal, Low* and *Default*. The default setting is *Default*.
Enable Voice Prioritization	Select this option if *Voice* traffic is prioritized on the WLAN. This gives priority to voice and voice management packets and is supported only on certain legacy VOIP phones manufactured by us. This feature is disabled by default.
Enable SVP Prioritization	Enabling *Spectralink Voice Prioritization* (SVP) allows the access point to identify and prioritize traffic from Spectralink/Polycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy VOIP phones manufactured by us. If the Wireless Client Classification is *WMM*, non-WMM devices recognized as voice devices have all 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 *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by WMM capable voice devices. This feature is enabled by default.
Enable QBSS Load IE	Select this option to enable support for WMM QBSS load information element in beacons and probe response packets. This feature is enabled by default.
Configure Non WMM Client Traffic	Use the drop-down menu to specify how non-WMM client traffic is classified on this access point WLAN if the *Wireless Client Classification* is set to *WMM*. Options include *Video, Voice, Normal* and *Low*. The default setting is Normal.

6 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 value is 94.
AIFSN	Set the current *Arbitrary Inter-frame Space Number (AIFSN)* from 2 - 15. Higher-priority 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	*ECW Min* is combined with *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	*ECW Max* is combined with *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.

7 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) from 2 - 15. Higher-priority 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	*ECW Min* is combined with *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	*ECW Max* is combined with *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.

8 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 *Arbitrary Inter-frame Space Number* (AIFSN) from 2 - 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. 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. The available range is from 0-15. The default value is 10.

9 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. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN from 2 - 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	*ECW Min* is combined with *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. The available range is from 0-15. The default value is 4.
ECW Max	*ECW Max* is combined with *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. The available range is from 0-15. The default value is 10.

10 Set the following **Other Settings** for the WLAN's QoS policy:

Trust IP DSCP	Select this option to trust IP DSCP values for WLANs. This feature is enabled by default.
Trust 802.11 WMM QoS	Select this option to trust 802.11 WMM QoS values for WLANs.This feature is enabled by default.

11 Select **OK** when completed to update this WLAN's QoS settings. Select **Reset** to revert the screen back to its last saved configuration.

Configuring a WLAN's QoS Rate Limit Settings

"WLAN QoS Policy"

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). AP6521 model access point does not support rate limiting on an individual client basis.

Before defining rate limit thresholds for WLAN upstream and downstream traffic, it is recommended that you 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) is dropped, resulting in intermittent outages and performance problems.

To configure a QoS rate limit configuration for a WLAN and connected clients:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.

4 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** to modify its configuration.

5 Select the **Rate Limit** tab.

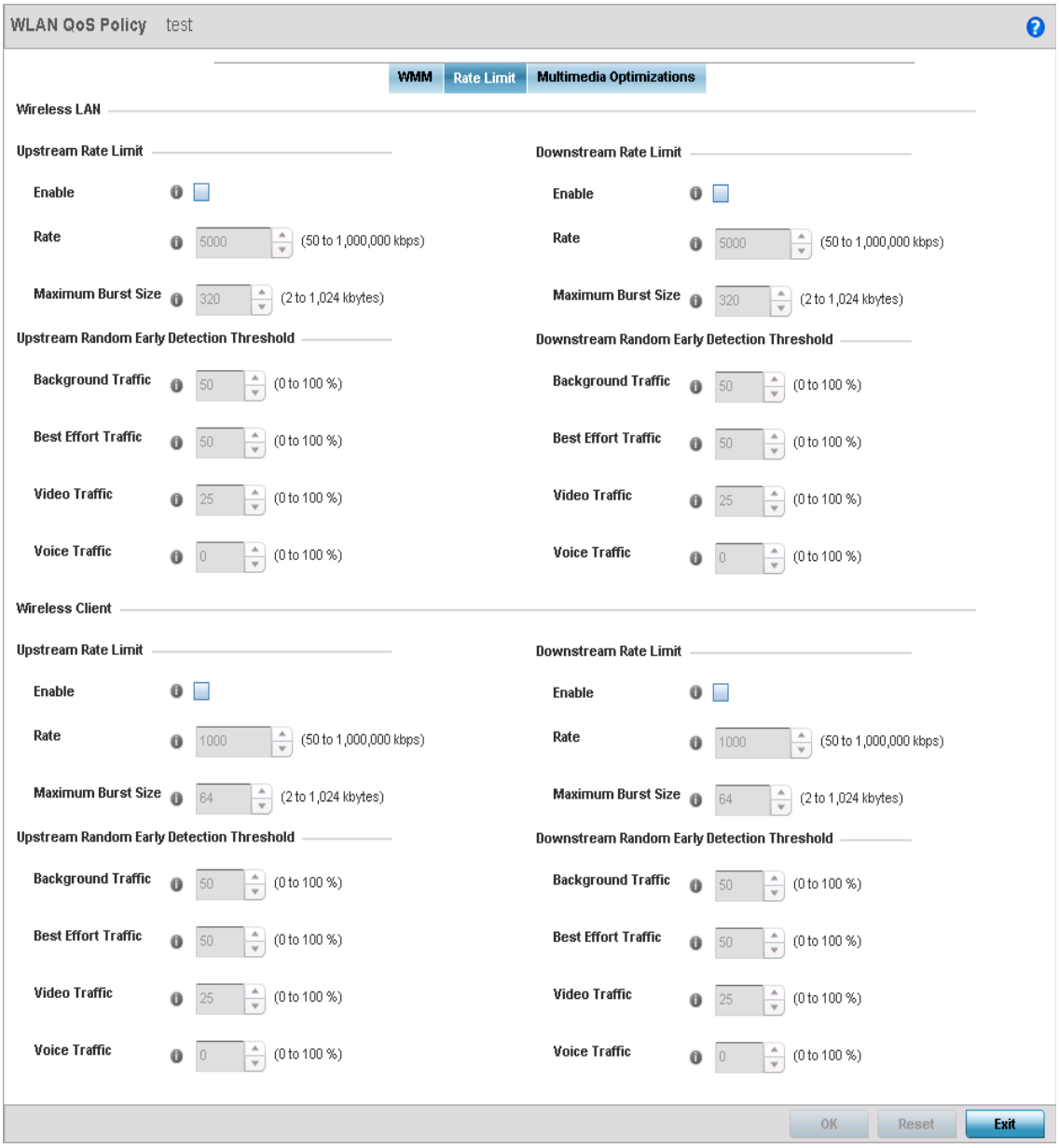


Figure 27: WLAN - WLAN QoS Policy screen - Rate Limit tab

6 Configure the following intended **Upstream Rate Limit** parameters for the selected WLAN:

Enable	Select this radio button to enable rate limiting for data transmitted from access point radios to associated clients on this WLAN. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.
Rate	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum number of packets transmitted or received over the WLAN (from all access categories). Traffic exceeding 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 from 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN'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 minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.

7 Set the following **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for the selected WLAN.

Background Traffic	Set a percentage for WLAN 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 for WLAN 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 for WLAN 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 for WLAN 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%.

8 Configure the following parameters in respect to the WLAN's intended **Downstream Rate Limit**, or traffic from wireless clients to associated access point radios:

Enable	Select this radio button to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
Rate	Define an upstream rate limit from 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 5,000 kbps.
Maximum Burst Size	Set a maximum burst size from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the WLANs 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 minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.

9 Set the following **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when a traffic stream falls below the set threshold for the selected WLAN.

Background Traffic	Set a percentage for WLAN 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 for WLAN 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 for WLAN 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 for WLAN 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 random drops will occur.

10 Configure the following intended **Upstream Rate Limit** parameters for wireless client traffic:

Enable	Select this radio button to enable rate limiting for data transmitted from access point radios to associated clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.
Rate	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received from clients (from all access categories). Traffic exceeding 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 from 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes.

11 Set the following **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

Background Traffic	Set a percentage for client 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 for client 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 for client 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 for WLAN 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%.

12 Configure the following intended **Downstream Rate Limit** parameters for wireless client traffic:

Enable	Select this radio button to enable rate limiting for data transmitted from access point radios to associated wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
Rate	Define an upstream rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received from clients. 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 from 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for wireless client traffic. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 64 kbytes.

13 Set the following **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is conducted when the amount of tokens for a traffic stream falls below the set threshold for wireless client traffic.

Background Traffic	Set a percentage for client 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 for client 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 for client 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 for client 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 random drops will occur.

Configuring Multimedia Optimizations

"WLAN QoS Policy"

To configure multimedia optimizations for a WLAN:

1 Select **Configuration.**

2 Select **Wireless.**

3 Select **Wireless LAN QoS Policy** to display a high level display of existing WLANs QoS policies.

4 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and **Edit** to modify its configuration.

5 Select the **Multimedia Optimizations** tab.

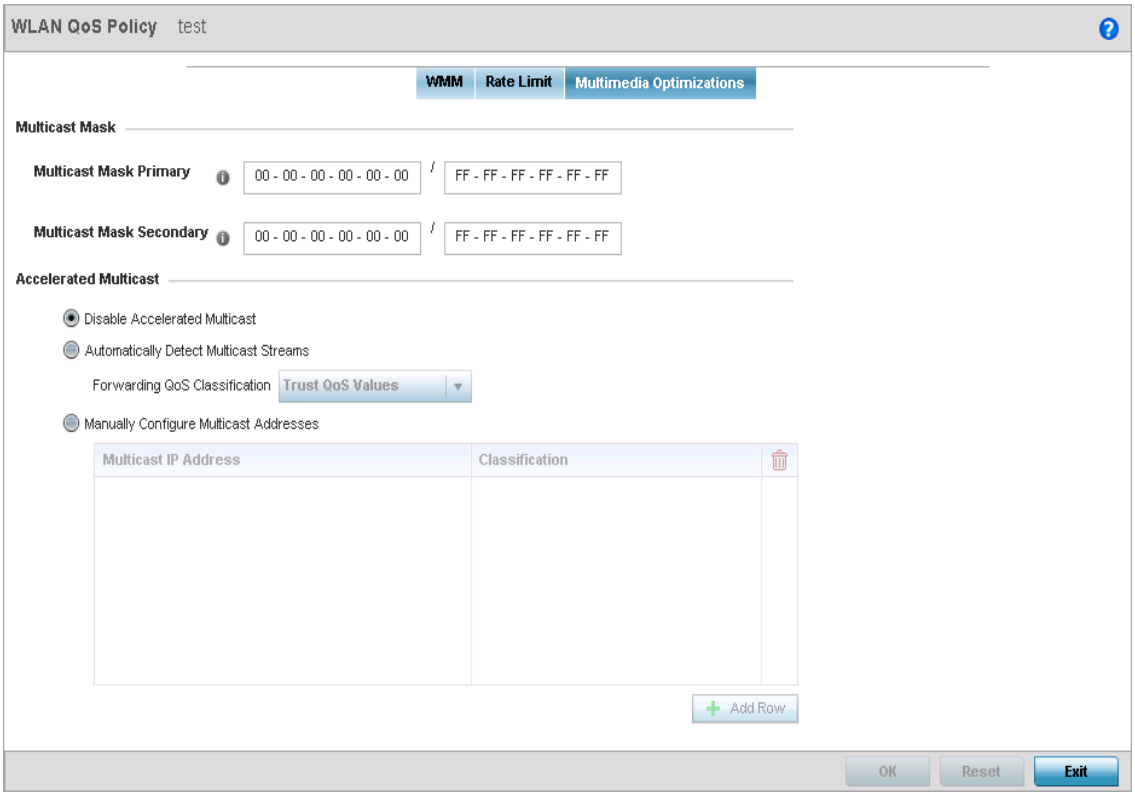


Figure 28: WLAN - WLAN QoS Policy Screen - Multimedia Optimizations

6 Configure the following parameters in respect to the intended **Multicast Mask**:

Multicast Mask Primary	Configure the primary multicast mask for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Mask Secondary	Set a secondary multicast mask for the WLAN QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.

7 Set the following **Accelerated Multicast** settings:

Disable Accelerated Multicast	Select this option to disable all accelerated multicast streaming on the WLAN.
Automatically Detect Multicast Streams	Select this option to convert multicast packets 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, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they want. Use the **Forwarding QoS Classification** drop-down list to select the classification to use.
Manually Configure Multicast Addresses	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

8 Select **OK** when completed to update this WLAN's Multimedia Optimizations settings. Select **Reset** to revert the screen back to its last saved configuration.

WLAN QoS Deployment Considerations

"WLAN QoS Policy"

Before defining a QoS configuration on a 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 access point 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 these access point radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must be also able to 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 as the bandwidth requirements are consistent and can be realistically trended over time. Applications such as Web, database and E-mail are harder to estimate, since bandwidth usage varies depending on how the applications are utilized.

Radio QoS Policy

"Wireless Configuration"

Without a dedicated QoS policy, a network operates on a best-effort delivery basis, meaning all traffic has equal priority and an 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 customization best suited to each QoS policy's intended wireless client base.

Our access point radios and wireless clients support several *Quality of Service* (QoS) techniques enabling real-time applications (such as voice and video) to co-exist simultaneously with lower priority background applications (such as Web, E-mail 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 high 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.

Within a wireless network, wireless clients supporting low and high priority traffic contend with one another for 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 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 improve battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. An access point managed wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must be also able to support WMM and use the values correctly while accessing WLAN to benefit.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected access point radios and their wireless clients. Parameters impacting access point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

Access points support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. An access point allows flexible WLAN mapping with a static WMM access control value. When enabled on a WLAN, traffic forwarded from to a client is prioritized and forwarded based on the WLAN's WMM access control setting.



NOTE

Statically setting a WLAN WMM access category value only prioritizes traffic to the client.

Wireless network administrators can also assign weights to each WLAN in relation to user priority levels. The lower the weight, the lower the priority. Use a weighted round robin technique to achieve different QoS levels across WLANs.

Optionally rate-limit bandwidth for WLAN sessions. This form of per-user rate limiting enables administrators to define uplink and downlink bandwidth limits for users and clients. This sets the level of traffic a user or client can forward and receive over the WLAN. If the user or client exceeds the limit, excessive traffic is dropped.

Rate limits can be applied externally from a RADIUS server using *Vendor Specific Attributes* (VSAs). Rate limits can be applied to users authenticating using 802.1X, captive portal authentication and devices using MAC authentication.

Configuring a Radio's QoS Policy

"Radio QoS Policy"

To configure an access point radio's QoS policy:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Radio QoS Policy** to display a high level display of existing Radio QoS policies.

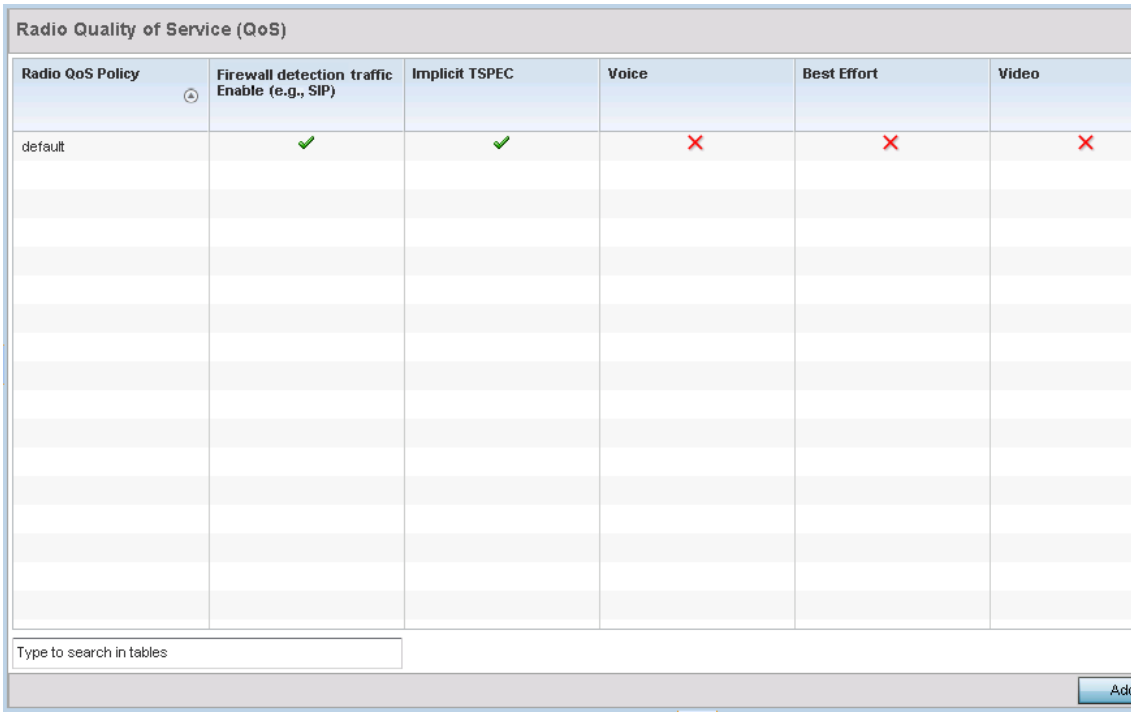


Figure 29: Radio Quality of Service (QoS) screen

4 Refer to the following information for a 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 used with the radio QoS policy. A red "X" defines the policy as having firewall detection disabled. When enabled, the firewall simulates the reception of frames for voice traffic when 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 to an access point 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 a client sends more traffic than 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 voice prioritization QoS is enabled on the radio. A red X indicates voice prioritization QoS is disabled on the radio.
Best Effort	A green check mark indicates best effort QoS is enabled on the radio. A red X indicates best effort QoS is disabled on the radio.
Video	A green check mark indicates video prioritization QoS is enabled on the radio. A red X indicates video prioritization QoS is disabled on the radio.
Background	A green check mark indicates background prioritization QoS is enabled on the radio. A red X indicates that background prioritization QoS is disabled on the radio.

5 Either select **Add** to create a new radio QoS policy, or select an existing policy and select **Edit** to modify its configuration.

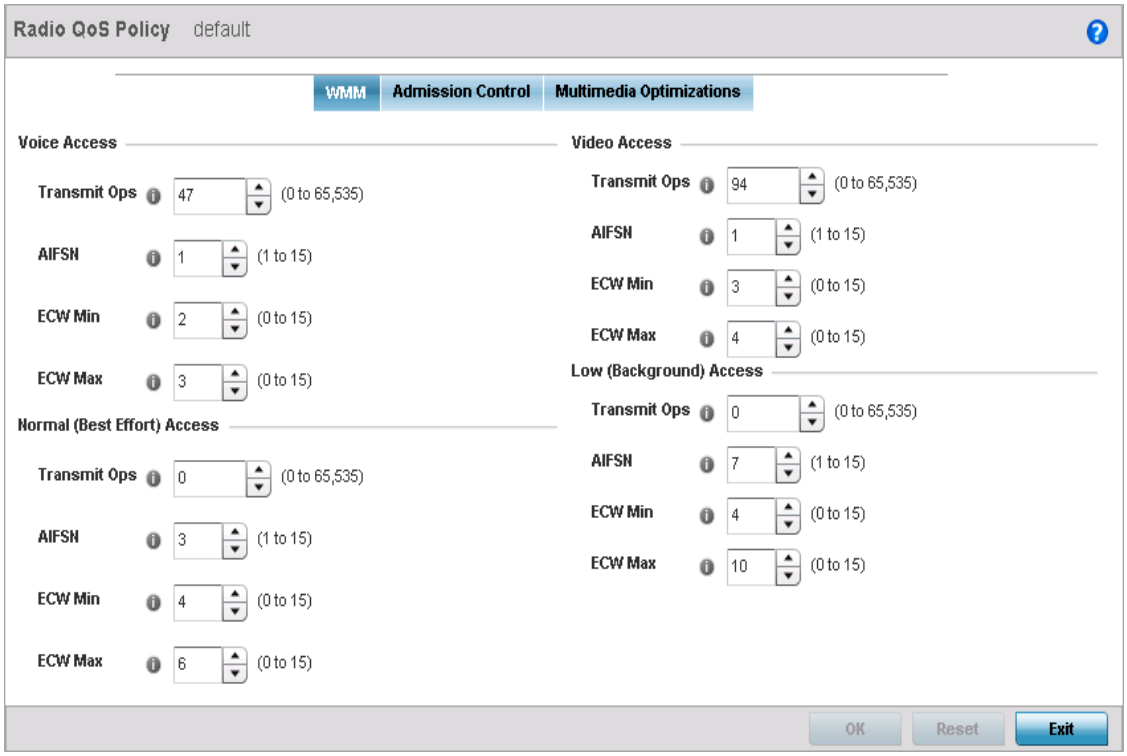


Figure 30: Radio QoS Policy screen - WMM tab

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.

6 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 real-time 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 value from 1 - 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 1.
ECW Min	*ECW Min* is combined with *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	*ECW Max* is combined with *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.

7 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 from 1 - 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 3.
ECW Min	*ECW Min* is combined with *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. Higher values are used for lower priority traffic (like normal). The available range is from 0-15. The default value is 4.
ECW Max	*ECW Max* is combined with *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. Higher values are used for lower priority traffic (like normal). The available range is from 0-15. The default value is 6.

8 Set the following **Video Access** settings for the radio QoS policy:

Transmit Ops	Use the spinner control to set the maximum duration a radio can transmit after obtaining a transmit opportunity. For higher-priority traffic categories (like video), this value should be set to a low number. The default value is 94.
AIFSN	Set the current AIFSN from 1 - 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 1.
ECW Min	*ECW Min* is combined with *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 (like video). The available range is from 0-15. The default value is 3.
ECW Max	*ECW Max* is combined with *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 (like video). The available range is from 0-15. The default value is 4.

9 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 from 1- 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 7.
ECW Min	*ECW Min* is combined with *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. Higher values are used for lower priority traffic (like low). The available range is from 0-15. The default value is 4.
ECW Max	*ECW Max* is combined with *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 (like video). The available range is from 0-15. The default value is 10.

10 Select **OK** when completed to update the radio QoS settings for this policy. Select **Reset** to revert back to last saved configuration.

11 Select the **Admission Control** tab to configure an admission control configuration for selected radio QoS policy. Admission control requires clients send their *traffic specifications* (TSPEC) to a managed access point before they can transmit or receive data within the access point managed network.

The name of the radio QoS policy, for which the admission control settings apply, displays in the banner of the QoS Policy screen.

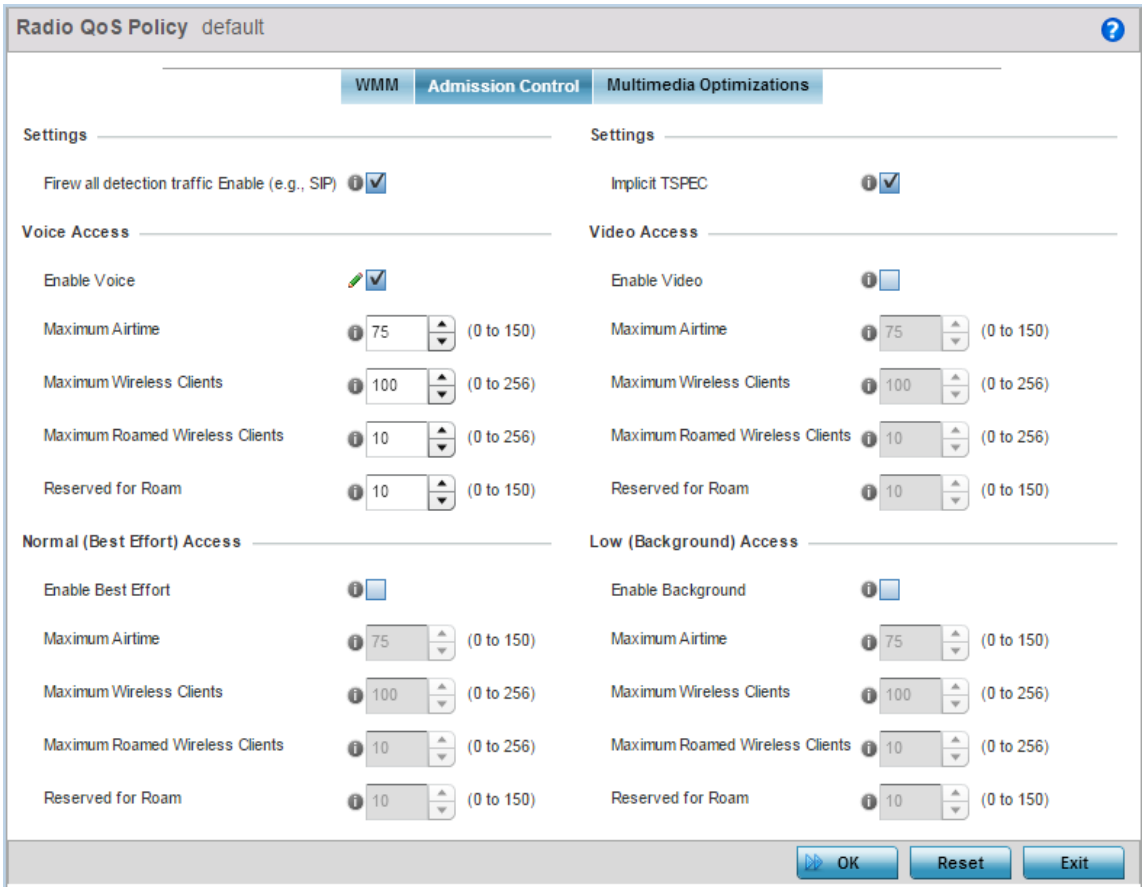


Figure 31: Radio QoS Policy screen - Admission Control tab

12 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 option is enabled by default.

13 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 just this radio's QoS policy. This option is enabled by default.

14 Set the following **Voice Access** admission control settings for the radio QoS policy:

Enable Voice	Select this check box to enable admission control for 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). 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 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 the radio is intended to support voice. The default 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 is 100.
Maximum Roamed Wireless Clients	Set the number of voice supported wireless clients allowed to roam to a different access point radio. Select from 0 - 256 clients. The default value is 10.
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 access point 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 **Normal (Best Effort) Access** admission control settings for the radio QoS policy:

Enable Best Effort	Select this check box to enable admission control for video traffic. Only normal background 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 normal 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). Normal background traffic only needs a short radio airtime to process, so set an intermediate airtime value if the radio QoS policy is reserved for background data support. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting background traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from 0 - 256 clients. The default value is 100.
Maximum Roamed Wireless Clients	Set the number of normal background supported wireless clients allowed to roam to a different managed access point radio. Select from 0 - 256 clients. The default value is 10.
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 managed radio. The available percentage range is from 0 - 150%, with 150% available to account for over-subscription. The default value is 10%.

16 Set the following **Video Access** admission control settings for the radio QoS policy:

Enable Video	Select this check box to enable admission control for 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 the radio QoS policy is intended to support video. The default value is 75%.
Maximum Wireless Clients	Set the number of video 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 video access category, as wireless clients supporting video use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default value is 100.
Maximum Roamed Wireless Clients	Set the number of video supported wireless clients allowed to roam to a different access point radio. Select from 0-256 clients. The default value is 10.
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 managed radio. The available percentage range is from 0 - 150%, with 150% accounting for over-subscription. The default value is 10%.

17 Set the following **Low (Background) Access** admission control settings for the radio QoS policy:

Enable Background	Select this check box to enable admission control for lower priority traffic. Only low 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 client traffic. The available percentage range is from 0 - 150%, with 150% being available to account for over-subscription. Best effort traffic only needs a short radio airtime to process, so set an intermediate airtime value if the radio QoS policy is reserved to support background data. The default value is 75%.
Maximum Wireless Clients	Set the number of low priority wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from 0 - 256 clients. The default value is 100.
Maximum Roamed Wireless Clients	Set the number of low priority supported wireless clients allowed to roam to a different access point radio. Select from 0-256 clients. The default value is 10.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for clients who have roamed to a different access point radio. The available percentage range is from 0 - 150%, with 150% available to account for over-subscription. The default value is 10%.

18 Select the **Multimedia Optimizations** tab to configure advanced multimedia QoS configuration and Smart Aggregation configuration for the radio's QoS policy.

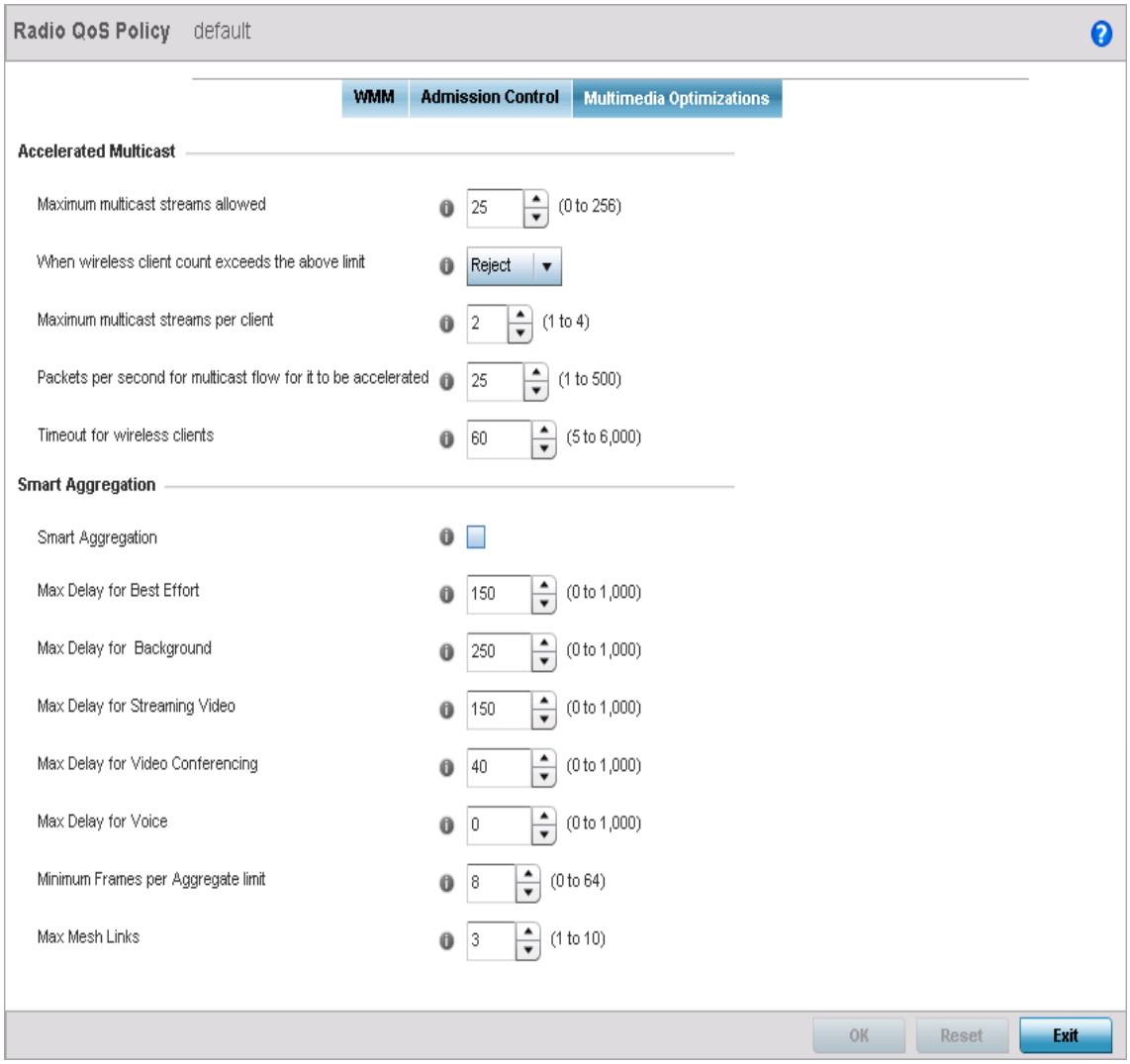


Figure 32: Radio QoS Policy screen - Multimedia Optimizations tab

19 Set the following **Accelerated Multicast** settings:

Maximum multicast streams allowed	Specify the maximum number of multicast streams (from 0 - 256) allowed 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 to *Revert* existing clients to a non-accelerated state. The default setting is Reject.
Maximum multicast streams per client	Specify the maximum number of multicast streams (from 1 - 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 (from 1 - 500) that triggers acceleration for wireless clients. The default value is 25.
Timeout for wireless clients	Specify a timeout value in seconds (from 5 - 6,000) for wireless clients to revert back to a non-accelerated state. The default value is 60 seconds.

20 Set the following **Smart Aggregation** settings:

Smart Aggregation enhances the existing implementation of frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In the normal implementation of frame aggregation, an aggregated frame is sent when it meets one of these conditions:

- When a preconfigured number of frames to aggregate is reached.
- When a preconfigured interval of time has elapsed since the first frame - of a set of frames to be aggregated - was received.
- When a preconfigured 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 to the standard frame aggregation, the time delay for aggregation is set individually for each traffic class. For example, voice traffic might not be aggregated but sent immediately, whereas, background data traffic is set a time delay for aggregating frames and these aggregated frames are sent.

Smart Aggregation	Select to enable Smart Aggregation and dynamically set the time when an aggregated frame is transmitted. This option is disabled by default.
Max Delay for Best Effort	Specify the maximum time in milliseconds to delay best effort traffic. The default setting is 150 millisecond.
Max Delay for Background	Specify the maximum time in milliseconds to delay background traffic. The default setting is 250 millisecond.
Max Delay for Streaming Video	Specify the maximum time in milliseconds to delay streaming video traffic. The default setting is 150 millisecond.
Max Delay for Video Conferencing	Specify the maximum time in milliseconds to delay video conferencing traffic. The default setting is 40 millisecond.
Max Delay for Voice	Specify the maximum time in milliseconds to delay voice traffic. The default setting is 0 millisecond.
Minimum frames per Aggregate limit	Specify the minimum number of frames to aggregate in a frame before it is transmitted. The default setting is 8 frames.
Max Mesh Links	Specify the maximum number of mesh links for Smart Aggregation. The default setting is 3.

21 Select **OK** to update radio QoS multimedia optimization settings Select **Reset** to revert to the last saved configuration.

Radio QoS Configuration and Deployment Considerations

"Radio QoS Policy"

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 co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a best effort access category.
- It is recommended that default WMM values be used for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.

- Overloading an access point radio with too much high priority traffic (especially voice) degrades the overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

Association ACL

"Wireless Configuration"

An Association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a WLAN.

An Association ACL allows an administrator to grant or restrict client access by specifying a wireless client MAC address or range of MAC addresses to either include or exclude from 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 WLAN Advanced Settings" on page 574.

Each supported access point model can support up to 32 Association ACLs, with the exception of AP6521 model that supports 16 WLAN Association ACLs.

To define an Association ACL deployable with a WLAN:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Association ACL** to display a high level display of existing Association ACL policies.

The **Association Access Control List (ACL)** screen lists existing Association ACL policies. Any of these policies can be selected and applied.

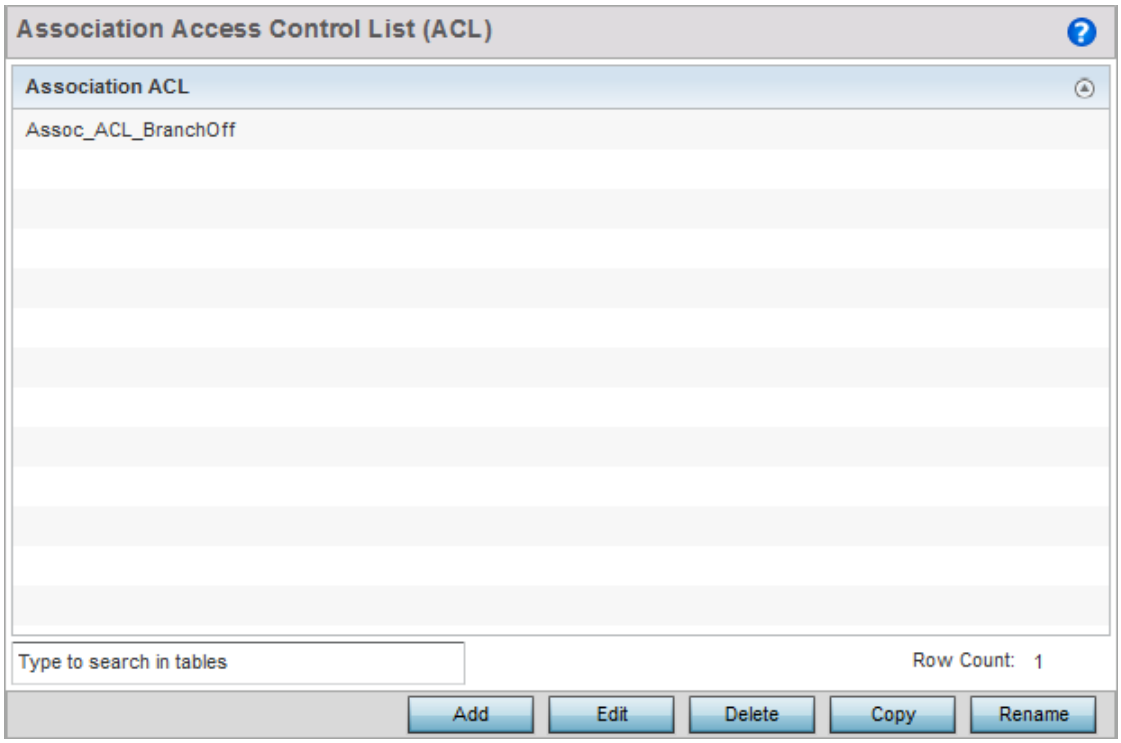


Figure 33: Association Access Control List (ACL) screen

4 Select **Add** to define a new ACL configuration, **Edit** to modify an existing ACL configuration or **Delete** to remove an existing one. Select **Copy** to make a copy of an existing ACL for further modifications. Select **Rename** to rename an existing ACL.

An **Association ACL** screen displays for defining a new ACL or modifying a selected ACL.

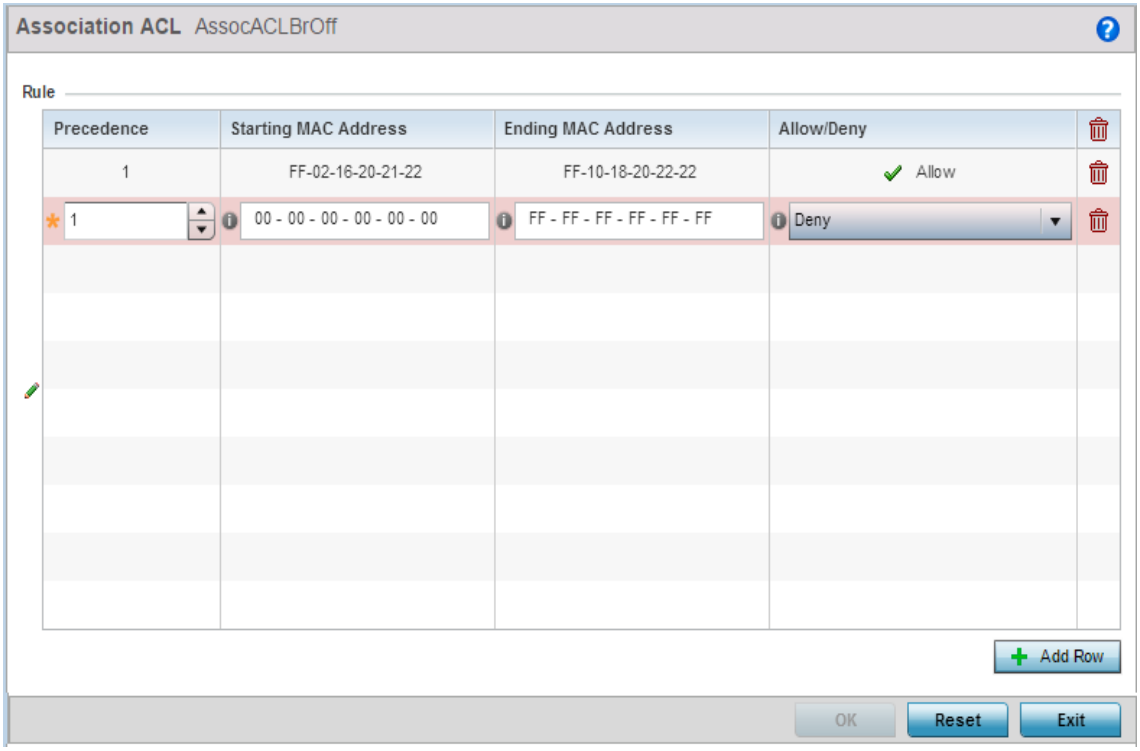


Figure 34: Association ACL screen

5 Select the **+ Add Row** button to add an association ACL template.

6 If 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.

7 Set the following parameters for the creation or modification of the Association ACL:

Precedence	The rules within a WLAN's ACL are applied to packets based on their precedence values. Every rule has a unique sequential precedence value you define. You cannot add two rules's with the same precedence value. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.
Starting MAC Address	Provide a starting client MAC address for non unicast and multicast packet transmissions.
Ending MAC Address	Provide an ending MAC address for non unicast and multicast packet transmissions.
Allow/Deny	Use the drop-down menu to either *Allow* or *Deny* access if a MAC address matches this rule.

8 Select the **+ Add Row** radio button to add MAC address ranges and allow/deny designations.

9 Select **OK** to update the Association ACL settings. Select **Reset** to revert to the last saved configuration.

Association ACL Deployment Considerations

"Association ACL"

Before defining an Association ACL configuration and applying it to a 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 they may map to. However, be careful not to name ACLs after specific WLANs, as 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

"Wireless Configuration"

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.

Smart RF can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each managed radio.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs through periodic re-calibration of the network. Re-calibration can be initiated manually or can be automatically scheduled to ensure the RF configuration is optimized to factor for RF environment changes (such as new sources of interference, or neighboring access points).



NOTE

Unlike a controller or service platform, an access point utilizes a single Smart RF configuration it can use with other access points of the same model. However, the Smart RF policy needs to be activated from any one of the Smart RF screens. Numerous Smart RF policies cannot be defined on behalf of the access point.

Smart RF also provides self-healing functions by monitoring the network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, 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.

It is recommended, when creating a Smart RF policy, to keep in mind that if a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels on detection of radar.

- 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 channels 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 point 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 CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.



NOTE

RF planning must be performed to ensure overlapping coverage exists at a deployment site for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.



CAUTION

The access point's Smart RF feature is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections and communication disruptions.

To define the Smart RF configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **Smart RF.**

The **Basic Configuration** screen displays by default.

4 Select the **Activate SMART RF Policy** check box to enable the parameters on the screen for configuration. The configuration cannot be applied to the access point profile unless this settings is selected and remains enabled.

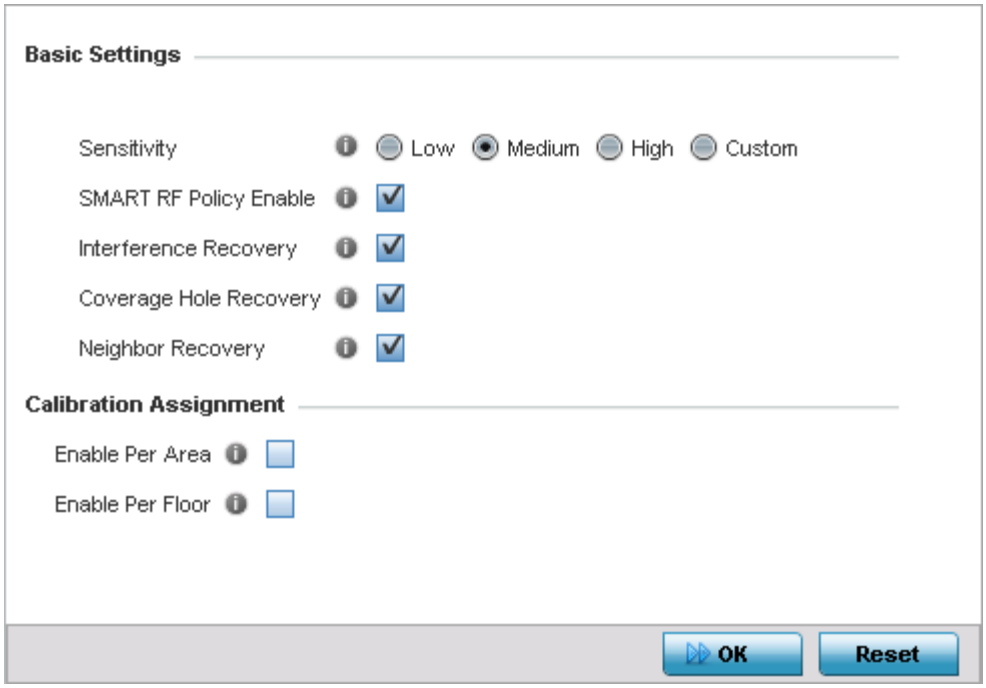


Figure 35: SMART RF - Basic Configuration screen

5 Refer to the **Basic Settings** field to enable a Smart RF policy and define its sensitivity and detector status.

Sensitivity	Select the radio button corresponding to the desired Smart RF sensitivity. Options include *Low*, *Medium*, *High* and *Custom*. The default setting is Medium.
SMART RF Policy Enable	Select this radio button to enable Smart RF for immediate inclusion within a RF Domain. Smart RF is enabled by default.
Interference Recovery	Select this radio button to enable compensations from neighboring radios when radio interference is detected. When interference is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client (as seen by the access point radio). If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is enabled by default.
Coverage Hole Recovery	Select this radio button to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart RF supported radio coverage area. When coverage hole is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client as seen by the access point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold. This option is enabled by default.
Neighbor Recovery	Select this radio button to enable automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. This option is enabled by default.

6 Refer to the **Calibration Assignment** field to define whether Smart RF Calibration and radio grouping is conducted by the floor the access point is deployed on or building in its entirety. Both options are disabled by default.

7 Select **OK** to update the access point's Smart RF Basic configuration. Select **Reset** to revert to the last saved configuration. The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand side, portion of the access point user interface.

8 Select **Channel and Power**. Ensure the **Activate SMART RF Policy** remains selected so the screen's parameters can be updated.

Use the Channel and Power screen to refine Smart RF power settings over both the 5.0 GHz and 2.4 GHz radio bands and select channel settings in respect to the access point's channel usage.

NOTE

The Power Settings and Channel Settings parameters are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

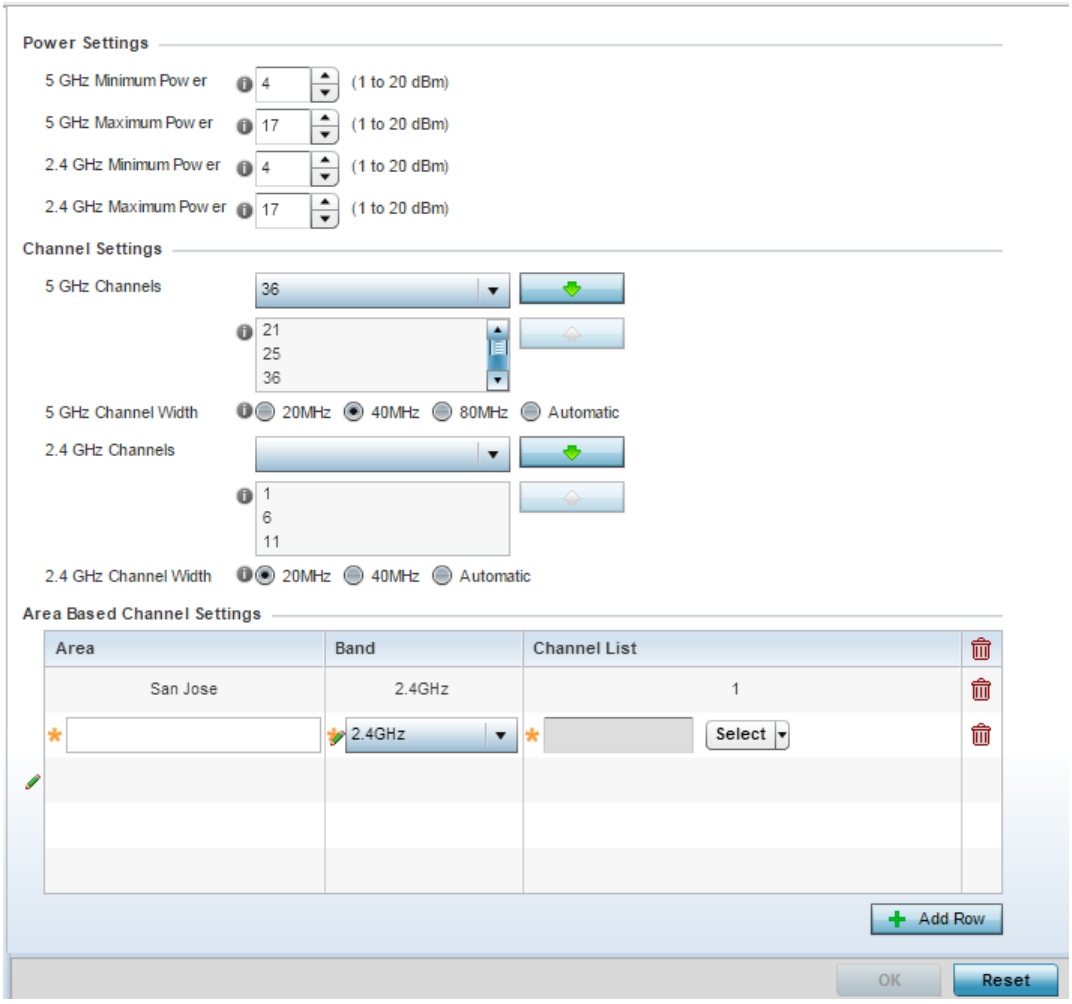


Figure 36: SMART RF - Channel and Power screen

9 Refer to the **Power Settings** field to define Smart RF recovery settings for the access point's 5.0 GHz (802.11a) and 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.

10 Set the following **Channel Settings** for the access point's 5.0 GHz and 2.4 GHz radio bands:

5 GHz Channels	Use the *Select* drop-down menu to select the 5.0 GHz channels used in Smart RF scans.
5 GHz Channel Width	20 MHz 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 2.4 GHz and 5.0 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 the automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. The default setting is 40 MHz.
2.4 GHz Channels	Use the *Select* drop-down menu to select 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 2.4 GHz and 5.0 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. 20 MHz is the default setting.

11 Select the **+Add Row** button to add **Area Based Channel Settings**.

12 Set the following **Area Based Channel Settings** for the access point:

Area	Use the text area to provide a name for the area being configured.
Band	Use the drop-down menu to select the radio band to use in the area being configured.
Channel List	Use the *Select* drop-down menu to select the channels used in Smart RF area based channel settings.

13 Select **OK** to update the Smart RF Channel and Power settings for this policy. Select **Reset** to revert to the last saved configuration. The Smart RF policy can be invoked at any point in the configuration process by selecting **Activate SMART RF Policy** from the upper, left-hand side, of the access point user interface.

14 Select **Scanning Configuration**. Ensure **Activate SMART RF Policy** remains selected so the screen's parameters can be updated. Additionally, the Smart RF configuration cannot be applied to the access point profile unless this setting remains selected.

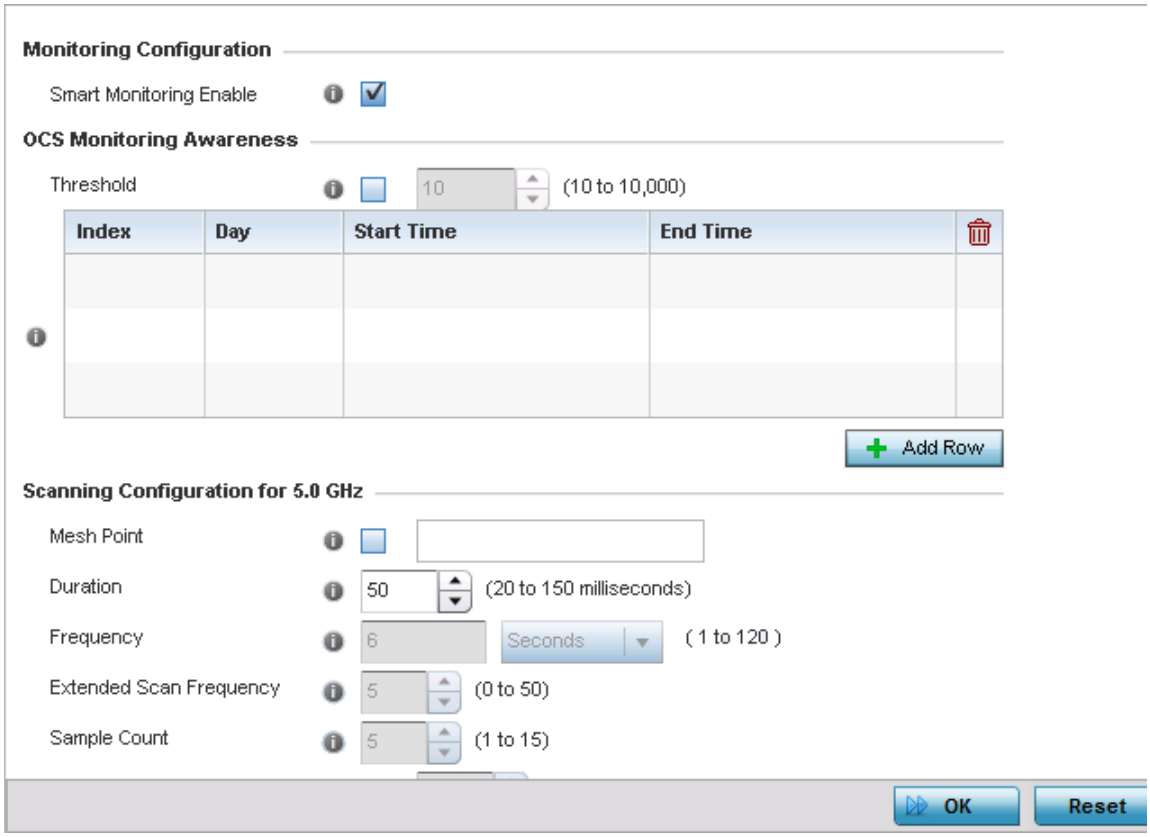


Figure 37: SMART RF - Scanning Configuration screen



NOTE

The monitoring and scanning parameters within the Scanning Configuration screen are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

15 Enable or disable **Smart Monitoring Enable** by selecting the option. The feature is enabled by default.

When enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

16 Set the following **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 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 day.
Start Time	This value sets the starting time of day(s) that 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	This value sets the ending time of day(s) 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*.

17 Set the following **Scanning Configurations** for *both* the 2.4 GHZ and 5.0 GHz radio bands:

Duration	Set a channel scan duration (from 20 - 150 milliseconds) 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 a 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 2.4 GHz and 5.0 GHz bands.
Extended Scan Frequency	Use the spinner control to set an extended scan frequency from 0 - 50. This is the frequency radios scan channels on non-peer radios. The default setting is 5 for both 2.4 GHz and 5.0 GHz bands.

Sample Count	Use the spinner control to set a sample scan count value from 1 - 15. This is the number of radio RF readings gathered before data is sent to the Smart RF master. The default setting is 5 for both 2.4 GHz and 5.0 GHz bands.
Client Aware Scanning	Use the spinner control to set a client awareness count (1 - 255) during off channel scans for either the 2.4 or 5.0 GHz radio. The default setting is 1 for both radio bands.
Power Save Aware Scanning	Select either the *Dynamic*, *Strict* or *Disable* radio button to define how power save scanning is set for Smart RF. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is Dynamic for both 2.4 GHz and 5.0 GHz bands.
Voice Aware Scanning	Select either *Dynamic*, *Strict* or *Disable* to define how voice aware recognition is set for Smart RF. Strict disables smart monitoring as long as a voice 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 2.4 GHz and 5.0 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.

18 Select **OK** to update the Smart RF Scanning Configuration settings. Select **Reset** to revert to the last saved configuration.

19 Select **Recovery**.

The **Neighbor Recovery** tab displays by default. Use the *Neighbor*, *Interference* and *Coverage Hole* recovery tabs to define how 2.4 and 5.0 GHz radios compensate for failed neighbor radios, interference, coverage holes and loss of root path requiring neighbor radio intervention.

20 Set the **Hold Time** for the Smart RF configuration.

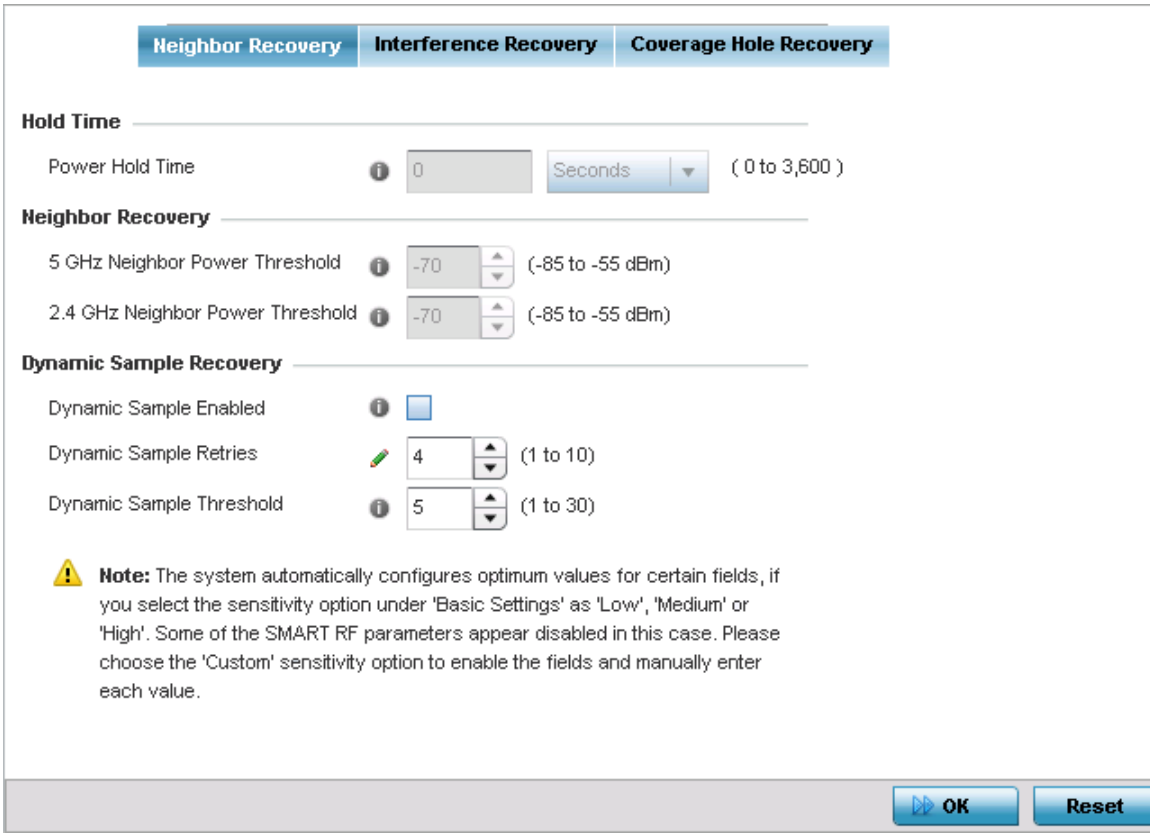


Figure 38: SMART RF Recovery Configuration screen - Neighbor Recovery tab

Power Hold Time	Defines 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.

21 Set the following **Neighbor Recovery** parameters:

NOTE

The recovery parameters within the *Neighbor Recovery*, *Interference* and *Coverage Hole Recovery* tabs are only enabled when *Custom* is selected as the Sensitivity setting from the Smart RF Basic Configuration screen.

5 GHz Neighbor Power Threshold	Use the spinner control to set a value from -85 to -55 dBm the access point's 5.0 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm.
2.4 GHz Neighbor Power Threshold	Use the spinner control to set a value from -85 to -55 dBm the access point's 2.4 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within the access point's radio coverage area. The default value is -70 dBm.

22 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	Use the spinner control to set the number of retries (1 - 10) before a power change is allowed to compensate for a potential coverage hole. The default setting is 3.
Dynamic Sample Threshold	Use the spinner control to set the number of sample reports (1 - 30) used before dynamic sampling is invoked for a potential power change adjustment. The default setting is 5.

23 Select **OK** to update the Smart RF Neighbor Recovery settings. Select **Reset** to revert to the last saved configuration.

24 Select the **Interference Recovery** tab.

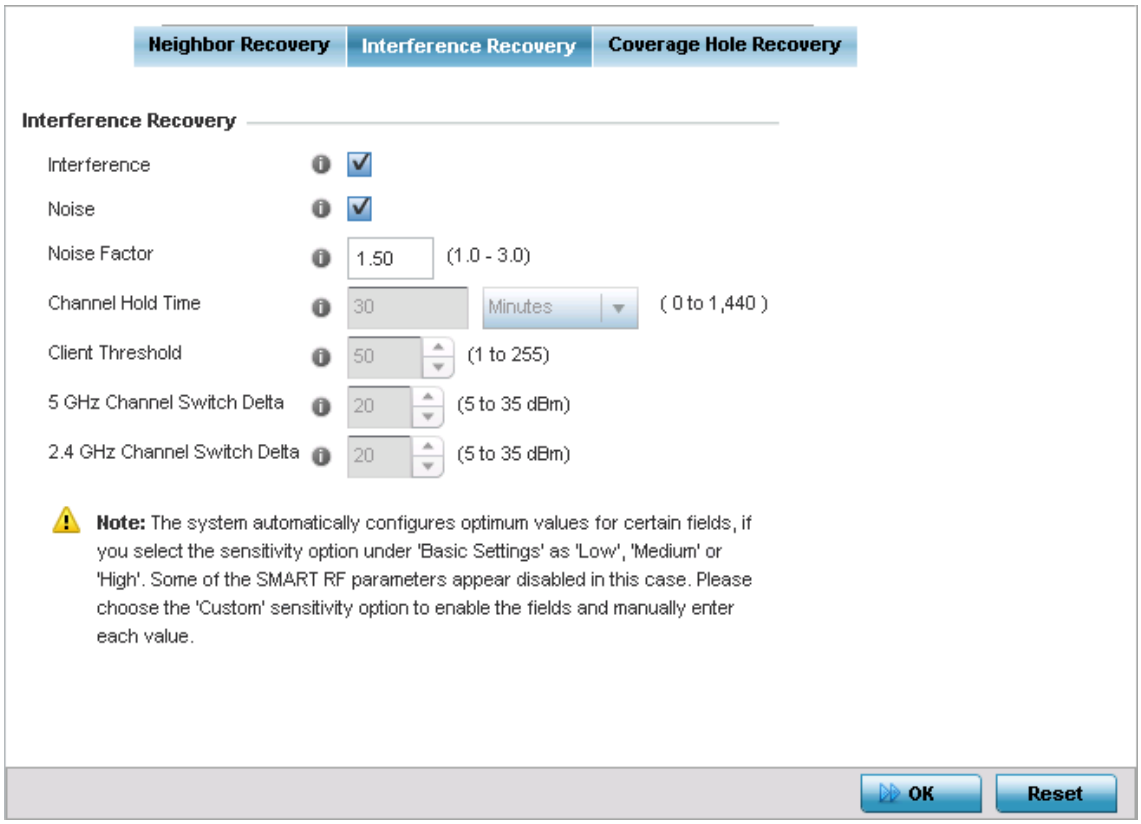


Figure 39: SMART RF Recovery Configuration screen - Interference Recovery tab

25 Set the following **Interference Recovery** parameters:

Interference	Select this radio button to allow Smart RF 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 radio button to allow Smart RF to scan for excess noise from WiFi devices. When detected, Smart RF supported access points can change their channel and move to a cleaner channel. This feature is enabled by default.
Noise Factor	Use this field to set the noise factor to take into consideration by Smart RF during interference recovery calculations. Set a value from 1.0 - 3.0.
Channel Hold Time	Defines the minimum time between channel changes during neighbor recovery. Set the time in either *Seconds* (0 - 86,400), *Minutes* (0 - 1,440) or *Hours* (0 - 24) or *Days* (0 - 1). The default setting is 30 minutes.
Client Threshold	Use the spinner to set a client threshold from 1 - 255. If the threshold defined 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	Use the spinner to set a channel switch 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	Use the spinner to set a channel switch 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.

26 Select **OK** to update the Smart RF Interference Recovery settings. Select **Reset** to revert to the last saved configuration.

27 Select the **Coverage Hole Recovery** tab.

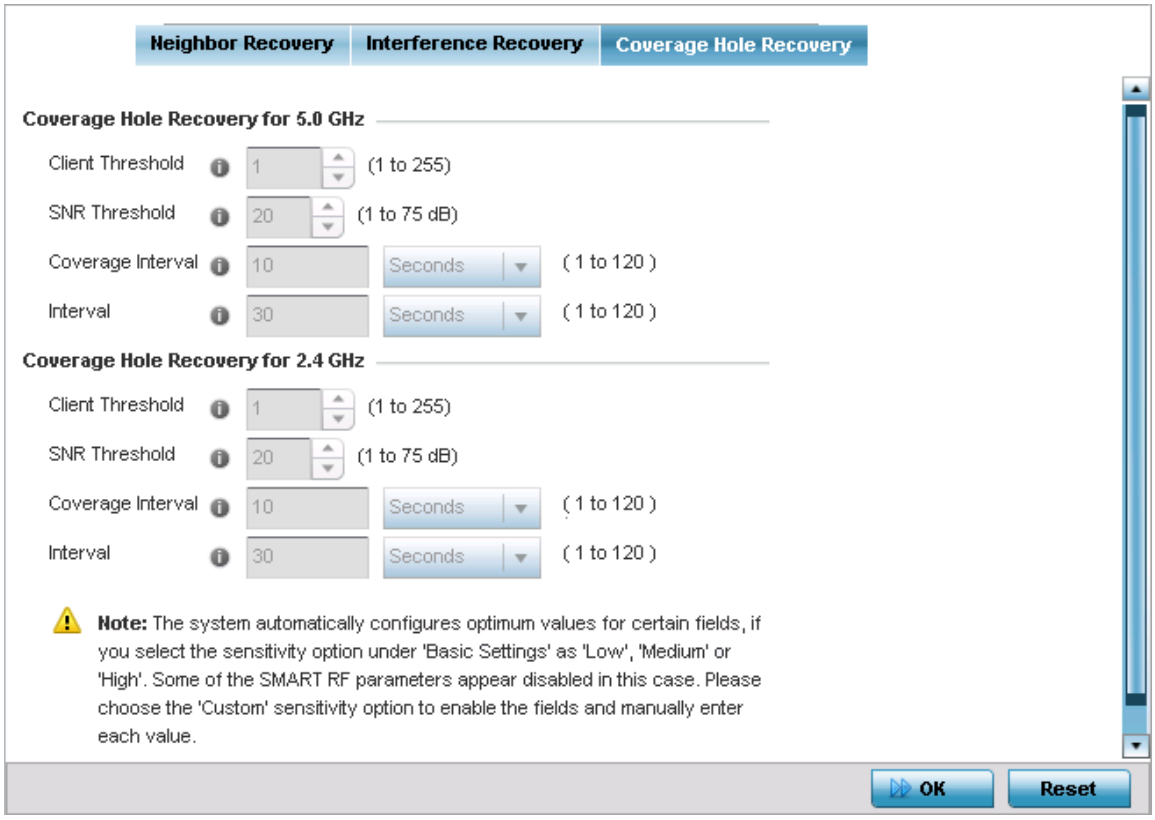


Figure 40: SMART RF Recovery Configuration screen - Coverage Hole Recovery tab

28 Set the following **Coverage Hole Recovery for 5.0 GHz** and **2.4 GHz** parameters:

Client Threshold	Use the spinner to set a client threshold from 1 - 255. This is the minimum number of clients a radio should have associated for coverage hole recovery to trigger. AP6522, AP6522M, AP6532, AP6562, AP8132, AP8232 and AP71XX model access points can support up to 256 clients per access point or radio. AP6521 model access point can support up to 128 clients per access point or radio. The default setting is 1.
SNR Threshold	Use the spinner control to set a *signal to noise* (SNR) threshold (from 1 - 75 dB). This is the SNR threshold for an associated client as seen by its associated AP radio. When exceeded, the radio increases its transmit power to increase coverage for the associated client. The default value is 20 dB.
Coverage Interval	Define the interval when coverage hole recovery should be initiated after a coverage hole is detected. The default is 10 seconds for both 2.4 GHz and 5.0 GHz radios.
Interval	Define the interval coverage hole recovery should be conducted after a coverage hole is detected. The default is 30 seconds for both 2.4 GHz and 5.0 GHz radios.

29 Select **OK** to update the Smart RF Coverage Hole Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

Smart RF Configuration and Deployment Considerations

"SMART RF"

Before defining a Smart RF supported configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections
- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when access points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

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 channels 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 point 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 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 Policy

"Wireless Configuration"

MeshConnex is a mesh networking technology 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 WiNG 5 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 will attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

To define a MeshConnex policy:

1 Select the **Configuration** tab from the Web UI.

2 Select **Wireless.**

3 Select **MeshConnex Policy** to display existing MeshConnex policies.

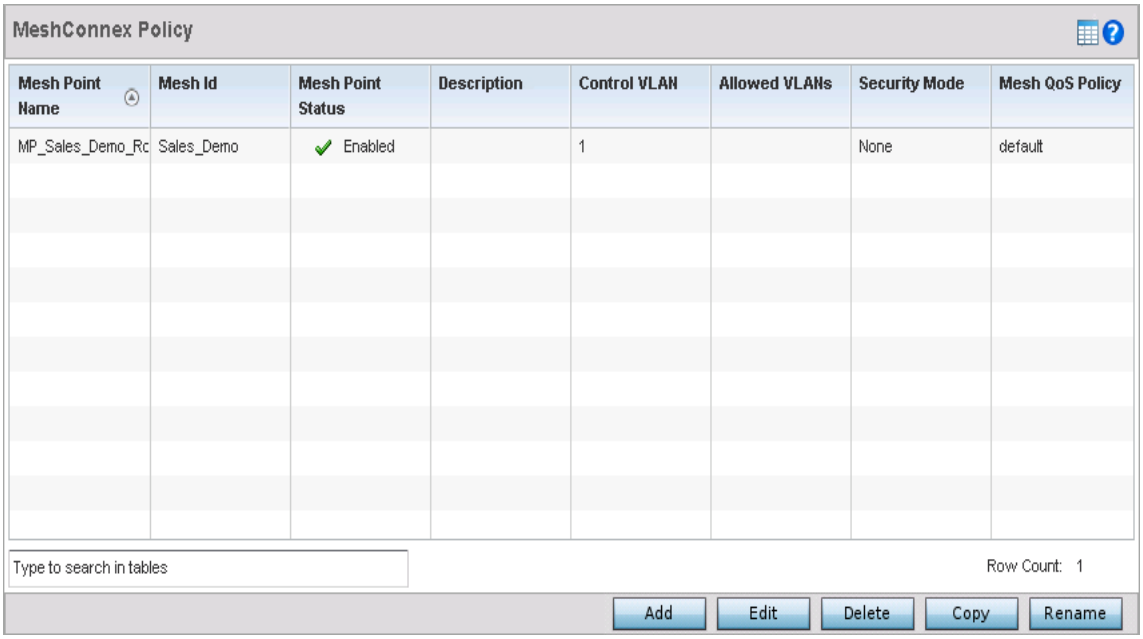


Figure 41: MeshConnex Policy screen

4 Refer to the following configuration data for existing MeshConnex policies:

Mesh Point Name	Displays the names of all configured mesh points.
Mesh ID	Displays the IDs of all mesh identifiers for the configured mesh points.
Mesh Point Status	Specifies the status of each configured mesh point, either *Enabled* or *Disabled*.

Description	Displays any descriptive text entered for each of the configured mesh points.
Control VLAN	Displays VLAN number for the control VLAN on each of the configured mesh points.
Allowed VLANs	Displays the list of VLANs allowed on each of the configured mesh points.
Security Mode	Displays the security for each of the configured mesh points. The field will display *none* for no security or *psk* for pre-shared key authentication.
Mesh QoS Policy	Displays the list of Mesh Quality of Service policies associated with each of the configured mesh points.

5 Select **Add** to create a new MeshConnex policy, **Edit** to modify the attributes of a existing policy or **Delete** to remove obsolete policies from the list of those available. Use **Copy** to create a copy of an existing policy for further modification. Use **Rename** to rename an existing MeshConnex policy.

The **Configuration** screen displays by default for the new or modified MeshConnex policy.

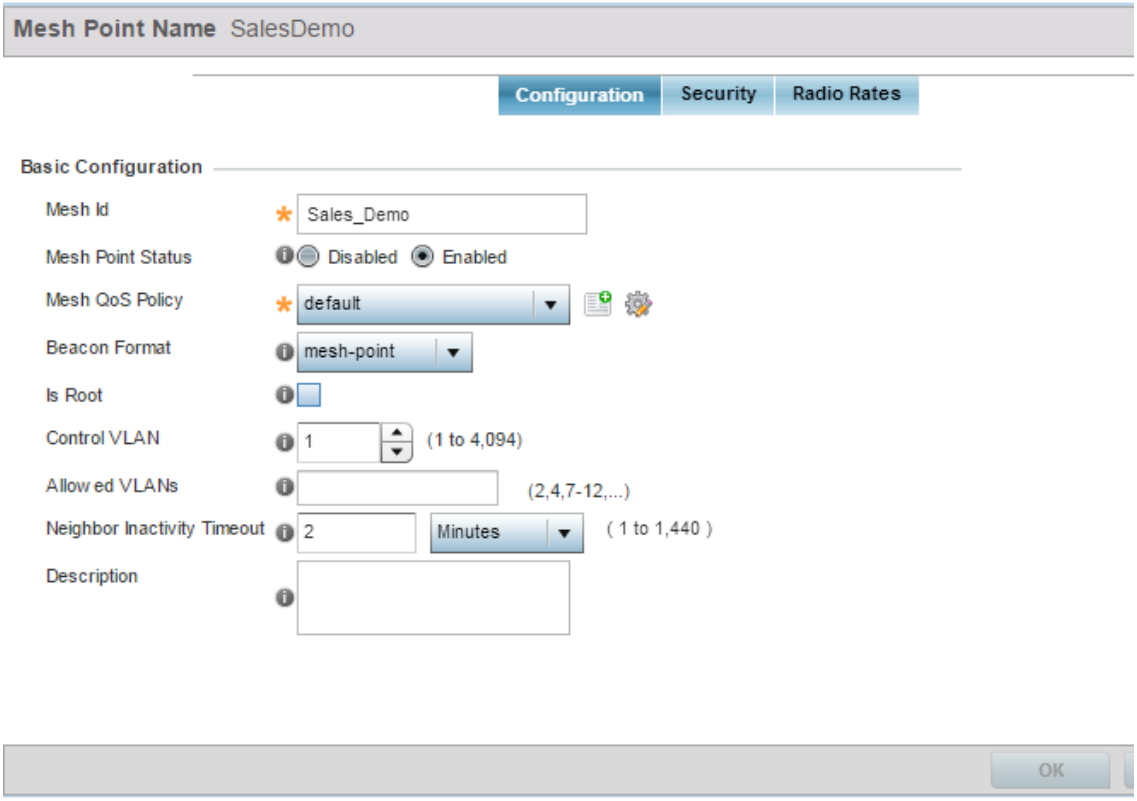


Figure 42: MeshConnex - Basic Configuration screen

6 Refer to the **Basic Configuration** section to define a MeshConnex profile.

Mesh Point Name	Specify a name for the new mesh point. The name should be descriptive of the mesh point to easily differentiate it from other mesh points. This field is mandatory.
Mesh id	Specify a mesh identifier for this mesh point. This field is optional.
Mesh Point Status	To enable this mesh point, select the *Enabled* radio button. To disable the mesh point select the *Disabled* button. The default value is enabled.
Mesh QoS Policy	Use the drop-down menu to specify the mesh 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	Use the drop-down menu to specify the format that 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 from the drop-down menu. The default value is mesh point.
Is Root	Select this option to specify the mesh point as a root.
Control VLAN	Use the spinner control to specify a VLAN to carry mesh point control traffic. The valid range for control VLAN is from 1 - 4094. The default value is VLAN 1.
Allowed VLANs	Specify the VLANs allowed to pass traffic on the mesh point. Separate all VLANs with a comma. To specify a range of allowed VLANs separate the starting VLAN and the ending VLAN with a hyphen. Aliases can be used to configure *Allowed VLANs*.
Neighbor Inactivity Timeout	Specify a Neighbor Inactivity Timeout in *seconds*, *minutes*, *hours* or *days*, up to a maximum of 1 day. *Neighbor Inactivity Timeout* is the allowed amount of time between frames received from a neighbor before their client privileges are revoked. The default value is 2 minutes.
Description	Enter any descriptive text about the mesh point.

7 Select **OK** to update the MeshConnex Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.

8 Select the **Security** tab.

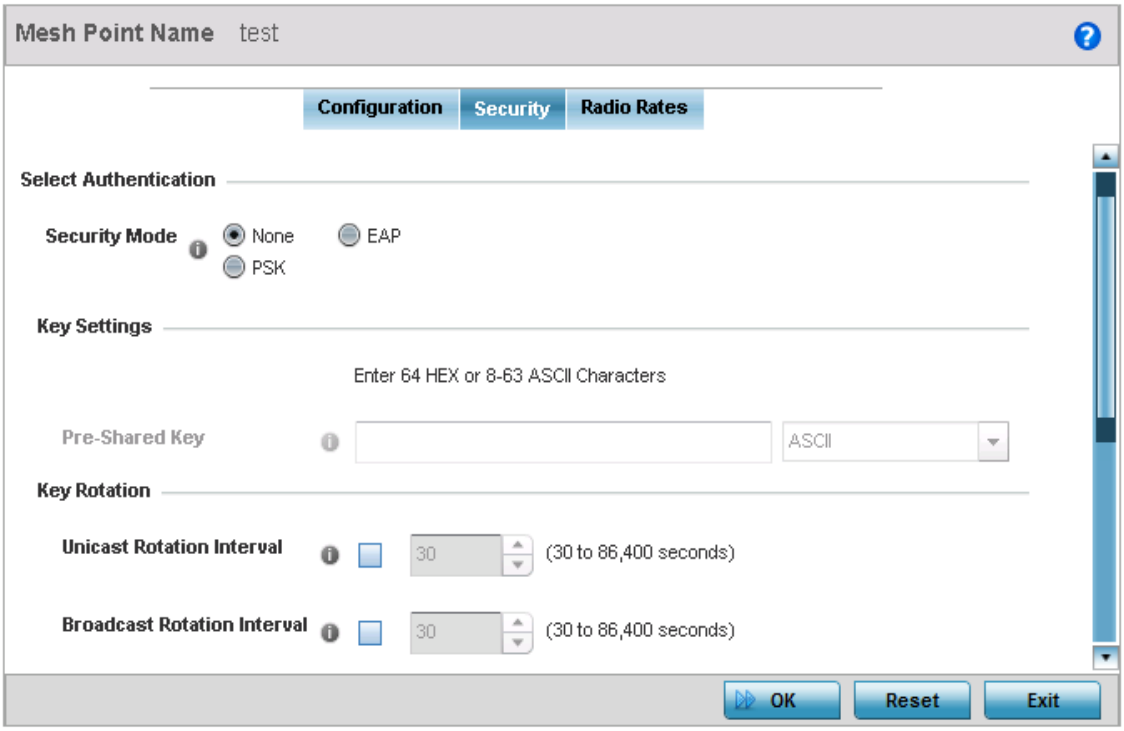


Figure 43: MeshConnex - Security screen

9 Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

Security Mode	Select a security authentication mode for the mesh point. Select *None* to have no authentication for the mesh point. Select *PSK* to set a pre-shared key as the authentication for the mesh-point. If PSK is selected, enter a pre-shared key in the *Key Settings* field. The default setting is *None*.

10 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.

11 Set the following **Key Rotation** for the mesh point:

Unicast Rotation Interval	Define an interval for unicast key transmission in *seconds* (30 - 86,400). This option is disabled by default.
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic will be alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in *seconds* (30 - 86,400). Key rotation enhances the broadcast traffic security on the WLAN. This option is disabled by default.

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

Set the following **EAP PEAP Authentication** information for the mesh point:

User ID	Configure the user name for PEAP MSCHAPv2 authentication.
Password	Configure the password associated with the specified username.
Trust Point	Configure the name of the Trust Point used for installing CA certificate and validating server certificate.
EAP TLS	Configure the name of the Trust Point used for installing client certificate, client private key, and CA certificate.
Type	Configure the EAP authentication method used by supplicants. The options are: PEAP-MSCHAPv2 and TLS
EAP Identity	Configure the EAP identity used during phase1 authentication. The value configured here need not the user's actual identity.
AAA Policy	Specify the AAA policy used with this EAP PEAP Authentication. Use the *Create* or *Edit* buttons to create a new AAA policy or edit and existing AAA policy.

13 Select the **Radio Rates** tab.

14 Set the following **Radio Rates** for both the 2.4 and 5.0 GHz radio bands:

2.4 GHz Mesh Point	Choose the *Select* button 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. If supporting 802.11n, select a Supported MCS index. 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. 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	Choose the *Select* button to configure radio rates for the 5.0 GHz band. Define both minimum *Basic* and optimal *Supported* rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. If supporting 802.11n, select a Supported MCS index. 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. 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.

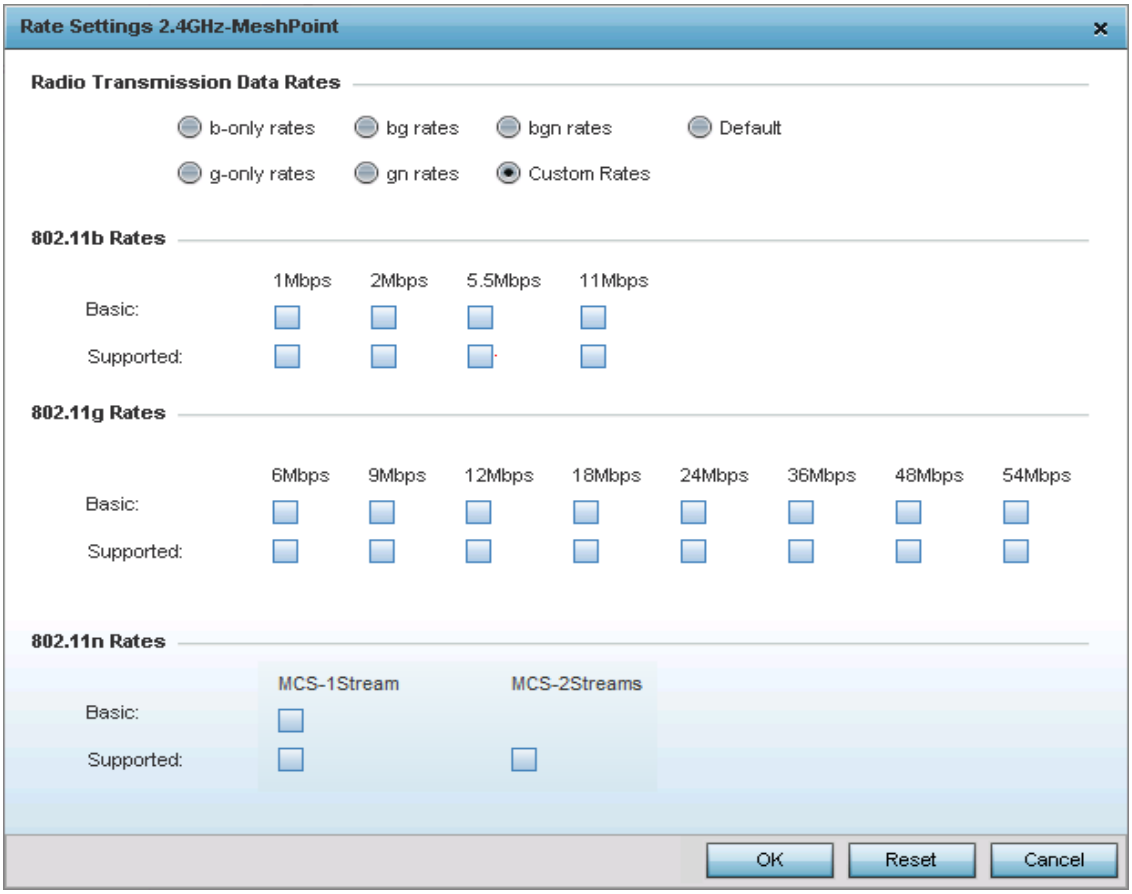


Figure 44: Advanced Rate Settings 2.4 GHz screen

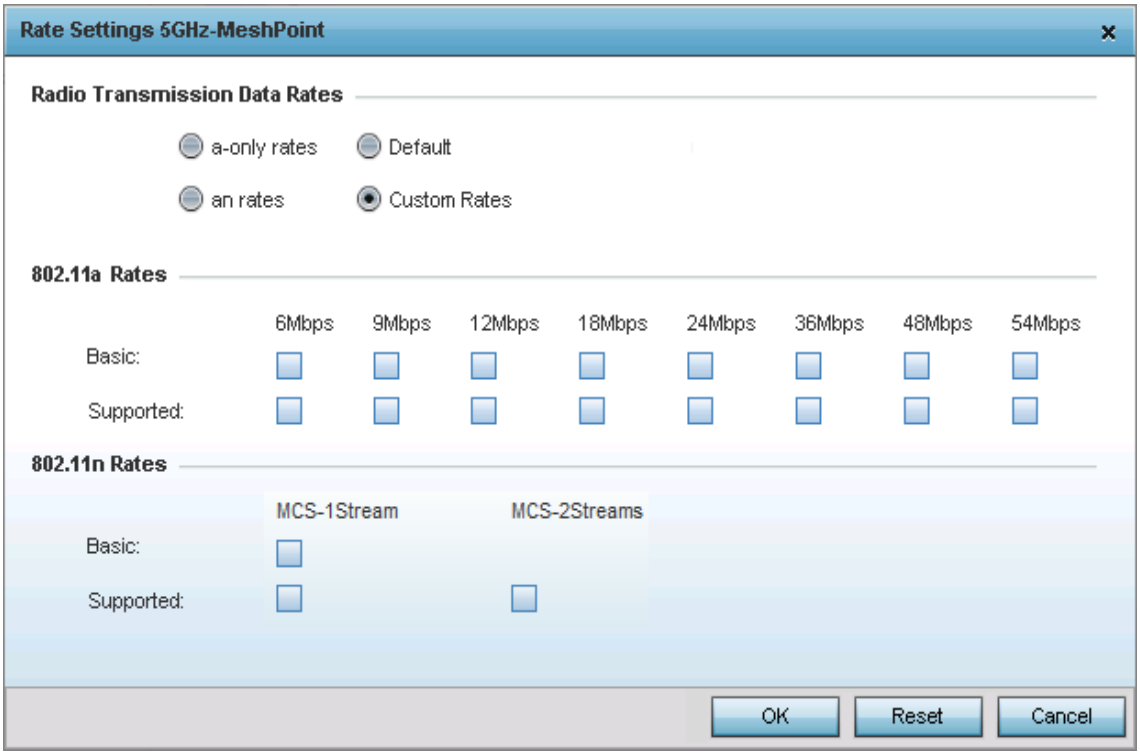


Figure 45: Advanced Rate Settings 5 GHz screen

15 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 supporting 802.11n, select a Supported MCS index. 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).

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

Mesh QoS Policy

"Wireless Configuration"

Mesh QoS provides a data traffic prioritization scheme that 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 the wireless controller's bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data. Packets within each category are processed based on the weights defined 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, select the **Add** button to create new policy. Select an existing Mesh QoS policy and select **Edit** to change the properties of the Mesh QoS policy.

To define a Mesh QoS policy:

1 Select **Configuration**.

2 Select **Wireless.**

3 Select **Mesh QoS Policy** to display existing Mesh QoS policies.

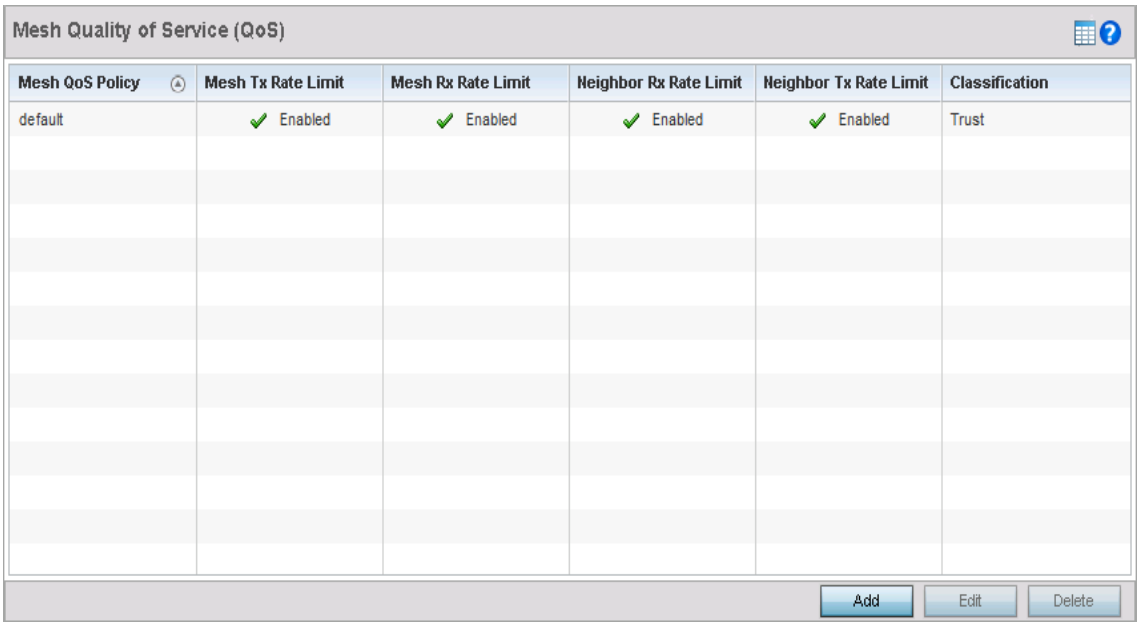


Figure 46: Mesh QoS Policy (QoS) screen

4 Refer to the following configuration data for existing Smart RF policies:

Mesh QoS Policy	Displays the name of each configured mesh QoS policy.
Mesh Tx Rate Limit	Displays whether or not a *Mesh Tx Rate Limit* is enabled for each Mesh QoS policy. This indicates rate limiting is enabled or disabled for all data received from any mesh point in the mesh. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Mesh Rx Rate Limit	Displays whether or not a *Mesh Rx Rate Limit* is enabled for each Mesh QoS policy. This indicates rate limiting is enabled or disabled for all data transmitted by the device to any mesh point in the mesh. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Neighbor Tx Rate Limit	Displays whether a *NeighborTx Rate Limit* is enabled for each Mesh QoS policy. This indicates rate limiting is enabled for data transmitted from connected wireless clients. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Neighbor Rx Rate Limit	Displays whether a *NeighborRx Rate Limit* is enabled for each Mesh QoS policy. This indicates rate limiting is enabled or disabled for data transmitted from the client to its associated access point radio and connected wireless controller. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Classification	Displays the forwarding QoS classification for each Mesh QoS policy.

5 Select the **Add** button to define a new Mesh QoS policy, or select an existing Mesh QoS policy and select **Edit** to modify its existing configuration. Existing QoS policies can be selected and deleted as needed.

The **Rate Limit** screen displays by default for the new or modified QoS policy.

Excessive traffic can cause performance issues or bring down the network completely. 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 mesh point) per neighbor. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the managed network and data transmitted from a mesh point's neighbor back to their associated access point radios and controller.

Before defining rate limit thresholds for mesh point transmit and receive traffic, it is recommended that you 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.

A connected neighbor can also have QoS rate limit settings defined in both the transmit and receive direction.

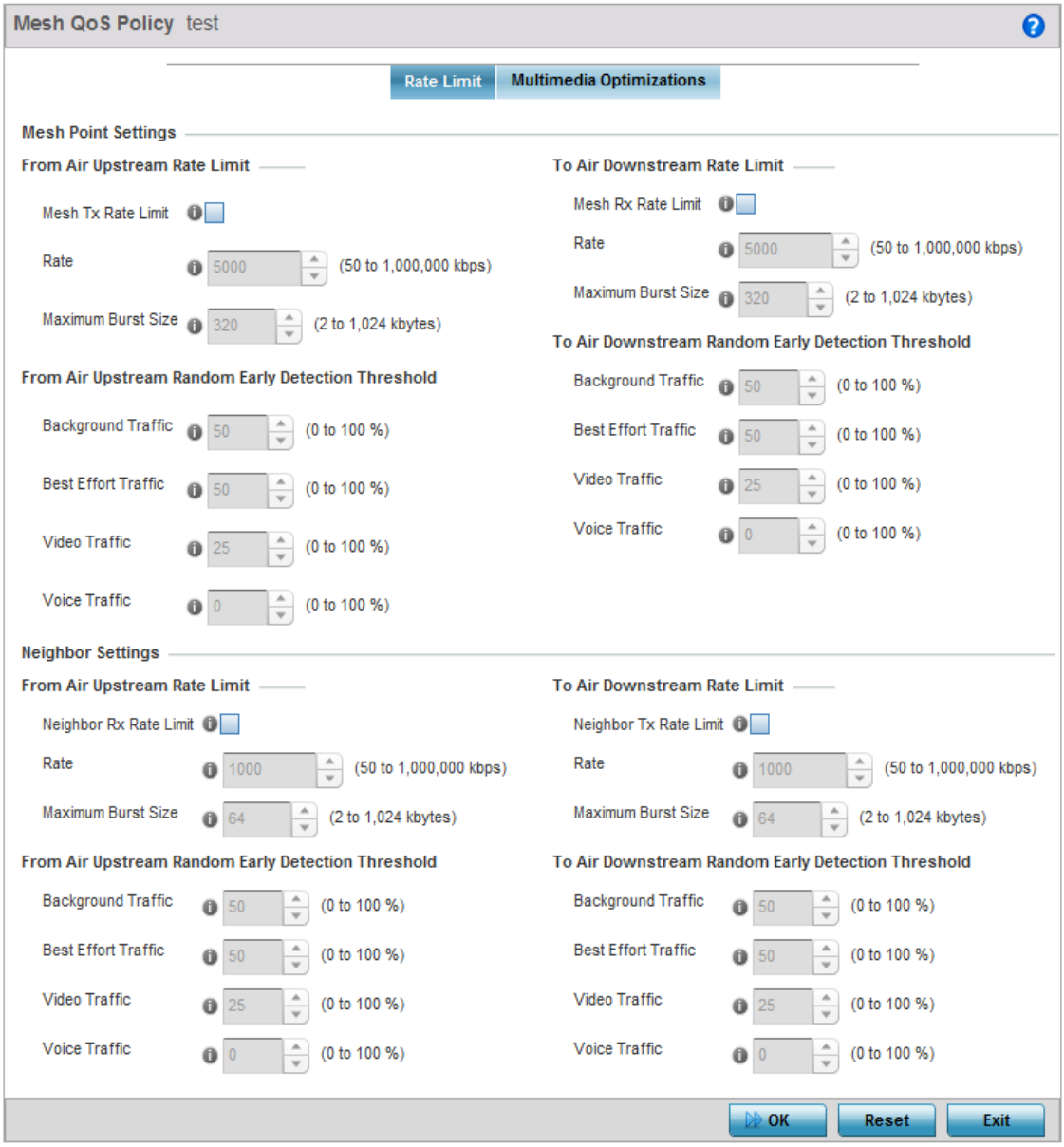


Figure 47: Mesh QoS Policy - Rate Limit screen

6 Configure the following parameters in respect to the intended **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 from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the 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 from 2 - 1024 kbytes. 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 320 kbytes.

7 Set the following **From Air 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 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%.

8 Configure the following parameters in respect to the intended **To Air Downstream Rate Limit,** or traffic from neighbors to associated access point radios and the controller:

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 an transmit rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the 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 from 2 - 1024 kbytes. The smaller the burst, the less likely the receive 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 minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.

9 Set the following **To Air 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 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 receive 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 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 receive 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 receive 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 transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

10 Configure the following parameters in respect to the intended **From Air Upstream Rate Limit** for the **Neighbor Settings** field:

Neighbor Rx Rate Limit	Select this radio button 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 receive direction. This feature is disabled by default.
Rate	Define an transmit rate limit from 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 from 2 - 1024 kbytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

11 Set the following **From Air Upstream Random Early Detection Threshold** settings for each access category:

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 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 transmit 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 transmit 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 receive 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.

12 Configure the following parameters in respect to the intended **To Air Downstream Rate Limit,** or traffic from a controller to associated access point radios and the wireless client:

Neighbor Tx Rate Limit	Select this radio button 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 receive rate limit from 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.
Maximum Burst Size	Set a maximum burst size from 2 - 64 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

13 Set the following **To Air Downstream 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 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 receive 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 receive 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 receive 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.

14 Select **OK** when completed to update this mesh QoS rate limit settings. Select **Reset** to revert the screen back to its last saved configuration.

15 Select the **Multimedia Optimizations** tab.

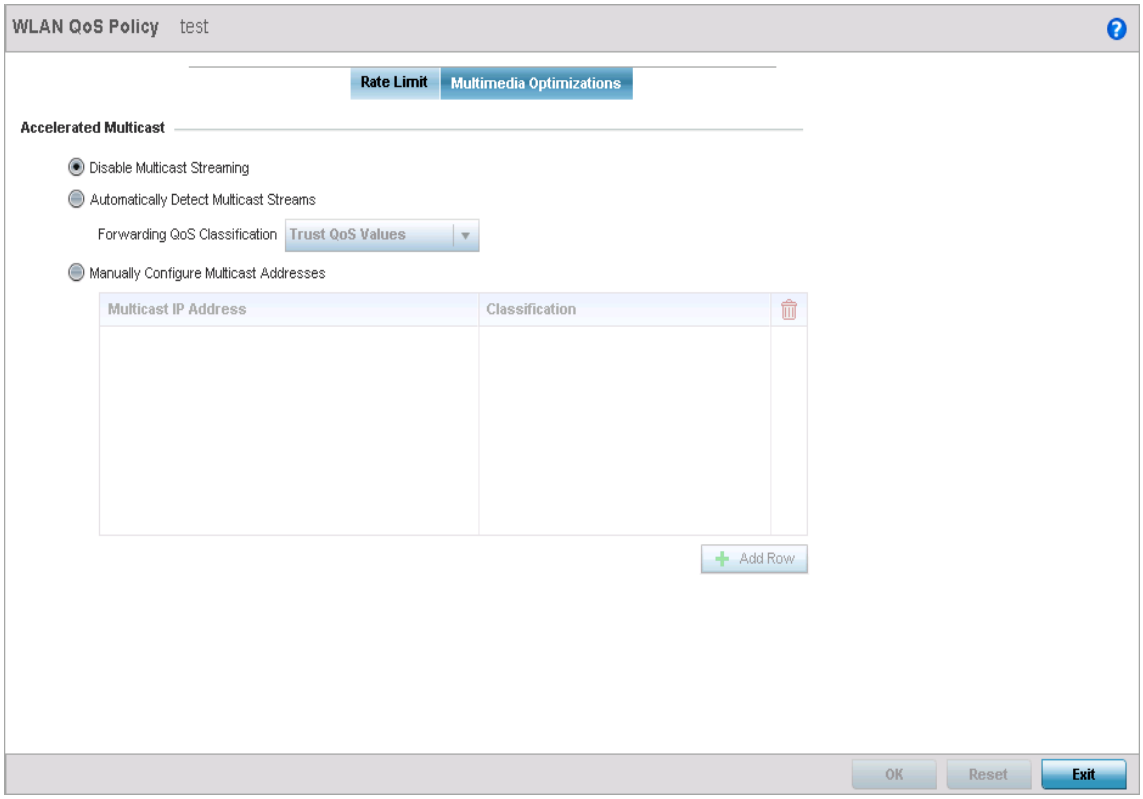


Figure 48: Mesh QoS Policy - Multimedia Optimizations screen

16 Set the following **Accelerated Multicast** settings:

Disable Multicast Streaming	Select this option to disable 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, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they would want. The classification types are *Trust, Voice*, *Video*, *Best Effort*, and *Background*.
Manually Configure Multicast Addresses	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

17 Select **OK** when completed to update the *Mesh Multimedia Optimizations* settings. Select **Reset** to revert to the last saved configuration.

Passpoint Policy

"Wireless Configuration"

A *Passpoint Policy* provides a mechanism by which devices can select the correct network by querying for information from the available networks and then deciding which network to associate with. A Passpoint policy is associated to a WLAN to enable the WLAN to provide hotspot services.

Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

A Passpoint policy contains configuration that enables a client to query a network for information such as WAN metric, domain names and other relevant information. Only relevant information is presented to the client which enables it to decide with network to join.

To define a **Passpoint Policy**:

1 Select **Configuration**.

2 Select **Wireless.**

3 Select **Passpoint Policy** to display existing Passpoint policies.

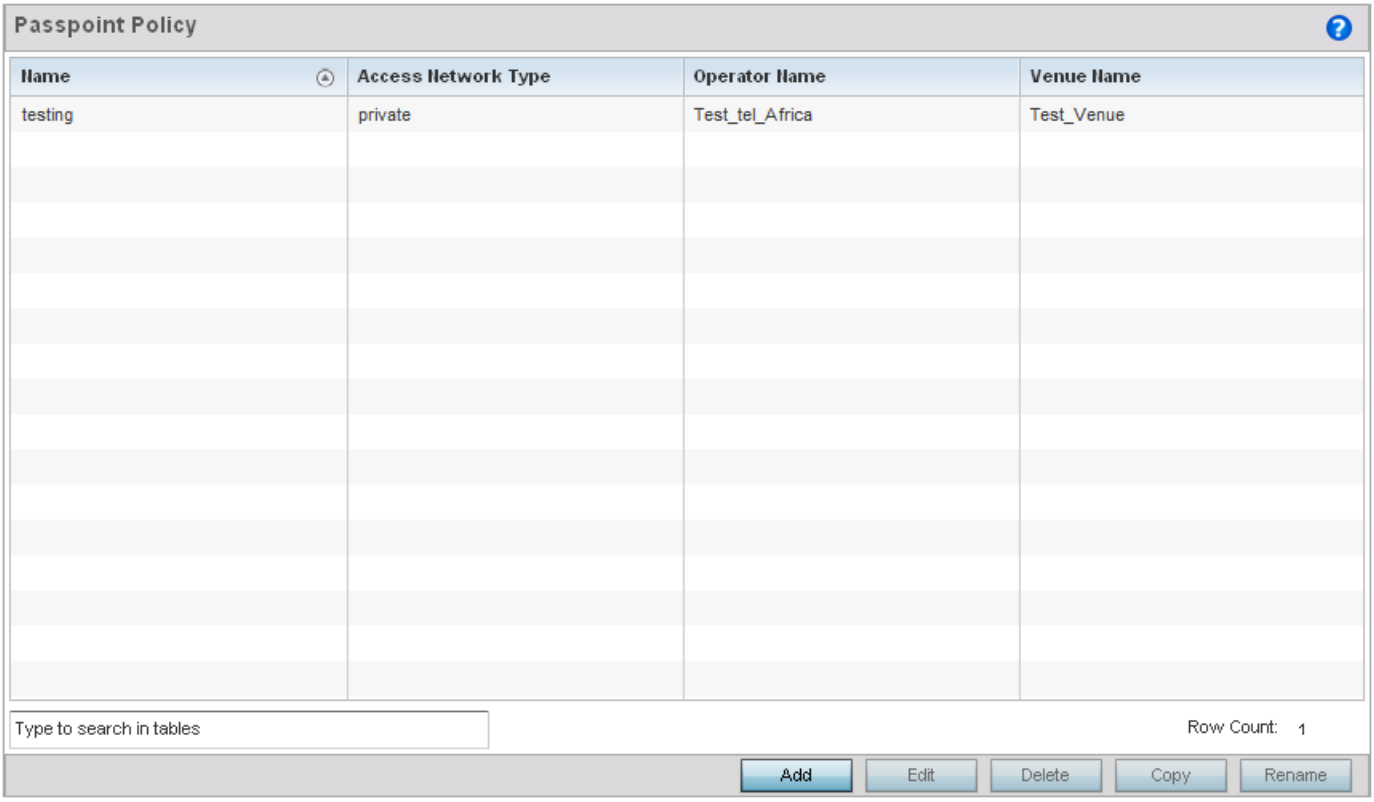


Figure 49: Wireless Passpoint Policy screen

4 Refer to the following configuration data for existing Passpoint policies:

Name	Displays the name of the configured Passpoint policy.
Access Network Type	Displays the *Access Network Type* for this Passpoint policy. Displays the type of hotspot which is advertised to all clients.
Operator Name	Displays the name of the operator running the hotspot.
Venue Name	Displays information about the venue hosting the hotspot.

5 Select the **Add** button to define a new Passpoint policy, or select an existing Passpoint policy and select **Edit** to modify its existing configuration. Existing Passpoint policies can be selected and deleted as needed. The *Configurations* tab displays by default.

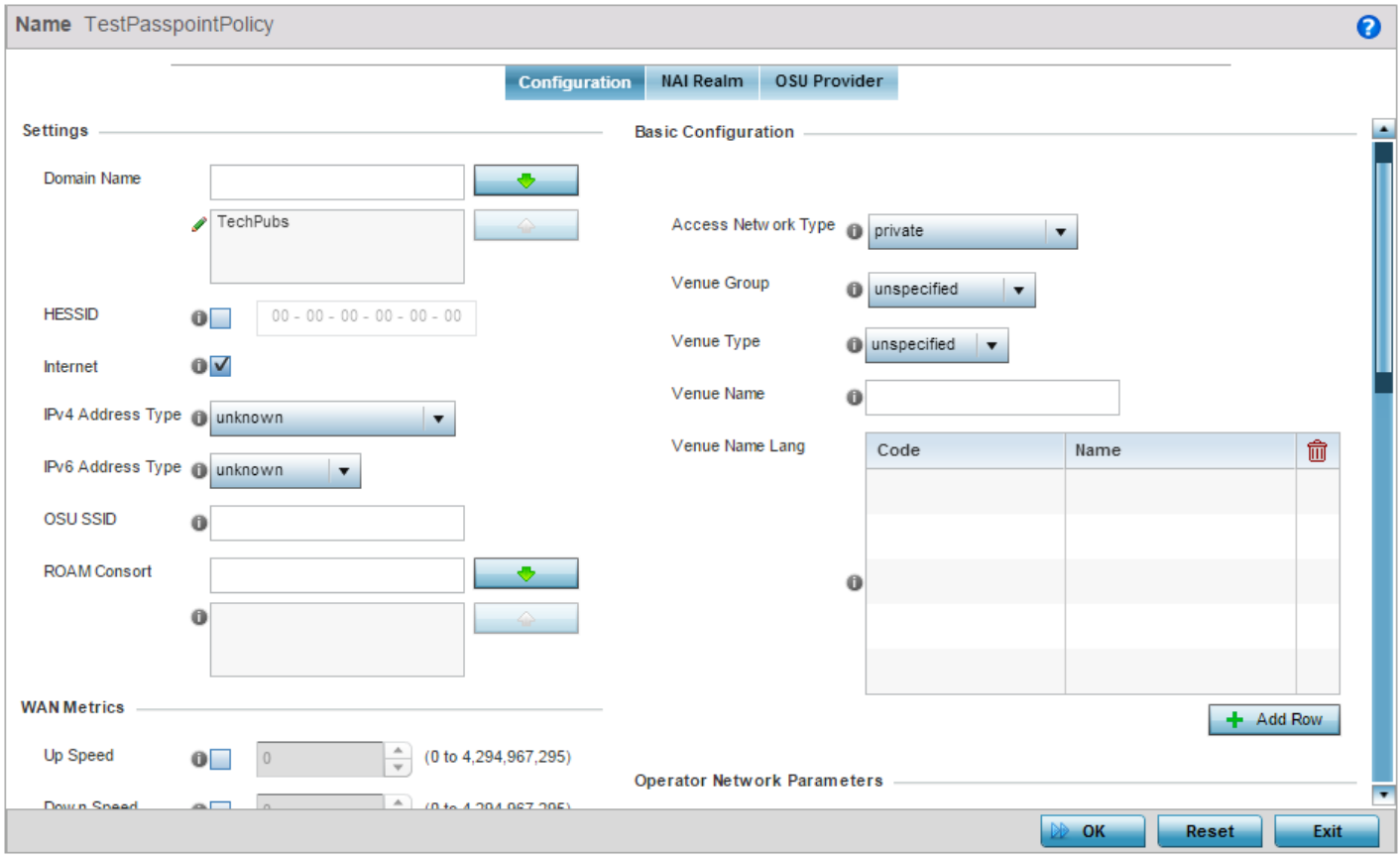


Figure 50: Wireless Passpoint Policy - Configuration screen

6 Refer to 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	Use the drop-down menu to select the IPv4 formatted address type for this passpoint policy. IPv4 is a connection less 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	Use the drop-down menu to select the IPv4 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.

7 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.

8 Set the following **Connection Capability** for 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.

9 Select **+ Add Row** to set a **Connection Capability Variable** to make specific virtual ports **open** or **closed** for Wi-Fi connection attempts, set rules for how the user is to connect with routing preference using this passpoint policy.

10 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.

11 Refer to the **Basic Configuration** field to set the following:

Access Network Type	Use the drop-down menu to 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 Lang	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.

12 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 Lang	Operator names can be listed in multiple languages. Select *+ Add Row* to add operator name languages. Enter the two or three character ISO-14962-1997 encoded string defining 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.

13 Select **OK** when completed to update the passpoint policy settings. Select **Reset** to revert the screen back to the last saved configuration.

14 Select the **NAI Realm** tab.

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.

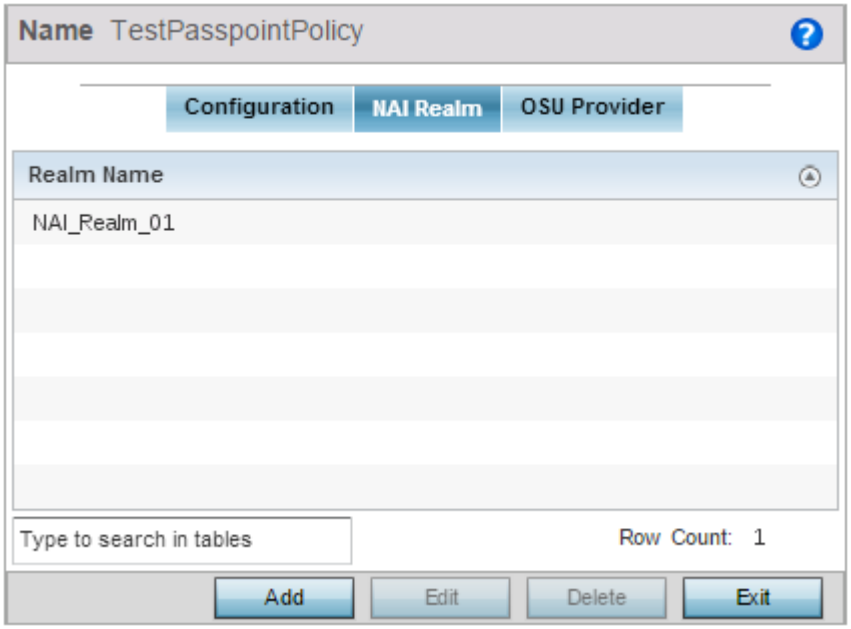


Figure 51: Wireless Passpoint Policy - NAI Realm screen

15 Either select **Add** to create a new NAI realm configuration for passpoint hotspot utilization, **Edit** to modify the attributes on an existing selected configuration or **Delete** to remove a selected configuration from those available. Provide a **Realm Name** or names (32 characters maximum) delimited by a semi colon. Select **+ Add Row** to create a **EAP Method** configuration for the NAI realm.

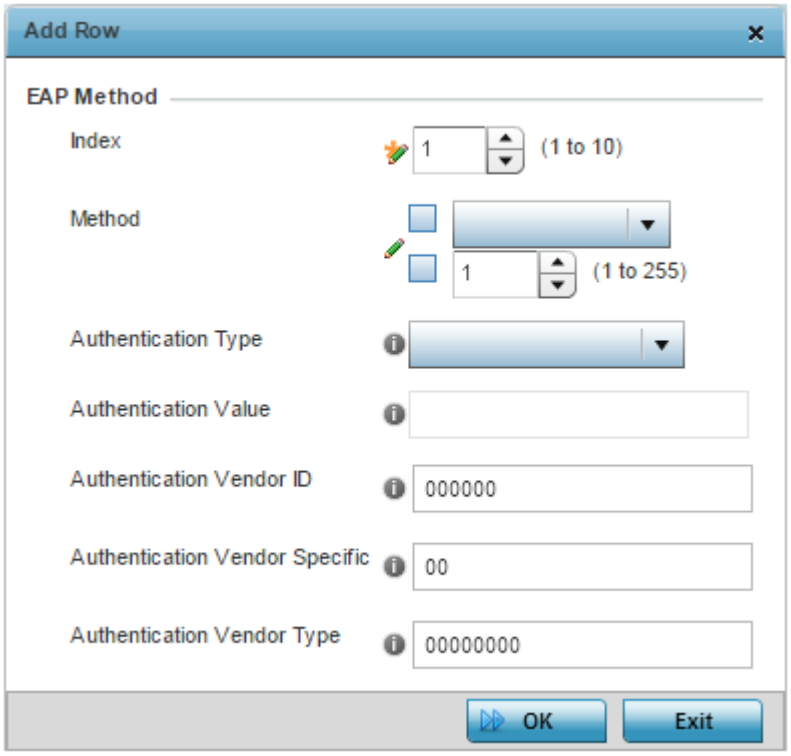


Figure 52: Wireless Passpoint Policy - NAI Realm - Add EAP Method screen

16 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	Use the drop-menu to 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 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 6 character authentication vendor ID that must match the one 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 is an a-FA -F0-9 format.
Authentication Vendor Type	Set an eight (8) character authentication vendor type used exclusively for the *expanded-eap* or *expanded-inner-eap* authentication types.

17 Select **OK** to save the updates to the NAI realm.

18 Select the **OSU Provider** tab.

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 four 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.

19 The OSU Provider screen displays those provider configurations created thus far for utilization with a passpoint policy.

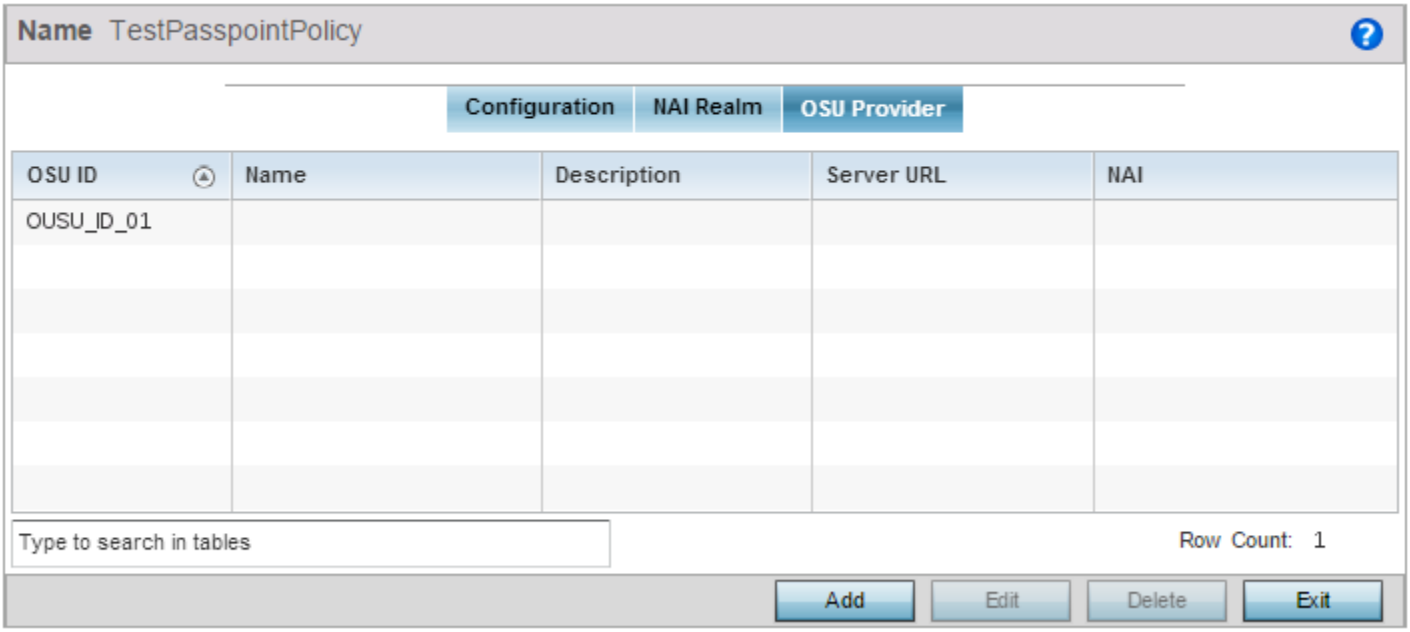


Figure 53: Wireless Passpoint Policy - OSU Provider screen

20 Either select **Add** to create a new OSU provider configuration for passpoint hotspot utilization, **Edit** to modify the attributes on an existing selected configuration or **Delete** to remove a selected configuration from those available.

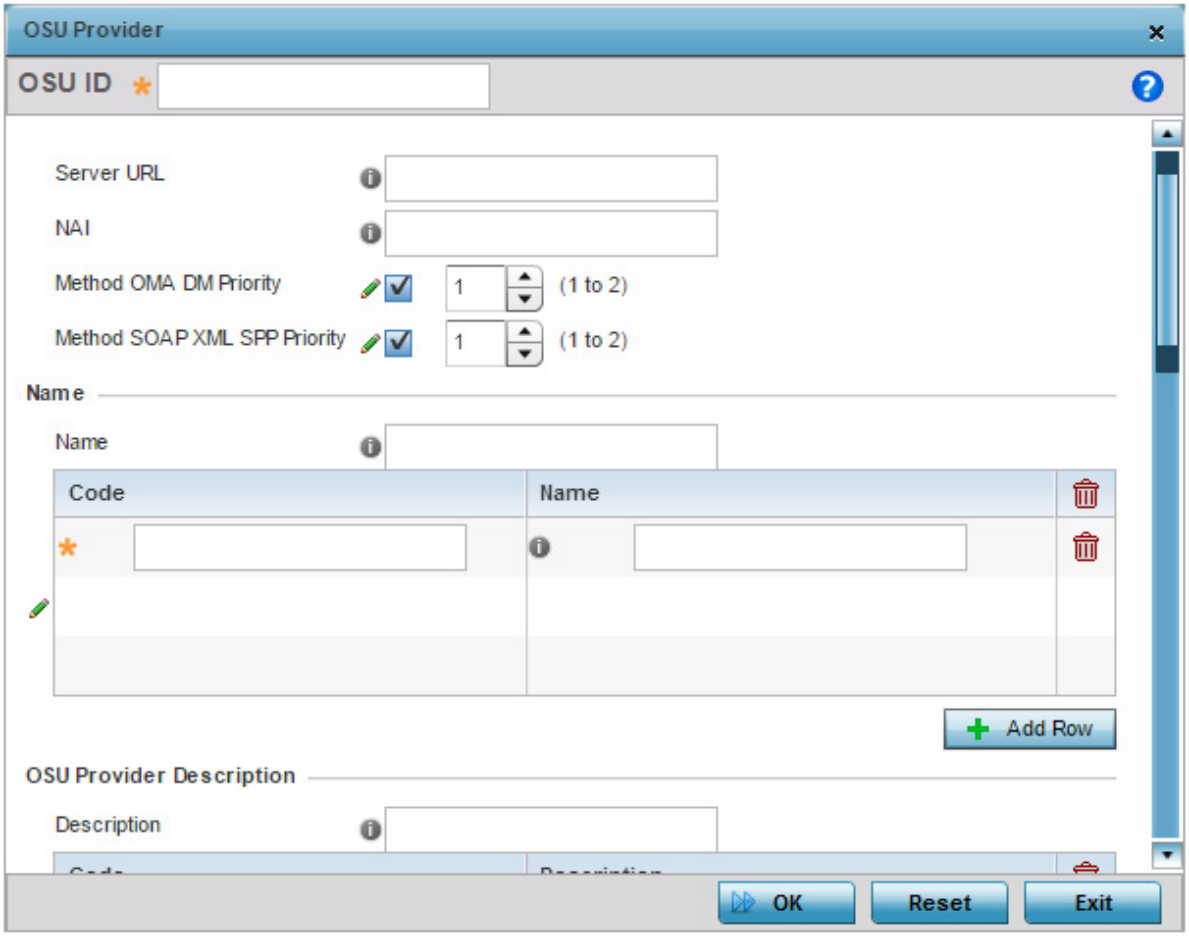


Figure 54: Wireless Passpoint Policy - OSU Provider - Add/Edit screen

21 If creating a new OSU provider configuration, provide it a 32 character maximum **OSU ID** serving as an online sign up identifier.

22 Set the following attributes to secure the NAI realm used by the passpoint policy:

Server URL	Provide a 255 character maximum sign up server URL for the OSU provider.
NAI	Enter a 255 character maximum *Network Access Identifier* (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. The 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.

23 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.

24 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.

25 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 to the icon file.
Height	Provide the icon height size in pixels from 0 - 65,535. The default setting is 0.
MIME Type	Set the icon 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 width size in pixels from 0 - 65,535. The default setting is 0.

26 Select **OK** to save the updates to the OSU provider configuration. Select **Reset** to revert to the last saved configuration.

Sensor Policy

"Wireless Configuration"

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

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

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

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

To define a sensor policy for use with a RF Domain:

1 Select **Configuration**.

2 Select **Wireless.**

3 Select **Sensor Policy** to display existing Sensor policies.

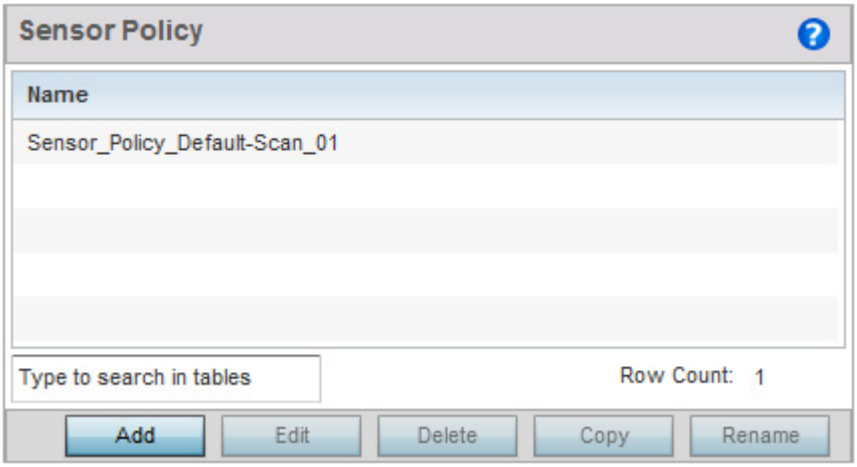


Figure 55: Wireless Sensor Policy screen

4 Refer to the following configuration data for existing Sensor policies:

Name	Displays the name of the configured Sensor policy.

5 Select the **Add** button to define a new Sensor policy, or select an existing Sensor policy and select **Edit** to modify its existing configuration.

When adding a new Sensor policy, the following screen displays:

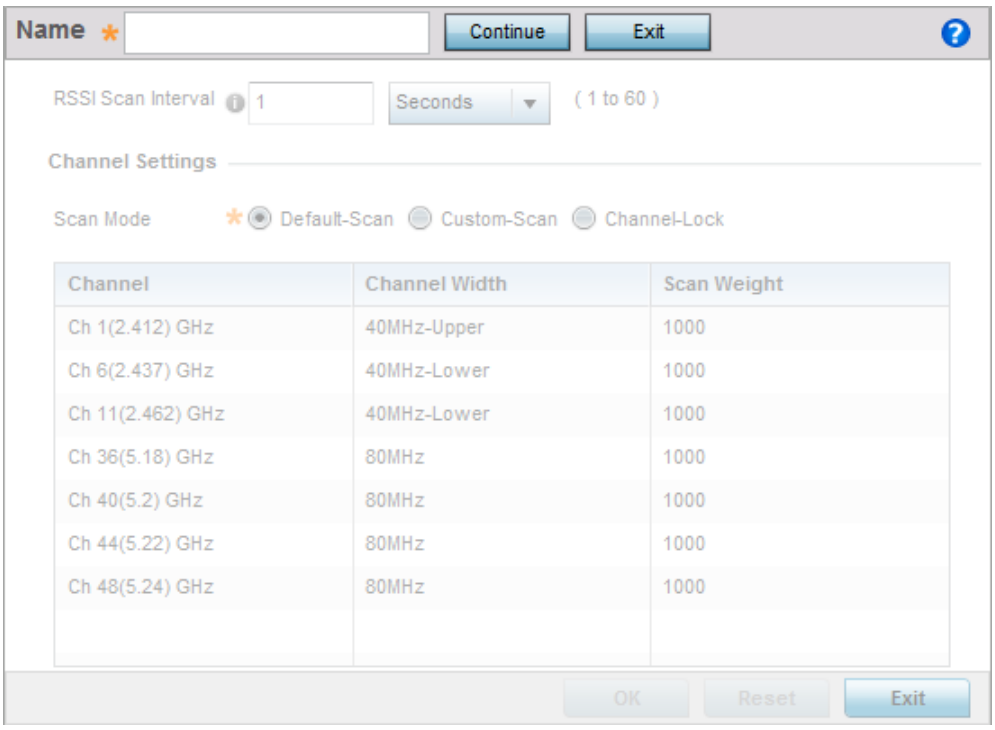


Figure 56: Wireless - Sensor Policy - Add New Sensor Policy screen

6 Provide a name for this sensor policy in the **Name** field. Sensor policy name cannot exceed 32 characters and cannot contain space. Select **Continue** to create the Sensor policy. Select **Exit** to exit this screen without creating a new sensor policy. The Sensor Policy addition screen displays with the **Scan Mode** set to *Default-Scan*. The user configurable parameters on this screen differ with the selected **Scan Mode**.

7 Use the **RSSI Scan Interval** drop-down menu to set a scan interval from 1 - 60 seconds. This is the scan period dedicated sensors (access point radios) utilize for RSSI (signal strength) assessments. Once obtained, the sensor sends the RSSI data to a specified MPact server resource (not an ADSP server) for the calculation of Wi-Fi device locations. The default is 1 second.

8 Set the following **Scan Mode** configuration.

1 **Default-Scan** – This is the default configuration. None of the fields are user configurable.

Channel	The list of available scan channels is fixed and defaults in a spread pattern of 1, 6, 11, 36, 40, 44 and 48. These channel cannot be changed.
Channel Width	Each channel's width is fixed and defaults to either 40MHz-Upper (Ch 1), 40MHz-Lower (Ch 6 and CH 11) or 80MHz (CH 36, CH 40, CH 44 and CH 48).
Scan Weight	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.

2 **Custom-Scan** – This scan mode enables configuration and selection of individual channels for scanning. Set the following parameters for the channels of interest:

Channel	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.
Channel Width	When custom channels are selected for RSSI scans, each selected channel can have its own width defined. Numerous channels have their width fixed at 20MHz, 802.11a radios support 20 and 40 MHz channel widths.
Scan Weight	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.

3 **Channel-Lock** – This scan mode locks the RSSI scan to a single selected channel. Use the drop-down to select the channel of interest.

4 Select **OK** to save the changes to the sensor policy configuration, or select Reset to revert to the last saved configuration.

5 To create a copy of a Sensor Policy, select the policy, then use the **Copy** button.

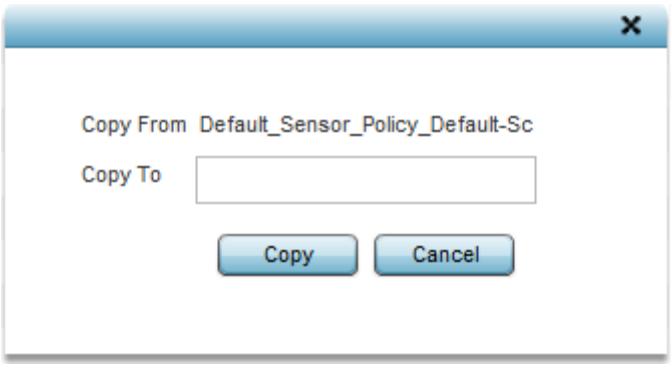


Figure 57: Wireless - Sensor Policy - Copy Policy screen

Use the **Copy To** field to provide a name for the Sensor Policy to be created by copy. The name of the new Sensor Policy cannot be longer than 32 characters and cannot contain spaces.

6 To rename an existing Sensor Policy, select the policy, then use the **Rename** button.

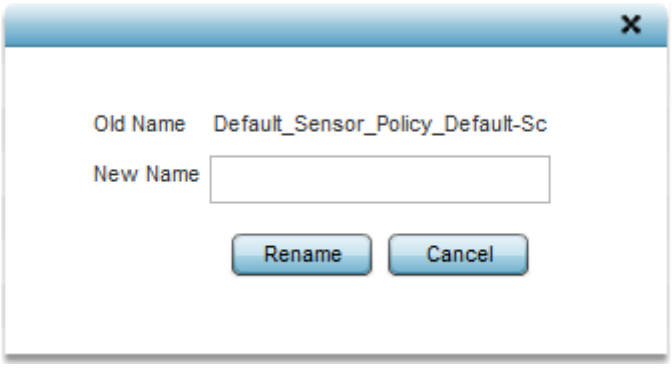


Figure 58: Wireless - Sensor Policy - Copy Policy screen

Use the **New Name** field to provide a new name for the Sensor Policy. The name of the Sensor Policy cannot be longer than 32 characters and cannot contain spaces.

7 To delete a Sensor Policy, select it, then select the **Delete** button. This removes the policy from the list of Sensor Policies.

7 Network Configuration

The access point allows packet routing customizations and additional route resources.

For more information on the network configuration options available to the access point, refer to the following:

- "Policy Based Routing (PBR)"
- "L2TP V3 Configuration"
- "Crypto CMP Policy"
- "AAA Policy"
- "AAA TACACS Policy"
- "Alias"
- "URL Filtering"
- "Web Filtering"
- "IPv6 Router Advertisement Policy"
- "Application Policy"
- "Application"
- "Schedule Policy"

For configuration caveats specific to **Configuration** > **Network** path, refer to "Network Deployment Considerations" on page 708.

Policy Based Routing (PBR)

"Network Configuration"

Define a *policy based routing* (PBR) configuration to direct packets to selective paths. PBR can optionally mark traffic for preferential services or *Quality of Service* (QoS). 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. Route-maps 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 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). 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 is 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:
  a If a defined next hop is reachable, it is used. If fallback is configured refer to (b).
  b Do normal destination based route lookup. If a next hop is found it is used, if not refer to (c)
  c If default next hop is configured and reachable, it is 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** tab from the Web UI.

2 Select **Network**.

3 Select **Policy Based Routing.**

The *Policy Based Routing* screen displays by default.

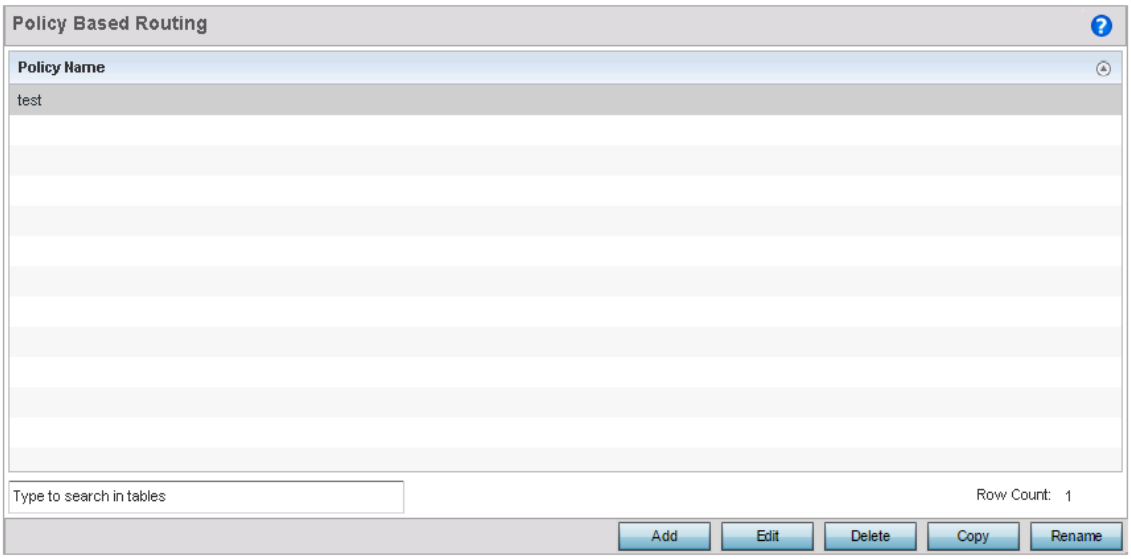


Figure 1: Policy Based Routing screen

4 Either 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.

5 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.

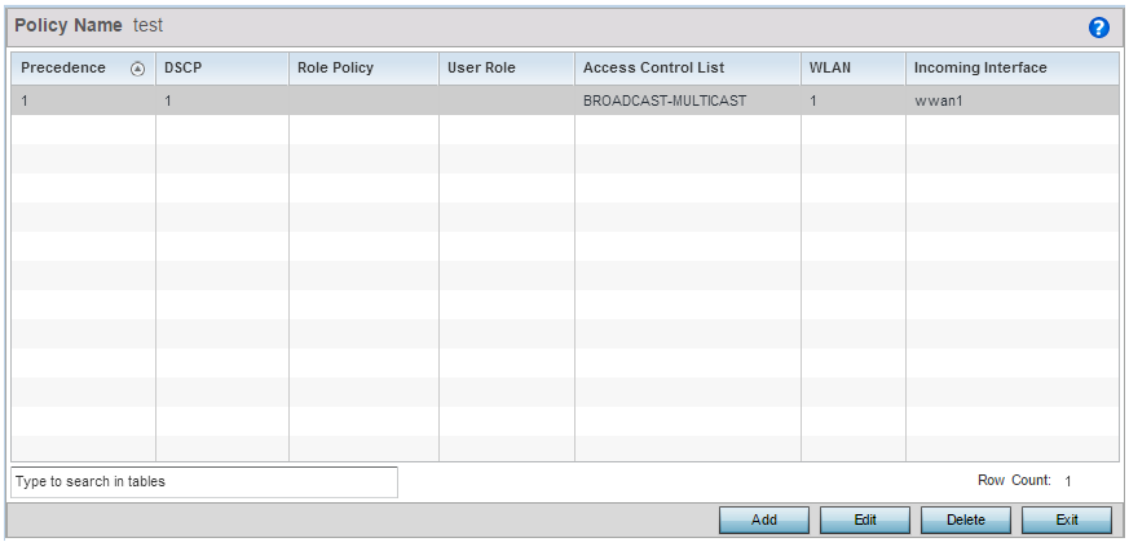


Figure 2: Policy Based Routing screen - Route Maps tab

6 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 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).
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.

7 Select **Add** or **Edit** to create or modify a route-map configuration. Use the **Delete** button to delete an existing route-map configuration. Select **Exit** button to exit this screen.

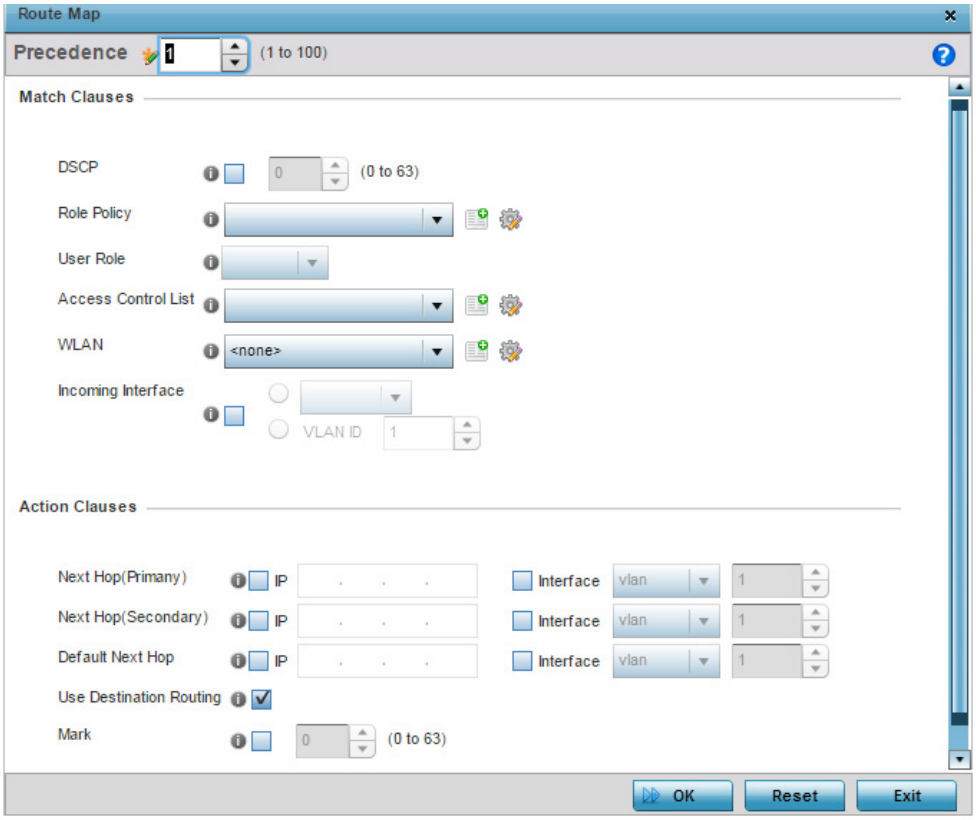


Figure 3: Policy Based Routing screen - Add a Route Map

8 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).

9 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.

10 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, it is 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.

11 Select **OK** to save the updates to the route-map configuration. Select **Reset** to revert to the last saved configuration.

L2TP V3 Configuration

"Network 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 devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WING supported 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 packet-switching network (PSN). 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 pseudowire 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**.

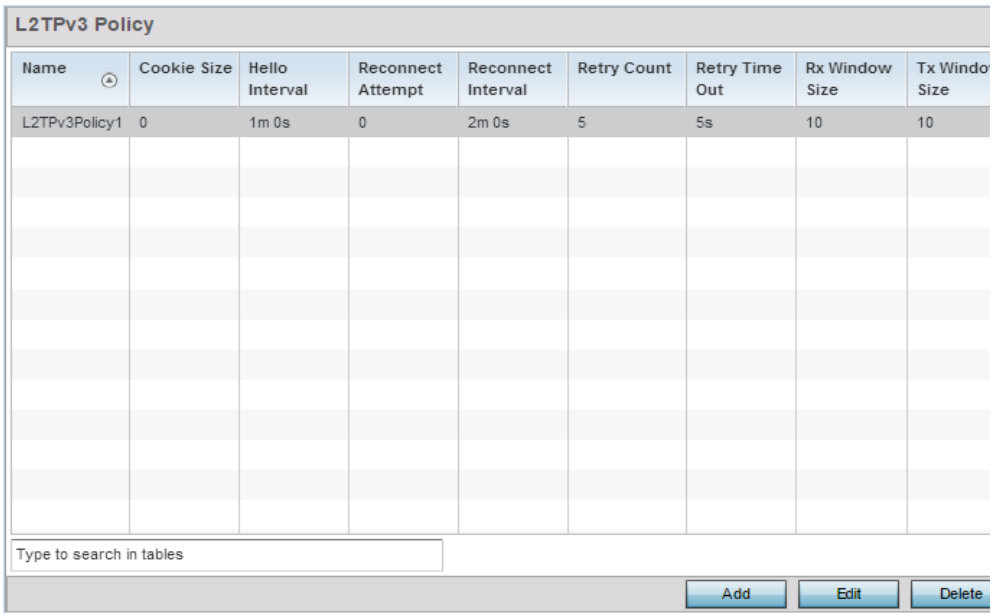


Figure 4: L2TP V3 Policy screen

The *L2TP V3* screen lists the policy configurations defined thus far.

2 Refer to the following to determine whether a new L2TP V3 policy 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, 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 control connection.
Reconnect Attempt	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 re-connection 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	Displays the time to wait before tunnel re-establishment.
Force L2 Path Recovery	Indicates if L2 Path Recovery is enabled to learn servers, gateways and other network devices behind a 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.

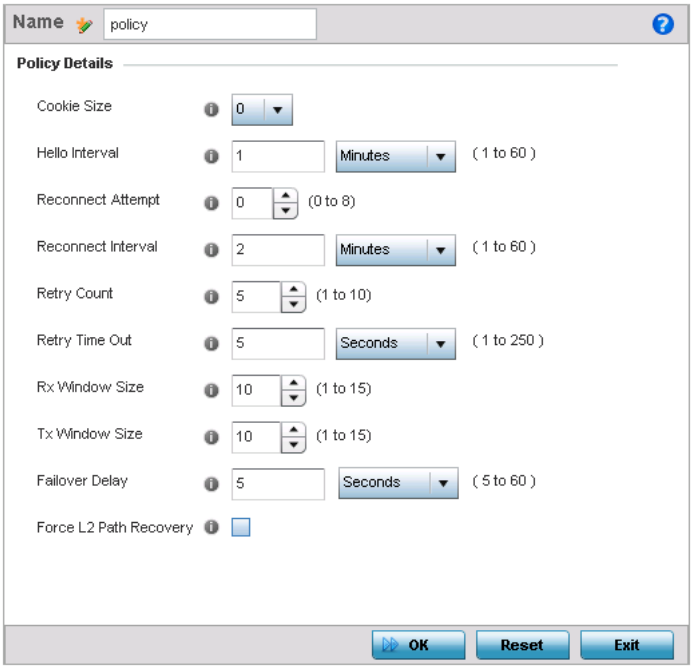


Figure 5: L2TP V3 Policy Creation screen

4 If creating a new L2TP V3 policy, assign it a **Name** up to 31 characters in length. 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, cookie size cannot be configured per session, and are the same size for all sessions with in a tunnel.
Hello Interval	Define an interval in either *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 Attempt	Use the spinner control to set a value (from 0 - 250) representing the maximum number of re-connection attempts initiated 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 re-connection 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 define the interval (in seconds) before initiating a retransmission of a L2TP V3 signaling message. The available range is from 1 - 250, with a default value of 5.
Rx Window Size	Specify the number of packets that can be received without sending an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
Tx Window Size	Specify the number of packets that can be transmitted without receiving an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
Failover Delay	Specify the wait time (in seconds) before re-establishing a failed tunnel. The available duration is 5 - 60 seconds or 1 minute with a default setting of 5 seconds.
Force L2 Path Recovery	Select to enable forcing the discovery of servers, gateways and other networks behind a L2TPV3 tunnel when a tunnel is being established or when a failed tunnel is being reestablished.

6 Select **OK** to save the updates to the L2TP V3 Policy Details. Select **Reset** to revert to the last saved configuration.

Crypto CMP Policy

"Network Configuration"

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.

To review, create or edit a Crypto CMP policy:

1 Select the **Configuration** tab from the Web UI.

2 Select **Network.**

3 Select **Crypto CMP Policy**.

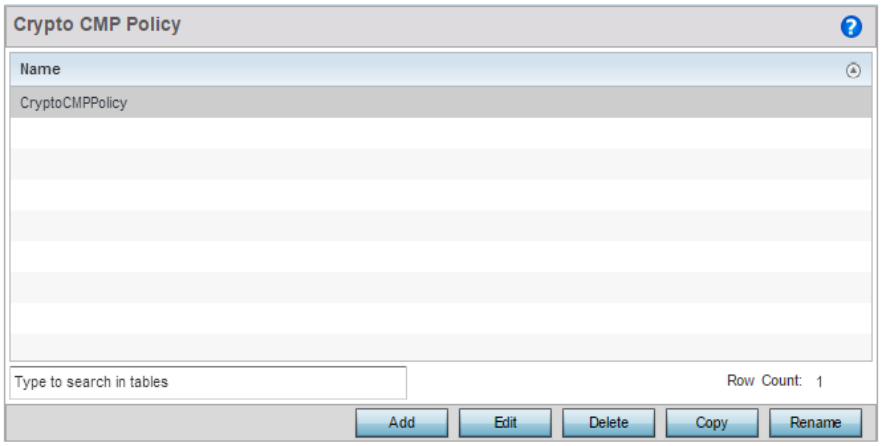


Figure 6: Crypto CMP Policy screen

The **Crypto CMP Policy** screen lists the policy configurations defined thus far.

4 Select **Add** to create a new Crypto CMP policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

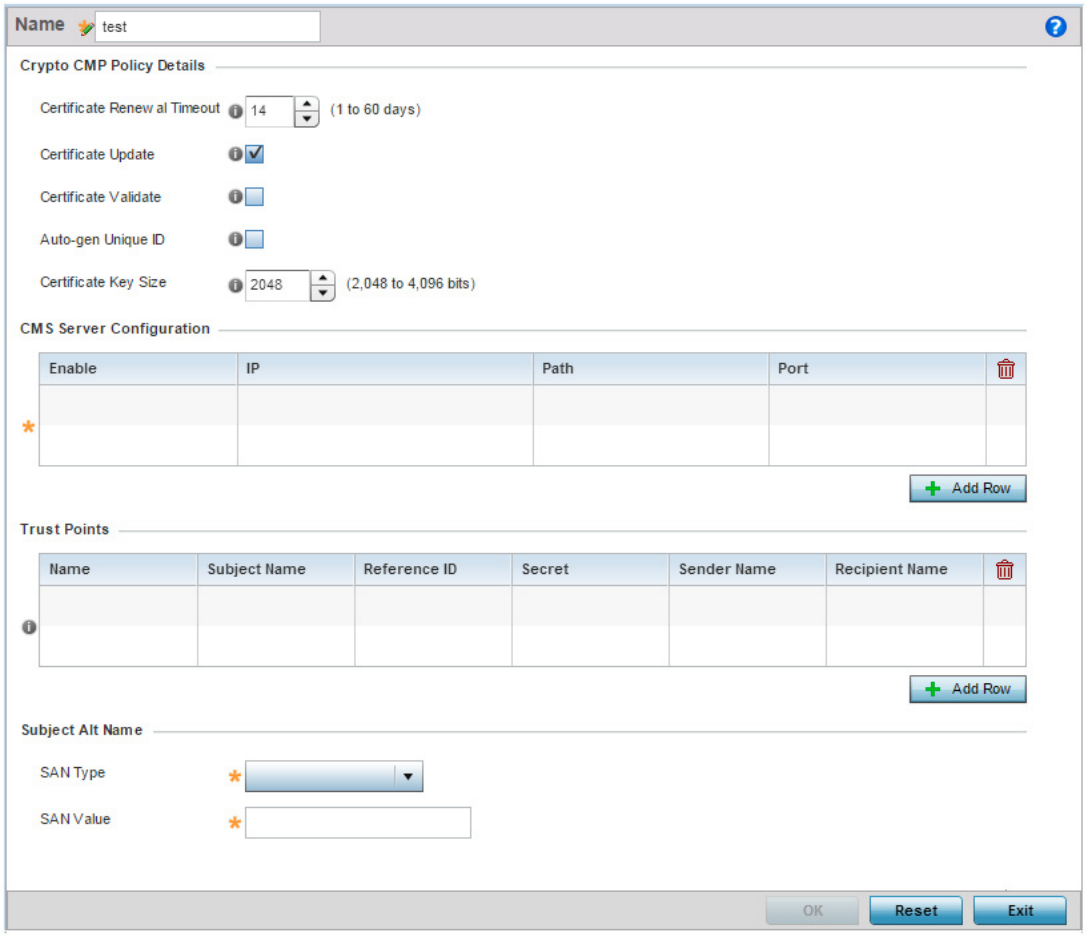


Figure 7: Crypto CMP Policy Creation screen

5 If creating a new Crypto CMP policy assign it a **Name** up to 31 characters to help distinguish it.

6 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.

7 Select **Certificate Update** to automatically trigger a certificate update request when a certificate expires.

8 Select **Certificate Validate** to automatically validate the cross certificate with the factory certificate.

9 Select **Auto-gen Unique ID** to prepend the device's auto-generated unique ID in the subject and sender fields.

10 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.

11 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.

12 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.

13 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.

14 Select **OK** to save the updates to the CMP Crypto policy, **Reset** to revert to the last saved configuration, or **Exit** to close the screen.

AAA Policy

"Network Configuration"

Authentication, Authorization, and Accounting (AAA) is the mechanism network administrators use to define access control within the access point managed network.

The access point can optionally use an external RADIUS and LDAP Servers (AAA Servers) to provide user database information and user authentication data. Each WLAN managed by the access point can maintain its own unique AAA configuration. AP6522, AP6522M,

AP6532, AP6562, AP8132, AP8232 and AP71XX model access points have an onboard RADIUS server resource, while AP6521 model does not.

AAA provides a modular way of performing 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 access point managed network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various access point 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 on the access point 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 is applied equally to all interfaces on the access point.
- *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 an 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 for the access point, it is applied equally to all interfaces on the access point's access servers.

To define unique WLAN AAA configurations:

1 Select the **Configuration** tab from the Web UI.

2 Select **Network.**

3 Select **AAA Policy** to display a high level display of existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA)** screen lists existing AAA policies. Any of these policies can be selected and applied to the access point.

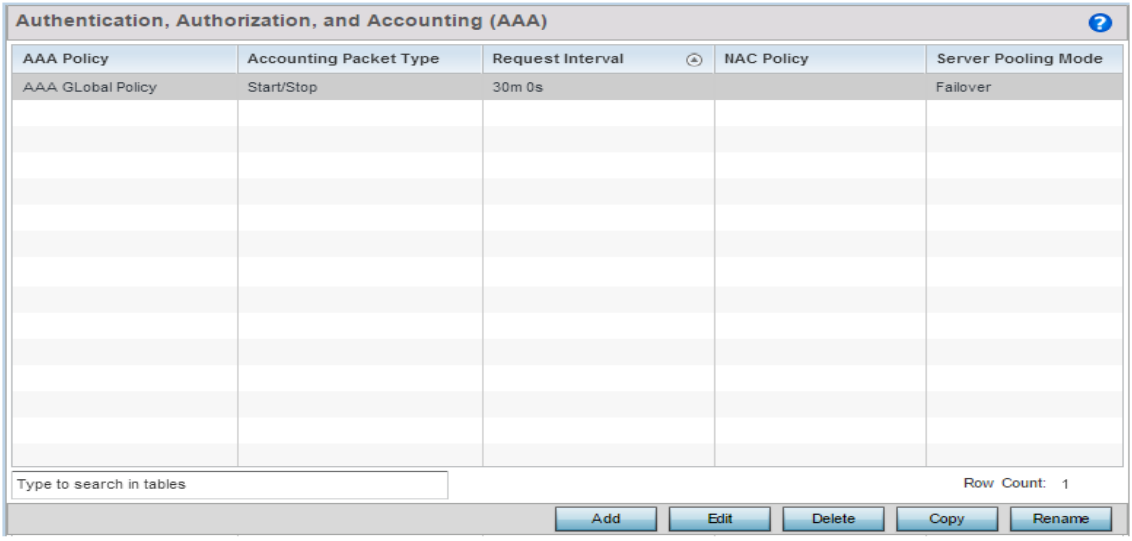


Figure 8: Authentication, Authorization, and Accounting (AAA) screen

4 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 the interval at which an access point sends a RADIUS accounting request to the RADIUS server.
NAC Policy	Lists the *Network Access Control* (NAC) filter used to either include or exclude clients from entering the access point managed network.
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.

5 To configure a new AAA policy, select the **Add** button. Select a policy and use the **Edit** button to edit the AAA policy or use the **Delete** button to remove the policy. Existing policies can be copied or renamed as needed.

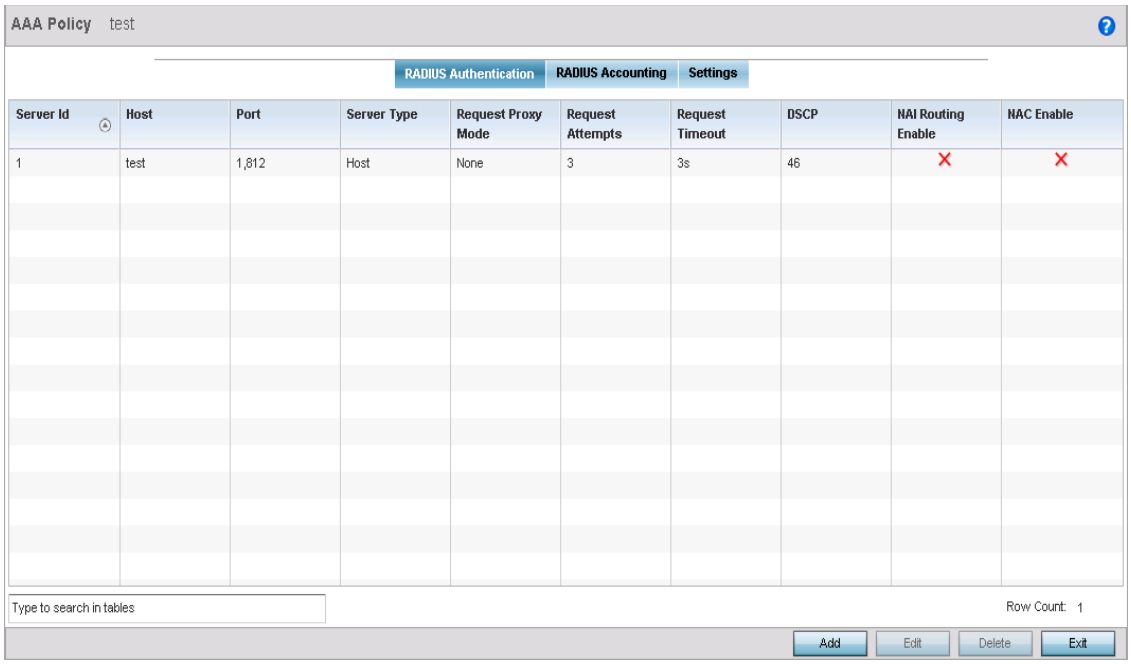


Figure 9: AAA Policy - RADIUS Authentication tab

6 Refer to the following configured **RADIUS Authentication** details:

Server Id	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
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.
Server Type	Displays the type of AAA server in use as either *Host*, *onboard-self* or *onboard-controller*.
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 access point's 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 value 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. 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.
NAC Enable	A green check mark defines NAC as enabled, while a red X defines NAC disabled with this AAA policy.

7 Select a server ID from the table and select **Edit,** or select **Add** to create a new policy. To delete a server ID use the **Delete** button.

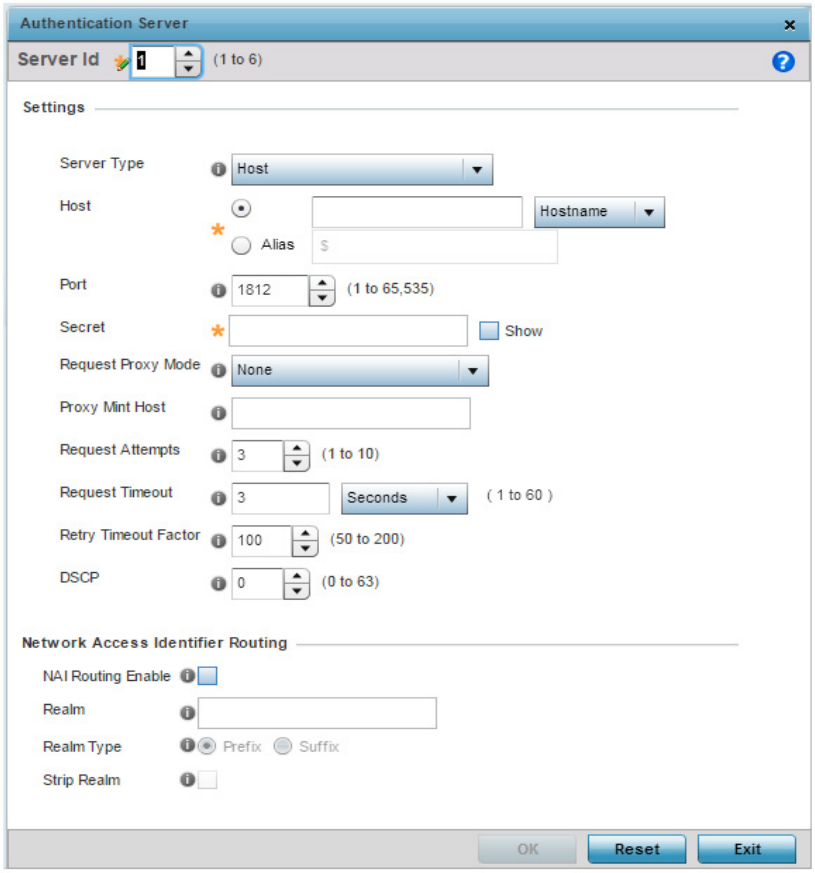


Figure 10: AAA Policy - RADIUS Authentication tab - Authentication Server screen

8 Define the following settings to add or modify AAA RADIUS authentication server configuration:

Server Id	Define the numerical server index (1-6) for the authentication server to differentiate it from others available to the access point's AAA policy.
Server Type	Select the type of AAA server as either *Host*, *onboard-self* or *onboard-controller*. AP6521 model does not have an onboard authentication resource and must use an external server or Virtual Controller AP resource.
Host	Specify the IP address or hostname of the RADIUS authentication server. Hostnames cannot include an underscore character. Select Alias to define the hostname alias once and use the alias character set across different configuration items.
Port	Define or edit the port on which the RADIUS server listens to traffic within then access point managed network. The port range is 1 to 65,535. The default port is 1812.
Secret	Specify the secret used for authentication on the selected RADIUS server. By default the secret will be displayed as asterisks.
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 M*int Host.

Proxy Mint Host	Specify the hostname (if the device is a Level-1 MiNT neighbor) or the Mint-ID of the Mint device to proxy hosts through.
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.
Retry 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 from 0 - 63, with a default value of 46.

9 Set the following **Network Address Identifier (NAI) Routing** settings:

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.

10 Select **Ok** to save the changes made to this window. Click **Exit** to close this window.

11 Select the **RADIUS Accounting** tab.

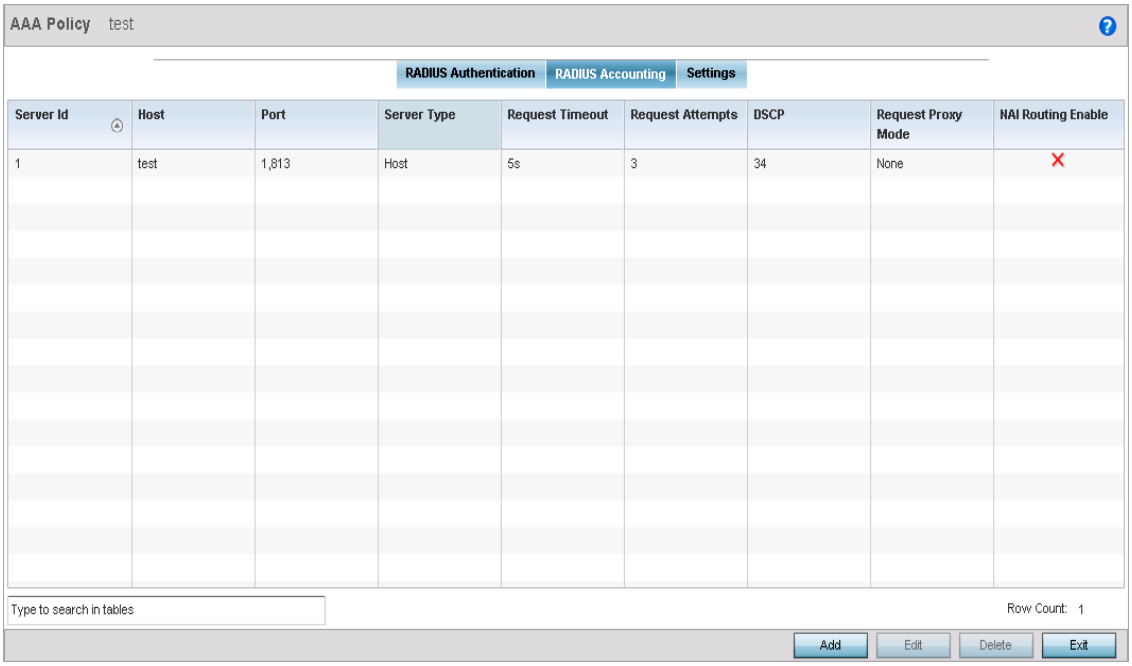


Figure 11: AAA Policy - RADIUS Accounting tab

12 Refer to the following configured RADIUS Accounting profile details:

Server ID	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
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 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 from 1 - 10. The default is 3.

Request Timeout	Displays the time from 1 - 60 seconds 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.
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.
Request Proxy Mode	Lists 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 the 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. 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.
NAC Enable	A green check defines NAC as enabled, while a Red X defines NAC disabled with this AAA policy.

13 To edit an existing accounting profile, select the profile then select the **Edit** button. To add a new policy, select the **Add** button.

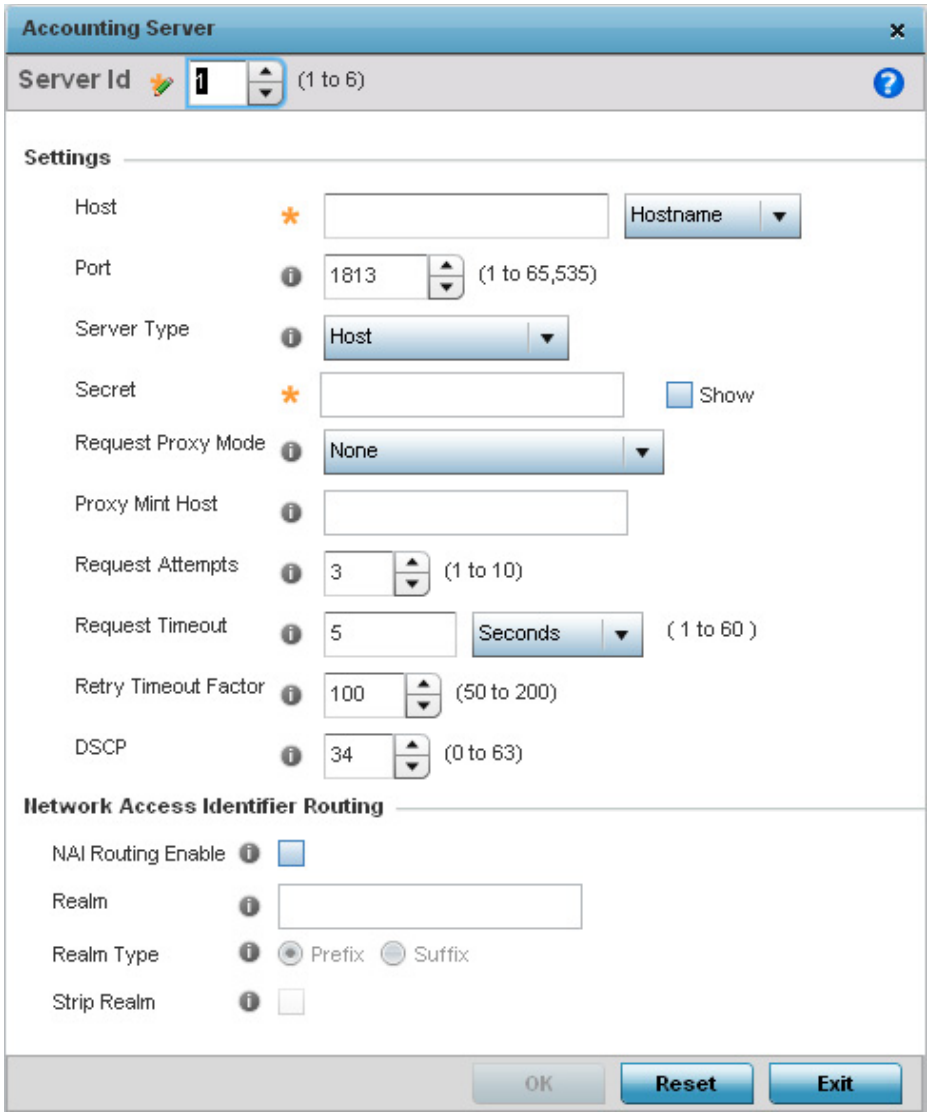


Figure 12: AAA Policy - RADIUS Accounting tab - Accounting Server screen

14 Define the following settings to add or modify AAA RADIUS accounting server configuration:

Server Id	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
Host	Specify the IP address or hostname of the RADIUS authentication server.
Port	Define or edit 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 1813.
Server Type	Select the type of AAA server as either *Host*, *onboard-self* or onboard-*controller*.
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* or *Through RF Domain Manager*.
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 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 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.
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. 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.
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 the realm as either *Prefix* or *Suffix*.
Strip Realm	Select this option to remove information from the packet when NAI routing is enabled.

15 Select **Ok** to save the changes made to this window. Click **Exit** to close this window.

16 Select the **Settings** tab.

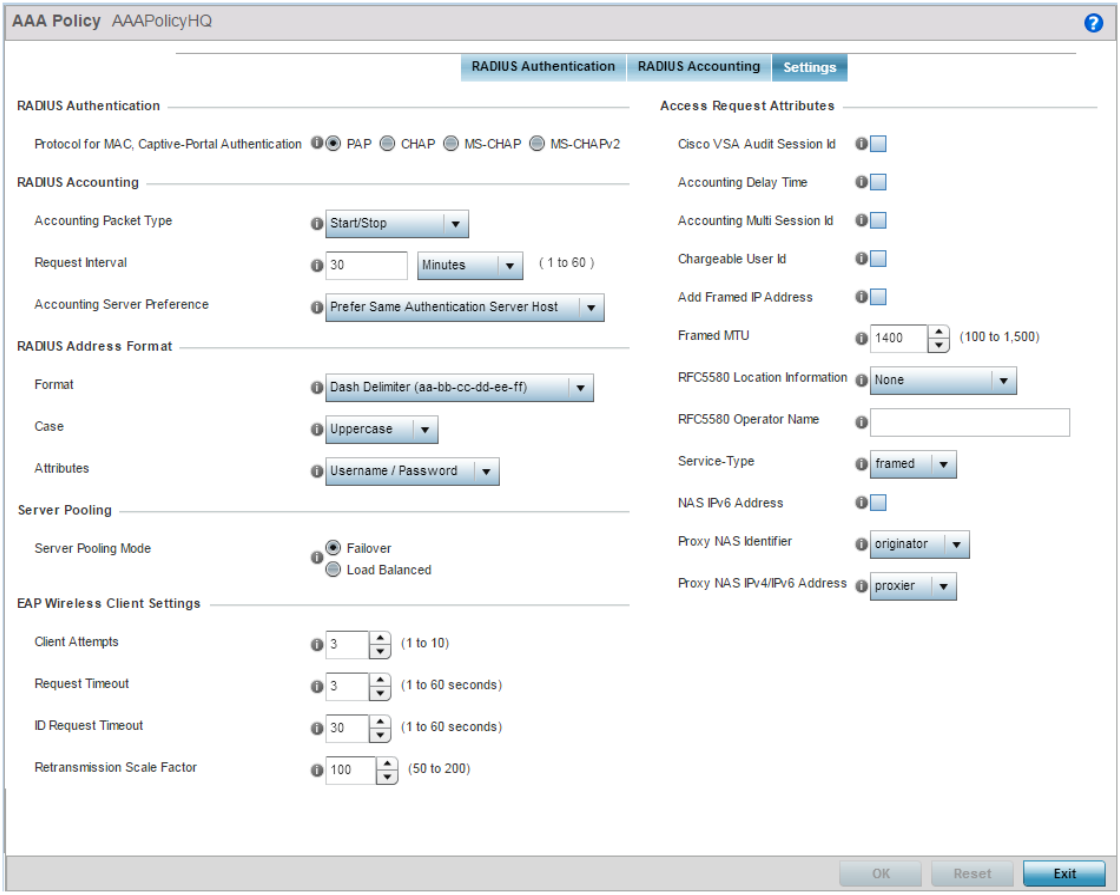


Figure 13: AAA-Policy - Settings screen

17 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 *Password Authentication Protocol* (PAP), *Challenge Handshake Authentication Protocol* (CHAP), *MSPAP* and *MSCHAP-V2*. 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. The default is 30 minutes.
Accounting Server Preference	Select the server preference for RADIUS Accounting. The options are: • *Prefer Same Authentication Server Host* - Uses the authentication server hostname 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 calling-station-id or called-station-id.
Server Pooling Mode	Controls how requests are transmitted across RADIUS servers. *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 wireless client before giving up. The default setting is 3.
Request Timeout	Defines the time after which an EAP Request to a wireless client is retried.
ID Request Timeout	Defines the time (1 - 60 seconds) after which an EAP ID Request to a wireless client is retried. The default setting is 30 seconds.
Retransmission Scale Factor	Configures 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 indicate more conservative (longer) timeouts on each successive attempt.
Cisco VSA Audit Session Id	Configures a *vendor specific attribute* (VSA) for CISCO to allow CISCO's *Identity Services Engine* (ISE) to validate the compliance of a client to the network's policies such as the validity of the virus definition files for the antivirus software or the definition files for a anti-spy ware software.
Accounting Delay Time	Select this option to enable the support of an accounting delay time attribute within accounting requests. This setting is disabled by default.
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 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).
Proxy NAS IPv6 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).

18 Select **OK** to save the updates. Select **Reset** to revert to last saved configuration.

AAA TACACS Policy

"Network Configuration"

Terminal Access Controller Access - Control System+ (TACACS+) is a protocol created by CISCO Systems which provides access control to network devices such as routers, network access servers and other networked computing devices through 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 resources.*



NOTE

For the rest of this section, the term TACACS will be used instead of TACACS+.

To define unique AAA TACACS configurations:

1 Select the **Configuration** tab from the Web UI.

2 Select **Network.**

3 Select **AAA TACACS Policy** to display a high level display of existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA) TACACS** screen lists existing AAA policies. Any of these policies can be selected and applied to the access point.

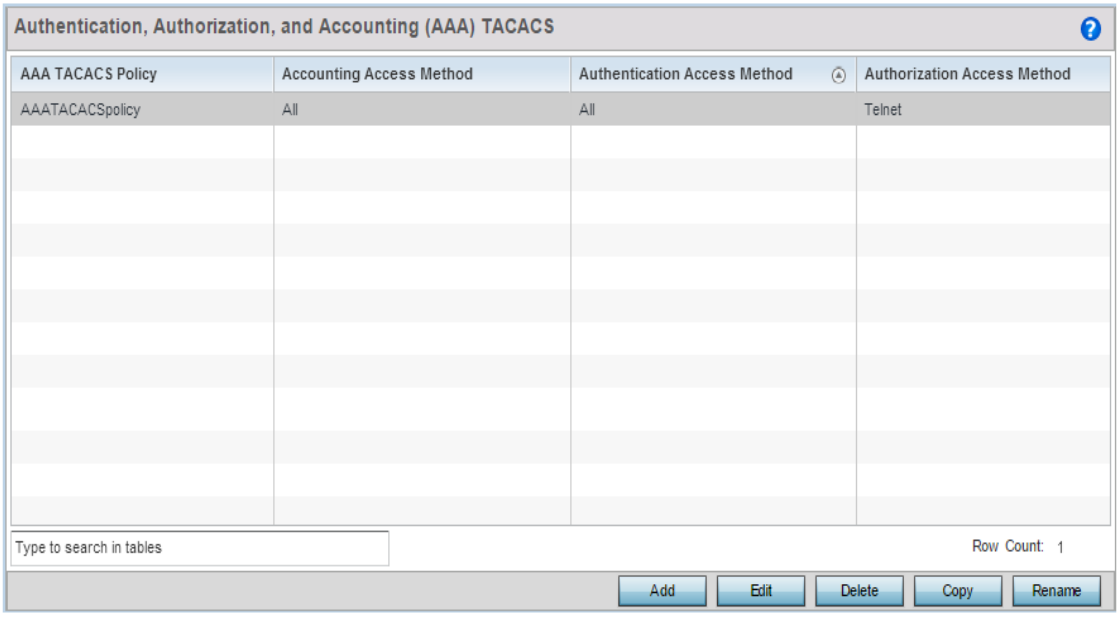


Figure 14: Authentication, Authorization, and Accounting (AAA) TACACS screen

4 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 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.*

5 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.

6 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.

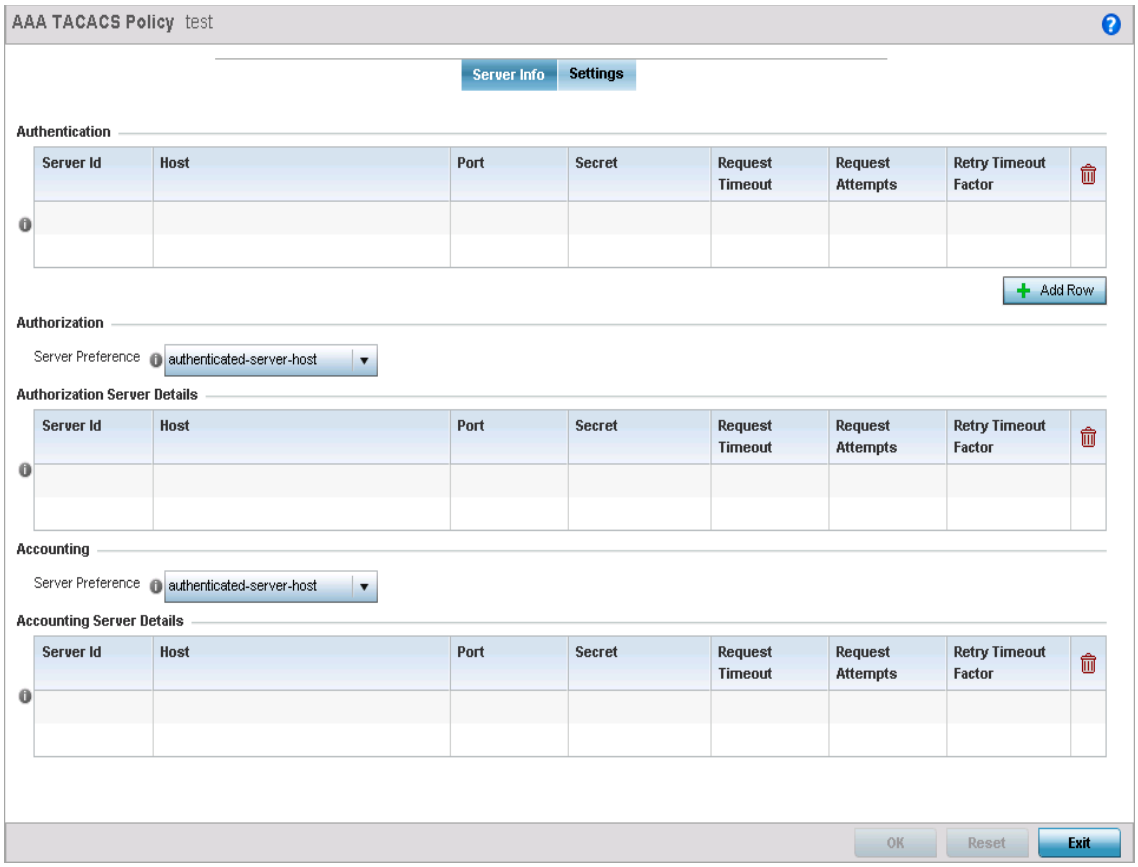


Figure 15: AAA TACACS Policy - Server Info tab

7 Under the **Authentication** table, select **+ Add Row**.

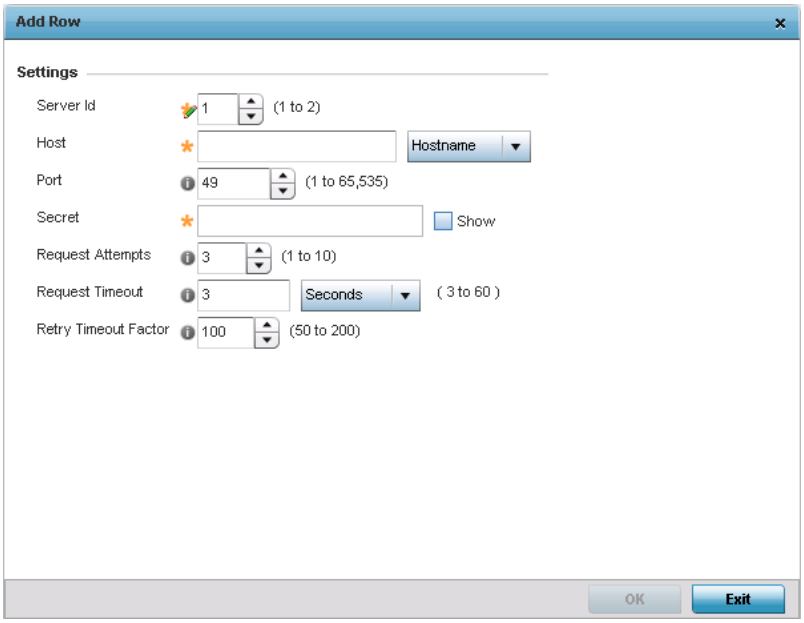


Figure 16: AAA TACACS Policy - Authentication - Add screen

8 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.

9 Select **OK** to save the changes or **Exit** to close the screen.

10 Set the **Authorization Server Preference** to specify which server, in the pool of servers, is selected to receive authorization requests. Options include *None*, *authenticated-server-host*, and *authenticated-server-number*. If selecting *None* or *authenticated-server-number* select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.

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.

11 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

12 Set the **Accounting Server Preference** to select the accounting server, from the pool of servers, to receive accounting requests. Options include *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.

13 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 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.

14 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

15 Select the **Settings** tab.

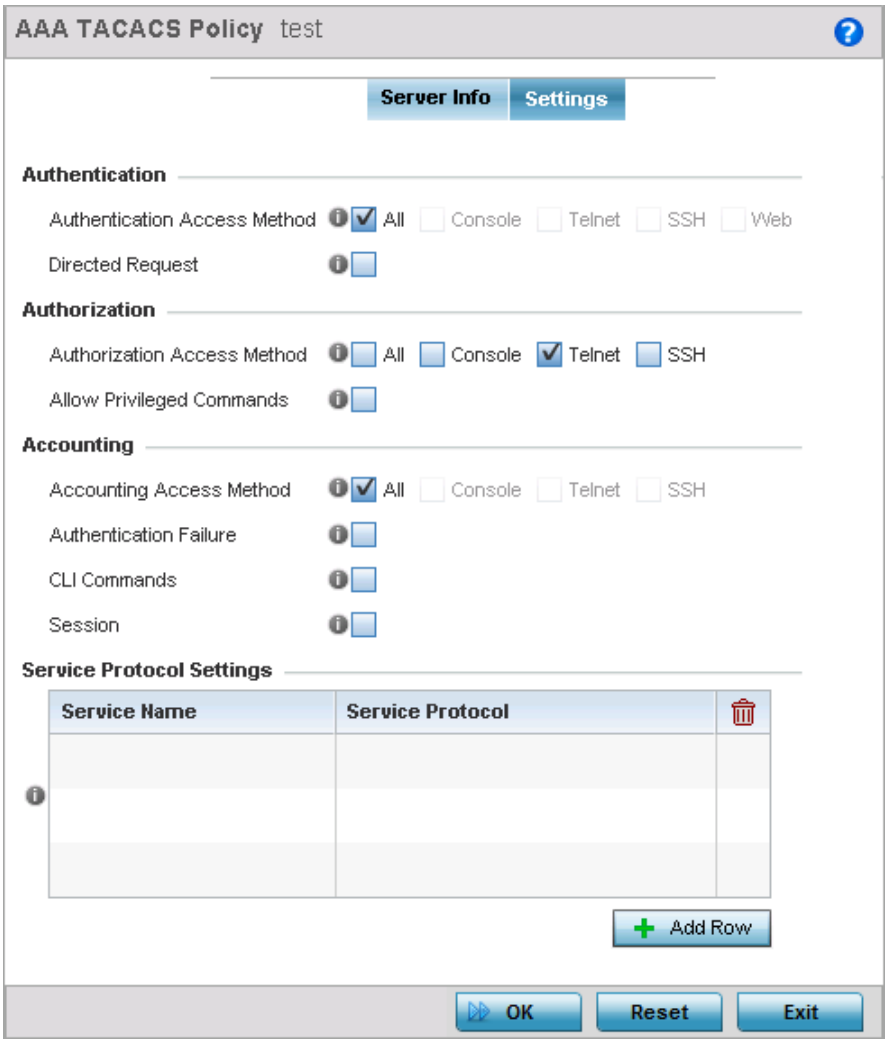


Figure 17: AAA TACACS - Settings screen

16 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.

17 Set the following AAA TACACS **Authorization** server configuration parameters:

Authorization Access Method	Specify the connection methods 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.

18 Set the following AAA TACACS **Accounting** server configuration parameters:

Accounting Access Method	Specify access methods for accounting server connections. • *All* – Accounting is performed for all types of access with none given priority. • *Console* – Accounting is performed for console access only. • *Telnet* – Accounting is performed only for access through Telnet. • *SSH* – Accounting is performed only for access through SSH.
Authentication Failure	Select this 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.

19 Select **+ Add Row** and set the following **Service Protocol Settings** parameters:



NOTE

A maximum or 5 entries can be made in the Service Protocol Settings table.

Service Name	Provide a 30 character maximum shell service for user authorization.
Service Protocol	Enter a protocol for user authentication using the service.

20 Select OK to save the updates to the AAA TACACS policy. Select Reset to revert to the last saved configuration.

Alias

"Network Configuration"

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

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

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

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

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

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

override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

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

Alias can be classified as:

- "Network Basic Alias"
- "Network Group Alias"
- "Network Service Alias"

Network Basic Alias

- "Alias"

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

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

To edit or delete a basic alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Network**.

3 Select the **Alias** item, the **Basic Alias** screen displays.

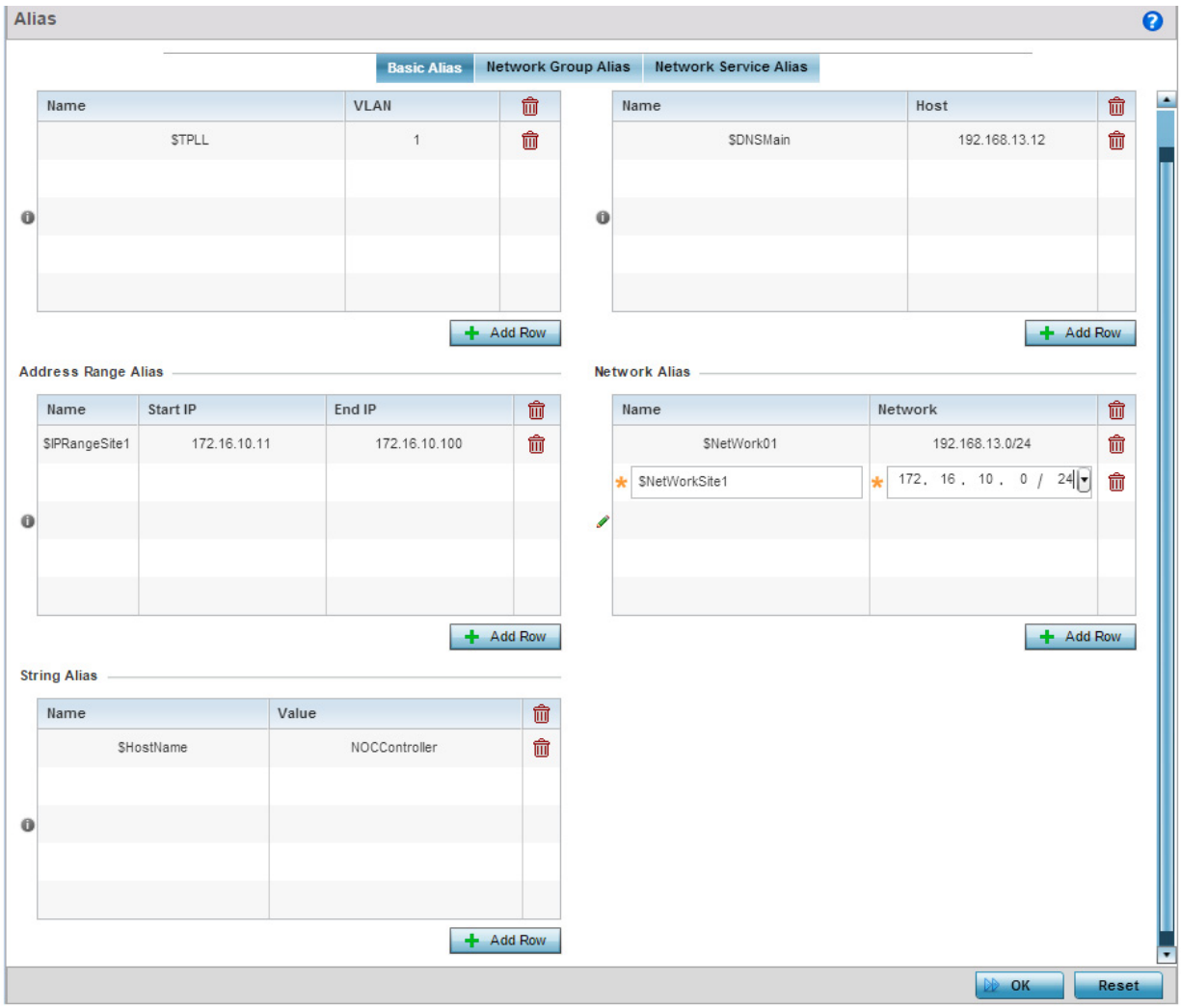


Figure 18: Network - Basic Alias Screen

4 Select **+ Add Row** to define **VLAN Alias** settings:

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

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

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

- Bridge VLAN
- IP Firewall Rules

- L2TPv3
- Switchport
- Wireless LANs

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

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

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

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

6 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 IP address of the host machine.

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

- IP Firewall Rules
- DHCP

7 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*.

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

- IP Firewall Rules
- DHCP

8 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 string value to use in the alias.

A *string alias* can be used to replace domain name strings 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

"Alias"

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

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

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

To edit or delete a network alias configuration:

1 Select **Configuration** tab from the user interface.

2 Select **Network.**

3 Select the **Alias** item. The **Basic Alias** screen displays.

4 Select the **Network Group Alias** tab.

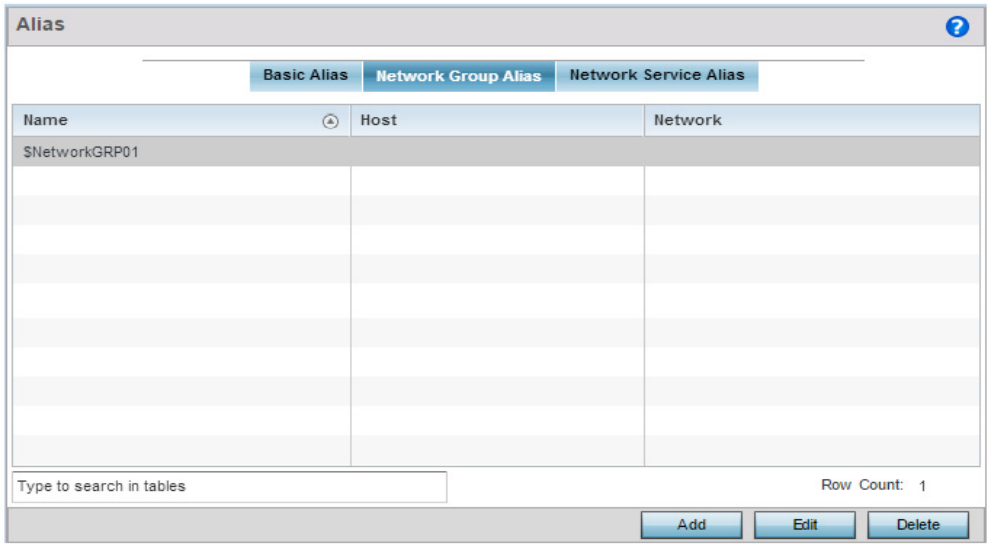


Figure 19: Network - Alias - Network Group Alias screen

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

5 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Group Alias**. **Copy** to copy an existing policy or **Rename** to rename an existing policy.

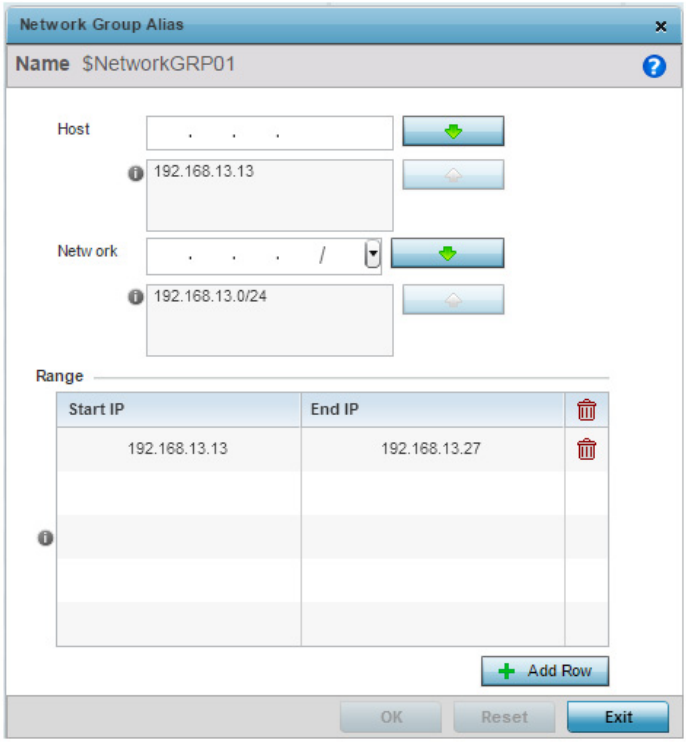


Figure 20: Network - Alias - Network Group Alias Add screen

6 If adding a new **Network Group Alias**, provide it a name of up to 32 characters.

NOTE

The Network Group Alias Name always starts with a dollar sign ($).

7 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.

8 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 an alias range entry to edit it.

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

Network Service Alias

- "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 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.

A *network service alias* can be used in IP firewall rules to substitute protocols and ports:

To edit or delete a service alias configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Network.**

3 Select the **Alias** item, the **Basic Alias** screen displays.

4 Select the **Network Service Alias** tab.

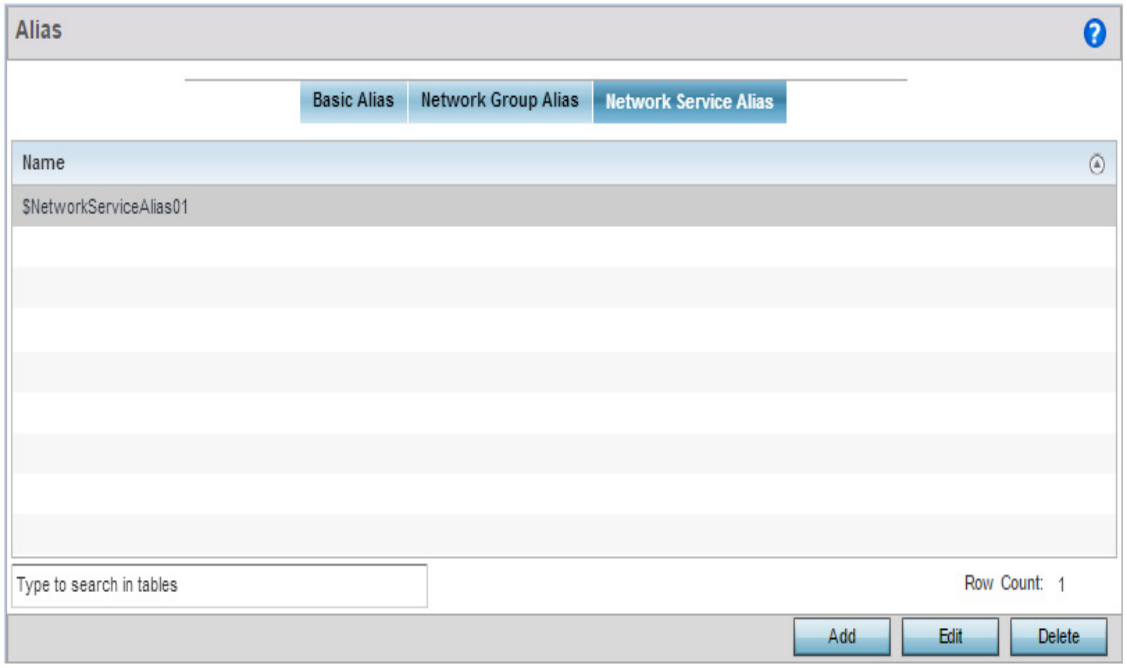


Figure 21: Network - Alias - Network Service Alias screen

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

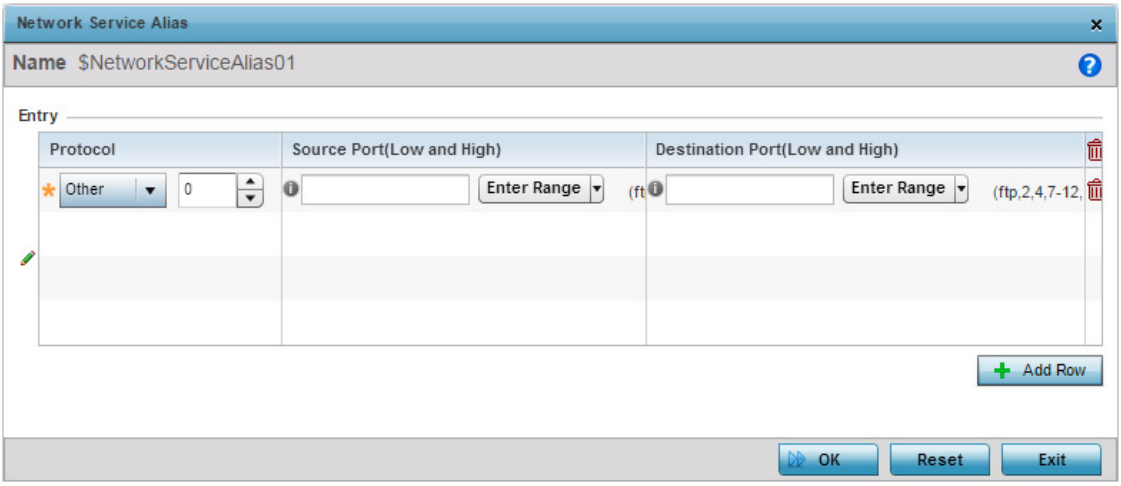


Figure 22: Network - Alias - Network Service Alias Add screen

6 If adding a new **Network Service Alias**, provide it a name up to 32 characters.

NOTE

The Network Service Alias Name always starts with a dollar sign ($).

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

Protocol	Specify the protocol for which the alias has to be created. Use the drop down 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)	Use this field only if the protocol is *tcp* or *udp*. Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	Use this field only if the protocol is *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Range* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

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

URL Filtering

"Network Configuration"

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 define a URL Filter:

1 Select **Configuration** > **Network** > **URL Filtering**.

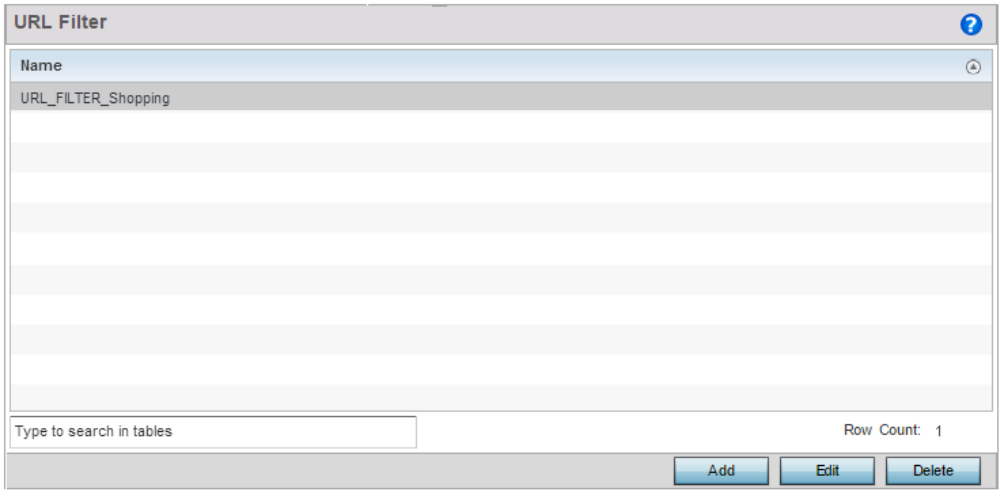


Figure 23: Network IPv6 Router Advertisement Policy screen

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.

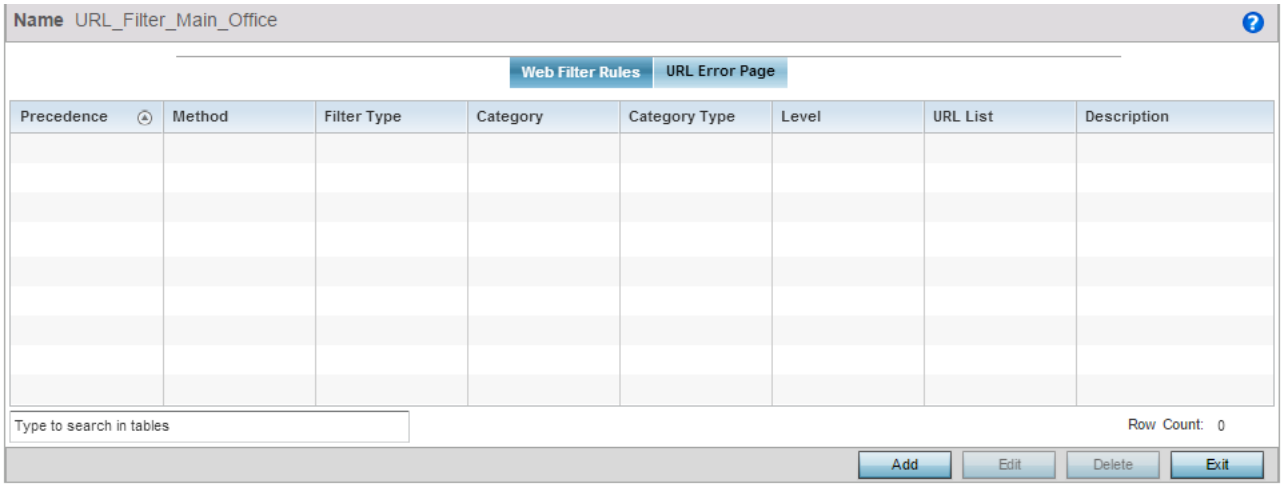


Figure 24: Network URL Filtering - Web Filter Rules screen

4 Set the following **Web Filter Rules** 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	Use the drop-down menu to 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	Use the drop-down menu to select the URL Filter Type as *level*, *category_type*, *category* or *url_list*.
Category	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 Type	If the *Filter Type* is set to category_type, use the drop-down menu to select from a list of predefined category types (adult-content, security-risk etc.) to either blacklist or whitelist all URLs in that category type. There are 12 category types available.
Level	If the *Filter Type* is set to level, use the drop-down menu to specify the level as *Basic*, *Low*, *Medium*, *medium-high* or *High*. 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, nor can the user add/ modify/remove the category types mapped to the filter-level settings.
URL List	If the *Filter Type* is set to url_list, use the drop-down menu to select pre-configured URL lists. If no URL list is available, click the *Create* icon to create a new URL list. To view and modify an existing URL list, click the *Edit* icon. 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.

5 Set the following **URL Error Page** settings:

The URL Error Page tab allows you 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.

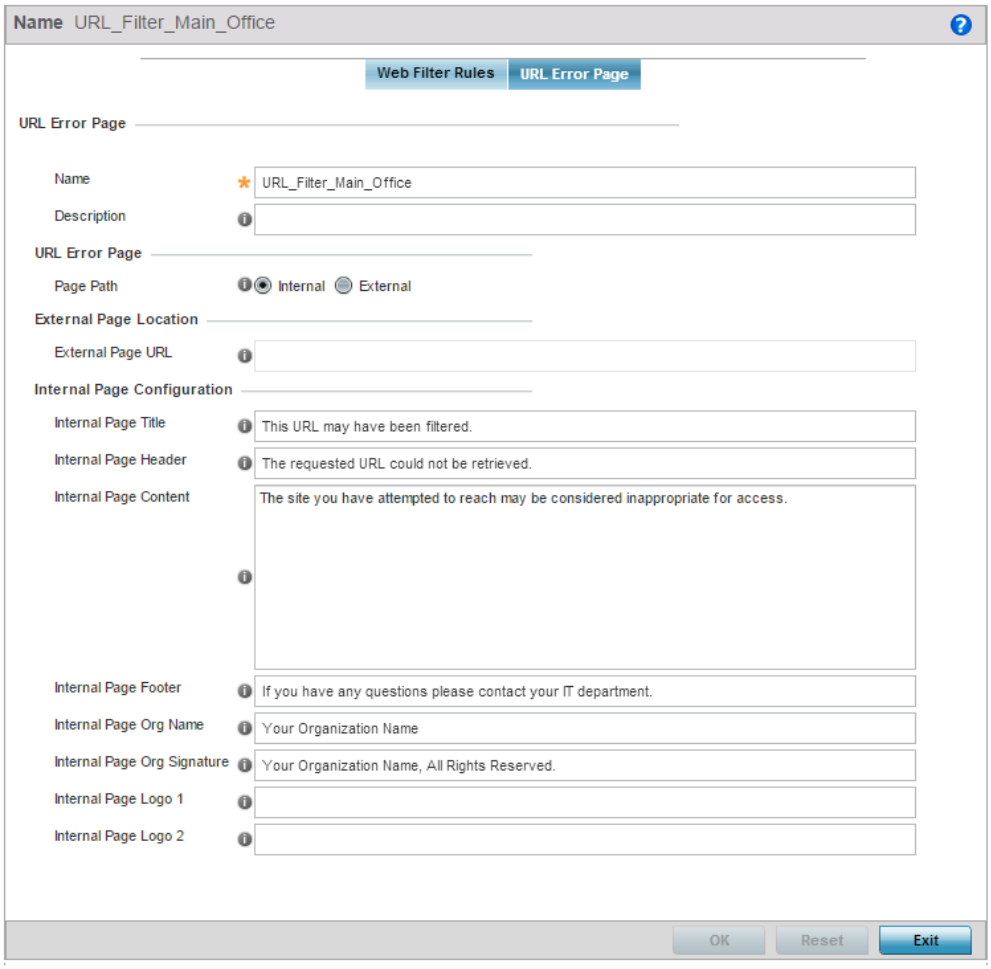


Figure 25: Network URL Filtering - URL Error Page screen

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.
External Page URL	If selecting *Page Path* as *External*, 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 Signature	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 Org Logo 1	Provide the location and filename of a small graphic image displayed in the blocking page.
Internal Page Org Logo 2	Provide the location and filename of a small graphic image displayed in the blocking page.

6 Select **OK** the updates to the URL filter configuration, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

Web Filtering

"Network Configuration"

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 define a URL filter:

1 Select **Configuration** > **Network** > **Web Filtering**.

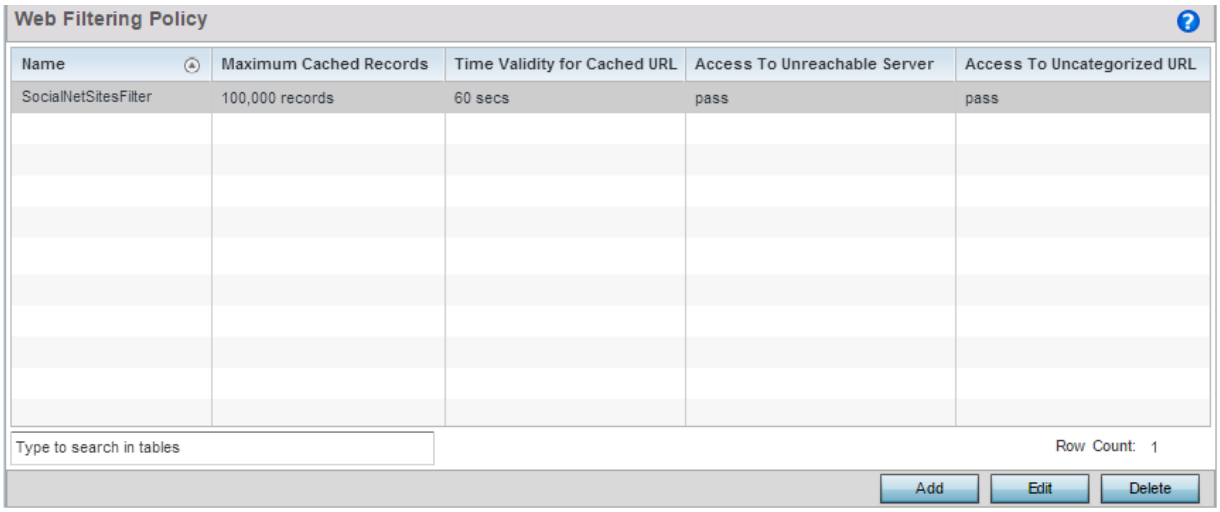


Figure 26: Network Web Filtering Policy screen

2 Select **Add** to create a new Web Filtering policy, **Edit** to modify the attributes of a selected Web Filtering policy or **Delete** to remove obsolete policies from the list of those available.

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.

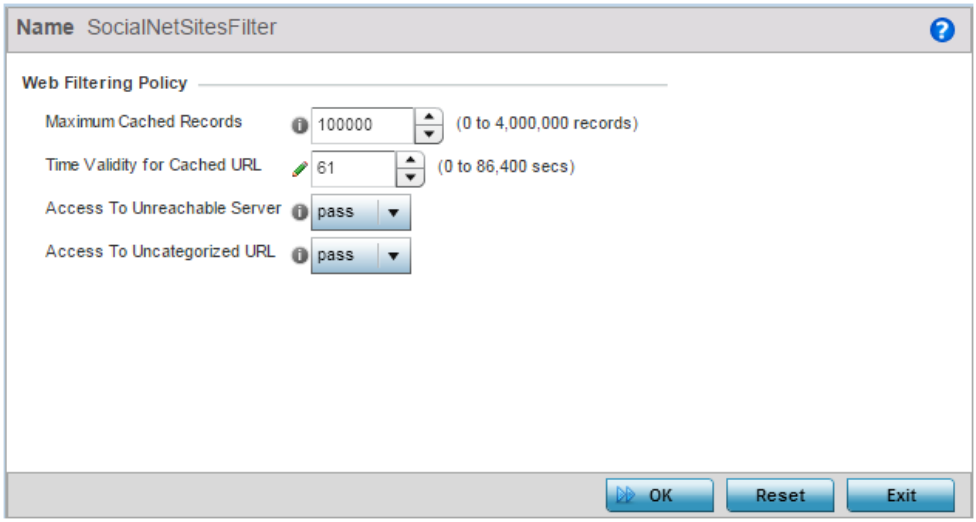


Figure 27: Network Web Filtering Policy - Add screen

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's cache. Consider the bandwidth depletion if caching a large number of records over the maximum permissible time validity.
Access to Unreachable Server	Use the drop-down menu to either select *pass* or *block* (filter) access to a cached URL when the categorization server is unreachable. The default setting is pass.
Access to Uncategorized URL	Use the drop-down menu to either select *pass* or *block* (filter) access to a cached URL when the categorization server fails to classify a request type. The default setting is pass.

5 Select **OK** to save the Web Filtering Policy settings, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

IPv6 Router Advertisement Policy

"Network Configuration"

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**.

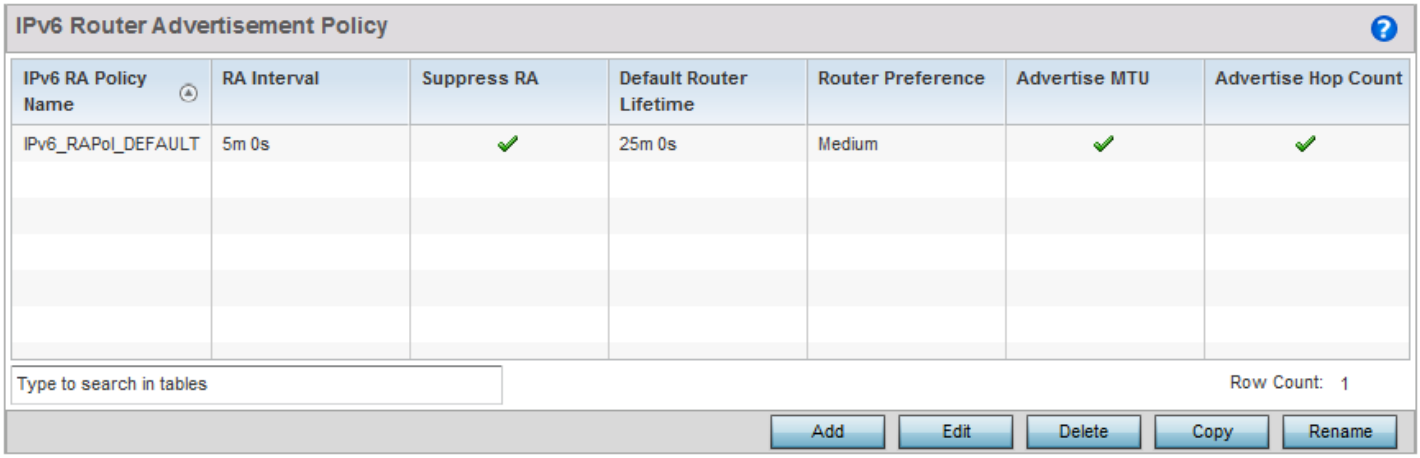


Figure 28: Network IPv6 Router Advertisement Policy screen

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.

The **IPv6 RA Policy Name** screen displays.

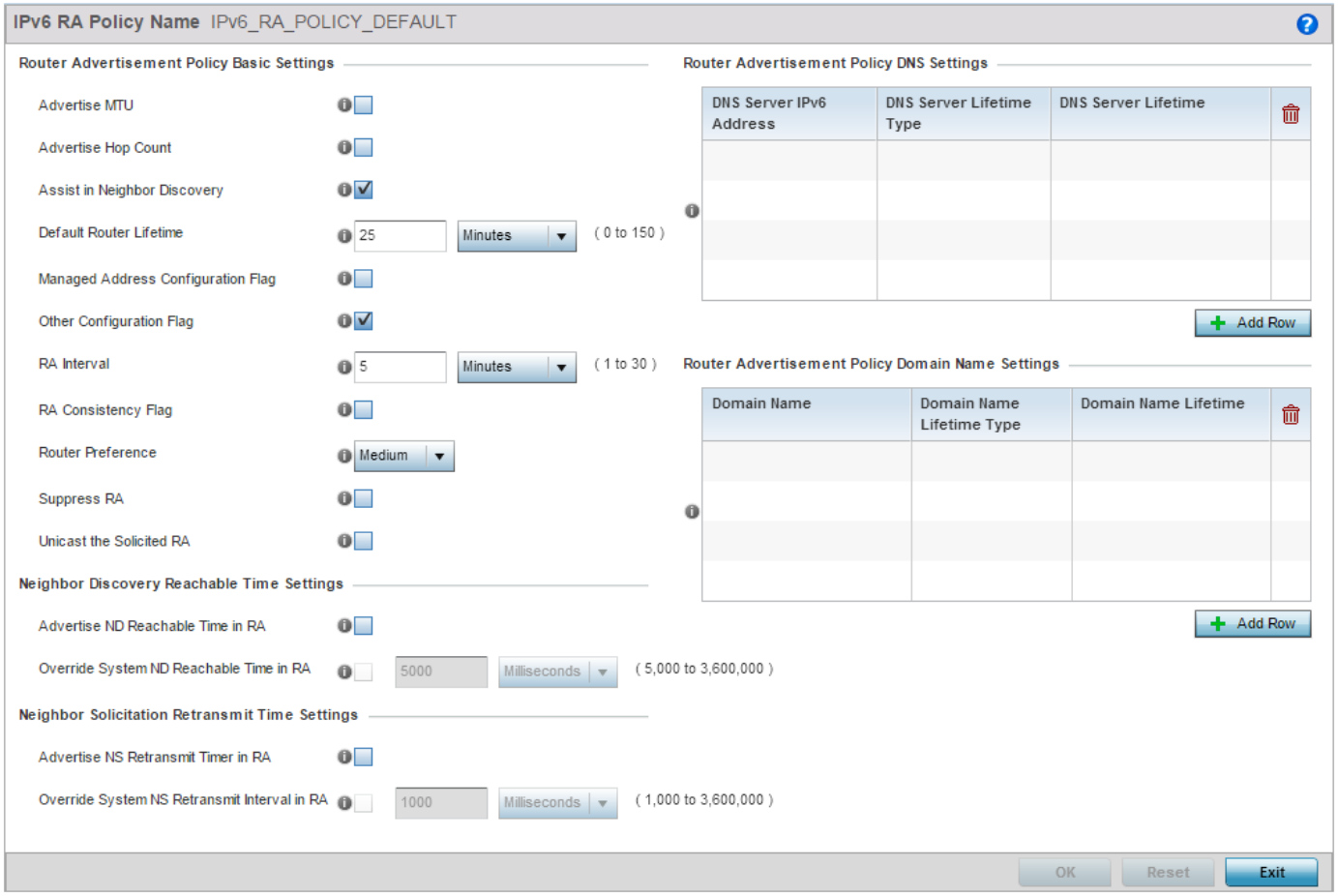


Figure 29: Network IPv6 RA Policy Name screen

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 if 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 minutes.
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 setting is disabled.

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 by default.
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.

Application Policy

"Network Configuration"



NOTE

This feature is only available on AP7522 and AP7532 access points.

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. The following are the rules/actions that can be applied in an application policy:

- *Allow* - Allow packets for a specific application and its defined category type (social networking etc.)
- *Deny* - Deny (restrict) action applied to a specific application or a specific application category
- *Mark* - Mark recognized packets with DSCP/8021p value
- *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. *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.

To define an application policy configuration:

1 Select **Configuration** > **Network** > **Application Policy**.

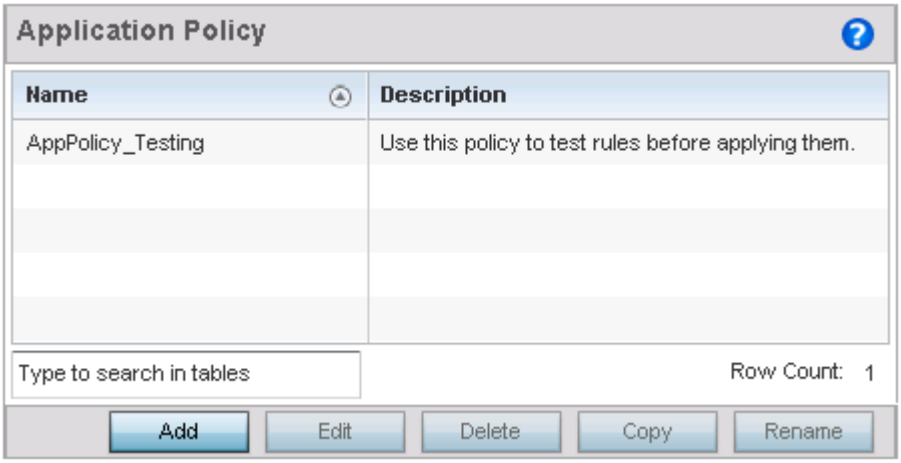


Figure 30: Network - Application Policy screen

The screen lists the application policy configurations defined thus far.

2 Refer to the following to determine whether a new application policy requires creation, modification or deletion:

Name	Lists the 32 character maximum name assigned to each listed application policy, designated upon creation.
Description	Displays the 80 character maximum description assigned to each listed application policy, as a means of further distinguishing policies with similar configurations.

3 Select **Add** to create a new application policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

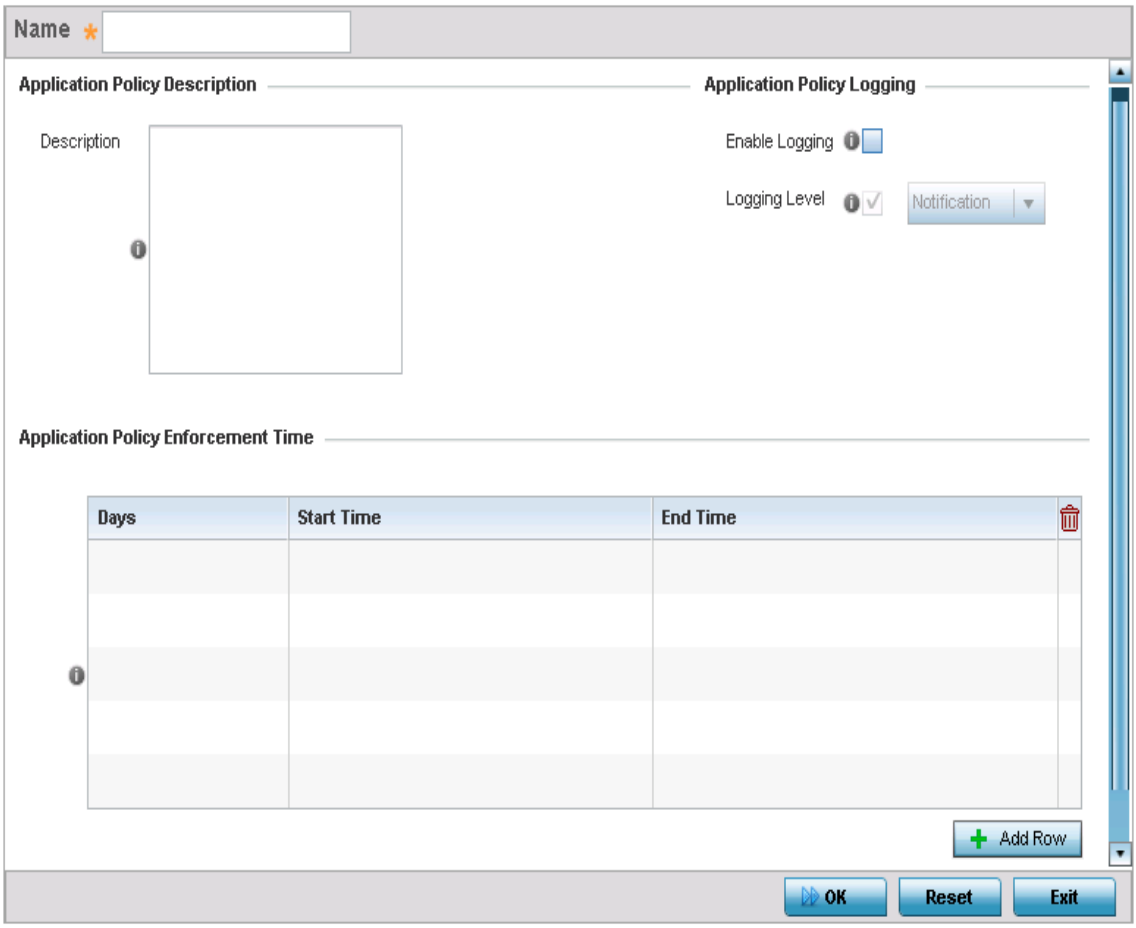


Figure 31: Network - Application Policy Add/Edit screen

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 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.

Select **+ Add Row** launch a screen to create a new policy rule.

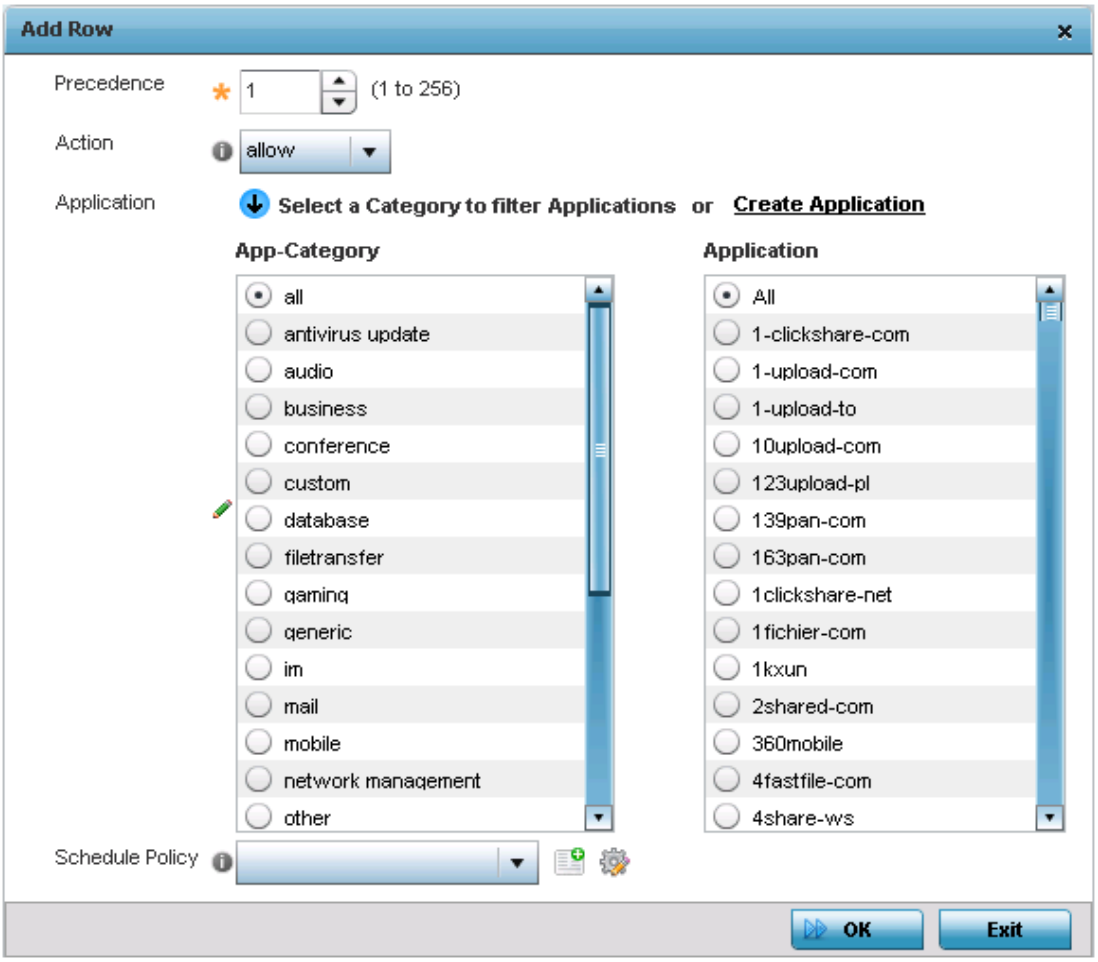


Figure 32: Network - Application Policy, Add Rule screen

9 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.

10 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 706.

11 Select **OK** to save the updates to the application policy. Select **Reset** to revert to the last saved configuration.

Application

"Network Configuration"

NOTE

This feature is only available on AP7522 and AP7532 access points

Use the **Application** screen to create custom application configurations.

To create a user-defined application:

1 Select **Configuration > Network > Application**.

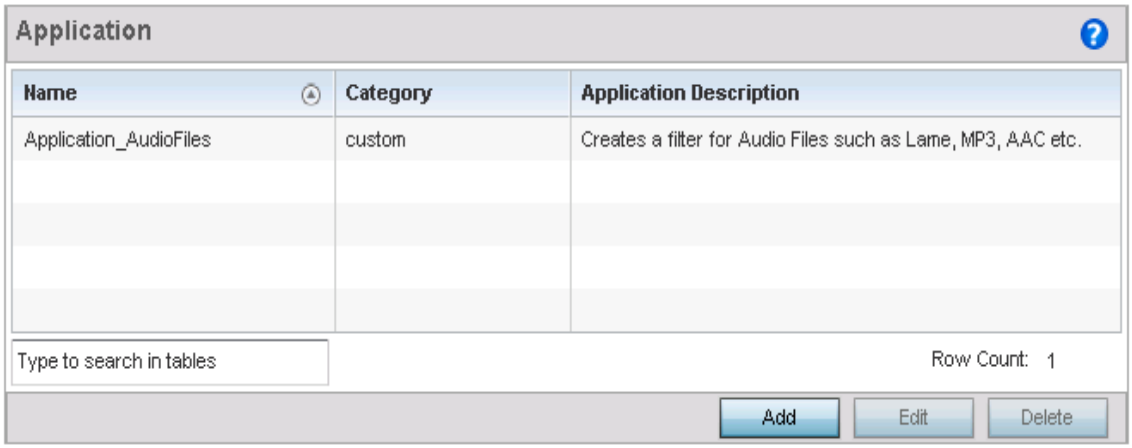


Figure 33: Network - Application screen

The screen lists the application configurations defined thus far.

2 Refer to the following to determine whether a application requires creation, modification or deletion:

Name	Displays the name of each user-defined application created using this application interface.
Category	Lists the category to which each listed user-defined application belongs.
Application Description	Lists the 80 character maximum description administratively assigned to each listed user-defined application.

3 Select **Add** to create a new application configuration, **Edit** to modify the attributes of a selected application or **Delete** to remove obsolete applications from the list of those available.

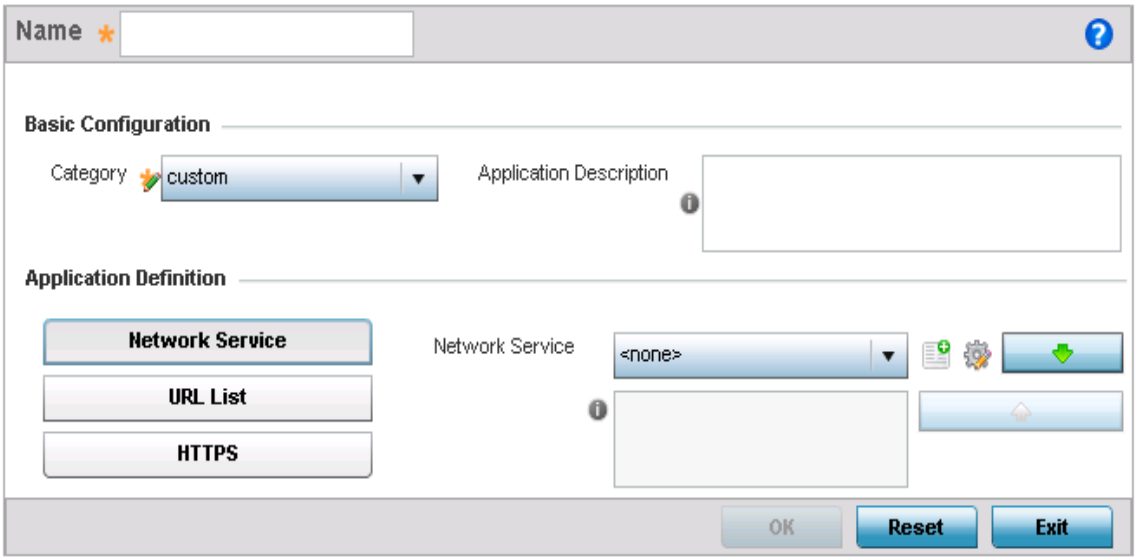


Figure 34: Network - Application Policy Add screen

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, pre-defined URL list or set of HTTPS parameters to the user-defined application.

Network Service	Use the drop-down menu to select an existing network service alias for the user-defined application. If there are no existing network service alias suited to this new user-defined application, select the **Create** icon to define a new alias or the **Edit** icon to modify an existing one. Provide or modify a 32 character maximum name, along with a protocol type or number and source and destination port value. Up to four (4) service aliases can be supported.
URL List	Use the drop-down menu to select a pre-defined URL list to apply to the user-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.

Schedule Policy

"Network Configuration"

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**.

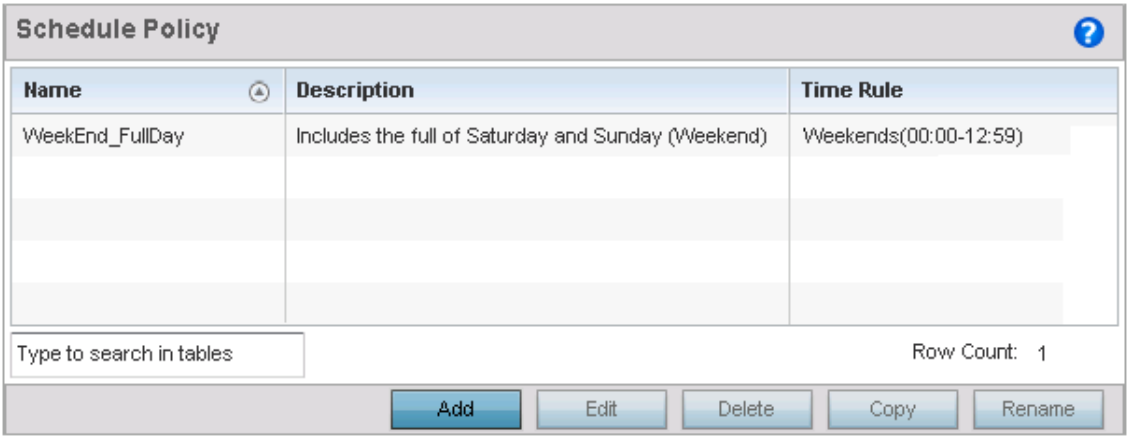


Figure 35: Network - Schedule Policy screen

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.

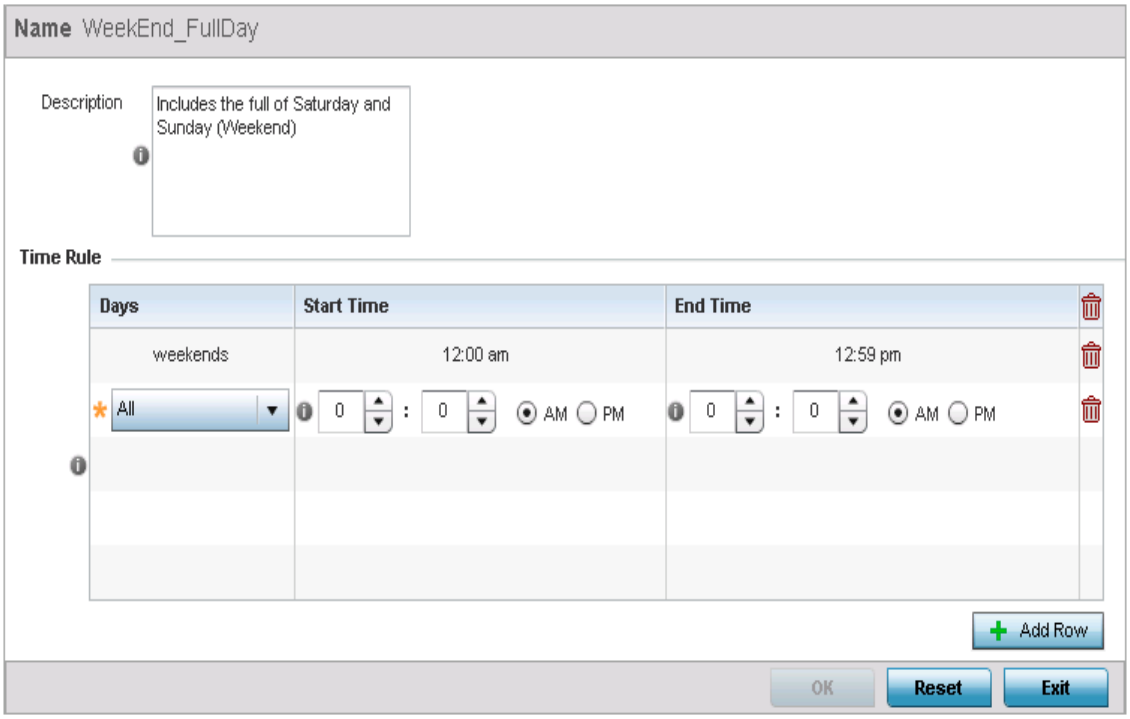


Figure 36: Network - Schedule Policy Add/Edit screen

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 the selected day.
Start Time	Set the start time when the schedule policy time rule applies. 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 when the time rule is no longer enforced. Use the spinner controls to select the hour and minute, in 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.

Network Deployment Considerations

"Network Configuration"

Before defining an access point network 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 Security Configuration

When taking precautions to secure wireless traffic from a client to an access point, the network administrator should not lose sight of the security solution in it's entirety, since the network's chain is as weak as its weakest link. An access point managed wireless network provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network. This security is offered at the most granular level, with role and location based secure access available to users based on identity as well as the security posture of the client device.

There are multiple dimensions to consider when addressing the security of an access point managed wireless network, including:

- "Wireless Firewall"
- "Configuring IP Firewall Rules"
- "Configuring MAC Firewall Rules"
- "Wireless IPS (WIPS)"
- "Device Categorization"
- "Device Fingerprinting"
- "Security Deployment Considerations"

Wireless Firewall

"Security Configuration"

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 firewalls are mechanisms that block and permit data traffic within the network. 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 in fact could provide a false sense of security.

With our access points, firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing wireless clients within the network. Well designed firewalls block traffic from outside the network, but permit 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 the network passes through the firewall, which examines each message and blocks those not meeting the defined security criteria (rules).

Firewall rules define traffic permitted or denied within the network. Rules are processed by a firewall device from first to last. When a rule matches the network traffic processed by an access point, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise of conditions and actions. A condition describes a packet traffic stream. A condition defines constraints on the source and destination devices, the service (for example, protocols and ports), and the incoming interface. An action describes what should

occur to packets matching set conditions. For example, if a packet stream meets all conditions, 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 being bridged by radios. IP and MAC filtering can be employed to permit or restrict traffic exchanged between hosts, hosts residing on separate WLANs or hosts forwarding traffic to wired devices.

For more information, refer to the following:

- "Defining a Firewall Configuration"
- "Configuring IP Firewall Rules"
- "Configuring MAC Firewall Rules"

Defining a Firewall Configuration

- "Wireless Firewall"

To configure a firewall:

1 Select **Configuration** tab from the Web user interface.

2 Select **Security.**

3 Select **Wireless Firewall** to display existing firewall policies.

The **Wireless Firewall** screen lists *Denial of Service*, *Storm Control* and *Advanced Settings* tabs used to create the single Firewall policy used by the access point and its connected devices. The **Denial of Service** tab displays be default.

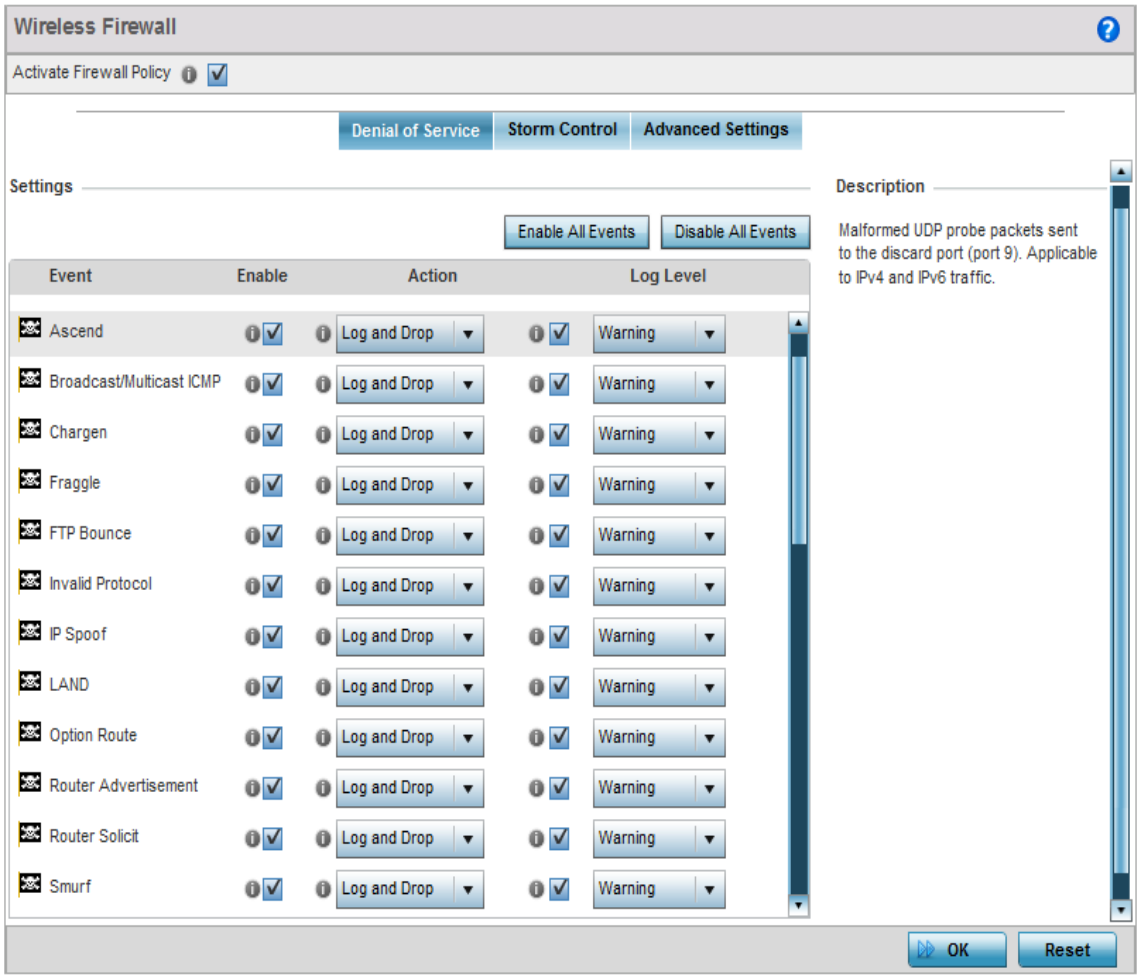


Figure 1: Wireless Firewall screen - Denial of Service tab

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.

4 Select the **Activate Firewall Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.

The **Settings** field lists all of the DoS attacks the firewall has filters for. Each DoS filter contains the following four items:

Event	Lists the name of each DoS attack.
Enable	Select *Enable* to set the firewall to filter the associated DoS attack based on the selection in the *Action* column.
Action	If a DoS filter is enabled, chose an action from the drop-down menu to determine how the firewall treats the associated DoS attack. Options include: • *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 is dropped. No further action is taken.
Log Level	Select this option to enable logging to the system log. Then select a standard Syslog level from the *Log Level* drop-down menu.

5 The following **Events** can be filtered on behalf of the firewall:

Ascend	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 requests. 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, call hijacking, or a DoS attack.
IP Spoof	IP Spoof is an 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 E-mail, 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	This is an attempt to predict the sequence number used to identify the 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 Net BIOS 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.

6 Select **OK** to update the Denial of Service settings. Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.

7 Select the **Storm Control** tab. Select the **Activate Firewall Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.

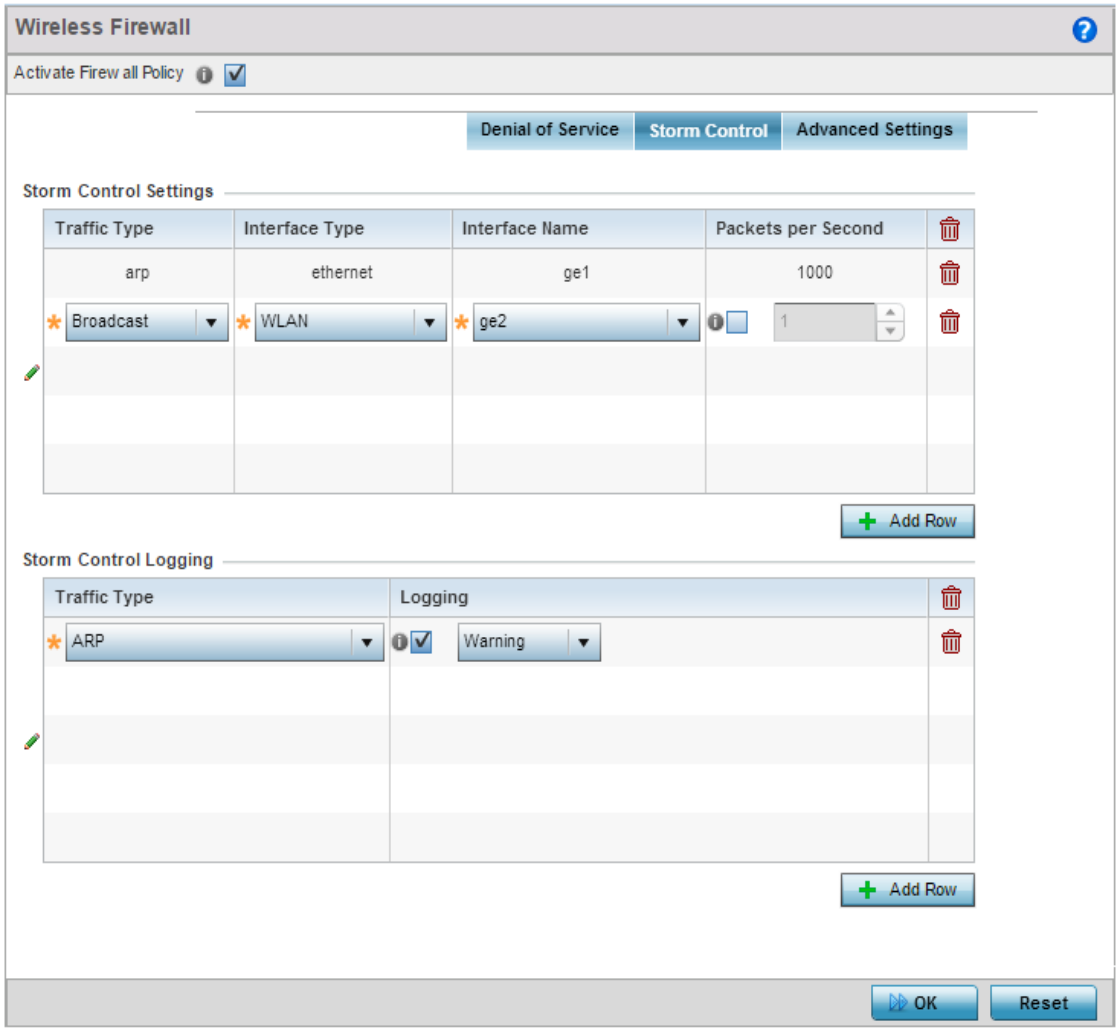


Figure 2: Wireless Firewall screen - Storm Control tab

The firewall maintains a facility to control packet storms. Storms are packet bombardments that exceed the high threshold configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the interface. Thresholds are configured in terms of packets per second.

8 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 to specify the packets per second threshold for activating the Storm Control mechanism.

9 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.

10 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 to specify the standard log level used if a Storm Control attack is detected. The default log level is Warning.

11 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.

12 Select **OK** to update the Storm Control settings. Select **Reset** to revert to the last saved configuration.The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.

13 Select the **Advanced Settings** tab.

Use the **Advanced Settings** tab to enable/disable the firewall, define application layer gateway settings, flow timeout configuration and TCP protocol checks.

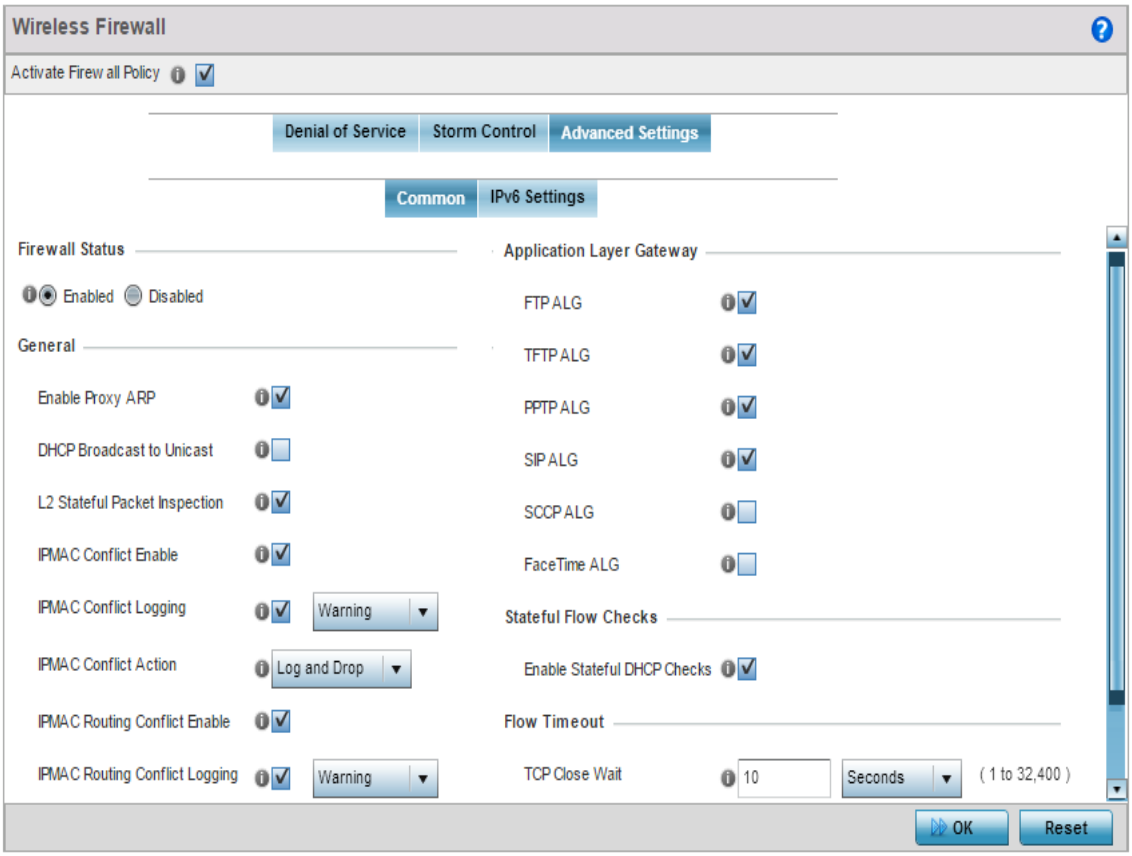


Figure 3: Wireless Firewall screen - Advanced Settings tab

14 Refer to the **Firewall Status** radio buttons to define the firewall as either *Enabled* or *Disabled*. The firewall is enabled by default.

If disabling the firewall, a confirmation prompt displays stating NAT, wireless hotspot, proxy ARP,
deny-static-wireless-client and *deny-wireless-client* sending not permitted traffic excessively will be disabled.

15 Refer to the **General** field to enable or disable the following firewall parameters:

Enable Proxy ARP	Select the radio button 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 the radio button 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 radio button to enable stateful packet inspection for routed interfaces within the Layer 2 Firewall. This feature is enabled by default.
IPMAC Conflict Enable	Select this option to log and act upon detected IPMAC conflicts. These occur when removing a device from the network and attaching another using the same IP address.
IPMAC Conflict Logging	When enabled, use the drop-down menu to set the logging level (*Error*, *Warning*, *Notification*, *Information* or *Debug*) if an attack is detected. The default setting is Warning.
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 MAC address.
IPMAC Routing Conflict Logging	Select enable logging for IPMAC Routing Conflict detection. This feature is enabled by default and set to Warning.
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 configuration for the maximum segment size of packets at a global level.
Max Fragments/ Datagram	Set the maximum number of fragments (from 2 - 8,129) allowed in a datagram before it is dropped. The default value is 140 fragments.
Max Defragmentations/ Host	Set the maximum number of defragmentations, from 1 - 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, from 8 bytes - 1,500 bytes, to enforce a minimum packet size before being subject to fragment based attack prevention.
Virtual Defragmentation	Select this option to enable IP Virtual Defragmentation, this helps prevent IP fragments based attacks, such as tiny fragments or large number of IP fragments.
Virtual Defragmentation Timeout	Set the virtual defragmentation timeout to prevent IP fragment based attacks. Set a value from 1 - 60 seconds. The default value is 1 second.

16 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 the *Enable* box to allow FTP traffic through the firewall using its default ports. This feature is enabled by default.
TFTP ALG	Select the *Enable* box to allow TFTP traffic through the firewall using its default ports. This feature is enabled by default.
PPTP ALG	Select the check box to allow PPTP traffic through the firewall. Microsoft uses PPTP in its Windows operating systems to establish VPN connection between two endpoints on the internet. PPP frames are used to tunnel packets through the IP backbone. PPTP uses a client-server model for connectivity. This feature is enabled by default.
SIP ALG	Select the *Enable* box to allow SIP traffic through the firewall using its default ports. This feature is enabled by default.
SCCP ALG	Select the check box to allow SCCP traffic through the firewall using its default ports. This feature is enabled by default. *Signalling Connection Control Part* (SCCP) is a network protocol that provides routing, flow control and error correction in telecommunication networks.
FaceTime ALG	Select the check box to allow Apple's FaceTime video calling traffic through the firewall using its default port. This feature is enabled by default.

17 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	Select this option to enable verbose logging for dropped packets. This setting is disabled by default.

18 Select the **Enable Stateful DHCP Checks** radio button 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.

19 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* (15 - 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* (15 - 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.

20 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.

21 Select the **IPv6 Settings** tab.

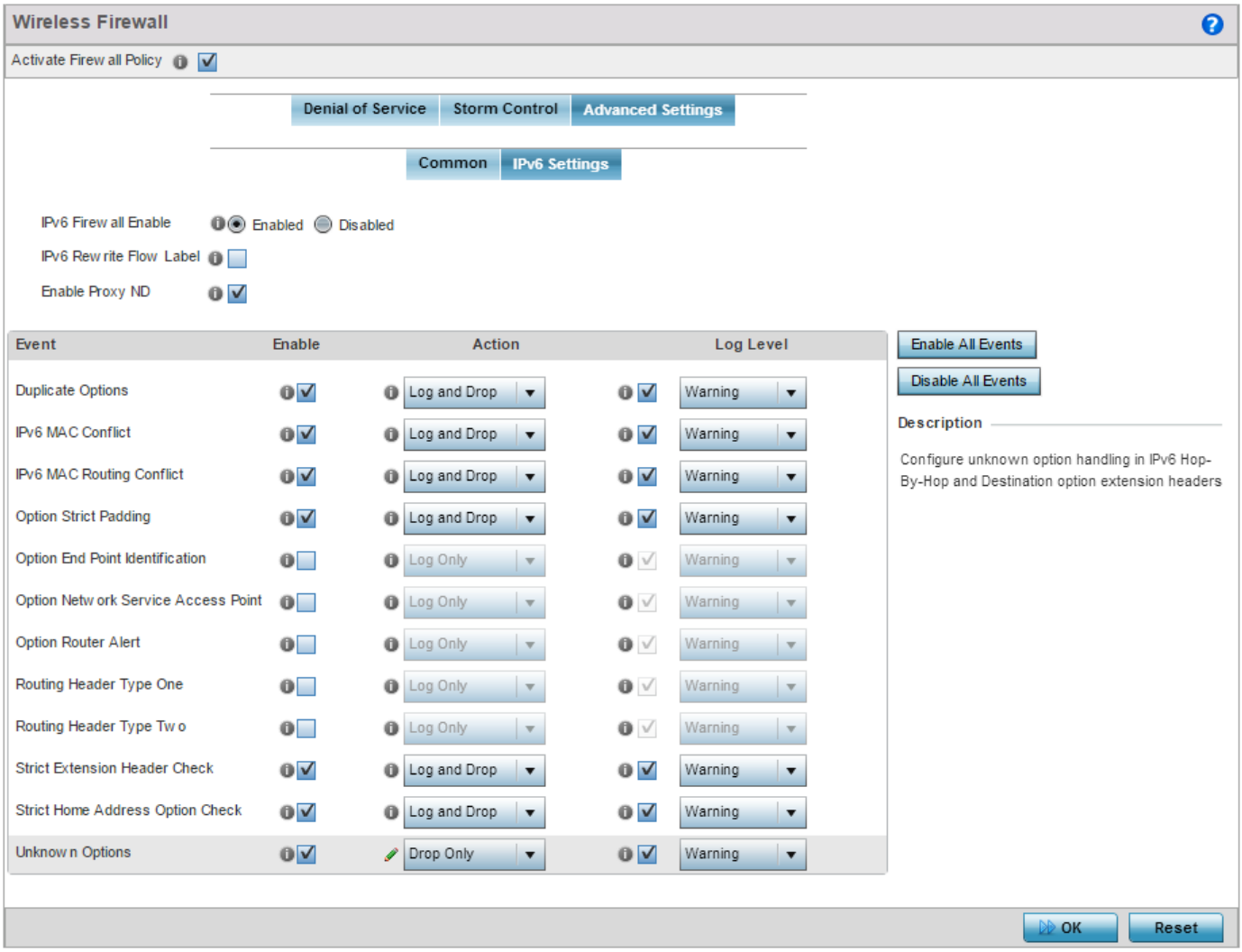


Figure 4: Wireless Firewall screen - Advanced Settings tab - IPv6 Settings tab

22 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.

23 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.

24 Select **Enable Proxy ND** to generate neighbor discovery responses on behalf of another 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.

25 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.

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.

26 The following **Events** can be filtered on behalf of the firewall:

Duplicate Options	Select to enable duplicate options handling in hop-by-hop and destination option extension headers. This configuration excludes *HAO* (Home Address Option) handling.
IPv6 MAC Conflict	Select to enable checking for conflicts between IPv6 addresses and MAC addresses.
IPv6 MAC Routing Conflict	Select to enable checking for IPv6 routing table (next-hop IPv6 address, MAC address) conflicts.
Option Strict Padding	Select to enable strict checks for validating *Pad1* and *PadN* options.
Option End Point Identification	Select to enable end point identification. This option is not enabled by default.
Option Network Service Access Point	Select to enable *Network Service Access Point* option. This option is not enabled by default.
Option Router Alert	Select to enable router alert option. This option is not enabled by default.

Routing Heading Type One	Select to enable checking for routing type one (1) in the *Routing Type* field of the Routing extension header for IPv6 packets. Routing Header 1 is used for NIMROD a project of DARPA. This option is not enabled by default.
Routing Heading Type Two	Select to enable checking for routing type two (2) in the *Routing Type* field of the Routing extension header for IPv6 packets. Routing Header 2 is used for Mobile IPv6 where it can hold the home address of the mobile node. This option is not enabled by default.
Strict Extension Header Check	Select to enable check for out of order and number of occurrences of extension headers in an IPv6 packet. The option is enabled by default.
Strict Home Address Option Check	Select to enable strict check for placement of home address option in the Destination option extension header. This option is enabled by default.
Unknown Options	Select to enable configuring unknown options handling in hop-by-hop and destination option extension headers.

27 Select **OK** to update the Firewall Policy Advanced Settings. Select **Reset** to revert to the last saved configuration. The firewall policy can be invoked at any point in the configuration process by selecting **Activate Firewall Policy** from the upper, left-hand side, of the access point user interface.

Configuring IP Firewall Rules

"Security Configuration"

Access points use IP based firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the IP address from which they arrive, 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 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 an access point 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 either IPv4 or IPv6, create access rules for traffic entering an access point interface, because if you are going to deny specific types of packets, it is recommended you do it before the access point spends time processing them, since access rules are processed before other types of firewall rules.

IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

For more information, see:

- "Setting an IPv4 or IPv6 Firewall Policy"
- "Setting an IP SNMP ACL Policy"
- "Setting a Network Group Alias"
- "Setting a Network Service Alias"

Setting an IPv4 or IPv6 Firewall Policy

"Configuring IP Firewall Rules"

Before defining a firewall configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

To add or edit an IP based Firewall Rule policy:

1.Select **Configuration** tab from the Web user interface.

28 Select **Security**.

29 Select **IPv4 ACL** or **IPv6 ACL** to display existing IP firewall policies.

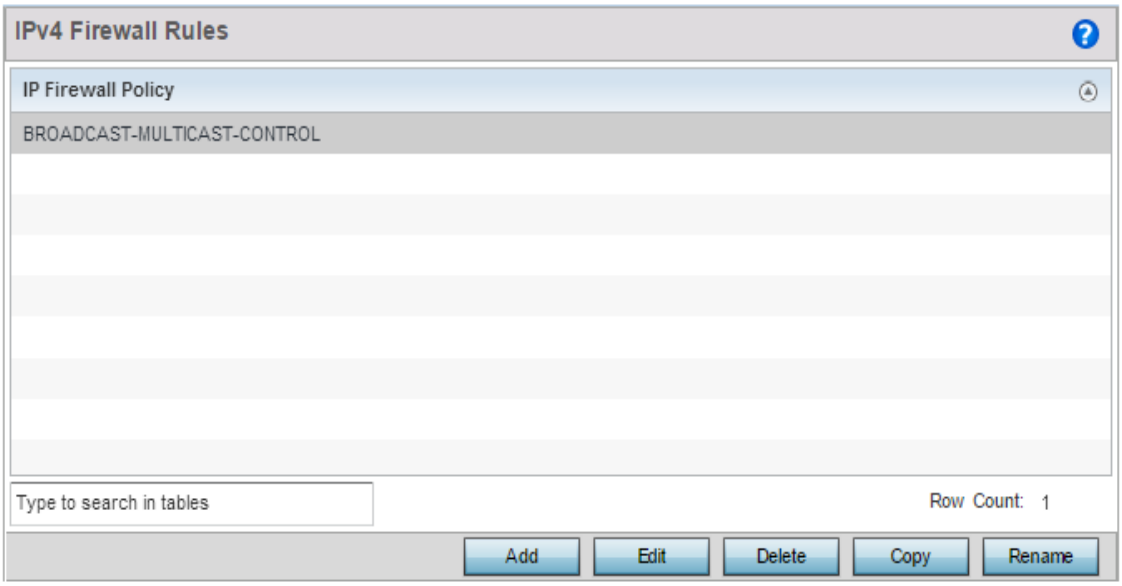


Figure 5: IP Firewall Policy screen

30 Select **Add** to create a new IPv4 or IPv6 Firewall Rule. Select an existing policy and select **Edit** to modify the attributes of the rule's configuration.

31 Select the added row to expand it into configurable parameters for defining a new rule.

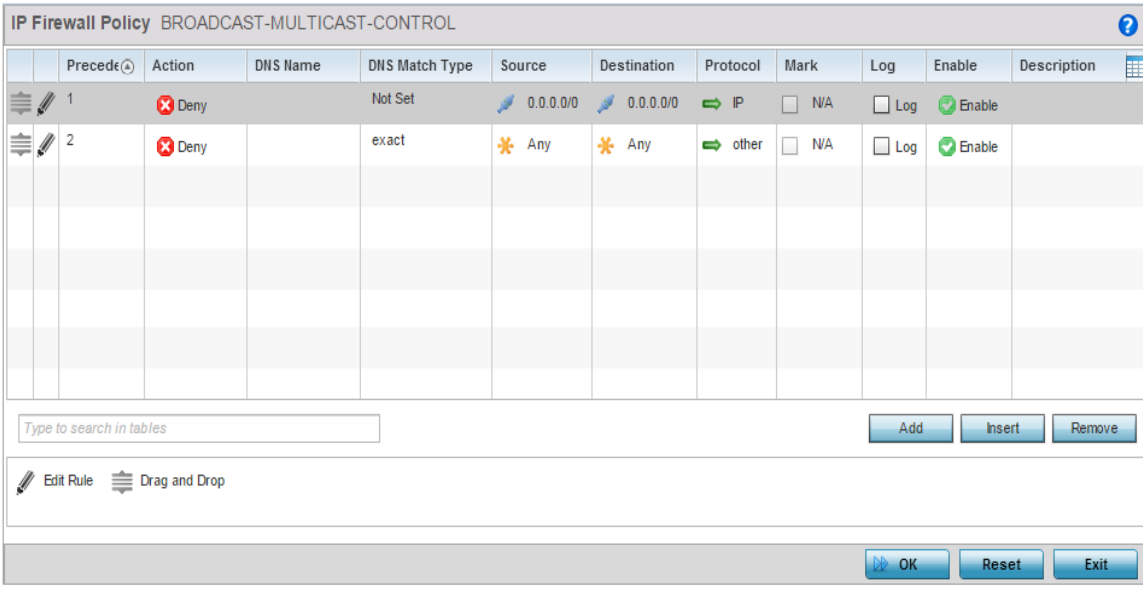


Figure 6: IP Firewall Rules screen - Adding a new rule

If adding a new rule, enter a name up to 32 characters.

32 Select **Add** to add a new firewall rule.

33 IP firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a. Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

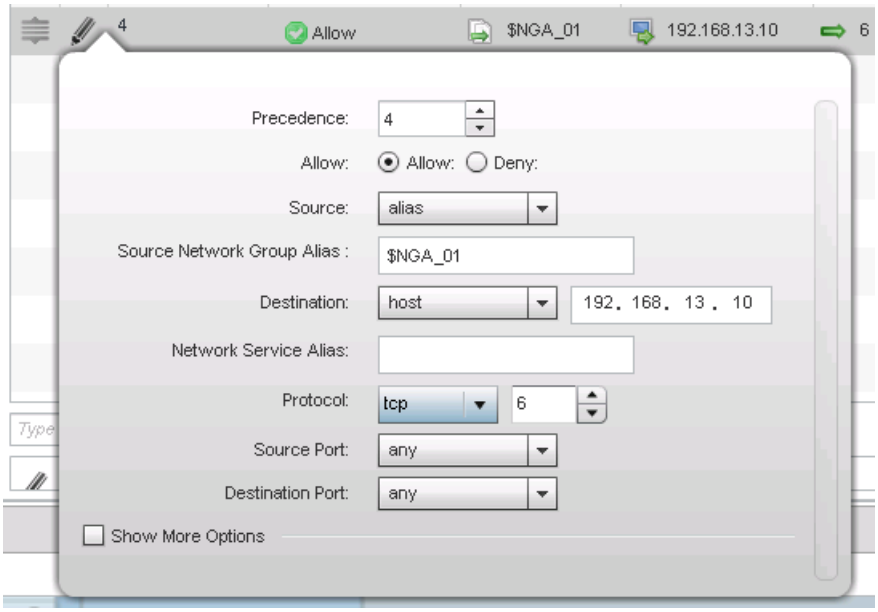


Figure 7: WLAN Security - IP Firewall Rules - Edit Rule screen

b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IPv4 or IPv6 ACL.

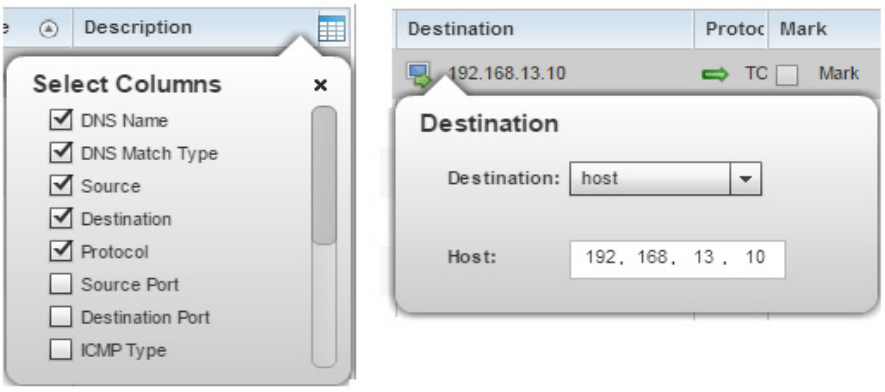


Figure 8: WLAN Security - IP Firewall Rules - IP Firewall Rules Add Criteria screen

NOTE

Only those selected IP ACL filter attributes display. Each value can have its current settings adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

Define the following parameters for the **IP Firewall Rule**:

Precedence	Specify or modify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
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. • *Allow* - Instructs the firewall to allow a packet to proceed to its destination.
Source	Select the source for creating the ACL. Source options include: • *Any* – Indicates any host device in any network. • *Network* – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IP address. • *Alias* – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.
Destination	Select the destination for creating the ACL. Destination options include: • *Any* – Indicates any host device in any network. • *Network* – Indicates all hosts in a particular network. Subnet mask information has to be provided for filtering based on network. • *Host* – Indicates a single host with a specific IP address. • *Alias* – Indicates a collection of IP addresses or hostnames or IP address ranges which are configured as a single unit. This is for ease of configuration of ACLs. When selected, all IP addresses or hostnames or IP address ranges are used in this ACL.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant.
Network Service Alias	The service alias is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $ character and containing one special character) and include the protocol as relevant. Selecting either tcp or udp displays an additional set of specific TCP/UDP source and destinations port options.
Source Port	If using either *tcp* or *udp* as the protocol, define whether the source port for incoming IP ACL rule application is any, equals or an administrator defined range. If not using *tcp* or *udp*, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting *equals* invokes a spinner control for setting a single numeric port. Selecting *range* displays spinner controls for Low and High numeric range settings. A source port cannot be a destination port.

Destination Port	If using either *tcp* or *udp* as the protocol, define whether the destination port for incoming IP ACL rule application is any, equals or an administrator defined range. If not using *tcp* or *udp*, this setting displays as N/A. This is the data local origination virtual port designated by the administrator. Selecting *equals* invokes a spinner control for setting a single numeric port. Selecting *range* displays spinner controls for Low and High numeric range settings.
ICMP Type	Selecting ICMP as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric type. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
ICMP Code	Selecting ICMP as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding code, helpful for troubleshooting network issues (*0 - Net Unreachable*, *1- Host Unreachable*, *2 - Protocol* Unreachable etc.).
Start VLAN	Select a Start VLAN icon within a table row to set (apply) a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
End VLAN	Select an End VLAN icon within a table row to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
Protocol	Select the protocol to filter for this ACL. Use the drop down to select from a list of predefined protocol or use the spinner control to set a particular protocol number.
Mark	Select this option to mark certain fields inside a packet before allowing them. Mark is only applicable for *Allow* rules. Mark sets the rule's 802.1p or dscp level (from 0 - 7).
Log	Select this option to create a log entry that a firewall rule has allowed a packet to be either denied or allowed.
Enable	Select this option to enable or disable this particular IP Firewall rule in this rule set.
Description	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a Select Columns screen used to add or remove IP ACL criteria from the table.

34 Select Add as needed to add additional IP Firewall Rule configurations. Select the Remove icon as required to remove selected IP Firewall Rules.

35 Select OK when completed to update the IP Firewall rules. Select Reset to revert back to the last saved configuration.

Setting an IP SNMP ACL Policy

"Configuring IP Firewall Rules"

SNMP performs network management functions using a data structure called a *Management Information Base* (MIB). SNMP is widely implemented but not very secure,

since 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.**

36 Expand the **IP Firewall** menu item and select **IP SNMP ACL**.

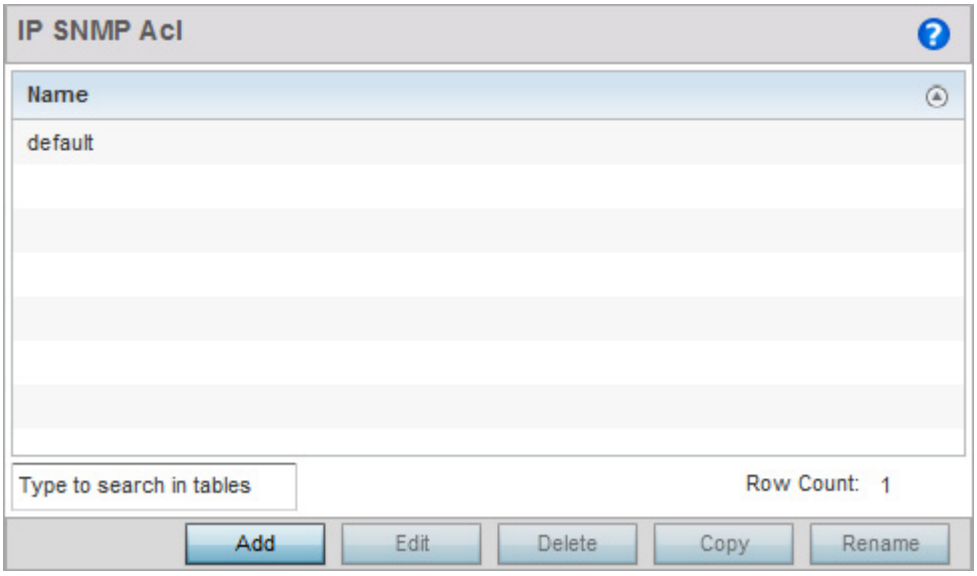


Figure 9: IP SNMP ACL screen

37 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**.

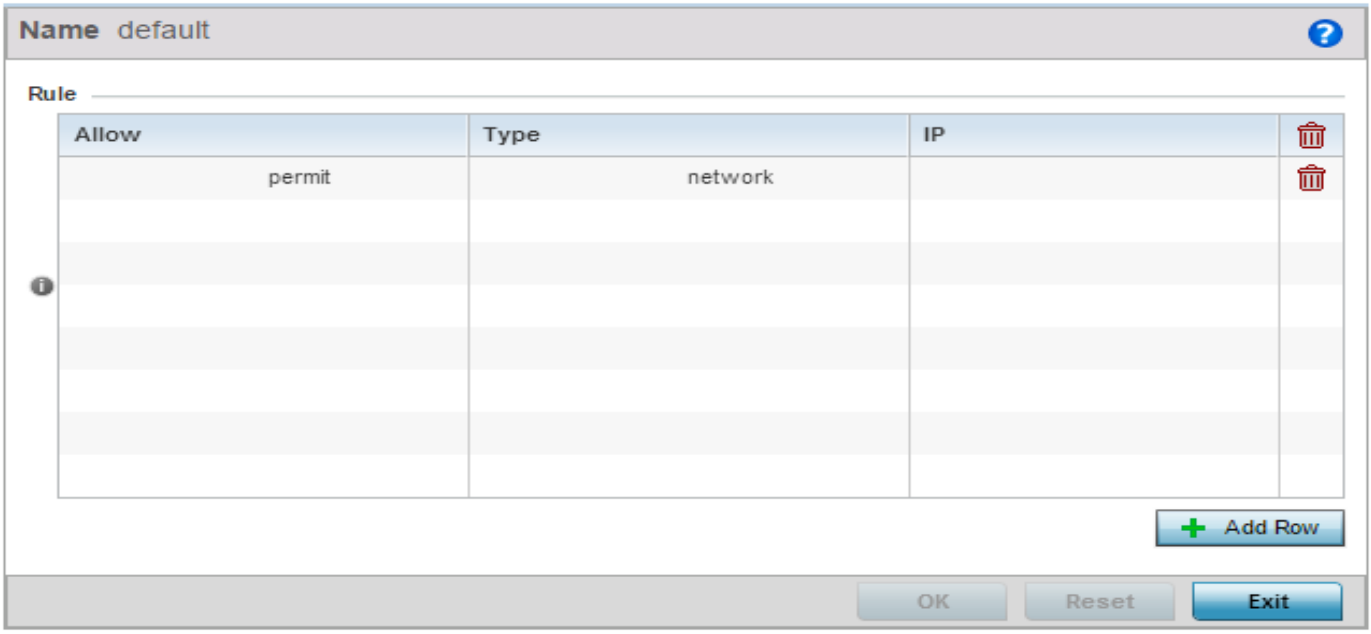


Figure 10: IP SNMP ACL Add screen

38 Provide a new IP SNMP ACL a **Name** up to 32 characters in length to help distinguish this ACL from others with similar rules.

39 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, a Network address and subnet mask or is applied to Any. The default setting is Network.
IP	If *Type* is not any, provide the IP address or host name in this field.

40 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.

41 Select **OK** when completed to update the IP Firewall rules. Select **Reset** to revert the screen back to its last saved configuration.

Setting a Network Group Alias

"Configuring IP Firewall Rules"

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.**

42 Expand the **IP Firewall** menu item and select **Network Group Alias**.

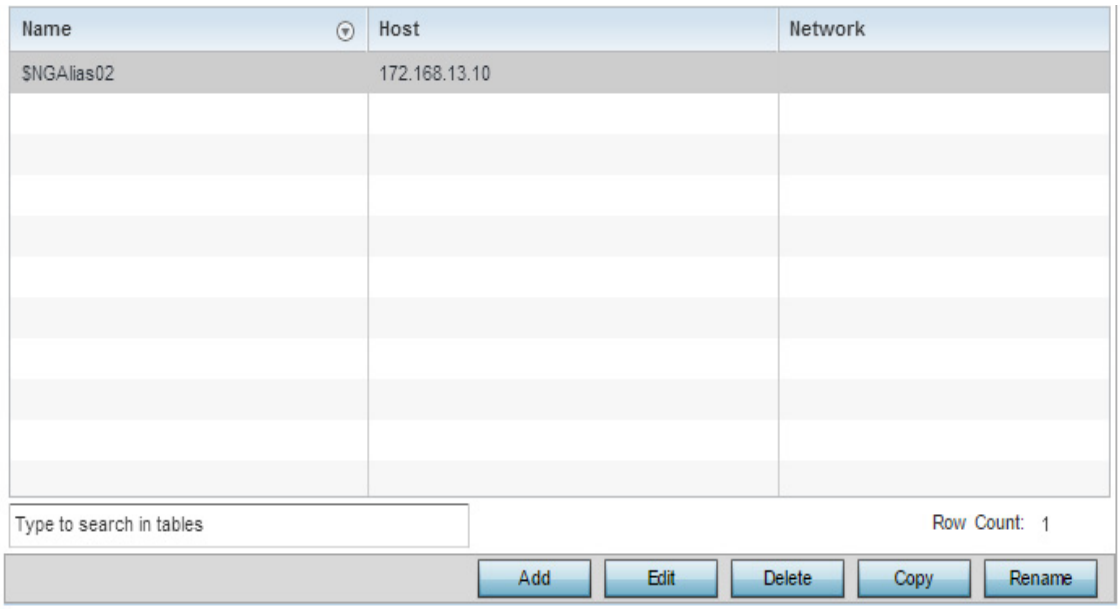


Figure 11: Network Group Alias screen

43 Select **Add** to create a new Network Group Alias. Select an existing Network Group Alias and click **Edit** to modify it. Select **Delete** to remove an existing Network Group Alias from those available in the list.

44 If creating a new Network Group Alias assign it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes. The network group alias name always starts with a dollar sign ($). Select **Reset** to revert to the last saved configuration. Select **Exit** to exit without creating a Network Group Alias.

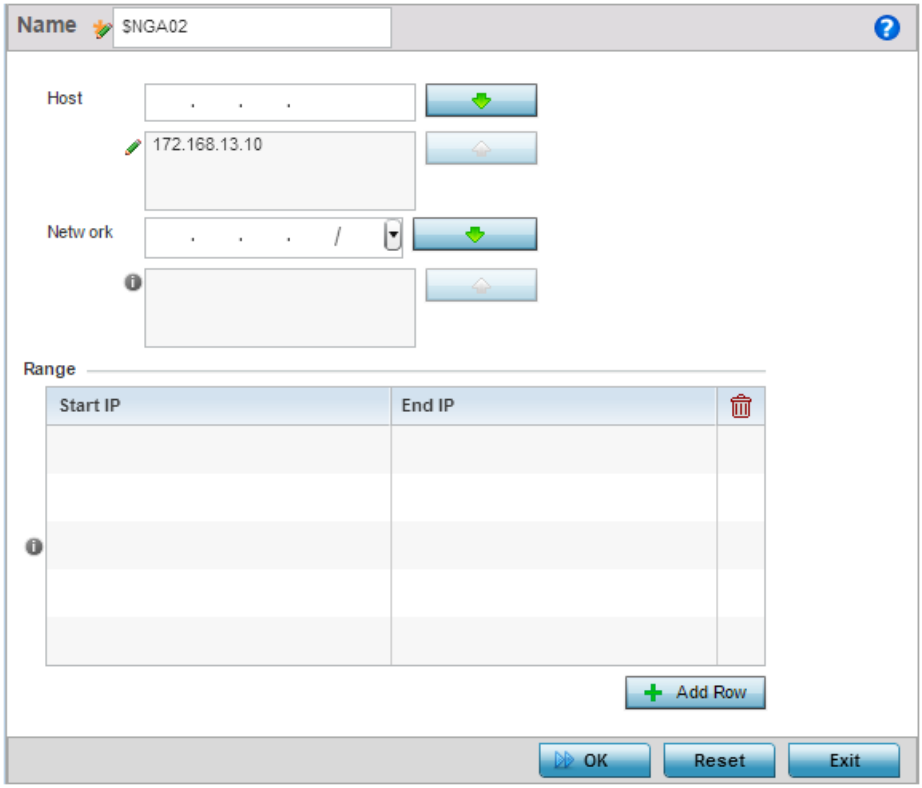


Figure 12: Network Group Alias Add screen

45 .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.

46 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 an alias range entry to edit it.

47 Select **OK** when completed to update the Network Group Alias settings. Select **Reset** to revert the screen back to its last saved configuration.

Setting a Network Service Alias

"Configuring IP Firewall Rules"

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 for an IP Firewall:

1.Select **Configuration** > **Security** > **IP Firewall.**

48 Expand the **IP Firewall** menu item and select **Network Service Alias**.

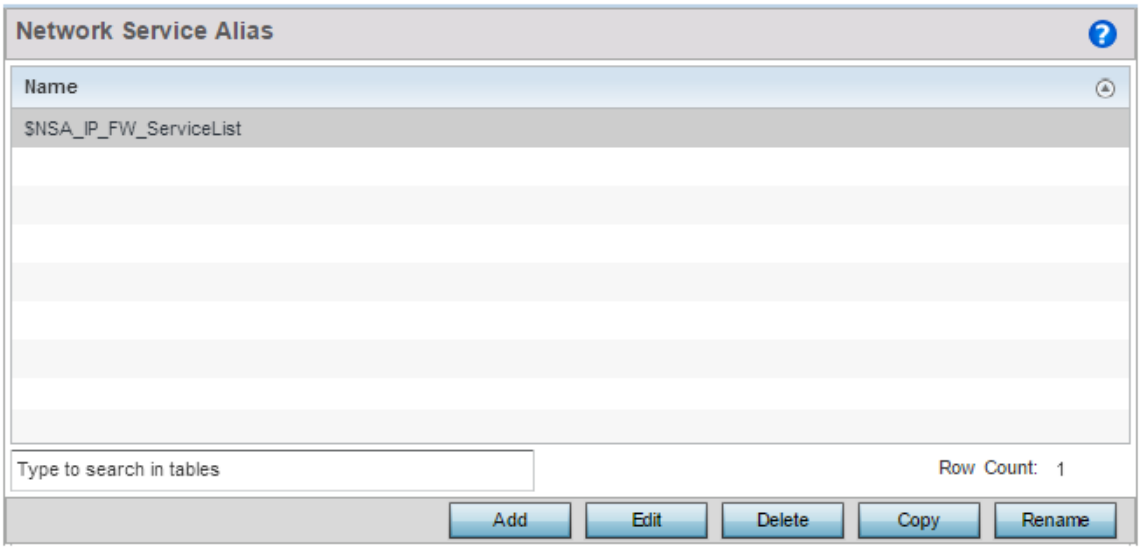


Figure 13: Network Service Alias screen

49 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.

50 If creating a new Network Service Alias assign it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes. The network group alias name always starts with a dollar sign ($). Select **Reset** to revert to the last saved configuration. Select **Exit** to exit without creating a Network Service Alias.

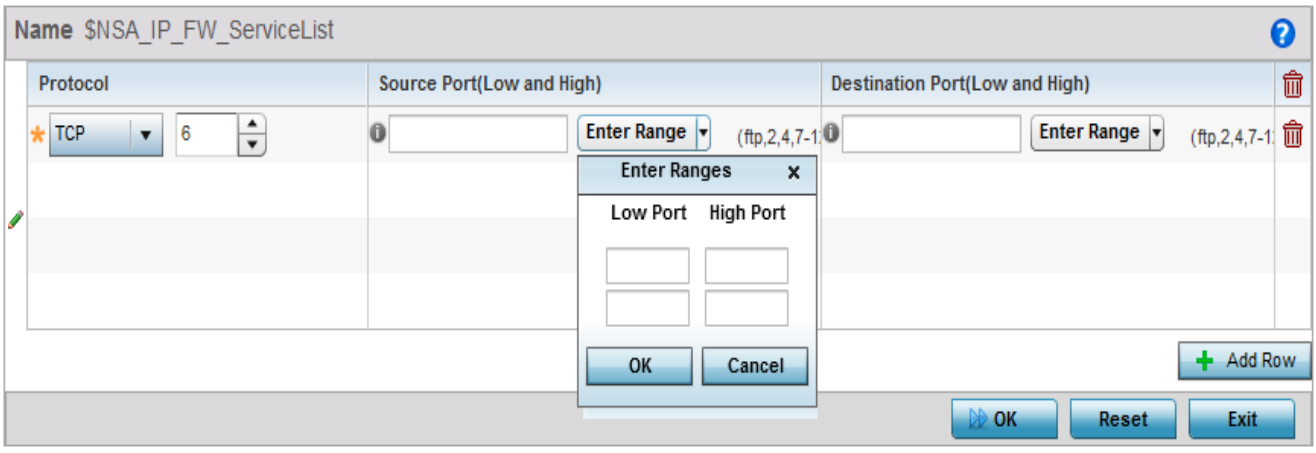


Figure 14: Network Service Alias Add screen

51 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 only relevant 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) ranges can be specified.
Destination Port (Low and High)	This field is only relevant 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.

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

53 Select **OK** when completed to update the Network Service Alias settings. Select **Reset** to revert the screen back to its last saved configuration.

Device Fingerprinting

"Security Configuration"

With the increase in popularity of *Bring Your Own Devices* (BYOD) for use in the corporate environment, there is an increase in the number of possible vectors of attacks on the network. BYOD devices are inherently unsafe as the organization does not have control on the level of security on these devices. The organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting feature enables administrators to control how BYOD devices access the network and control their access permissions.



NOTE

Ensure DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

To configure device fingerprinting:

1.Select **Configuration** tab from the Web user interface.

54 Select **Security**

55 Select **Device Fingerprinting** to display existing device fingerprinting configuration screens. The **Client Identity** screen displays:

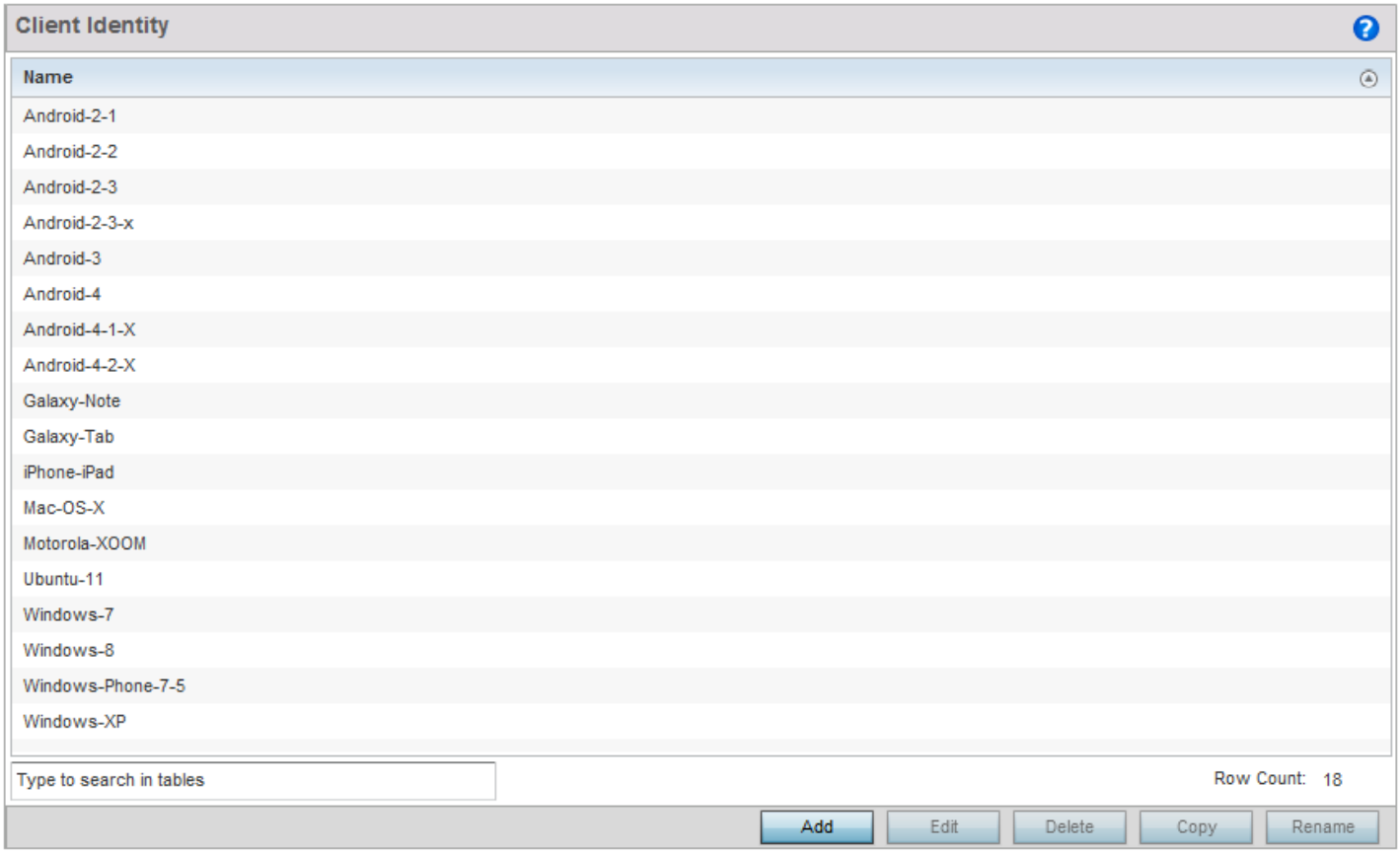


Figure 15: Security - Device Fingerprinting - Client Identity screen

56 Select **Add** to create a new client identity policy. Client identity policies configure the signatures used to identify clients and then use these signatures to classify and assign permissions to them. A set of pre-defined client identities are included.

Click **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

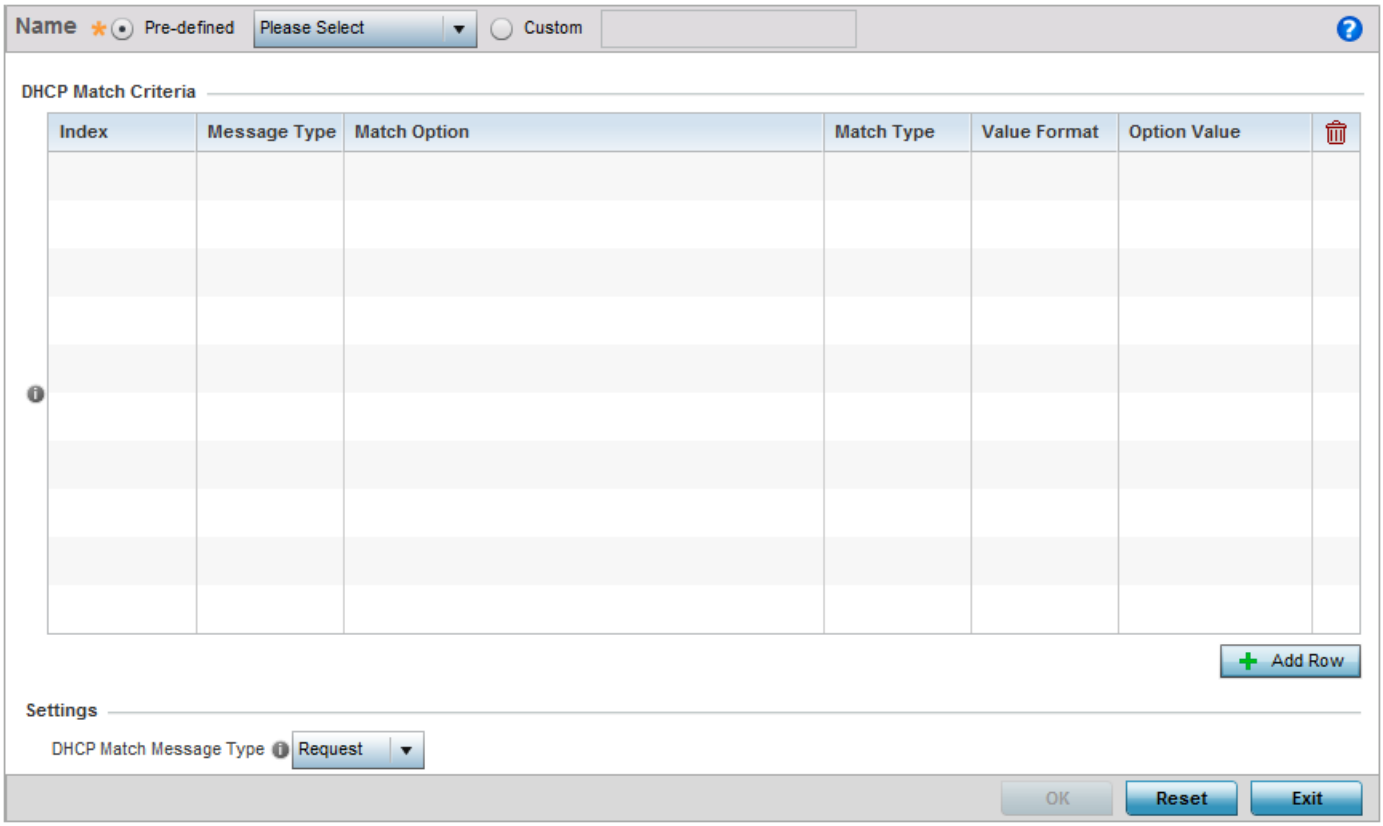


Figure 16: Security - Device Fingerprinting - New Client Identity screen

57 Select **Pre-defined** and use the drop-down menu to select from a list of pre-defined client identities. Once a client identity is selected from the drop-down menu, the **DHCP Match Criteria** field is populated with the fingerprints for the selected client identity.

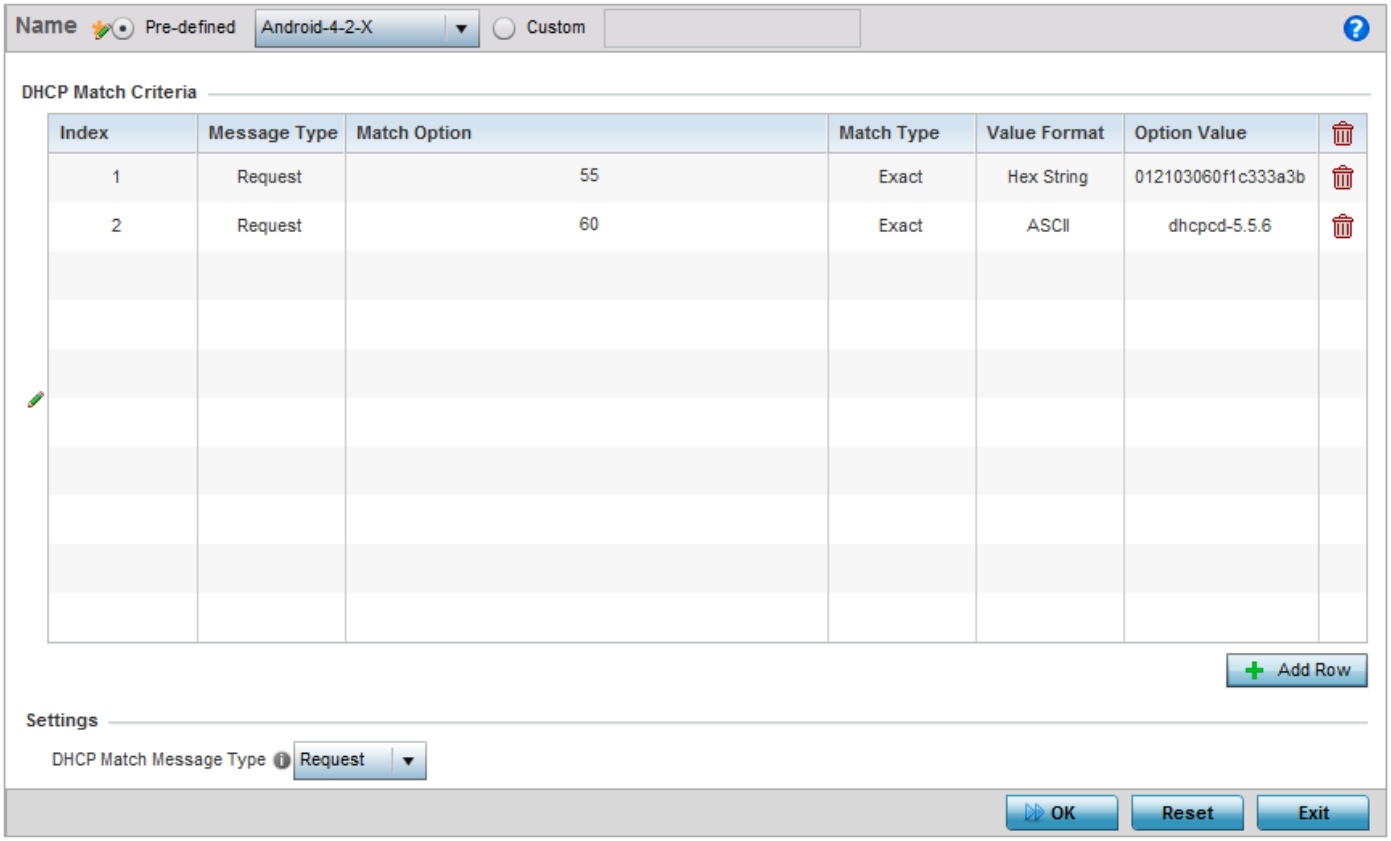


Figure 17: Security - Device Fingerprinting - New Client Identity - Pre-defined Identity screen

58 To create a custom client identity, select **Custom** and provide a name in the adjacent field and click the **OK** button at the bottom of the screen.

59 From the **DHCP Match Message Type** drop-down menu, select the message type to match. The available options are *request*, *discover*, *any* and *all*. Use this option to select the message type on which the fingerprint is matched.

- *request* - Indicates the fingerprint is only checked with any DHCP request message received from any device.
- *discover* - Indicates the fingerprint is only checked with any DHCP discover message received from any device.
- *any* - Indicates the fingerprint is checked with either the DHCP request or the DHCP discover message.
- *all* - Indicates the fingerprint is checked with both the DHCP request and DHCP discover message.

60 Click the **Add Row** to add a new signature to include in the client identity.

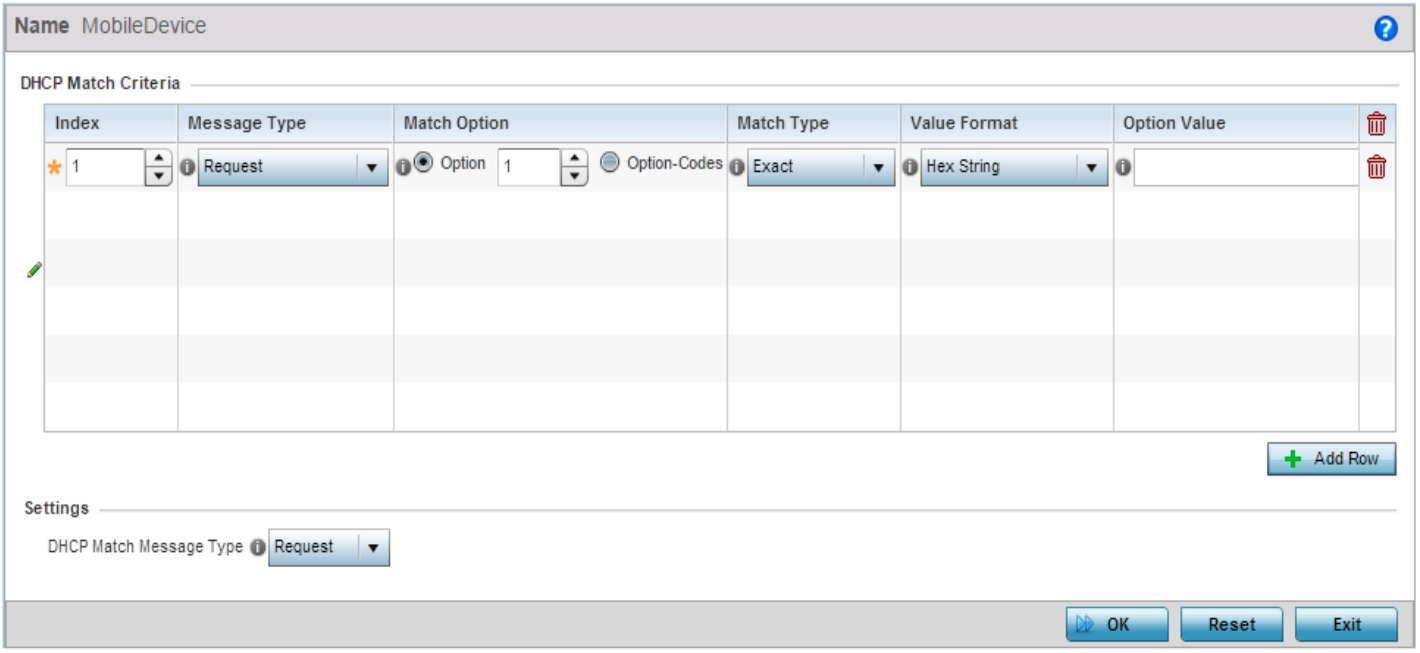


Figure 18: Security - Device Fingerprinting - Client Signature screen

61 Provide the following information for each device signature:

Index	Use the spinner control to assign an index for this signature. A maximum of 16 signatures can be created in each Client Identity.
Message Type	Use the drop-down menu to designate the DHCP message to look for the signatures. • *Request* – look for signature in the DHCP request messages. • *Discover* – look for signature in the DHCP discover messages.
Match Option	The *Match Option* field contains the following options: • *Option-Codes* – This indicates that the Option Codes passed in the DHCP request/discover message is used for matching. Options are passed in the DHCP discover/request messages as *Option Code, Option Type, Option Value* sets. When *Option Codes* is selected, all the Option Code passed in the DHCP discover/request are extracted and a fingerprint is derived. This derived fingerprint is used to identify the device. • *Option* – This indicates that a specific DHCP Option is used to identify the device. When this option is selected, a text box is enable to input the DHCP Option that is used for fingerprinting.
Match Type	Use the drop-down menu to select how the signatures are matched. The available options are: • *Exact* – The complete signature string completely 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 a particular string specified in the *Option Value* field.
Value Format	Use the drop-down menu to select the format of the value that is being checked. The value can be either *ASCII* or *Hexa String.*
Option Value	Use this text box to set the 64 character maximum DHCP option value to match.

62 Click **Ok** to save changes. Click **Reset** to revert all changes made to this screen.

Click **Exit** to close the *Client Identity* screen.

63 From the main menu on the left, select **Client Identity Group** item.

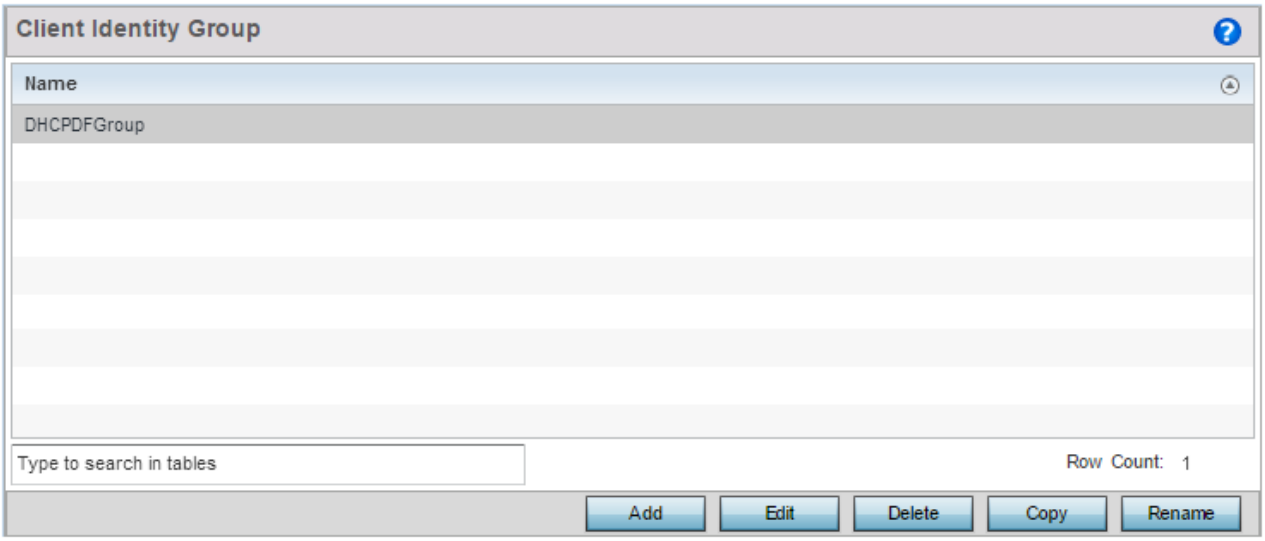


Figure 19: Security - Device Fingerprinting - Client Identity Group

Client Identity Group is a collection of *Client Identities*. Each client identity included in a client identity group is set a priority value that indicates the priority for that identity when device fingerprinting.

Device fingerprinting relies on specific information sent by a wireless client when acquiring IP address and other configuration information from a DHCP server. The feature uses the DHCP options sent by the wireless client in the DHCP request or discover packets to derive a unique signature specific to the class of devices. For example, Apple devices have a different signature from Android devices. This unique signature can then be used to classify the devices and assign permissions and restrictions on each device class.

64 Select **Add** to create a new *Client Identity Group* policy. Client Identity Group policies configure the signatures used to identify clients and then use these signatures to classify and assign permissions to them.

Click **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

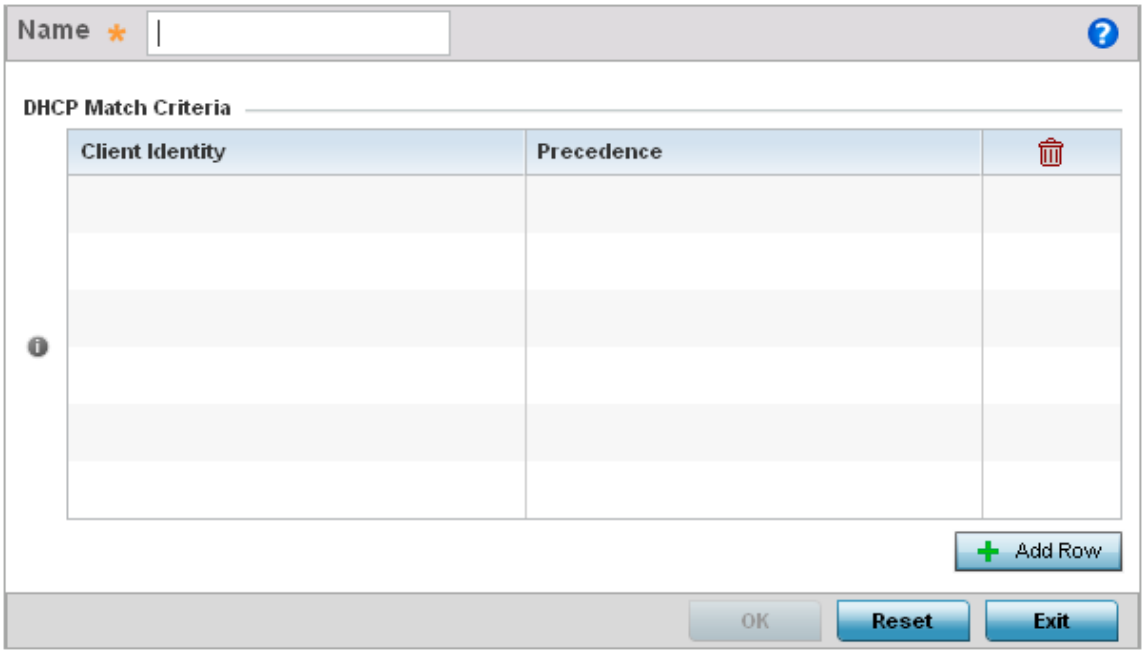


Figure 20: Security - Device Fingerprinting - Client Identity Group - New Client Identity Group

65 Provide a name in the **Name** field for the new client identity and click the **OK** button at the bottom of the screen.

66 Click the **Add Row** to add a new signature included in the client identity.

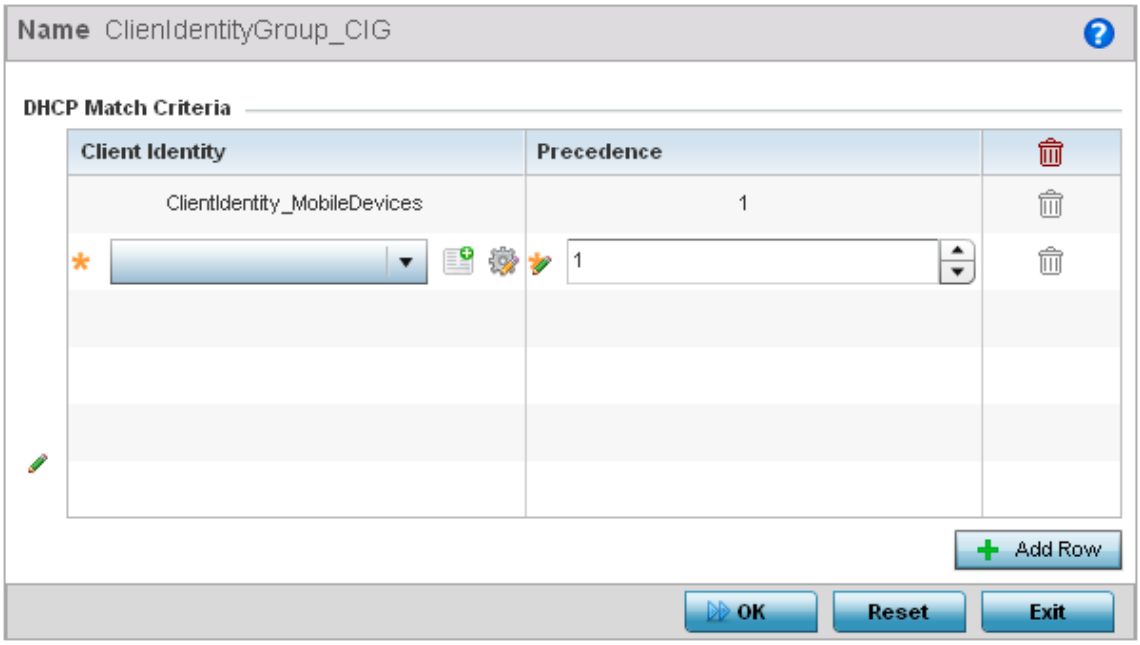


Figure 21: Security - Device Fingerprinting - Client Identity Group - New Client Identity Group

67 From the drop-down, select the *Client Identity Policy* to include in this group. Use the buttons next to the drop-down to manage and create new *Client Identity* policies.

68 Use the **Precedence** control to set the precedence for the Client Identity. This index sets the sequence the client identity in this Client Identity Group is checked or matched.

69 Click **Ok** to save changes. Click **Reset** to revert all changes made to this screen.

Click **Exit** to close the *Client Identity Group* screen.

Configuring MAC Firewall Rules

"Security Configuration"

Access points can use MAC based firewalls 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.

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** tab from the Web user interface.

70 Select **Security.**

71 Select **MAC Firewall Rules** to display existing MAC Firewall Rule policies.

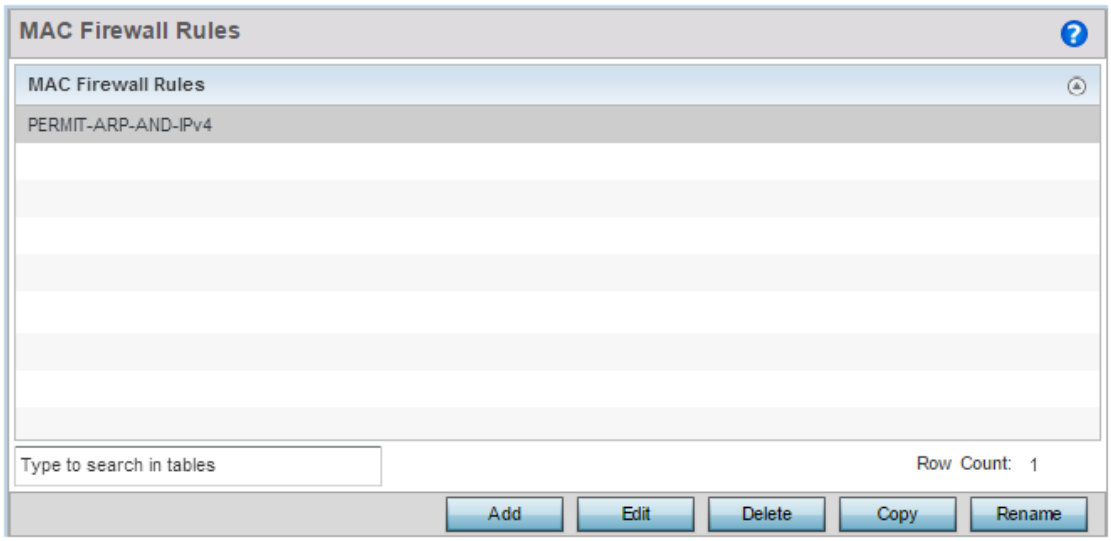


Figure 22: MAC Firewall Rules screen

72 Select **Add** to create a new MAC Firewall Rule. Select an existing policy and select **Edit** to modify the attributes of the rule's configuration.

73 Select the added row to expand it into configurable parameters for defining the MAC based firewall rule.

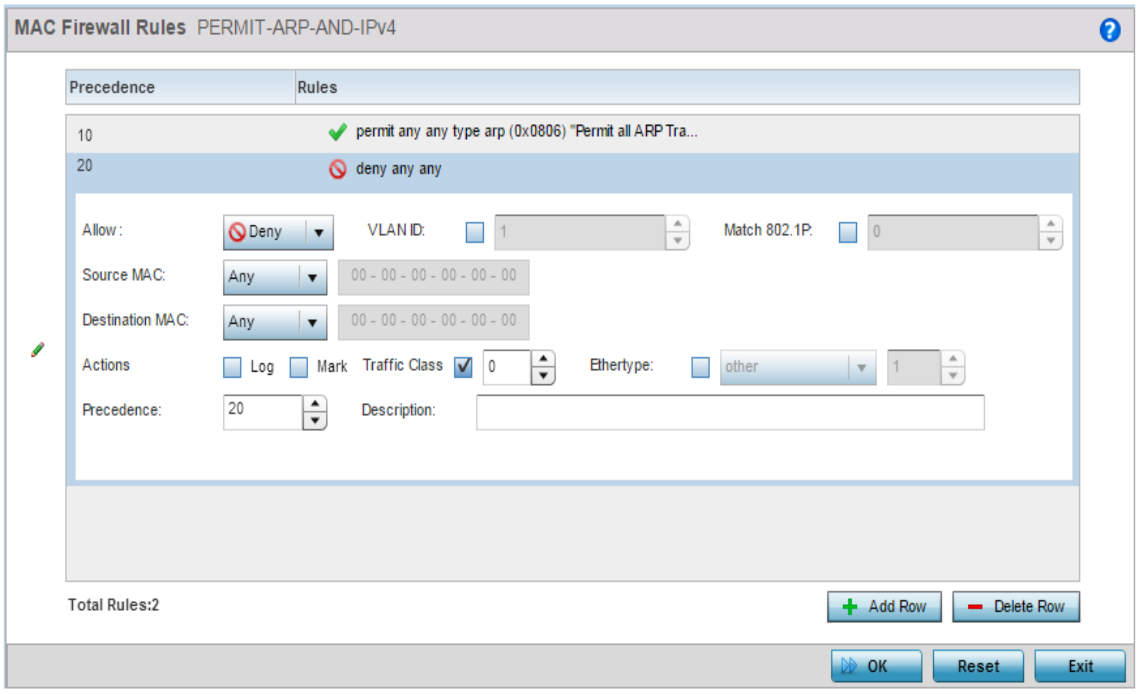


Figure 23: MAC Firewall Rules screen - Adding a new rule

74 If adding a new **MAC Firewall Rule**, provide a name up to 32 characters in length.

75 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 not to allow a packet to proceed to its destination. • *Permit* - Instructs the firewall to allow a packet to proceed to its destination.
Source MAC / Destination MAC	Enter both *Source MAC* and *Destination MAC* addresses. Access points use the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.

Actions	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
	• *Mark, Log* - Conducts both mark and log functions.

Precedence	Use the spinner control to specify a precedence for this MAC firewall rule from 1 - 5000. Rules with lower precedence are always applied first to packets.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the RADIUS server). The VLAN ID can be from 1 - 4094.
Traffic Class	Select this option to enable filtering using Traffic Class. Use the spinner control to specify a traffic class. Traffic class can be from 1 - 10.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting from 0 - 7.
Ethertype	Use the drop-down menu to specify an Ethertype of either *other, ipv4, arp, rarp, appletalk, aarp, mint, wisp,ipx, 802.1q* and *ipv6*. An Ethertype is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame.
Description	Provide a description (up to 64 characters) for the rule to help differentiate the it from others with similar configurations.

76 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.

77 Select **OK** when completed to update the MAC Firewall Rules. Select **Reset** to revert to the last saved configuration.

Wireless IPS (WIPS)

"Security Configuration"

The access point supports *Wireless Intrusion Protection Systems* (WIPS) to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. An access point

supports WIPS through the use of dedicated sensor devices designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

Unauthorized APs are untrusted and unsanctioned access points connected to a LAN that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured access points that do not adhere to corporate policies. An attacker can install a unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the middle attack or take control of wireless clients to launch denial-of-service attacks.



NOTE

WIPS is not supported natively by an AP6521 model access point and must be deployed using an external WIPS server resource.

A WIPS server can be deployed as a dedicated solution within a separate enclosure. When used with associated access point radios, a WIPS deployment provides the following enterprise class security management features:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the wireless network.
- *Rogue Detection and Segregation* - A WIPS supported network distinguishes itself by both identifying and categorizing nearby access points. WIPS identifies threatening versus non-threatening access points by segregating access points attached to the network (unauthorized APs) from those not attached to the network (neighboring access points). The correct classification of potential threats is critical for administrators to act promptly against rogues and not invest in a manual search of thousands of neighboring access points.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues though the identification and removal of their connected access points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys.

To define an access point's WIPS configuration:

1 Select **Configuration** tab from the Web user interface.

2 Select **Security**

3 Select **Wireless IPS** to display existing Wireless Intrusion Protection policy.

The **Wireless IPS** screen displays the **Settings** tab by default.

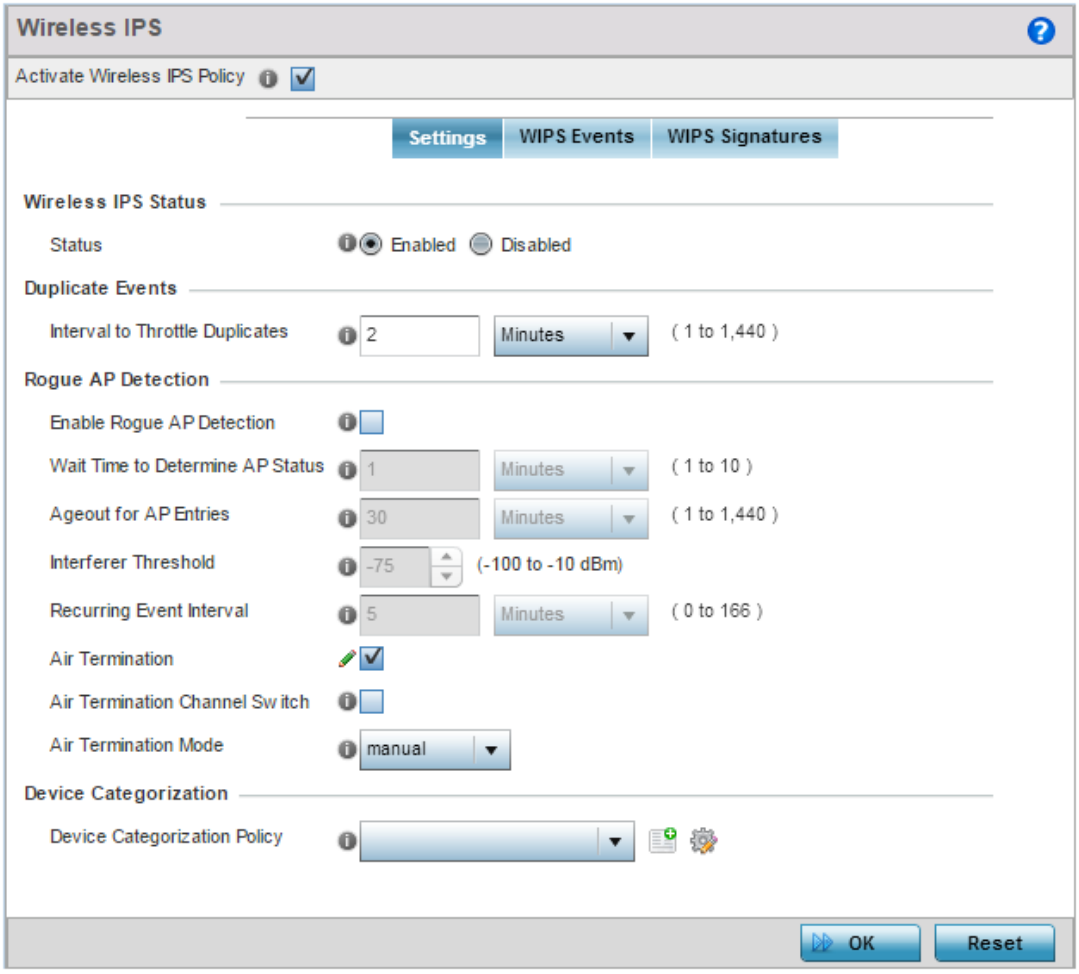


Figure 24: Wireless IPS screen - Settings tab

4 Select the **Activate Wireless IPS Policy** option on the upper left-hand side of the screen to enable the screen's parameters for configuration. Ensure this option stays selected to apply the configuration to the access point profile.

5 Within the **Wireless IPS Status** field, select either *Enabled* or *Disabled* to activate or de-activate WIPS. The default setting is enabled.

6 Enter an **Interval to Throttle Duplicates** in either *Seconds* (1 - 86,400), *Minutes* (1 - 1,400), *Hours* (1 - 24) or *Days* (1). This interval represents the duration event duplicates are *not* stored in history. The default setting is 120 seconds.

7 Refer to the **Rogue AP Detection** field to define the following detection settings for this WIPS policy:

Enable Rogue AP Detection	Select the check box to enable the detection of unsanctioned APs from this WIPS policy. The default setting is disabled.
Wait Time to Determine AP Status	Define a wait time in either *Seconds* (10 - 600) or *Minutes* (0 - 10) before a detected AP is interpreted as a rogue (unsanctioned) device, and potentially removed. The default interval is 1 minute.
Ageout for AP Entries	Set the interval the WIPS policy uses to ageout rogue devices. Set the policy in either Seconds (30 - 86,400), Minutes (0- 1,440), Hours (1 - 24) or Days (1). The default setting is 5 minutes.
Interferer Threshold	Specify a RSSI threshold (from -100 to -10 dBm) after which a detected access point is classified as an interferer (rogue device).
Recurring Event Interval	Set an interval that, when exceeded, duplicates a rogue AP event if the rogue devices is still active (detected) in the network. The default setting is 5 minutes.
Air Termination	Select this option to enable the termination of detected rogue AP devices. Air termination lets you terminate the connection between your wireless LAN and any access point or client associated with it. If the device is an access point, all clients dis-associated with the access point. If the device is a client, its connection with the access point is terminated. This setting is disabled by default.
Air Termination Channel Switch	Select this option to allow neighboring access point to switch channels for rogue AP termination. This setting is disabled by default.
Air Termination Mode	If termination is enabled, use the drop-down menu to specify the termination mode used on detected rogue devices. The default setting is manual.

8 Refer to the **Device Categorization** field to associate a Device Categorization Policy with this Wireless IPS policy.

Select the **Add** icon to create a new Device Categorization policy, or select the **Edit** icon to modify an existing Device Categorization policy. For more information on Device Categorization, see "Device Categorization" on page 755.

9 Select **OK** to update the settings. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

10 Select the **WIPS Events** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters. This option need to remain selected to apply the WIPS configuration to the access point profile.

The **Excessive** tab displays by default, with additional **MU Anomaly** and **AP Anomaly** tabs also available.

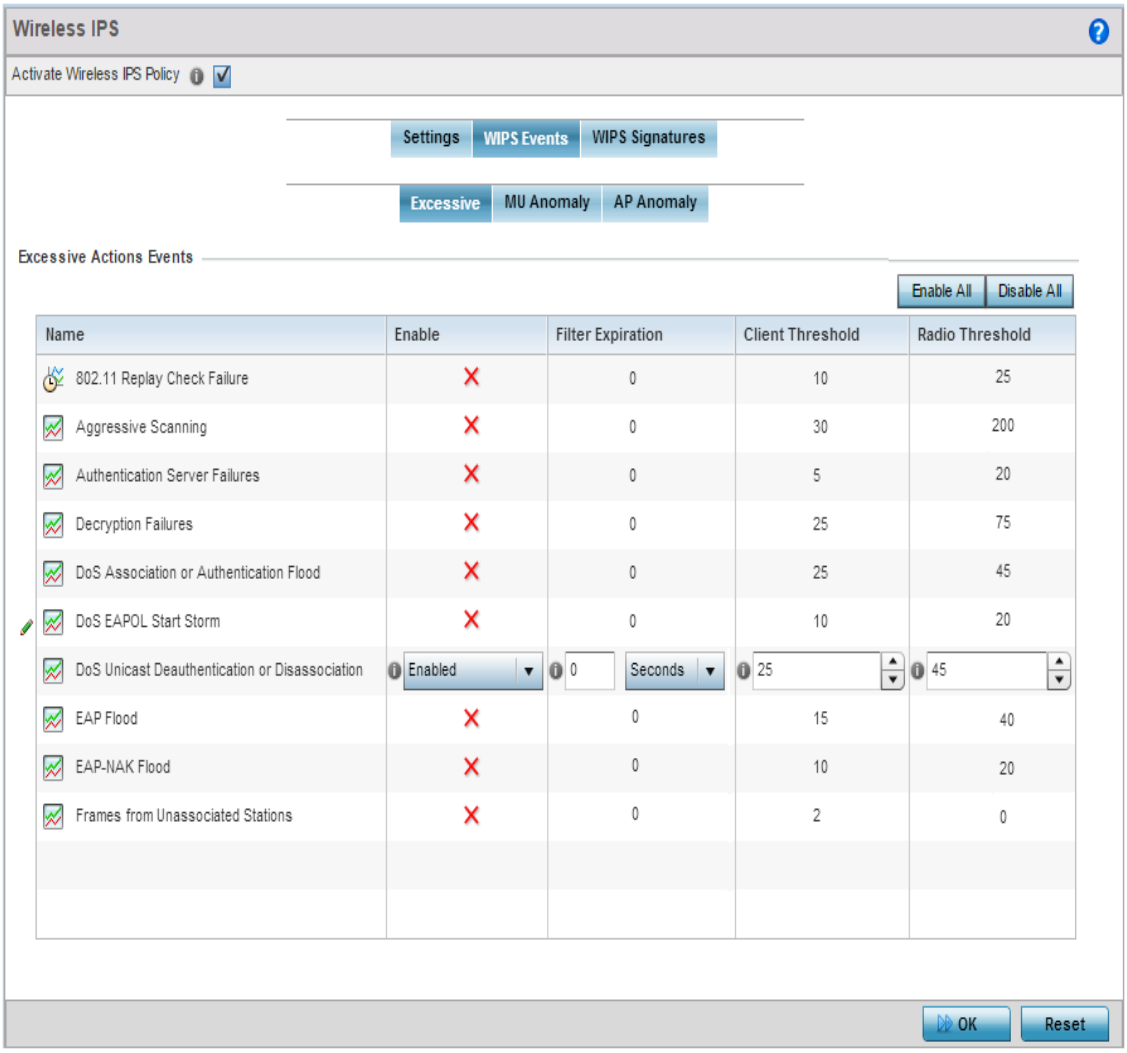


Figure 25: Wireless IPS screen - WIPS Events - Excessive tab

The **Excessive** tab lists events with the potential of impacting network performance. An administrator can enable or disable event filtering and set the thresholds for the generation of the event notification and filtering action.

An *Excessive Action Event* is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the **Excessive Actions Events** table to select and configure the action taken when events are triggered.

11 Set the following **Excessive Action Event** configurations:

Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default.
Filter Expiration	Set the duration an event generating client is filtered. This creates a special ACL entry, and frames coming from the client are dropped. The default setting is 0 seconds. This value is applicable across the RF Domain. If a station is detected performing an attack and is filtered by an access point, the information is passed to the domain controller. The domain controller then propagates this information to all the access points in the RF Domain.
Client Threshold	Set the client threshold after which the filter is triggered and an event generated.
Radio Threshold	Set the radio threshold after which an event is recorded to the event history.

Use the **Enable All** button to enable all Excessive Action Events. Use **Disable All** button to disable all Excessive Action Events.

12 Select **OK** to save the updates to the to Excessive Actions configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

13 Select the **MU Anomaly** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

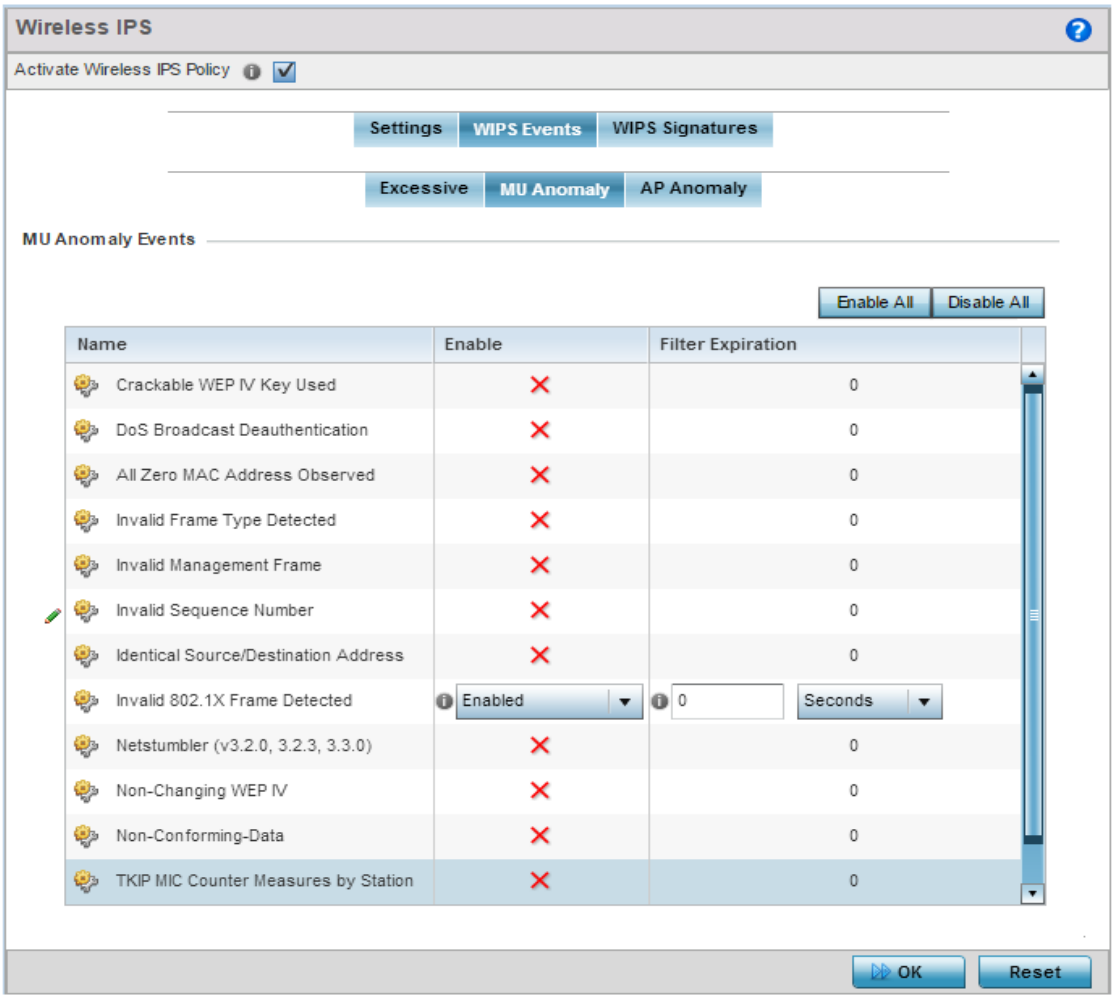


Figure 26: Wireless IPS screen - WIPS Events - MU Anomaly tab

MU Anomaly events are suspicious events by wireless clients that can compromise the security and stability of the network. Use the MU Anomaly screen to set the intervals clients can be filtered upon the generation of each event.

14 Set the following **MU Anomaly Event** configurations:

Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each MU Anomaly event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold. A red “X” defines the event as disabled, and not tracked by the WIPS policy. Each event is disabled by default.
Filter Expiration	Set the duration a client is filtered. This creates a special ACL entry, and frames coming from the client are silently dropped. The default setting is 0 seconds. For each violation, define a time to filter value (in seconds) which determines how long received packets are ignored from an attacking device once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.

Use the **Enable All** button to enable all MU Anomaly Rules. Use **Disable All** button to disable all MU Anomaly Rules.

15 Select **OK** to save the updates to the MU Anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

16 Select the **AP Anomaly** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

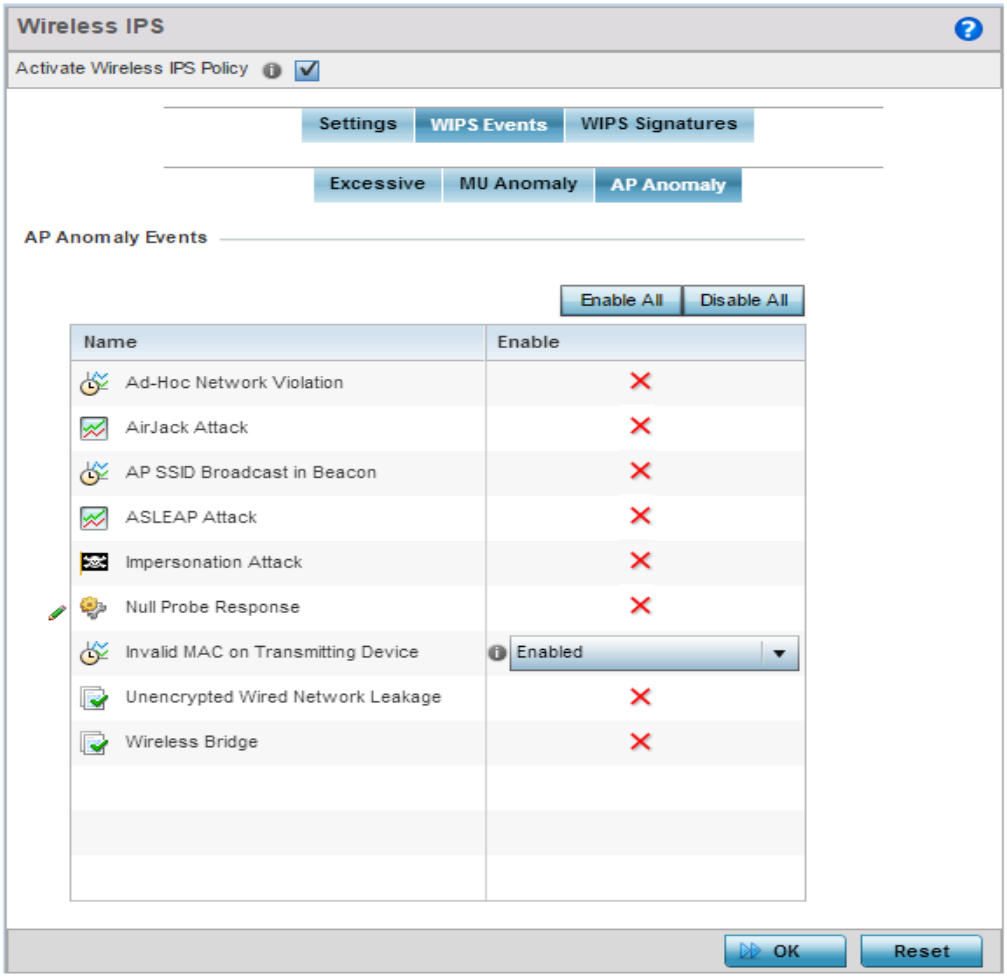


Figure 27: Wireless IPS screen - WIPS Events - AP Anomaly tab

AP Anomaly events are suspicious frames sent by neighboring APs. Use the **AP Anomaly** tab to enable or disable an event.

17 Enable or disable the following **AP Anomaly Events**:

Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each AP Anomaly event. Use the drop-down menu to enable/disable events as required. A green check mark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default.

Use the **Enable All** button to enable all AP Anomaly Events. Use **Disable All** button to disable all AP Anomaly Events.

18 Select **OK** to save the updates to the AP Anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked at any point in the configuration process by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

19 Select the **WIPS Signatures** tab. Ensure the **Activate Wireless IPS Policy** option remains selected to enable the screen's configuration parameters.

A WIPS signature is the set or parameters, or pattern, used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them.

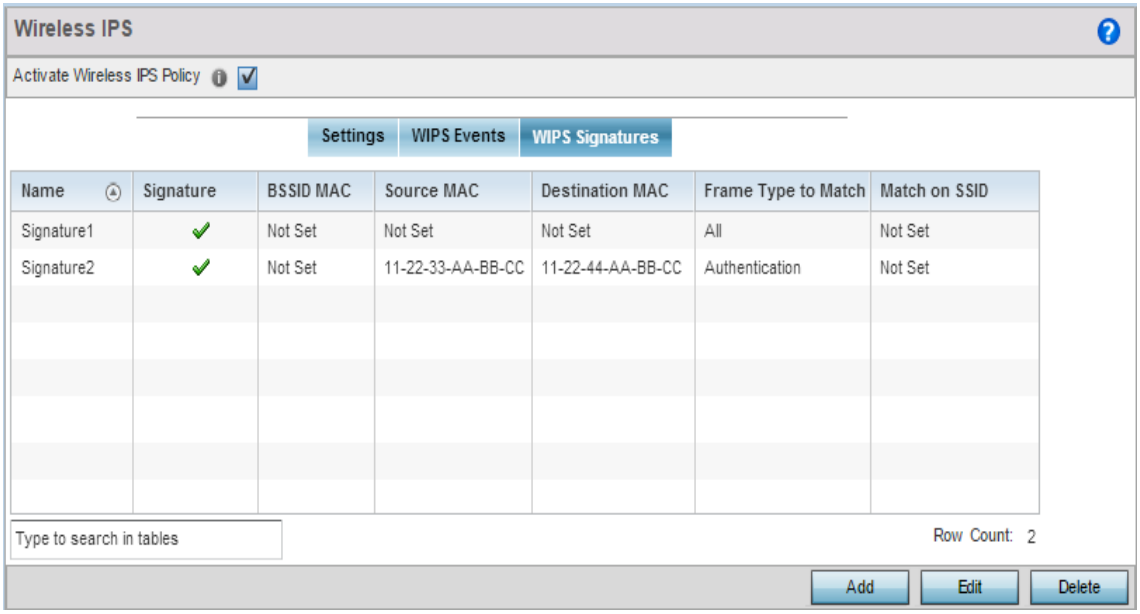


Figure 28: Wireless IPS screen - WIPS Signatures tab

20 The **WIPS Signatures** tab displays the following read-only configuration data:

Name	Lists the name assigned to each signature when it was created. A signature name cannot be modified as part of the edit process.
Signature	Displays whether the signature is enabled. A green checkmark defines the signature as enabled. A red "X" defines the signature as disabled. Each signature is disabled by default.
BSSID MAC	Displays each BSS ID MAC address used for matching purposes.
Source MAC	Displays each source packet MAC address for matching purposes.
Destination MAC	Displays each destination packet MAC address for matching purposes.
Frame Type to Match	Lists the frame types specified for matching with the WIPS signature.
Match on SSID	Lists each SSID used for matching purposes.

21 Select **Add** to create a new WIPS signature, **Edit** to modify the attributes of a selected WIPS signature or **Delete** to remove obsolete signatures from the list of those available.

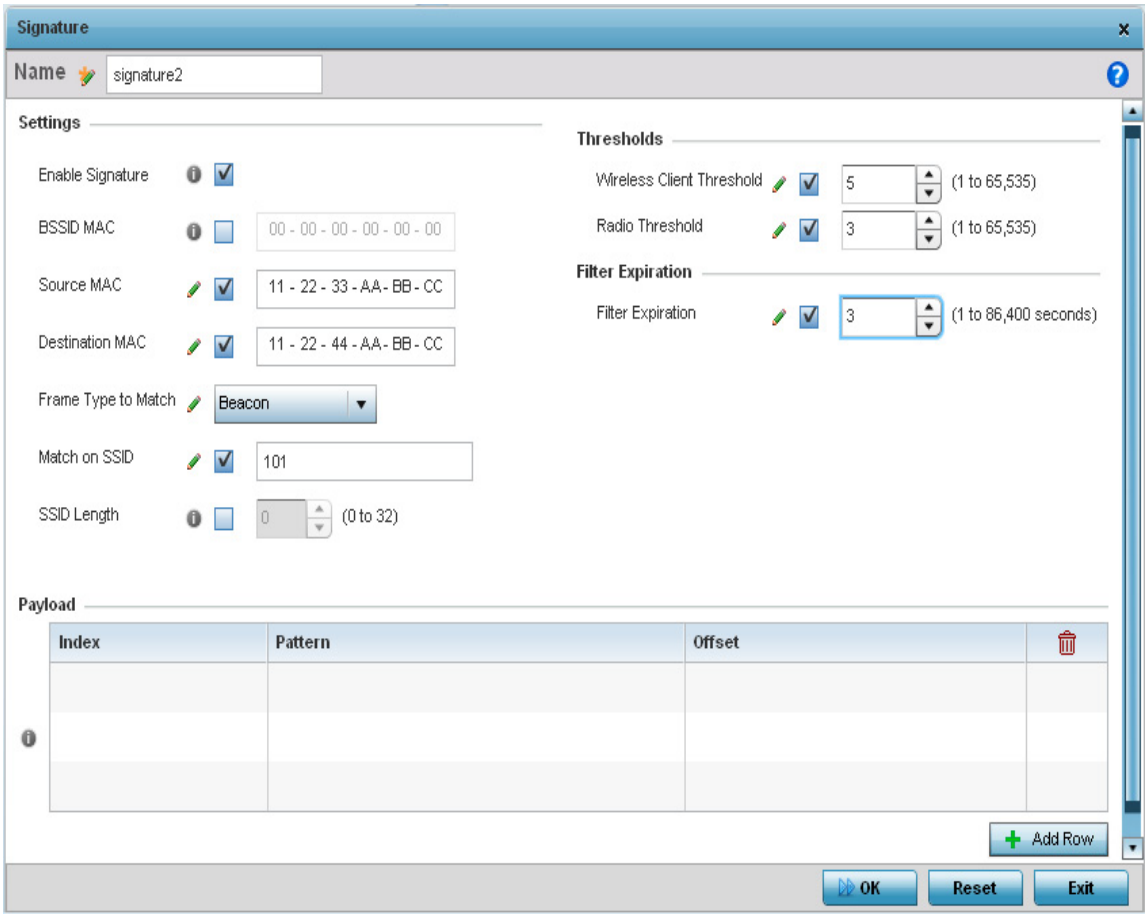


Figure 29: WIPS Signature Configuration screen

22 If adding a new WIPS signature, define a **Name** to distinguish it from others with similar configurations. The name cannot exceed 64 characters.

23 Set the following network address information for a new or modified WIPS Signature:

Enable Signature	Select the radio button to enable the WIPS signature for use with the profile. The default signature is enabled.
BSSID MAC	Define a BSS ID MAC address used for matching and filtering with the signature.
Source MAC	Define a source MAC address for the packet examined for matching, filtering and potential device exclusion using the signature.
Destination MAC	Set a destination MAC address for a packet examined for matching, filtering and potential device exclusion using the signature.
Frame Type to Match	Use the drop-down menu to select a frame type for matching with the WIPS signature.
Match on SSID	Sets the SSID used for matching. Ensure it is specified properly or the SSID won't be properly filtered.
SSID Length	Set the character length of the SSID used for matching purposes. The maximum length is 32 characters.

24 Refer to **Thresholds** field to set the thresholds used as filtering criteria.

Wireless Client Threshold	Specify the threshold limit per client that, when exceeded, signals the event. The configurable range is from 1 - 65,535.
Radio Threshold	Specify the threshold limit per radio that, when exceeded, signals the event. The configurable range is from 1 - 65,535.

25 Set a **Filter Expiration** from 1 - 86,400 seconds that specifies the duration a client is excluded from radio association when responsible for triggering a WIPS event.

26 Refer to the **Payload** table to set a numerical index and offset for the WIPS signature.

27 Select **OK** to save the updates to the WIPS Signature configuration. Select **Reset** to revert to the last saved configuration. The WIPS policy can be invoked and applied to the access point profile by selecting **Activate Wireless IPS Policy** from the upper, left-hand side, of the access point user interface.

Device Categorization

"Security Configuration"

A proper classification and categorization of access points and clients can help suppress unnecessary unauthorized access point alarms, and allow an administrator to focus on alarms on devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization.

Authorized access points and clients are generally known to you and conform with your organization's security policies. Unauthorized devices are those detected as interoperating within the network, but have not been approved. These devices should be filtered to avoid jeopardizing the data managed by the access point and its connected clients. Use the **Device Categorization** screen to apply neighboring and sanctioned (approved) filters on peer access points operating in this access point's radio coverage area. Detected client MAC addresses can also be filtered based on their classification in this access point's coverage area.

To categorize access points and clients as authorized or unauthorized:

1.Select **Configuration** tab from the Web user interface.

28 Select **Security**

29 Select **Device Categorization** to display existing device categorization policies.

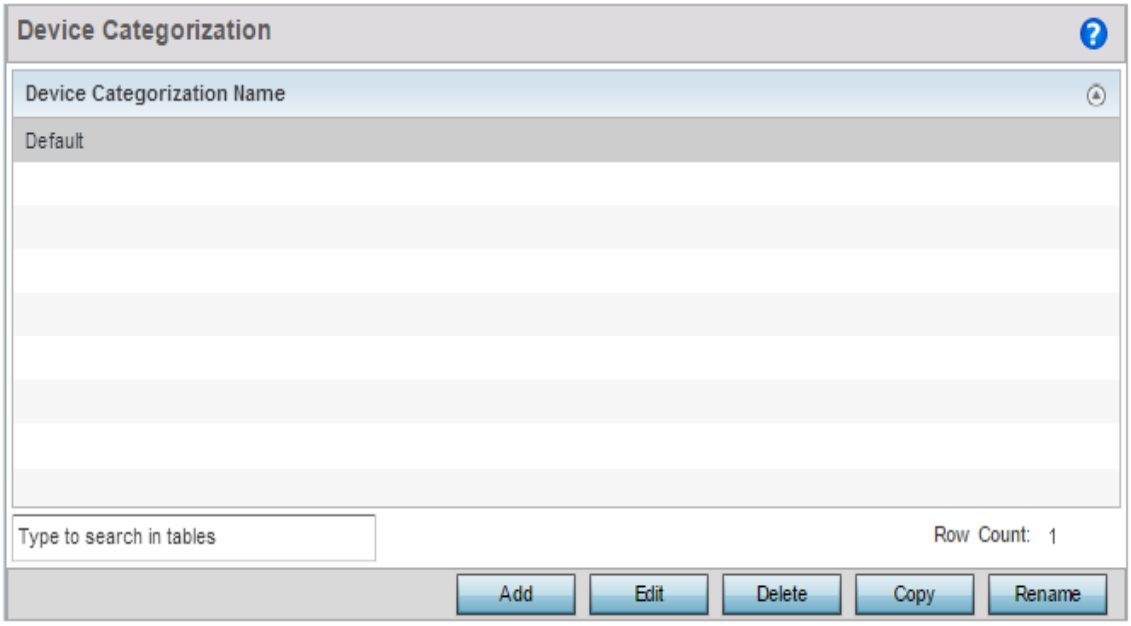


Figure 30: Device Categorization screen

The *Device Categorization* screen lists the device authorizations defined thus far.

30 Select **Add** to create a new Device Categorization policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

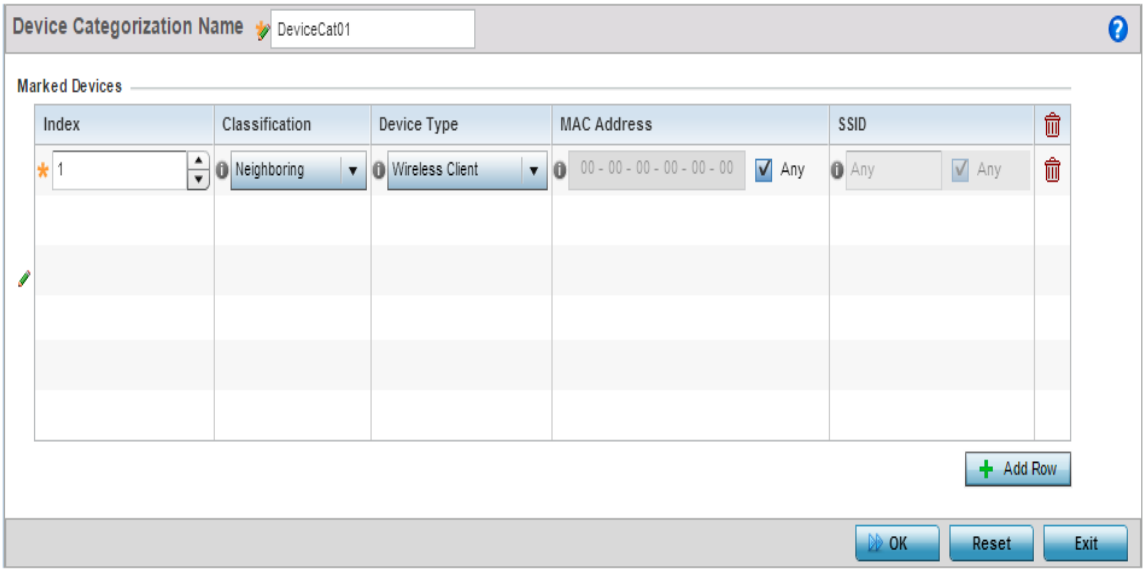


Figure 31: Device Categorization screen - Marked Devices

31 If creating a new Device Categorization filter, provide it a **Name** (up to 32 characters). Select **OK** to save the name and enable the remaining device categorization parameters.

32 Select **+ Add Row** to populate the **Marked Devices** field with parameters for classifying an access point or client and defining the target device's MAC address and SSID. Select the red (-) **Delete Row** icon as needed to remove an individual table entry.

33 Define the following parameters to add a device to a list of devices sanctioned for network operation:

Index	Use the spinner control to designate a index value to this entry. Use a value in the range 1 - 1000.
Classification	Use the drop-down menu to designate the target device as either *Sanctioned* or *Neighboring*.
Device Type	Use the drop-down menu to designate the target device as either an access point or *client*.
MAC Address	Enter the factory coded MAC address of the target device. This address is hard coded by the device manufacturer and cannot be modified. This MAC address is defined as authorized or unauthorized as part of the device categorization process.
SSID	Enter the SSID of the target device requiring categorization. The SSID cannot exceed 32 characters.

34 Select **OK** to save the updates to the **Marked Devices** List. Select **Reset** to revert to the last saved configuration.

Security Deployment Considerations

"Security Configuration"

Before defining a firewall supported configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Firewalls implement access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value.
- It's important to recognize the firewall's configuration is a mechanism for enforcing a network access policy.
- A role based firewall requires an advanced security license to apply inbound and outbound firewall policies to users and devices. Role based firewalls are not supported on AP6521 model access point.
- Firewalls cannot protect against tunneling over application protocols to poorly secured wireless clients.
- Firewalls should be deployed on WLANs implementing weak encryption to minimize access to trusted networks and hosts in the event the WLAN is compromised.
- Firewalls should be enabled when providing Captive Portal guest access. Firewalls should be applied to Captive Portal enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.
- Before configuring WIPS support, refer to the following deployment guidelines to ensure the configuration is optimally effective:
- WIPS is best utilized when deployed in conjunction with a corporate or enterprise wireless security policy. Since an organization's security goals vary, the security policy

should document site specific concerns. The WIPS system can then be modified to support and enforce these additional security policies

- WIPS reporting tools can minimize dedicated administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be to investigated and minimize the need for network monitoring.
- It is important to keep your WIPS system firmware and software up to date. A quarterly system audit can ensure firmware and software versions are current.
- Only a trained wireless network administrator can determine the criteria used to authorize or ignore devices. You may want to consider your organization's overall security policy and your tolerance for risk versus users' need for network access. Some questions that may be useful in deciding how to classify a device are:
- Does the device conform to any vendor requirements you have?
- What is the signal strength of the device? Is it likely the device is outside your physical radio coverage area?
- Is the detected access point properly configured according to your organization's security policies?
- Trusted and known access points should be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.

9 Services Configuration

The WING software supports services providing captive portal access, leased DHCP IP address assignments to requesting clients and local RADIUS client authentication.

For more information, refer to the following:

- "Configuring Captive Portal Policies"
- "Setting the DNS Whitelist Configuration"
- "Setting the DHCP Server Configuration"
- "Setting the Bonjour Gateway Configuration"
- "Setting the DHCPv6 Server Policy"
- "Setting the RADIUS Configuration"
- "Setting the URL List"

Refer to "Services Deployment Considerations" on page 824 for tips on how to optimize the access point's configuration.

Configuring Captive Portal Policies

"Services Configuration"

A *captive portal* is an access policy that provides temporary and restrictive access to the access point managed wireless network.

A captive portal policy 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 the wireless network. Once logged into the captive portal, additional *Terms and Conditions*, *Welcome* and *Fail* pages provide the administrator with a number of options on screen flow and appearance.

Captive portal authentication is used primarily for guest or visitor access to the network, 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.

Each supported access point model can support up to 32 captive portal policies, with the exception of AP6521 model, which can only support 16 captive portal policies.

Configuring a Captive Portal Policy

"Configuring Captive Portal Policies"

To configure a captive portal policy:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

The upper, left-hand, side of the user interface displays an area where *Captive Portal*, *DNS Whitelist* and *DHCP Server Policy* configuration options can be selected.

3 Select **Captive Portals**.

The **Captive Portal** screen displays the configurations of existing policies. New captive portal access policies can be created, existing policies can be modified or existing policies deleted.

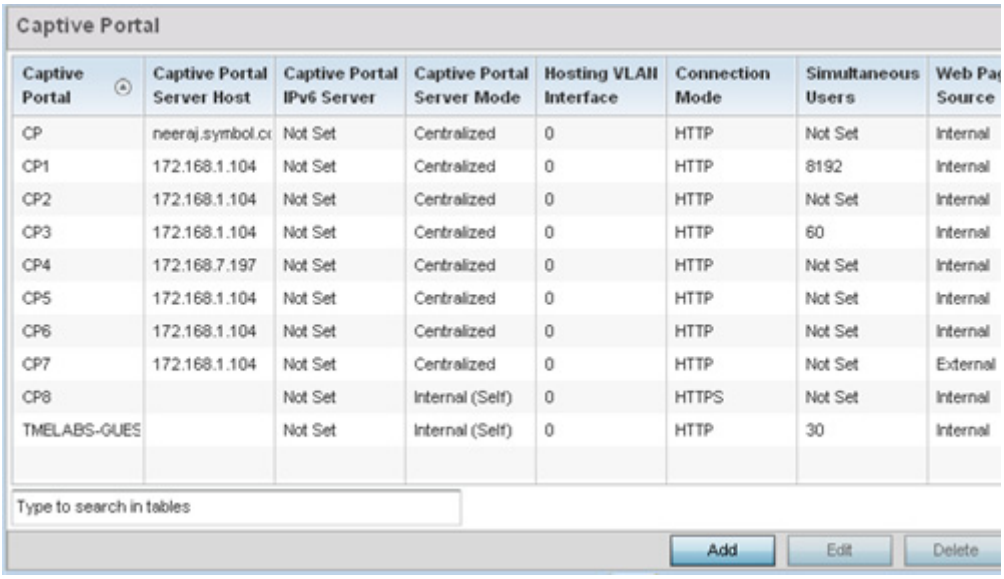


Figure 1: Captive Portal screen

4 Refer to the following captive portal policy configurations to determine whether a new policy requires creation, or an existing policy requires edit or deletion:

Captive Portal Policy	Displays the name assigned to the captive portal guest access policy when it was initially created. A policy name cannot be modified as part of the edit process.
Captive Portal Server Host	Lists the IP address (or DNS hostname) of the external (centralized) server validating guest user permissions for the listed captive portal policy.
Captive Portal IPv6 Server	Lists the IPv6 formatted IP address (non DNS hostname) of the external (fixed) IPv6 server validating user permissions for the listed captive portal policy. This item remains empty if the captive portal is hosted locally. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Captive Portal Server Mode	Lists each hosting mode as either *Internal* (Self) or *External* (centralized). If the mode is Internal (Self), the access point maintains the captive portal internally, while External (centralized) means the captive portal is running on the adopting wireless controller.

Hosting VLAN Interface	When *Centralized Server* is selected as the *Captive Portal Server Mode*, a VLAN is defined where the client can reach the controller. 0 is the default value.
Connection Mode	Lists each policy's connection mode as either *HTTP* or *HTTPS*. It is recommended to use HTTPS as it offers client transmissions a measure of data protection HTTP cannot provide.
Simultaneous Access	Displays the number of users permitted at one time for each listed policy. A captive portal can support from 0-8192 users simultaneously
Web Page Source	Displays whether the captive portal HTML pages are maintained *Internally, Externally* (on an external system you define) or are *Advanced* pages maintained and customized by the network administrator. Internal is the default setting.
AAA Policy	Lists each AAA policy used to authorize client guest access requests. The security provisions provide a way to configure advanced AAA policies that can be applied to captive portal policies supporting authentication. When a captive portal policy is created or modified, a AAA policy must be defined and applied to authorize, authenticate and account user requests.

5 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. Use **Rename** to rename an existing captive portal policy.

The **Basic Configuration** tab displays by default. Define the policy's security, access and whitelist basic configuration before defining HTML pages for guest user access.

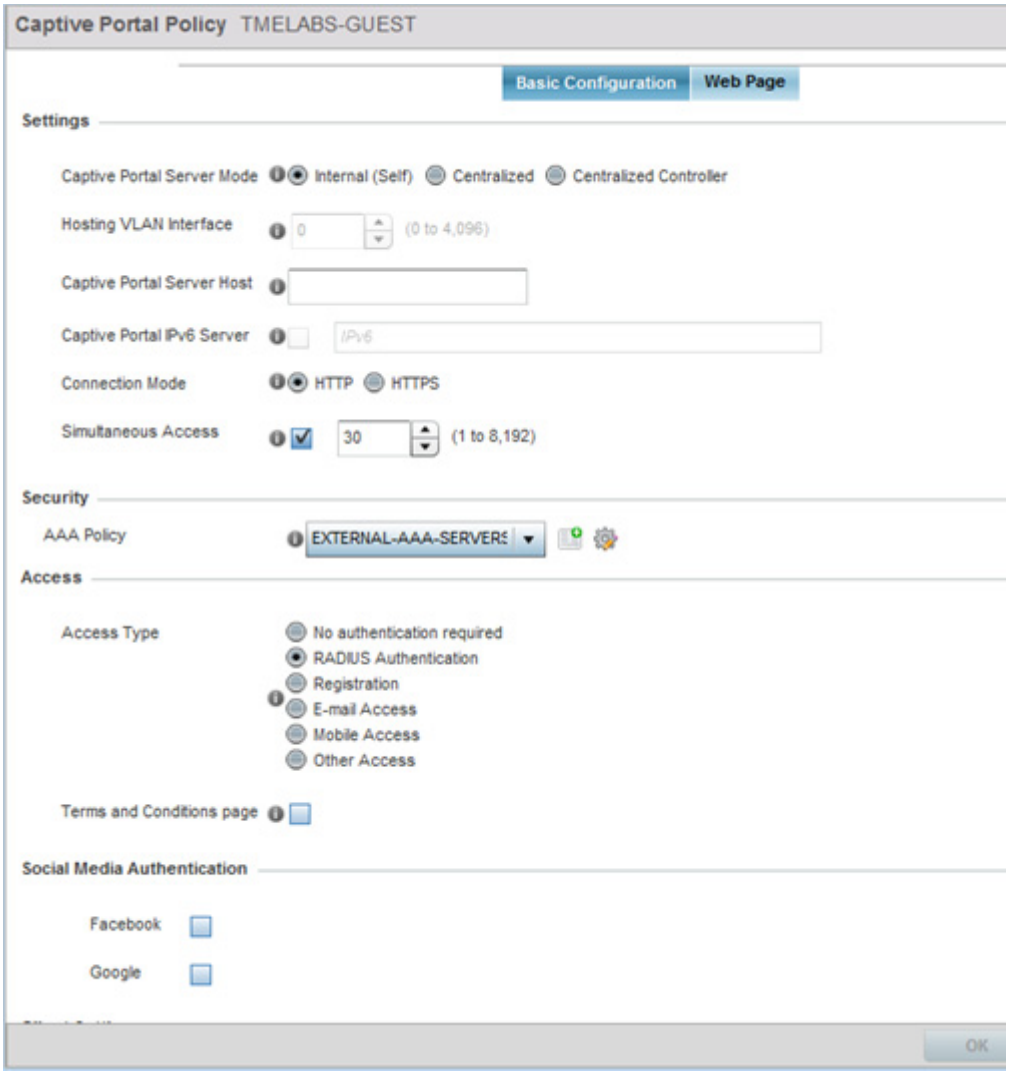


Figure 2: Captive Portal Policy screen - Basic Configuration tab

6 Define the following **Settings** for the captive portal policy:

Captive Portal Policy	If creating a new policy, assign a name representative of its access permissions, location or intended wireless client user base. If 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 *Internal* (Self), *Centralized* or *Centralized Controller*. Select Internal (Self) to maintain the captive portal configuration (Web pages) internally on the access point. Select External (Centralized) if the captive portal is supported on an external server. Select Centralized Controller for the captive portal to reside on the access point's connected Virtual Controller AP. The default value is Internal (Self).
Hosting VLAN Interface	When *Centralized Server* is selected as the *Captive Portal Server Mode*, use the spinner control to set the VLAN where the client can reach the controller. 0 is the default value.
Captive Portal Server Host	When *Centralized* is selected as the *Captive Portal Server Mode*, use this field to set the IP address or host name of the wireless controller or access point acting as the captive portal server host. When *Centralized Controller* is selected, use this field to provide the hostname of the controller or controllers acting as the captive portal server host
Captive Portal IPv6 Server	Set a numeric IP address (non DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is only available if hosting the captive portal on an External (Centralized) server resource.
Connection Mode	Select either *HTTP* or *HTTPS* to define the connection medium. It is recommended to use HTTPS, as it offers additional data protection HTTP cannot provide. The default value however is HTTP.
Simultaneous Access	Select the check box and use the spinner control to set from 1 - 8192 users (client MAC addresses) allowed to simultaneously access and use the access point's captive portal.

7 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 guest 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 selecting the **Edit** icon. For information on creating a AAA policy, see "AAA Policy" on page 663.

8 Set the following **Access** parameters to define captive portal access, RADIUS lookup information and whether the login pages contain terms that must be accepted before access is granted:

Access Type	Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Within the WiNG UI there are 6 options available. The WiNG CLI uses 5 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 and validation. • *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 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.

9 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.

10 Refer to the **Bypass** field to enable or disable **Bypass Captive Portal Detection** capabilities. When enabled, captive portal detection requests are bypassed. This feature is disabled by default.

11 Set the following **Client Settings** to define the duration clients are allowed captive portal access and when they're timed out due to inactivity:

RADIUS VLAN Assignment	Select this option to enable the RADIUS server to assign a VLAN post authentication. Once a captive portal user is authenticated, the user is assigned the VLAN as configured in the *Post Authentication VLAN* field.
Post Authentication VLAN	Use the spinner control to define the VLAN that a captive portal user is assigned once authenticated by a RADIUS server.
Client Access Time	Use the spinner control to define the duration wireless clients are allowed access to the network using the captive portal policy. 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*.

12 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 theaccess 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 disabled 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 704.

13 Use the **DNS White List** drop-down menu to use a set of allowed destination IP addresses for the captive portal. These allowed DNS destination IP addresses are called a *Whitelist*. If no whitelist entry exists with the correct set of IP addresses, select the **Create** icon (to the right of the drop-down menu) and define a new whitelist. For more information, see "Setting the DNS Whitelist Configuration" on page 773.

Each supported access point model can support up to 32 whitelists, with the exception of AP6521 model which can only support up to 16 whitelists.

To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist.

Refer to the drop-down menu of existing **DNS White List** entries to select a policy to be applied to this captive portal policy.

1 If creating a new whitelist, assign it a name up to 32 characters. Use the + Add Row button to populate the whitelist table with Host and IP Index parameters that must be defined for each whitelist entry.

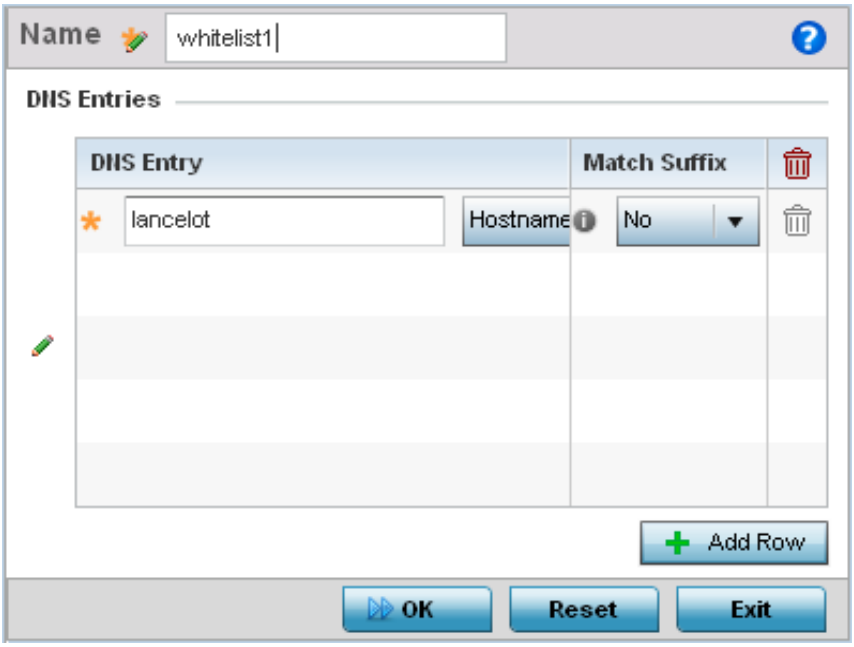


Figure 3: Captive Portal DNS Whitelist screen

a Provide a numerical IP address or Hostname within the **DNS Entry** parameter for each destination IP address or host in the whitelist.

b Use the **Match Suffix** parameter to match any hostname or domain name as a suffix. The default setting is disabled.

c If necessary, select the radio button of an existing whitelist entry and select the **- Delete** icon to remove the entry from the whitelist.

2 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 for the captive portal. When the radio button is 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 a *host name* 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.
Syslog Port	When syslog accounting is enabled, define the numerical syslog port to route traffic with the external syslog server. The default port is 514.

3 Set the following **Data Limit** parameters:

Limit	Select this option to enable limiting usage. Use the spinner to set a maximum usage limit in megabytes.
Action	Use the drop-down to configure the action to be taken once the data limit is reached. Choose from one of: • *Log Only* – Logs the event • *log-and-disconnect* – Logs the event and disconnects the user.

4 Set the following **Logout FQDN** parameters:

Logout FQDN	Configure the *fully qualified domain name* (FQDN) of the domain where the user will be redirected after logging out of the captive portal.

5 Set the following **Localization** settings to add an URL to trigger a one-time redirect demand. The configured URL is called from a mobile application to derive the location information from the wireless network so that an application can be localized to a particular store or region.

FQDN	Configure the *fully qualified domain name* (FQDN) of the page which is to be used for obtaining localization parameters for the client.
Response	Enter a response message (512 character maximum) directed back to the client for localization HTTP requests.

6 Refer to the **Destination Ports for Redirection** item, 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 is entered by the administrator.

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

8 Select the **Web Page** tab to create HTML pages requesting wireless clients use to login and navigate within the captive portal.

The **Login** page displays by default.

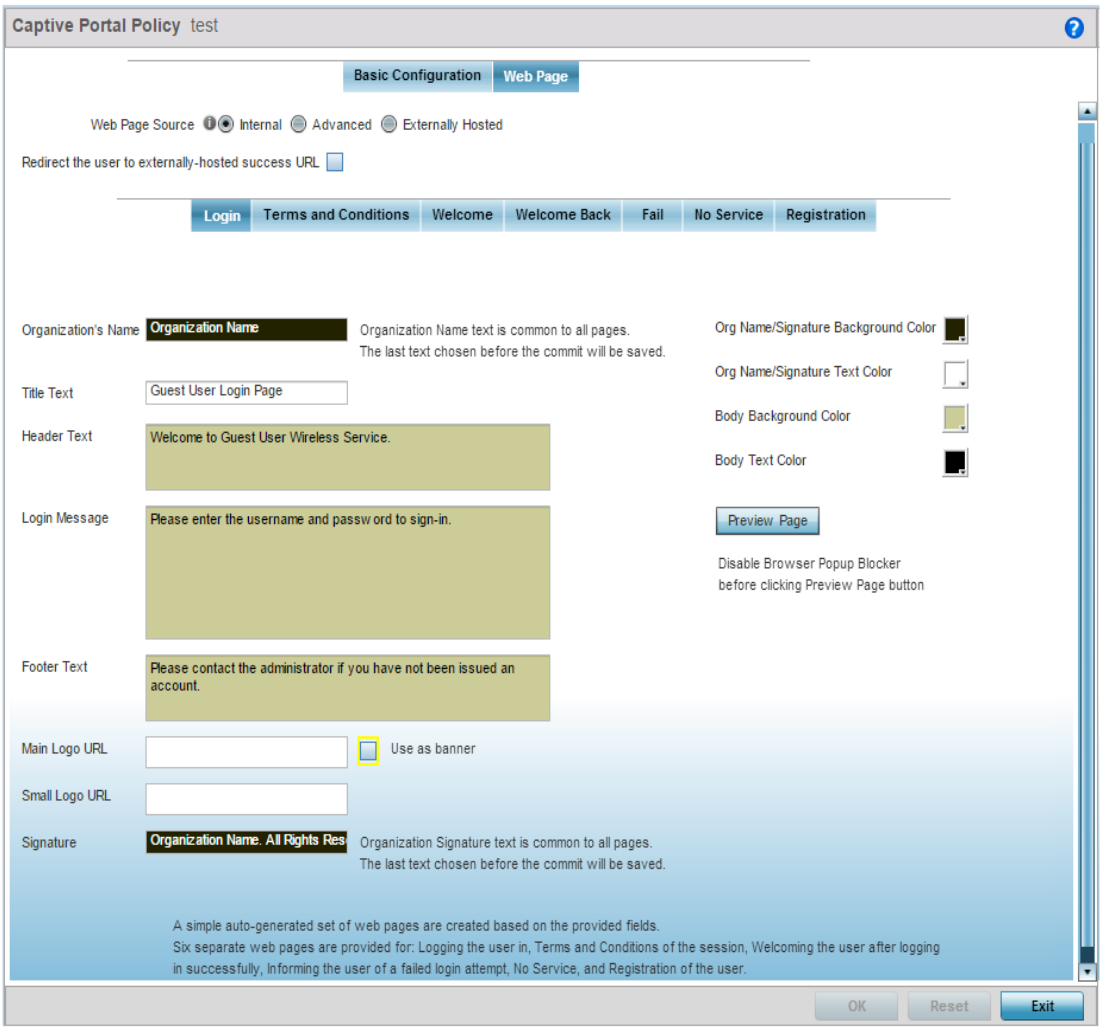


Figure 4: Captive Portal Policy screen - Web Page tab

The Login screen prompts 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 wireless client guest access is provided for the captive portal policy. The *Welcome* page asserts a user has logged in successfully and can access the captive portal. The *Fail* page asserts the authentication attempt has failed, and the user is not allowed access (using this captive portal policy) and must provide the correct login information again to access the Internet. The *No Service* page asserts that the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically re-connected to the portal.

9 Provide the following required information when creating **Login, Terms and Conditions, Welcome**, Fail and No Service pages maintained internally:

Organization's Name	If the captive portal is defined on behalf of an organization, that name can be associated as sponsoring the captive portal. This field is only displayed when configuring the *Login* page.
Title Text	Set the title text displayed on the *Login*, *Terms and Conditions*, *Welcome* and *Fail* pages when wireless clients access each page. The text should be in the form of a page title describing the respective function of each page and should be unique to each login, terms, welcome and fail 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 accessing each specific page. In the case of the Terms and Conditions page, the message can be the conditions requiring agreement before guest 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 the Login, Terms and Conditions, Welcome and Fail pages. Use the *Browse* button to navigate to the location of the target file.
Small Logo URL	The Small Logo URL is the URL for a small logo image displayed on the Login, Terms and Conditions, Welcome and Fail pages. Use the *Browse* button to navigate to the location of the target file.
Signature	Specify a signature message. This is primarily used to display copyright messages. This field is only displayed on the Login page.

10 Refer to the right-hand side of each screen to define how the **Org Name Signature Background Color**, **Org Name. Signature Text Color**, **Body Background Color** and **Body Text Color** display for current screen.

Select the box to the right of each of these four items to launch a color palette where screen colors can be selected uniquely. Select **Preview Page** to review your color selections before committing the updates to captive portal screens. Each of the *Login*, *Terms and Conditions*, *Welcome*, *Fail*, *No Service* and *Registration* screens can have their background and signature colors set uniquely.

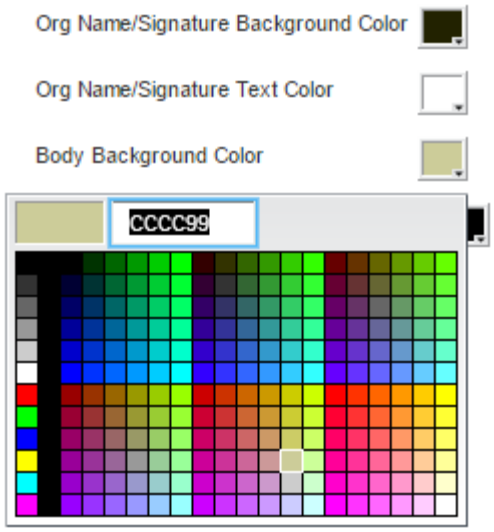


Figure 5: Captive Portal Page Color Palette screen

11 When setting the properties of the **Registration** screen, refer to the bottom portion of the screen to define email, country, gender, mobile, zip, street and name filters used as additional authentication criteria. Guest users are redirected to the registration portal on association to the captive portal SSID. Users are displayed an internal (or) externally hosted registration page where the guest user must complete the registration process if not previously registered.

These fields are customizable to meet the needs of retailers providing guest access. The captive portal sends a message to the user (on the phone number or Email address provided at registration) containing an access code. The user inputs the access code and the captive portal verifies the code before returning the Welcome page and providing access. This allows a retailer to verify the phone number or Email address is correct and can be traced back to a specific individual.

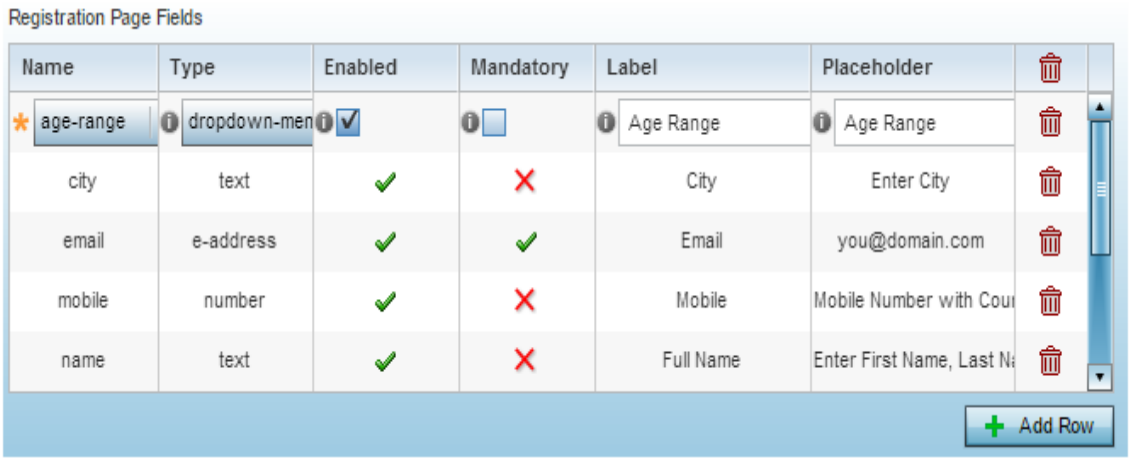


Figure 6: Registration screen customizable filters

12 Select **OK** to save the changes made within the Internal Pages screen. Selecting **Reset** reverts the settings back to the last saved configuration.

13 If hosting the captive portal on an external system, select the **Externally Hosted** radio button.

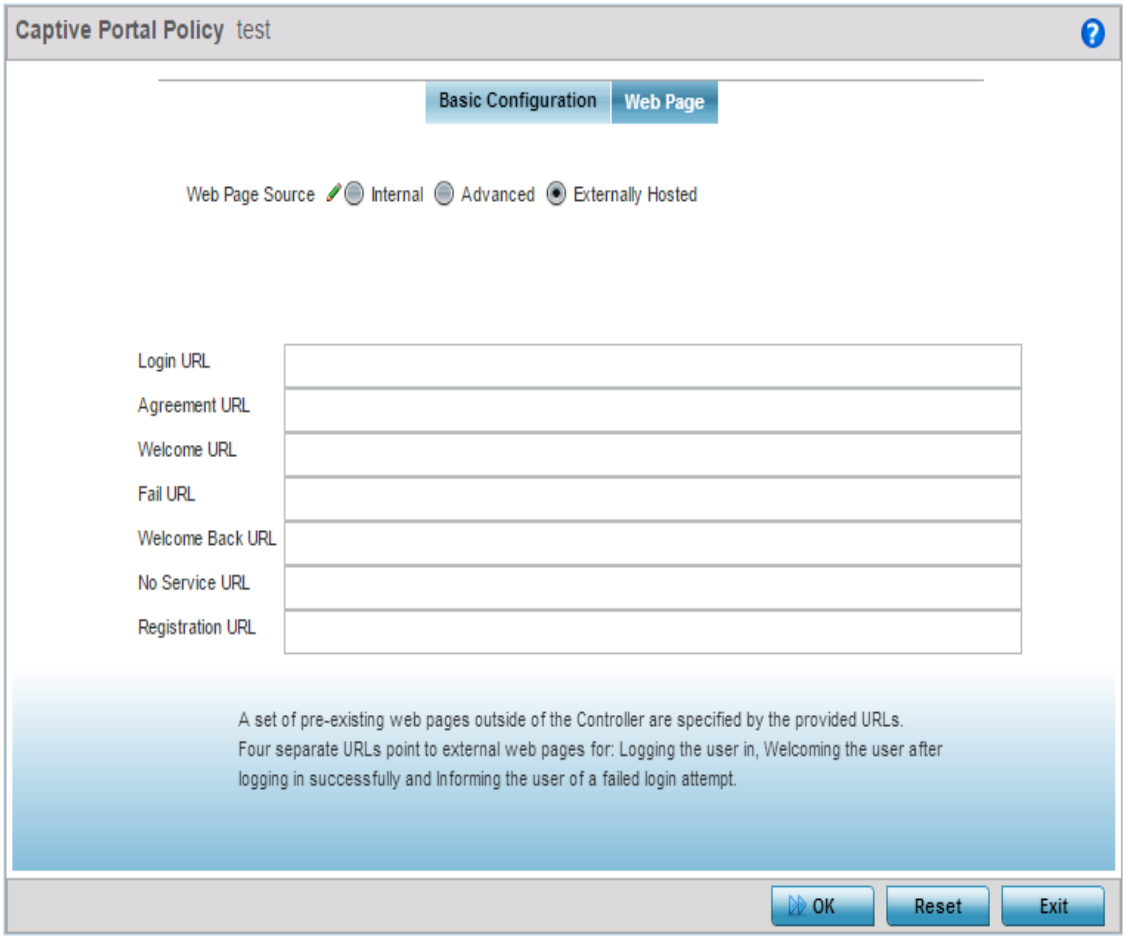


Figure 7: Captive Portal Policy screen - Web Page tab - Externally Hosted Web Page screen

14 Set the following URL destinations for externally hosted captive portal pages:

Login URL	Define the complete URL for the location of the Login page. The Login screen prompts the user for a username and password to access the Terms and Conditions or Welcome page.
Agreement URL	Define the complete URL for the location of the Terms and Conditions page. The Terms and Conditions page provides conditions that must be agreed to before wireless client access is provided.

Welcome URL	Define the complete URL for the location of the Welcome page. The Welcome page asserts the user has logged in successfully and can access resources via the captive portal.
Fail URL	Define the complete URL for the location of the Fail page. The Fail page asserts authentication attempt has failed, and the client cannot access the captive portal and the client needs to provide correct login information to regain access.
Welcome Back URL	Define the complete URL for the location of the Welcome Back page. The Welcome Back page asserts the user has re-logged in successfully and can access resources via the captive portal.
No Service URL	Define the complete URL to the location of the No Service page. The No Service URL is needed by users encountering difficulties connecting to the external resource used to host the captive portal pages.
Registration URL	Define the complete URL to the location of the Registration page. The Registration page is displayed to new users to register (provide user information) in order to access the captive portal managed Internet resources.

15 Select **OK** when completed to update the captive portal policy settings. Select **Reset** to revert the screen back to its last saved configuration.

16 Select **Advanced** to use a custom directory of Web pages copied to and from the access point for captive portal support.

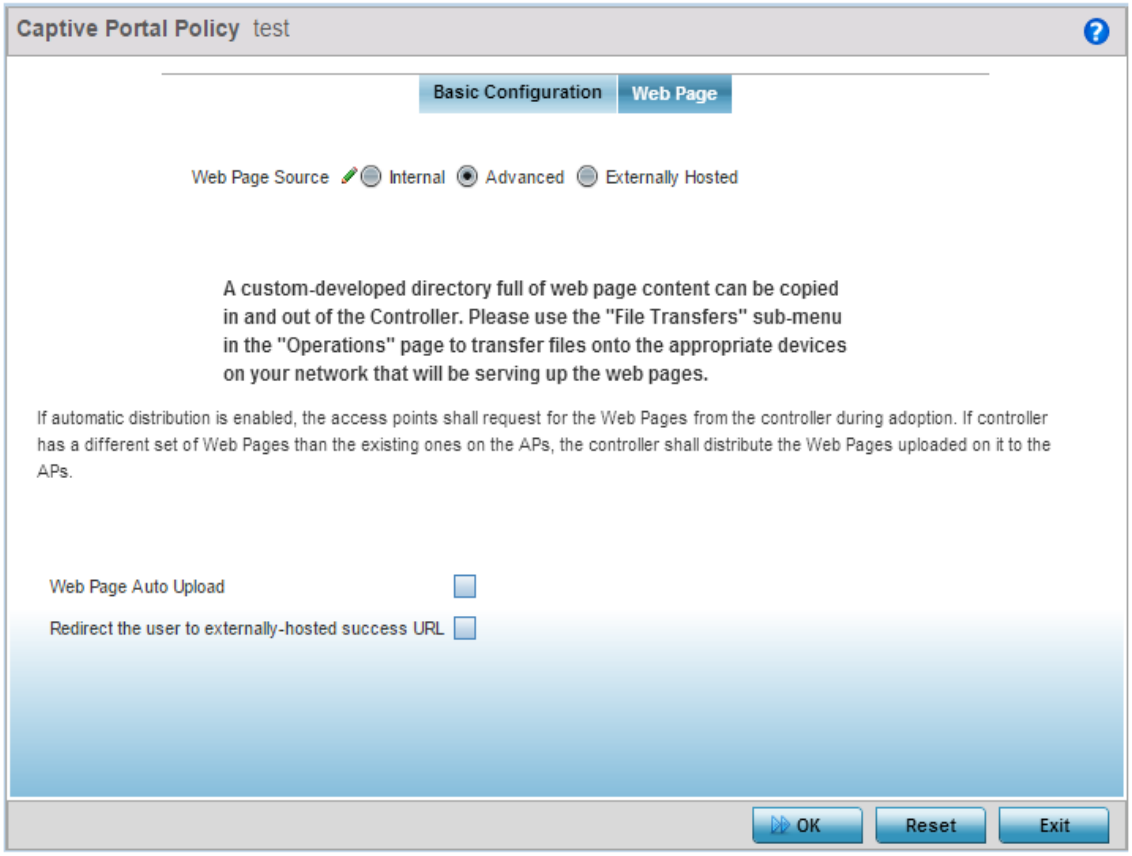


Figure 8: Captive Portal Policy screen - Web Page tab - Advanced Web Page screen

17 The access point maintains its own set of Advanced Web pages for custom captive portal creation. Refer to **Operations** > **Devices** > **File Transfers** and use the *Source* and *Target* fields to move captive portal pages as needed to managed devices that may be displaying and hosting captive portal connections.

Select the **Web Page Auto Upload** check box to enable automatic upload of captive portal Web pages.

Select the **Redirect the user to externally-hosted success URL** check box, if the Welcome page is externally hosted.

For more information, refer to "File Management" on page 889.

Setting the DNS Whitelist Configuration

"Services Configuration"

A DNS whitelist is used in conjunction with a captive portal to provide captive portal services to wireless clients. Use the DNS whitelist parameter to create a set of allowed destination IP addresses within the captive portal. These allowed IP addresses are called the *Whitelist*. To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist. Each supported access point model can support up to 32 whitelists, with the exception of AP6521 model which can only support up to 16 whitelists.

To define a DNS whitelist:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Select **DNS Whitelist**.

The *DNS Whitelist* screen displays those existing whitelists available to a captive portal.

4 Select **Add** to create a whitelist, **Edit** to modify a selected whitelist or **Delete** to remove a whitelist.

To create a whitelist:

1 If creating a whitelist, assign it a name up to 32 characters. Use the + Add Row button to populate the whitelist table with Host and IP Index parameters that must be defined for each whitelist entry.

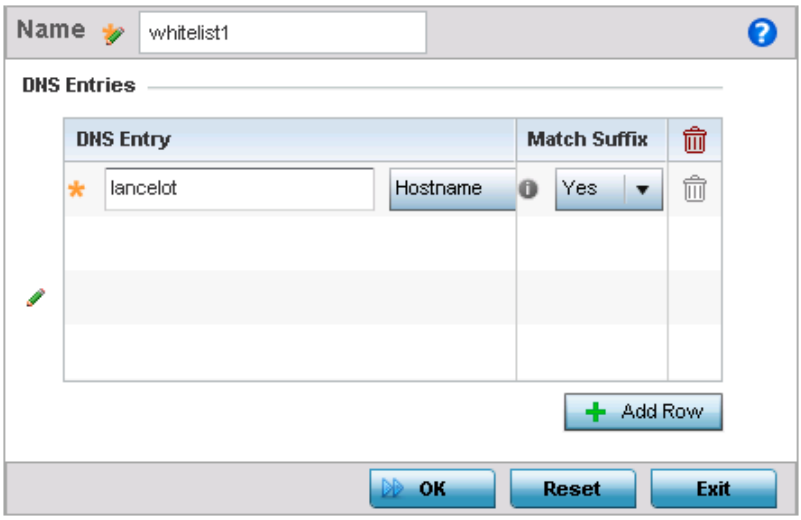


Figure 9: DNS Whitelist screen

2 Provide a numerical IP address or Hostname within the DNS Entry parameter for each destination IP address or host in the whitelist.

3 Use the Match Suffix parameter to match any hostname or domain name as a suffix. The default setting is disabled.

4 If necessary, select the radio button of an existing whitelist entry and select the - Delete icon to remove the entry from the whitelist.

5 Select **OK** when completed to update the whitelist screen. Select **Reset** to revert the screen to its last saved configuration.

Setting the DHCP Server Configuration

"Services Configuration"

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 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 expired). Therefore, IP address management is conducted by the DHCP server, not an administrator.

WiNG managed access points have an internal DHCP server resource. However, AP6521 model does not have an onboard DHCP server resource and an external resource must be used.

The 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. 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.

A single DHCP server configuration is supported by the access point, no separate DHCP policies can be defined and maintained. For more information, refer to the following:

- "Defining DHCP Pools"
- "Defining DHCP Server Global Settings"
- "DHCP Class Policy Configuration"
- "DHCP Deployment Considerations"

To access the local DHCP server configuration screen:

1 Select **Configuration** > **Services** > **DHCP Server Policy**.

The **DHCP Server** screen displays. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are then compared against classes.

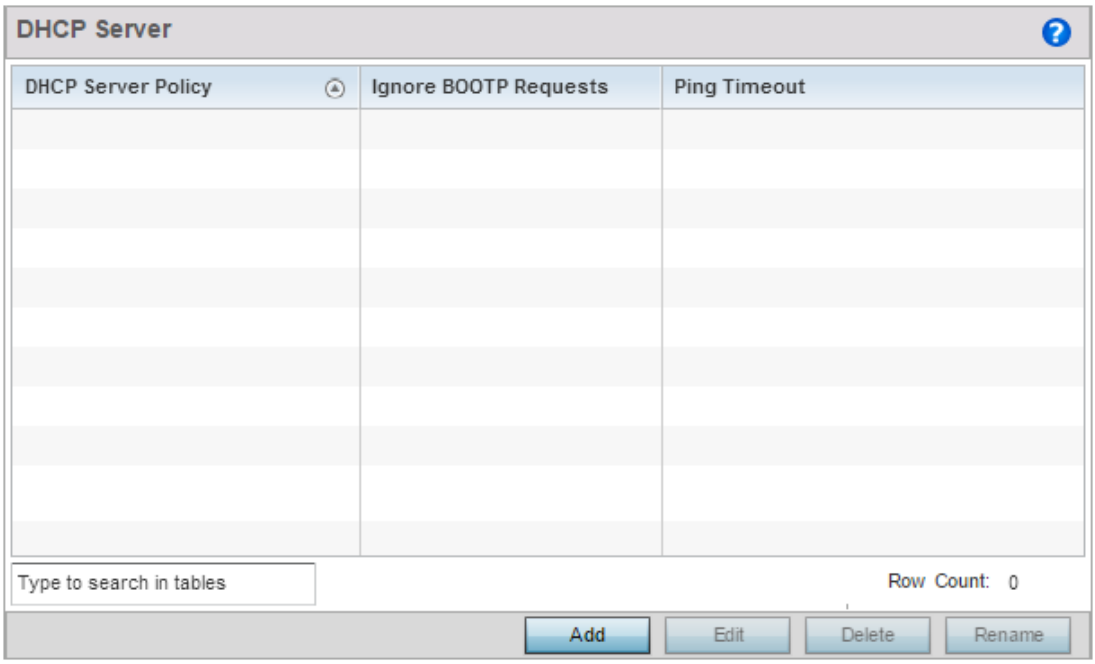


Figure 10: DHCP Server Policy screen

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 Select **Add** to create a new DHCP server policy, or 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 **DHCP Pool** tab by default.

Defining DHCP Pools

"Setting the DHCP Server Configuration"

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 within the network 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 such as a 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 specified by the DHCP client's vendor.

To define the parameters of a DHCP pool:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Select **DHCP Server**. The DHCP Pool tab displays by default.

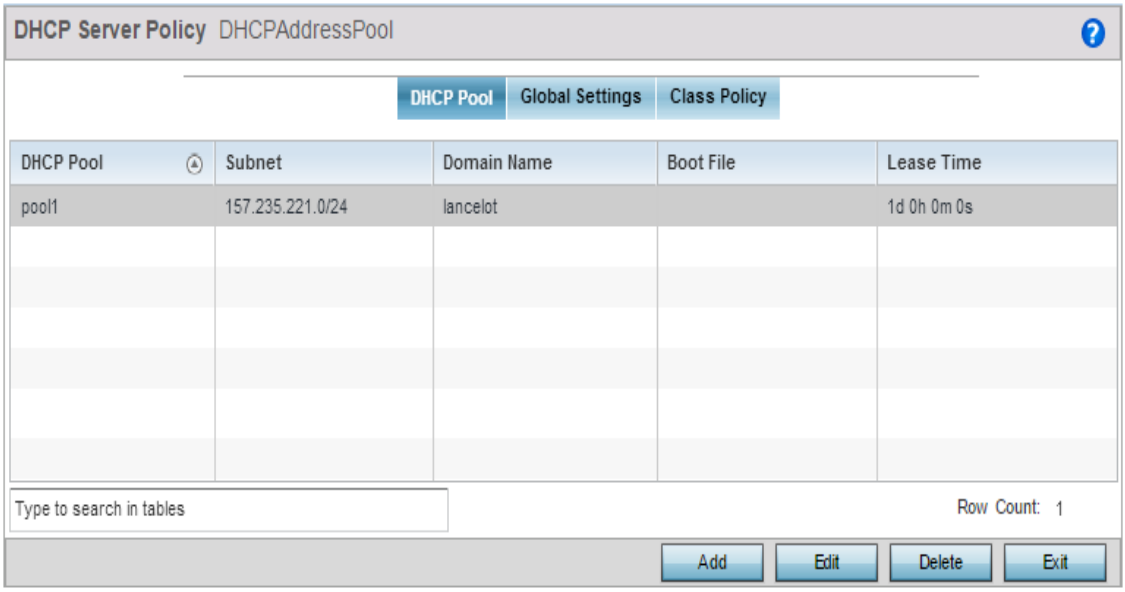


Figure 11: DHCP Server Policy screen - DHCP Pool tab

4 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 agroup of IP addresses used to assign to DHCP clients upon request. The name assigned cannot be modified as part of the edit process. If a 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 used with this network pool. Hostnames are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a hostname 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 as an interval between 1 - 9,999,999 seconds. DHCP leases provide addresses for defined times to various clients. If a client does not use a leased address for the defined time, that IP address can be re-assigned to another DHCP supported client.

5 Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool or **Delete** to remove a pool.

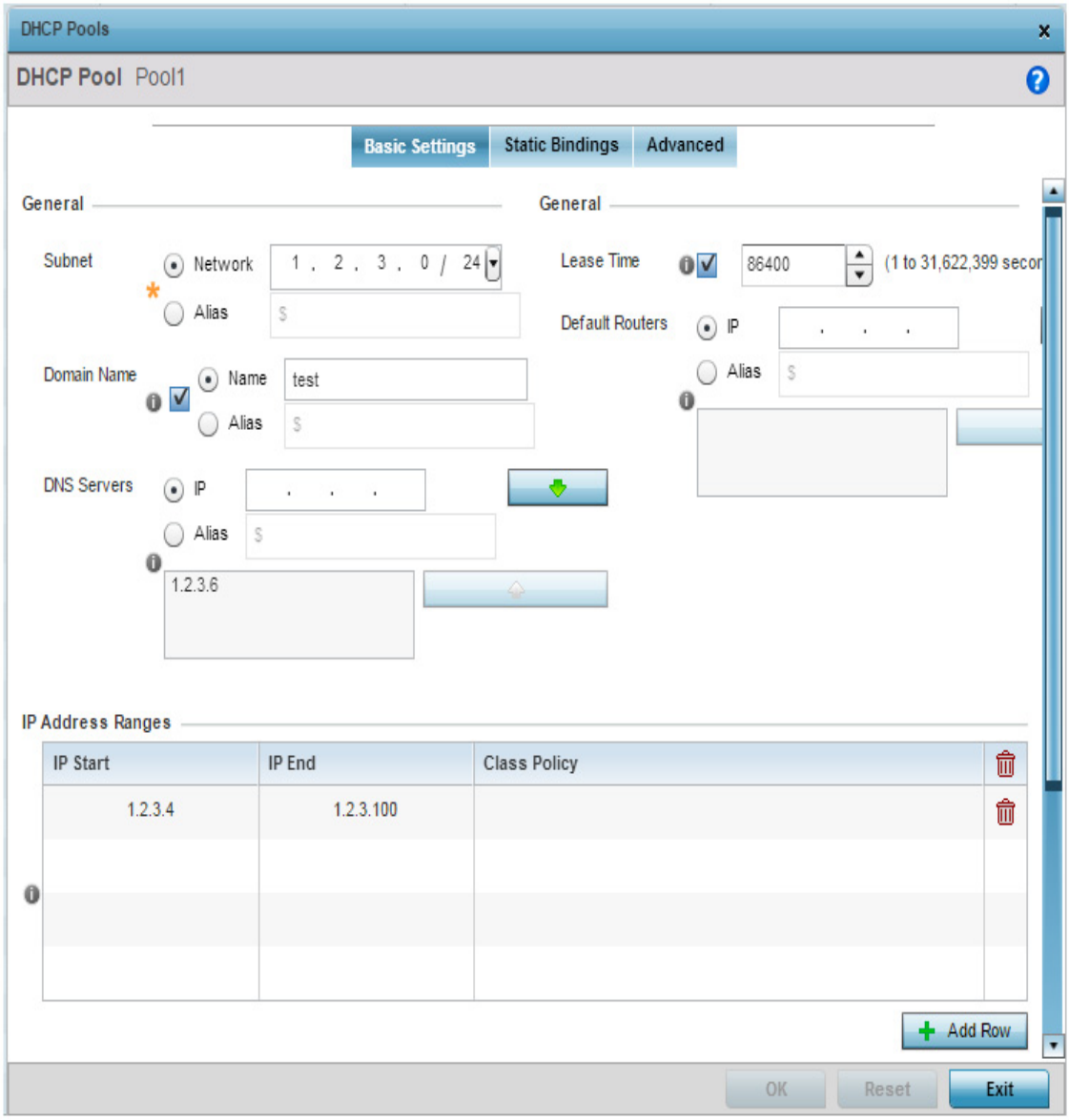


Figure 12: DHCP Pools screen - Basic Settings tab

If 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 a DHCP pool.

6 Set the following **General** parameters:

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 and Subnet Mask used for DHCP discovery and requests between the DHCP Server and DHCP clients. The IP address and subnet mask of the pool are required to match the addresses of the layer 3 interface for the addresses to be supported through that interface. Select *Alias* to use a network alias with the subnet configuration. For more information see "Alias" on page 683.
Domain Name	Provide the domain name used with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. An FQDN consists of a hostname plus a domain name. For example, computername.domain.com. Select *Alias* to use a string alias with the domain name configuration. For more information see "Alias" on page 683.
DNS Servers	Define one or a group of *Domain Name Servers* (DNS) to translate domain names to IP addresses. Select *Clear* to remove any single IP address as needed. Up to 8 IP addresses can be supported. Select *Alias* to use a host alias with the DNS servers configuration. For more information see "Alias" on page 683.
Lease Time	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 DHCP supported client. Select this option to assign a lease time 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 of one or a group of routers used to map hostnames into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported. Select *Alias* to use a host alias with the default routers configuration. For more information see "Alias" on page 683.

7 Use the **IP Address Ranges** and **Excluded IP Address Ranges** fields to define the range of included (starting and ending) IP addresses and excluded (starting and ending) IP addresses for this particular pool.

Refer to the IP Address Ranges field and select the + **Add Row** button at the bottom of the field to add a new range. At any time you can select the radio button of an existing IP address range and select the **Delete** icon to remove it from the list of those available.

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 DHCP supported wireless clients within the network.

Select the **Create** icon or **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.

8 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 DHCP 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.

9 Select **OK** to save the updates to the **DHCP Pool Basic Settings** tab. Select **Reset** to revert to the last saved configuration.

10 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 provide the assignment of 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.

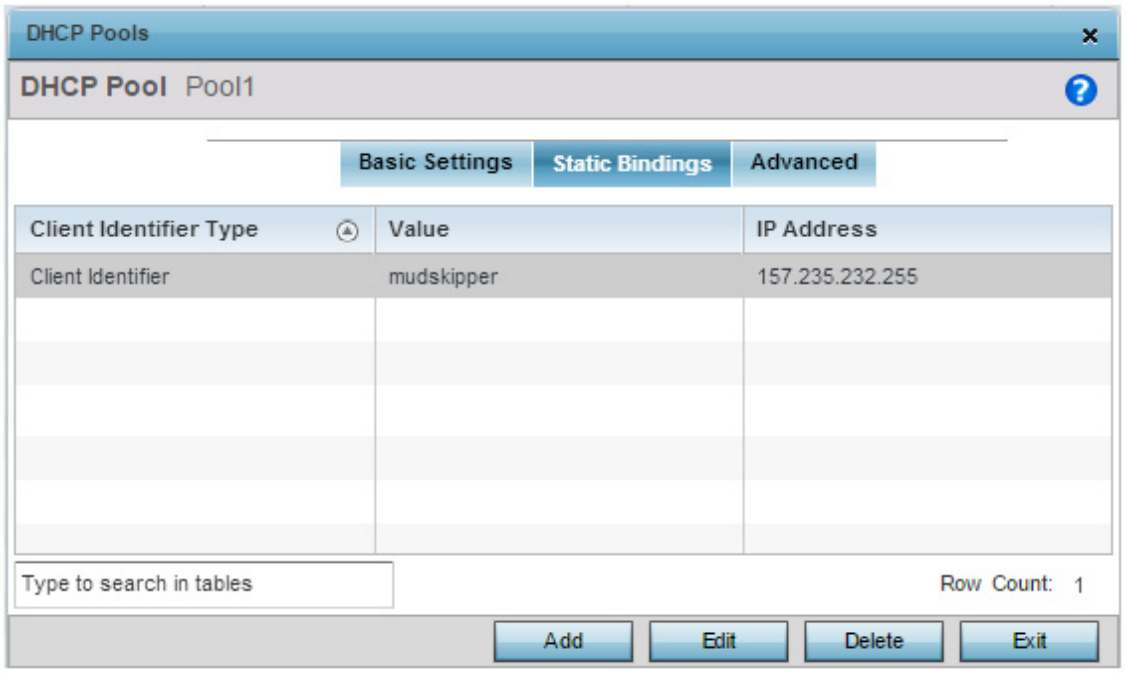


Figure 13: DHCP Pools screen - Static Bindings tab

11 Review existing DHCP pool static bindings to determine if a static binding can be used as is, a new one requires creation or edit, or if one requires deletion:

Client Identifier Type	Lists whether the reporting client is using a *Hardware Address* or *Client Identifier* as its identifier type.
Value	Lists the hardware address or client identifier value assigned to the client when added or last modified.
IP Address	Displays the IP address of the client on this interface that's currently using the pool name listed.

12 Select **Add** to create a new static binding configuration, **Edit** to modify an existing static binding configuration or **Delete** to remove a static binding from amongst those available.

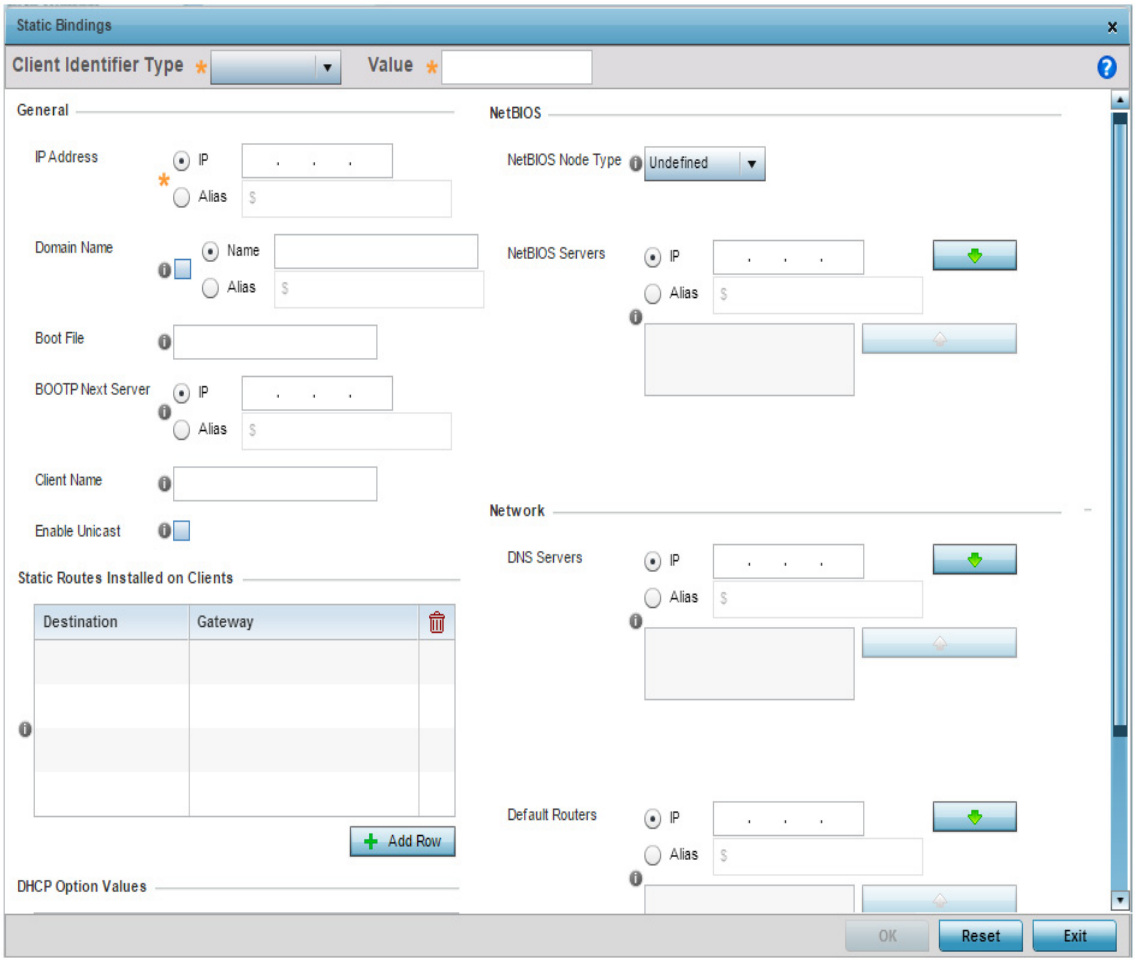


Figure 14: Static Bindings Add screen

13 Define the following **General** parameters required to complete the creation of the static binding configuration:

Client Identifier Type	Use the drop-down menu whether the DHCP client is using a *Hardware Address* or *Client Identifier* as its identifier type with a DHCP server.
Value	Provide a hardware address or client identifier value to help differentiate the client from other client identifiers.
IP Address	Set the IP address of the client using this host pool. Select *Alias* to use a network alias with the IP address configuration. For more information see "Alias" on page 683.

Domain Name	Provide a domain name of the current interface. Domain names aren't case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a hostname plus a domain name. For example, *computername.domain.com*. Select *Alias* to use a string alias with the domain name configuration. For more information see "Alias" on page 683.
Boot File	Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed
BOOTP Next Server	Provide the numerical IP address of the server providing BOOTP resources. Select *Alias* to use a network alias with the BOOTP Next Server configuration. For more information see "Alias" on page 683.
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.

14 Define the following **NetBIOS** parameters required to complete the creation of the static binding configuration:

NetBIOS Node Type	Set the NetBIOS Node Type used with this particular pool. The node can have one of the following types: • *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. • *None* - No node type is applied.
NetBIOS Servers	Specify a numerical IP address of a single or group of NetBIOS WINS servers available to DHCP supported wireless clients. A maximum of 8 server IP addresses can be assigned. Select *Alias* to use a network alias with the NetBIOS server configuration. For more information see "Alias" on page 683.

15 Refer to the **Static Routes Installed on Clients** field to set **Destination** IP and **Gateway** addresses enabling 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.

16 Scroll down 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.

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. At any time you can select the radio button of an existing option and select the **- Delete** button to remove it from the list of those available.

Assign a **Value** to each option with codes in the range of 1 through 254. A vendor specific option definition only applies to the vendor class for which it is defined.

17 Within the **Network** field, define one or group of **DNS Servers** to translate domain names to IP addresses. Up to 8 IP addresses can be provided and translated. Select **Alias** to use a network alias with the DNS server configuration. For more information see "Alias" on page 683.

Within the **Network** field, define one or more **DNS Servers** and **Default Routers** to resolve routes to other parts of the network. Up to 8 IP addresses can be provided for Default Routers. Select **Alias** to use a network alias with the default routers configuration. For more information see "Alias" on page 683.

18 Select **OK** when completed to update the static bindings configuration. Select **Reset** to revert to the last saved configuration.

19 Select the **Advanced** tab to define additional NetBIOS and Dynamic DNS parameters.

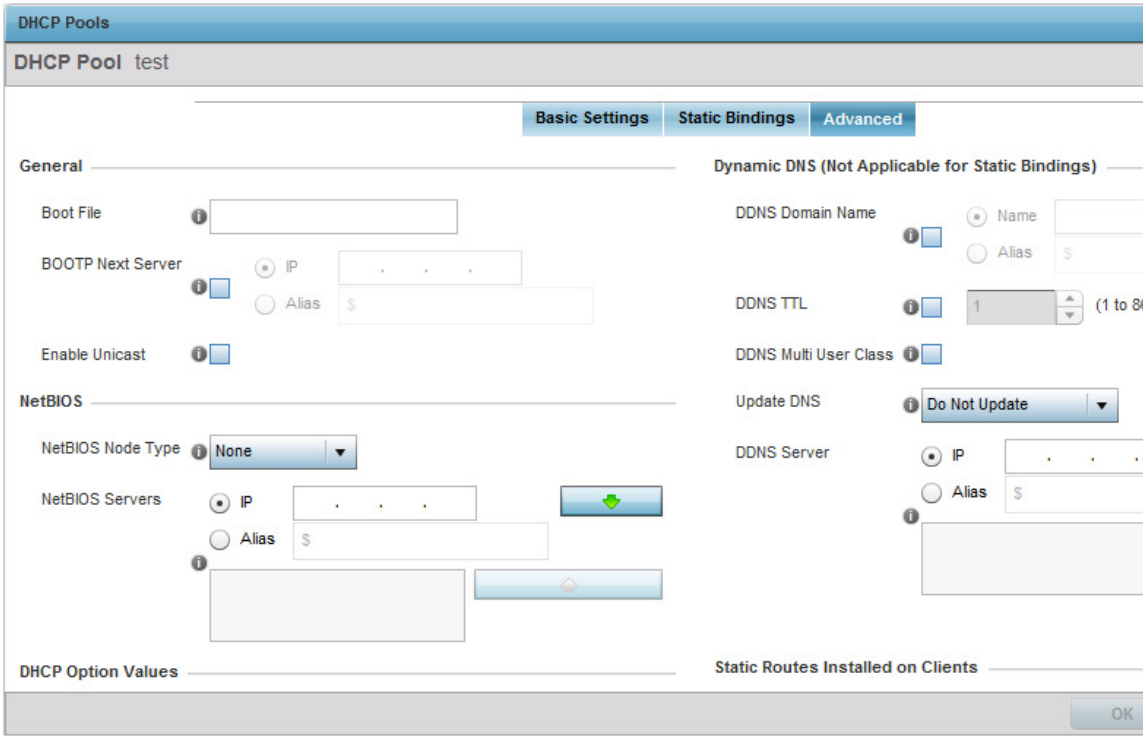


Figure 15: DHCP Pools screen - Advanced tab

20 The addition or edit of the DHCP pool's advanced settings requires the following **General** parameters be set:

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 of the server providing BOOTP resources. Select *Alias* to use a network alias with the BOOTP Next Server configuration. For more information see "Alias" on page 683.
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.

21 Set the following **NetBIOS** parameters for the network pool:

NetBIOS Node Type	Set the NetBIOS Node Type used with this pool. The following types 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* - Is a mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address. • *Hybrid* - Is a combination of two or more nodes. • *None* - No NetBIOS Node Type is used.
NetBIOS Servers	Specify a numerical IP address of a single or group of NetBIOS WINS servers available to DHCP supported wireless clients. Select *Alias* to use a network alias with the NetBIOS server configuration. For more information see "Alias" on page 683.

22 Refer to the **DHCP Option Values** table to set global DHCP options applicable to all clients, whereas a set of subnet options applies to just the clients on a specified subnet.

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. At any time you can select the radio button of an existing option and select the **Delete** icon to remove it from the list of those available.

Assign a **Value** to each option with codes in the range 1 through 254. A vendor-specific option definition only applies to the vendor class for which it is defined.

23 Set the following **Dynamic DNS** parameters for the network pool. DDNS enables controllers, service platforms and access point the ability to notify 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.

24 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.

25 Select **OK** to save the updates to the DHCP pool's Advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

Defining DHCP Server Global Settings

"Setting the DHCP Server Configuration"

Setting a DHCP server global configuration entails defining whether BOOTP requests are ignored and setting DHCP global server options.

To define DHCP server global settings:

1 Select the **Global Settings** tab and ensure the **Activate DHCP Server Policy** button remains selected. This option must remain selected to implement the configuration as part of the access point profile.

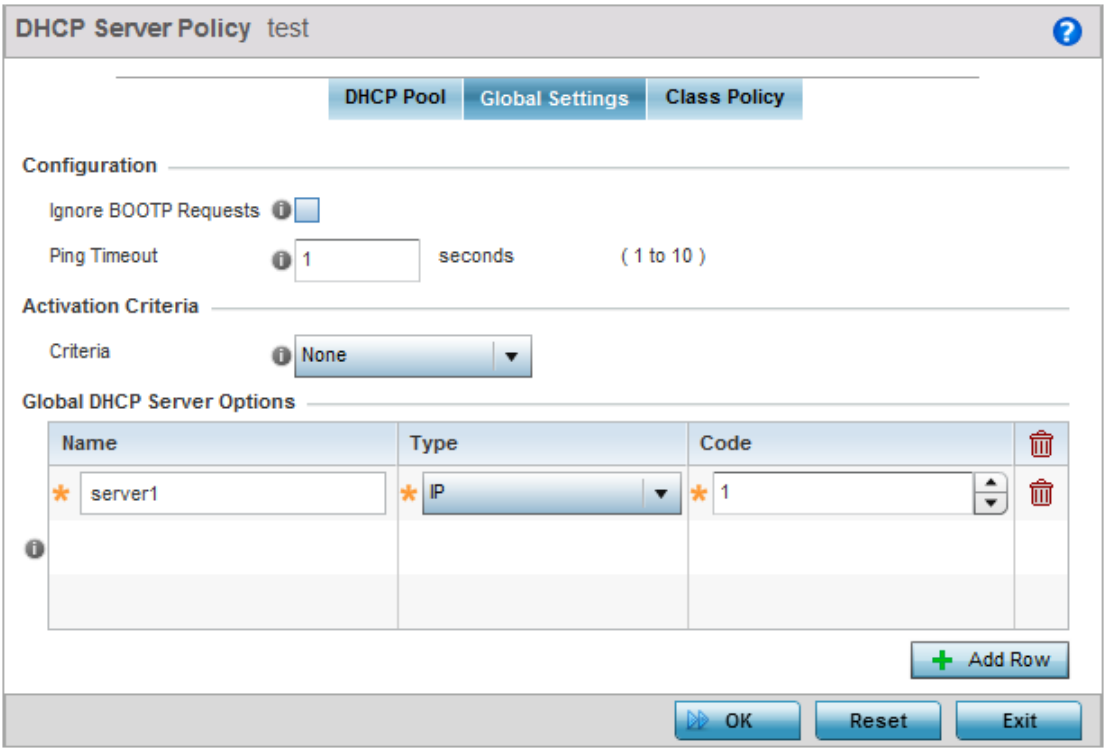


Figure 16: DHCP Server Policy screen - Global Settings tab

2 Set the following parameters within the **Configuration** field:

Ignore BOOTP Requests	Select the check box to ignore BOOTP requests. BOOTP requests boot remote systems within the network. BOOTP messages are encapsulated inside UDP messages and are 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 used to intermittently ping and discover whether a client requested IP address is already used.

3 Set the **Activation Criteria** for this DHCP Server Policy. Use the drop-down menu to select the criteria from one of *none, vrrp-master*, *cluster-master* or *rf-domain-manager*. The default value is *none.*

4 Refer to the **Global DHCP Server Options** field.

Use the **+ Add Row** button at the bottom of the field to add a new global DHCP server option. At any time you can 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.

Use the **Type** drop-down menu to specify whether the DHCP option is being defined as a numerical IP address or ASCII string or Hex string. Highlight an entry from within the Global Options screen and click the Remove button to delete the name and value.

5 Select **OK** to save the updates to the DHCP server global settings. Select **Reset** to revert to the last saved configuration.

DHCP Class Policy Configuration

"Setting the DHCP Server Configuration"

The DHCP server assigns IP addresses to DHCP enabled wireless clients based on user class option names. Clients with a defined set of user class option names are identified by their user class name. The DHCP server can assign IP addresses from as many IP address ranges as defined by the 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 multiple option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

To review DHCP class policies:

1 Select the **Class Policy** tab and ensure the **Activate DHCP Server Policy** button remains selected. This option must remain selected to implement the configuration as part of the access point profile.

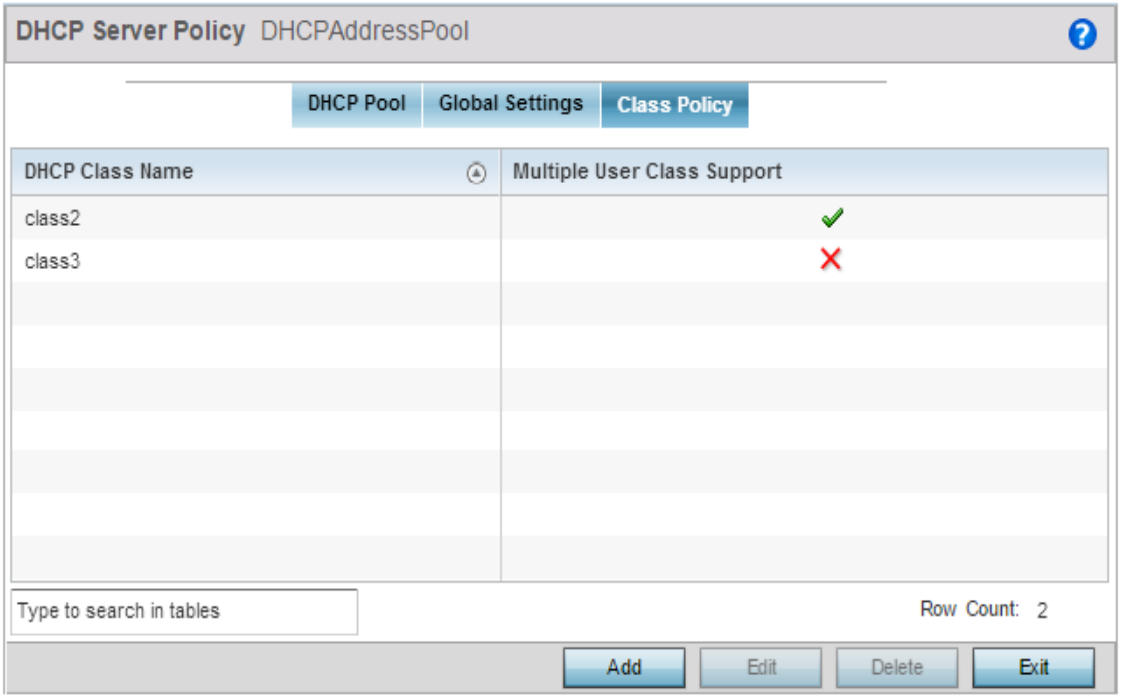


Figure 17: DHCP Server Policy screen - Class Policy tab

2 Select **Add** to create a new DHCP class policy, **Edit** to update an existing policy or **Delete** to remove an existing policy.

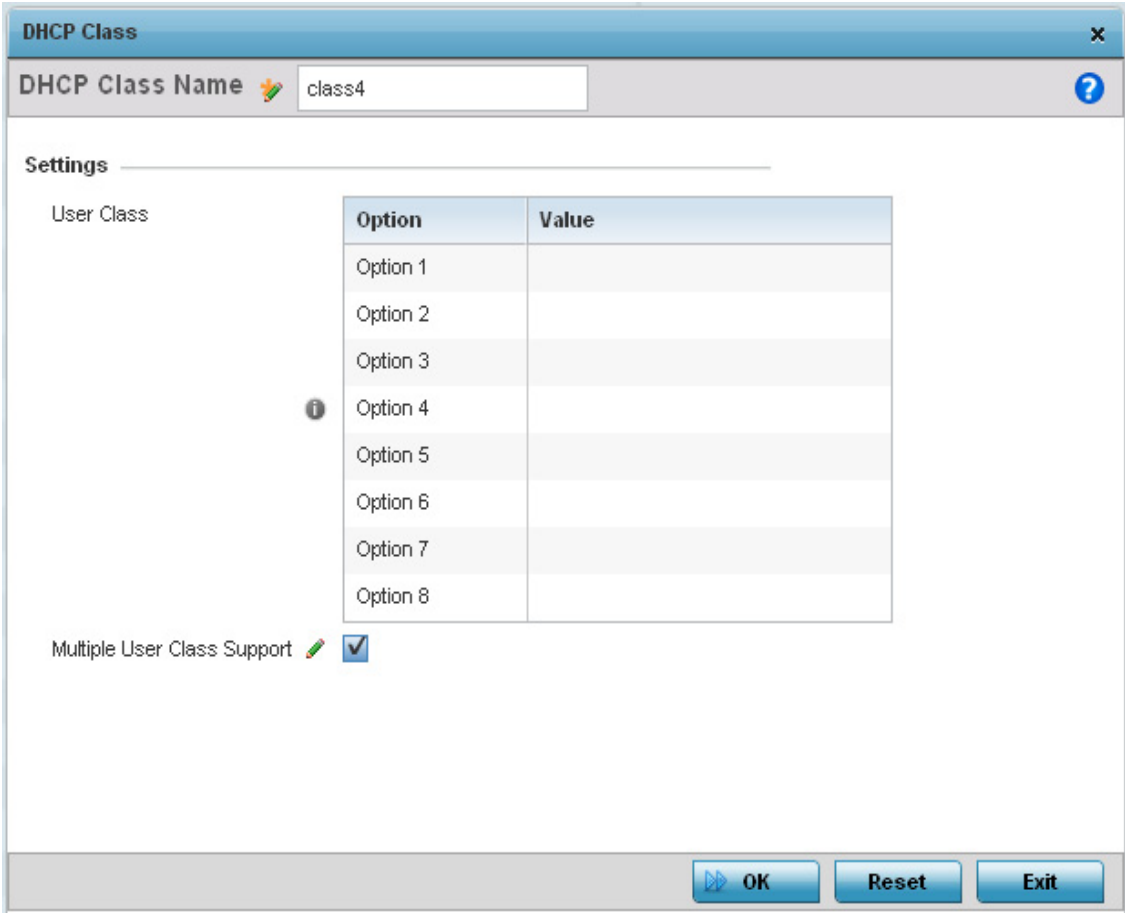


Figure 18: DHCP Class - Name Add screen

3 If adding a new **DHCP Class Name**, assign a name representative of the device class supported. The DHCP user class name should not exceed 32 characters.

4 Select a row within the **Value** column to enter a 32 character maximum value string.

5 Select the **Multiple User Class Support** radio button to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.

6 Select **OK** to save the updates to this DHCP class policy. Select **Reset** to revert to the last saved configuration.

DHCP Deployment Considerations

Before defining an internal DHCP server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- DHCP option 189 is required when AP650 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 is impossible to check if a client is authorized to use this parameter.

- Ensure traffic can pass on UDP ports 67 and 68 for clients receiving DHCP information.

Setting the Bonjour Gateway Configuration

"Services Configuration"

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.



NOTE

Up to eight (8) Bonjour Discovery Policies can be configured.

The following options can be configured:

- "Configuring the Bonjour Discovery Policy"
- "Configuring the Bonjour Forwarding Policy"

Configuring the Bonjour Discovery Policy

"Setting the Bonjour Gateway Configuration"

The Bonjour Discovery Policy configures how Bonjour services can be 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**.

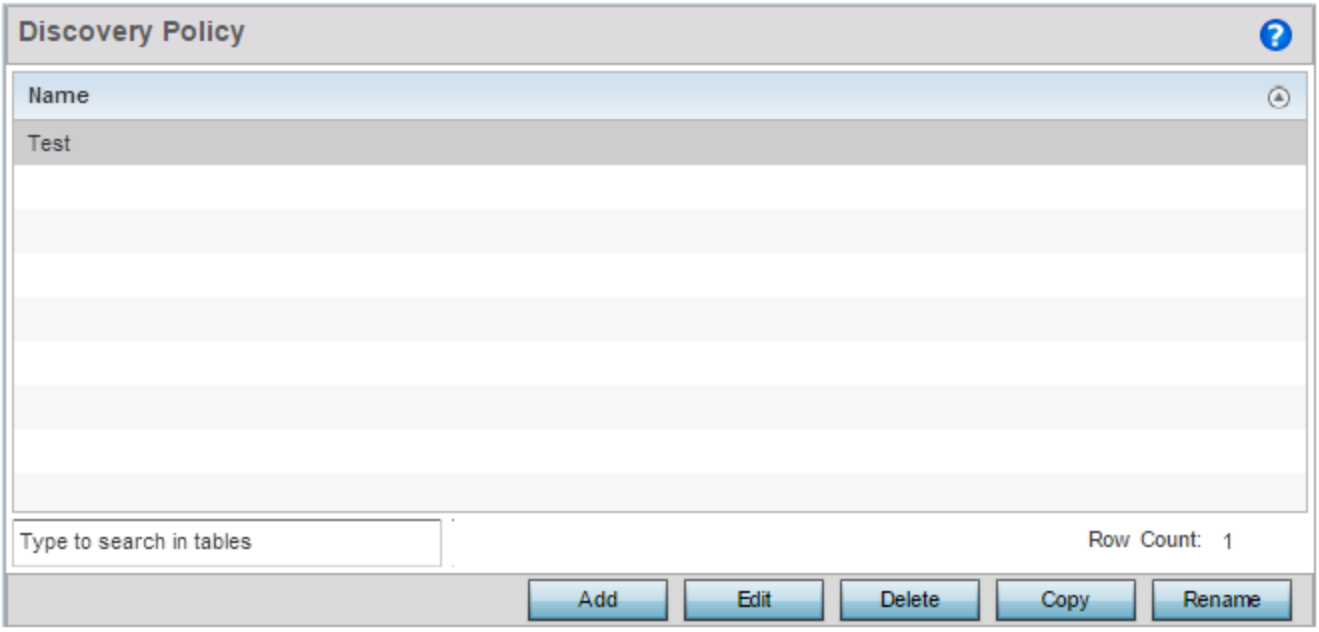


Figure 19: Bonjour - Discovery Policy screen

This screen displays the name of the configured Bonjour discovery policies.

5 Select an existing policy and click **Edit** to edit it. To add a new policy, select **Add**. Select an existing policy and click **Delete** to delete the policy or use **Copy** to create a copy of a policy for further modifications.

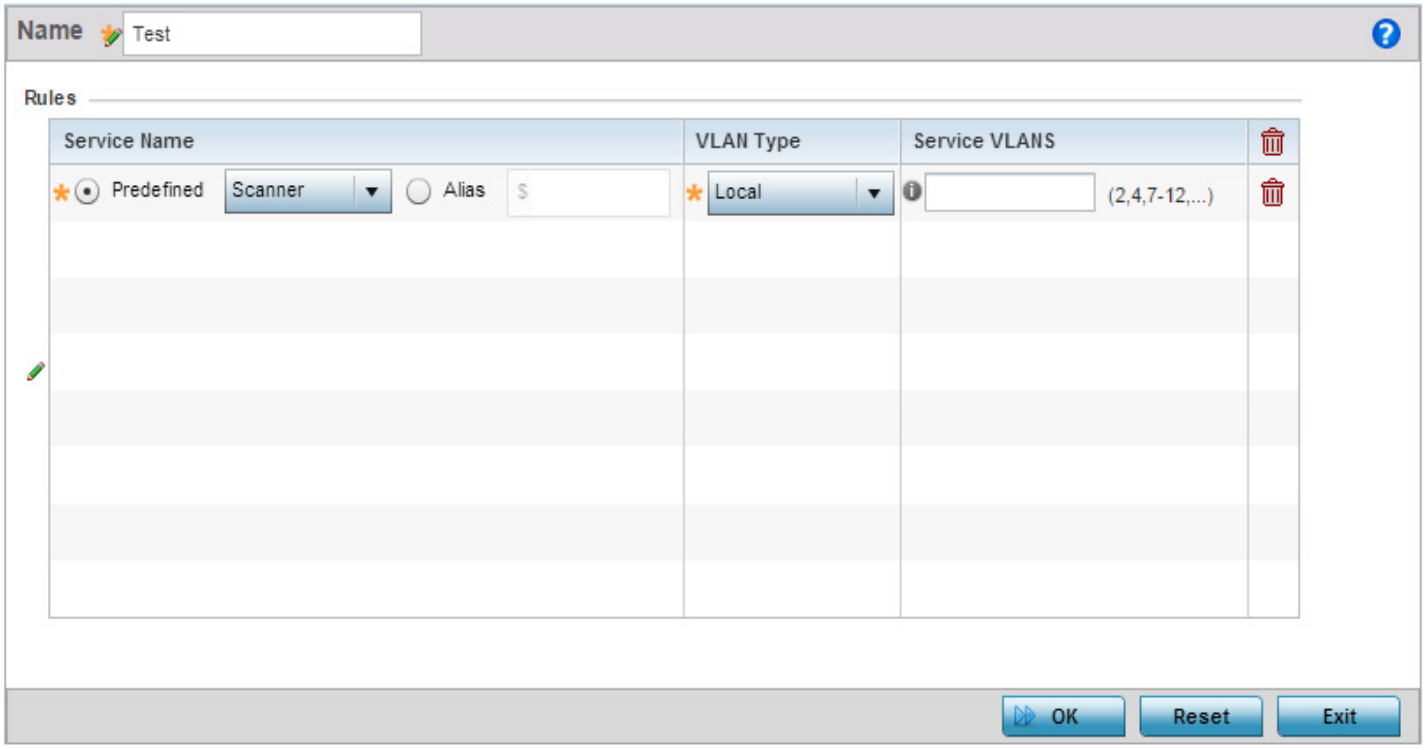


Figure 20: Bonjour - Discovery Policy - Add/Edit Policy screen

6 Select the **+ Add Row** button to add a rule to the Bonjour Discovery Policy. These are the services which can be discovered by the Bonjour Gateway.

Refer to the following for more information on the discovery rules.

Service Name	Configures 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. • *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* – Indicates that the VLAN(s) defined in *Service VLAN* field is local in nature. • tunneled – Indicates that the VLAN(s) defined in Service VLAN field are tunneled.
Service VLANs	Provide a VLAN or a list of VLANs on which the selected service is discoverable.

7 Select **OK** to save the updates to this Bonjour Discovery Policy. Select **Reset** to revert to the last saved configuration.

Configuring the Bonjour Forwarding Policy

"Setting the Bonjour Gateway Configuration"

Bonjour Forwarding Policy enables discovery of services on VLANs which are not visible to the device running the Bonjour Gateway. Bonjour forwarding enables forwarding of Bonjour advertisements across VLANs to enable the Bonjour Gateway device to build a list of services and the VLANs where these services are available.

NOTE

Only one (1) Bonjour Forwarding Policy can be configured.

NOTE

There must be Layer 2 connectivity between the devices for forwarding to work.

To display Bonjour Discovery Policy information:

1 Select **Configuration**.

2 Select **Services**.

3 Select **Bonjour Gateway** to expand its submenu.

4 Select **Forwarding Policy**.

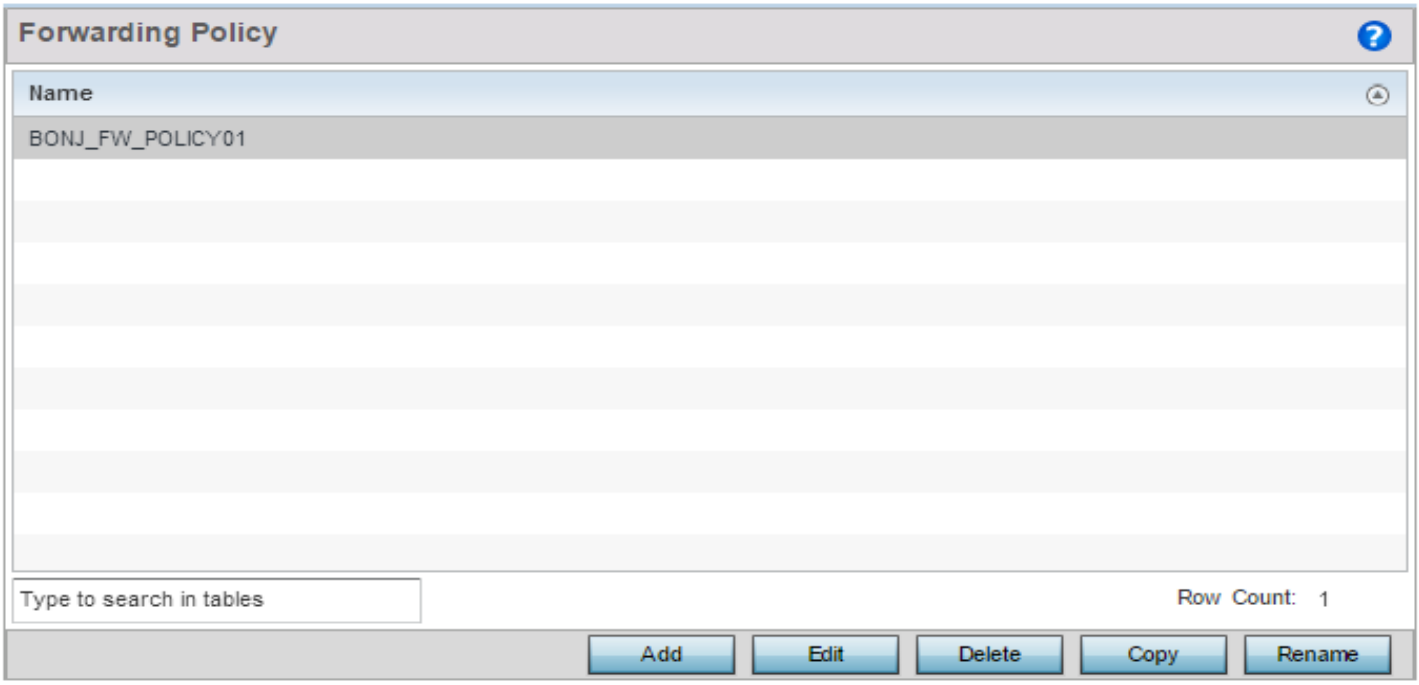


Figure 21: Bonjour Gateway - Forwarding Policy screen

This screen displays the name of the configured Bonjour forwarding policies.

5 Select an existing policy and click **Edit** to edit it. To add a new policy, select **Add**.

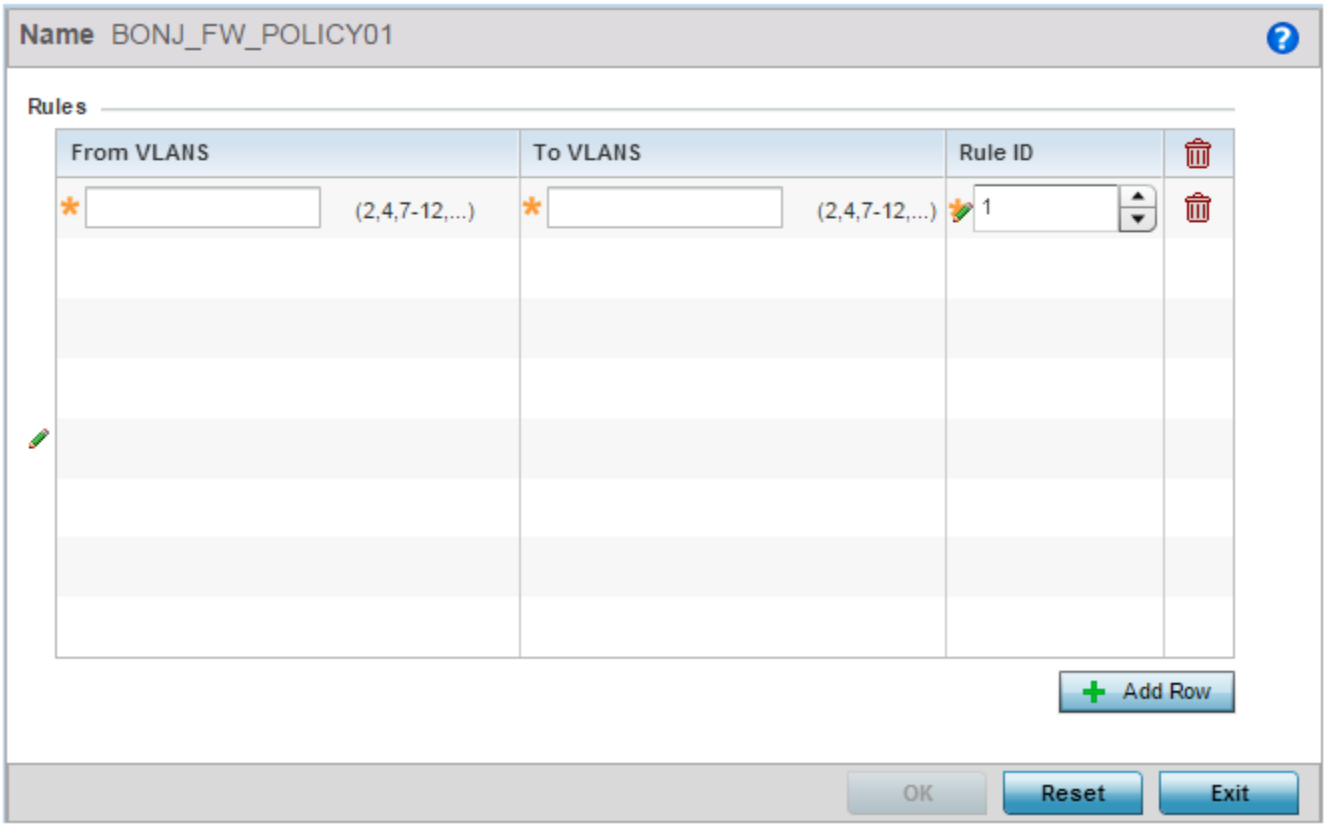


Figure 22: Bonjour Gateway - Forwarding Policy - Add screen

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 VLANs 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 VLANs 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 for this rule.

7 Select **OK** to save the updates to this Bonjour Gateway Forwarding Policy. Select **Reset** to revert to the last saved configuration.

Setting the DHCPv6 Server Policy

"Services Configuration"

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.

To access and review the local DHCPv6 server configuration:

1 Select **Configuration**.

2 Select **Services**.

3 Select **DHCPv6 Server Policy**.
The **DHCPv6 Server Policy** screen displays.

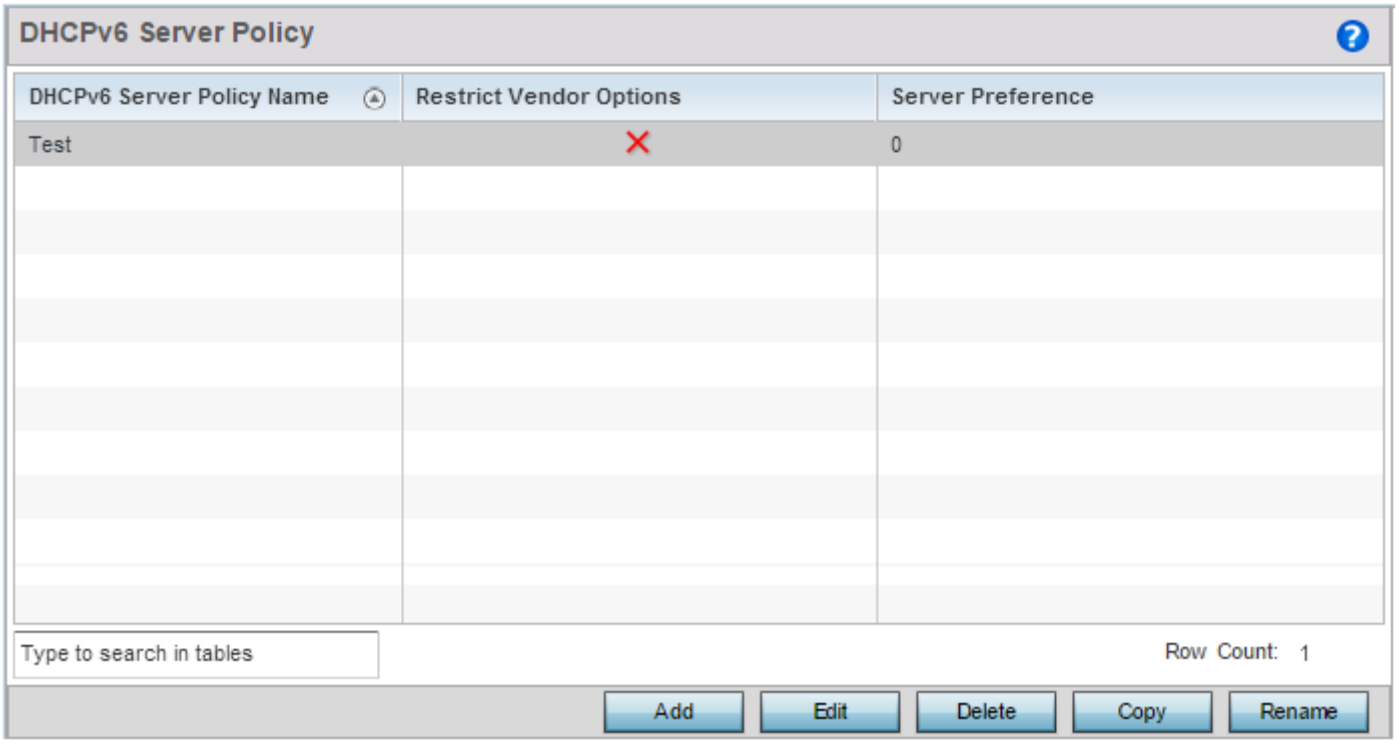


Figure 23: DHCPv6 Server Policy screen

4 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	Lists 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 are only applicable to the vendor class defined.
Server Preference	Lists the server preference (from 0 - 255) specified for each DHCPv6 server policy. The default value is 0.

5 Select **Add** to create a new DHCPv6 server policy, choose an existing policy and select the **Edit** button to modify the policy's properties or choose an existing policy and select **Delete** to remove the policy from those available. Adding or Editing a DHCP server policy displays the **DHCPv6 Server Policy Name** screen by default.

Defining DHCPv6 Options

"Setting the DHCPv6 Server Policy"

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.**

2 Select **Services**.

3 Select **DHCPv6 Server Policy**.

Select **Add** to create a new policy or **Edit** to modify the policy's properties of a selected DHCPv6 server policy.
Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.

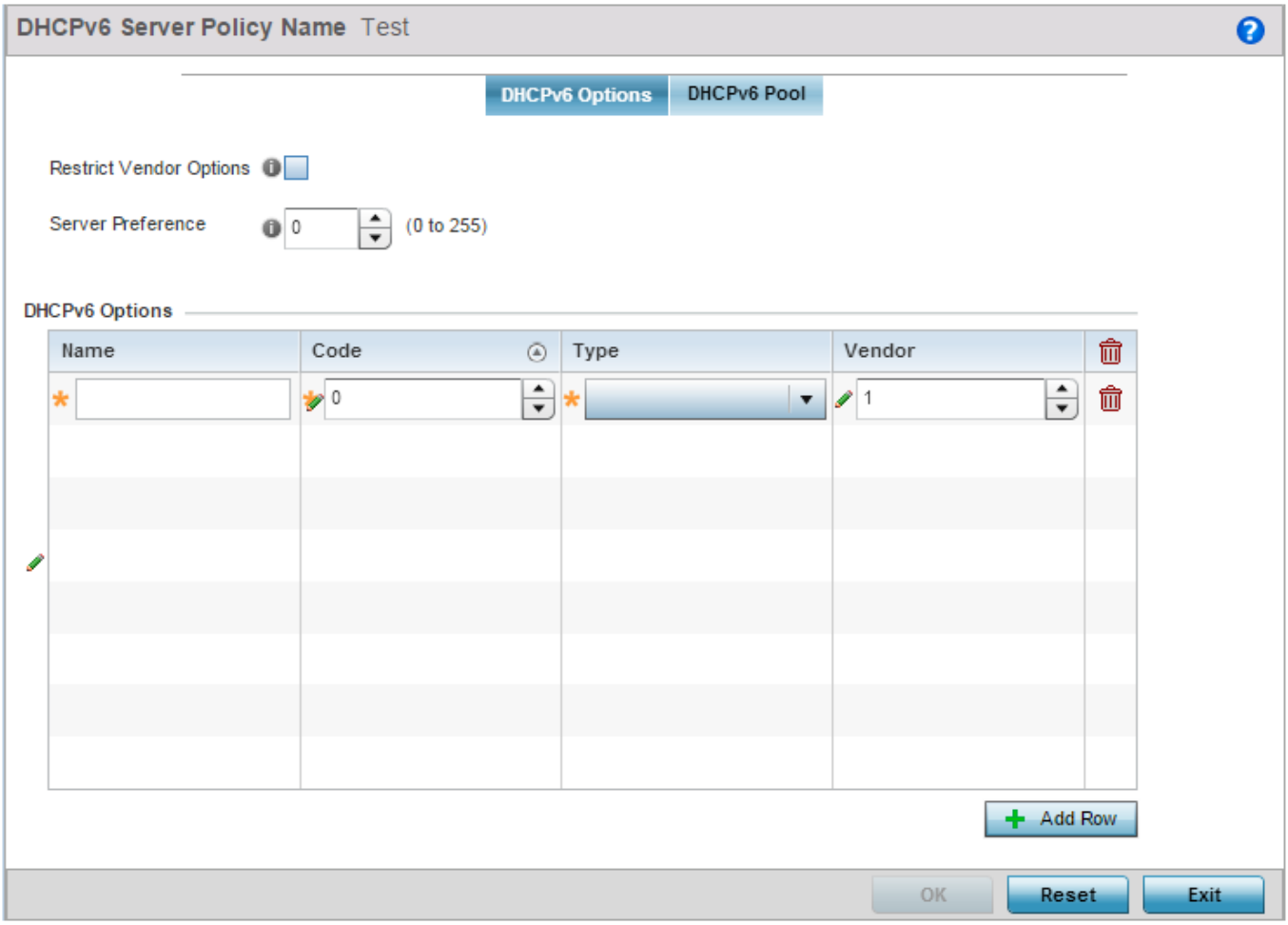


Figure 24: DHCP v6Server Policy - DHCPv6 Options tab

4 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.

5 Use the spinner control to select a **DHCPv6 Server Preference** from 0 - 255. The default value is 0.

6 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.

7 Select **OK** to save the updates to the DHCPv6 options. Select **Reset** to revert the screen back to its last saved configuration.

DHCPv6 Pool Configuration

"Setting the DHCPv6 Server Policy"

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 **Configuration.**

2 Select **Services**.

3 Select **DHCPv6 Server Policy**.

4 Select **Add** to create a new policy or **Edit** to modify the policy's properties of a selected DHCPv6 server policy. Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration. The **DHCPv6 Options** tab displays by default.

5 Select the **DHCPv6 Pool** tab.

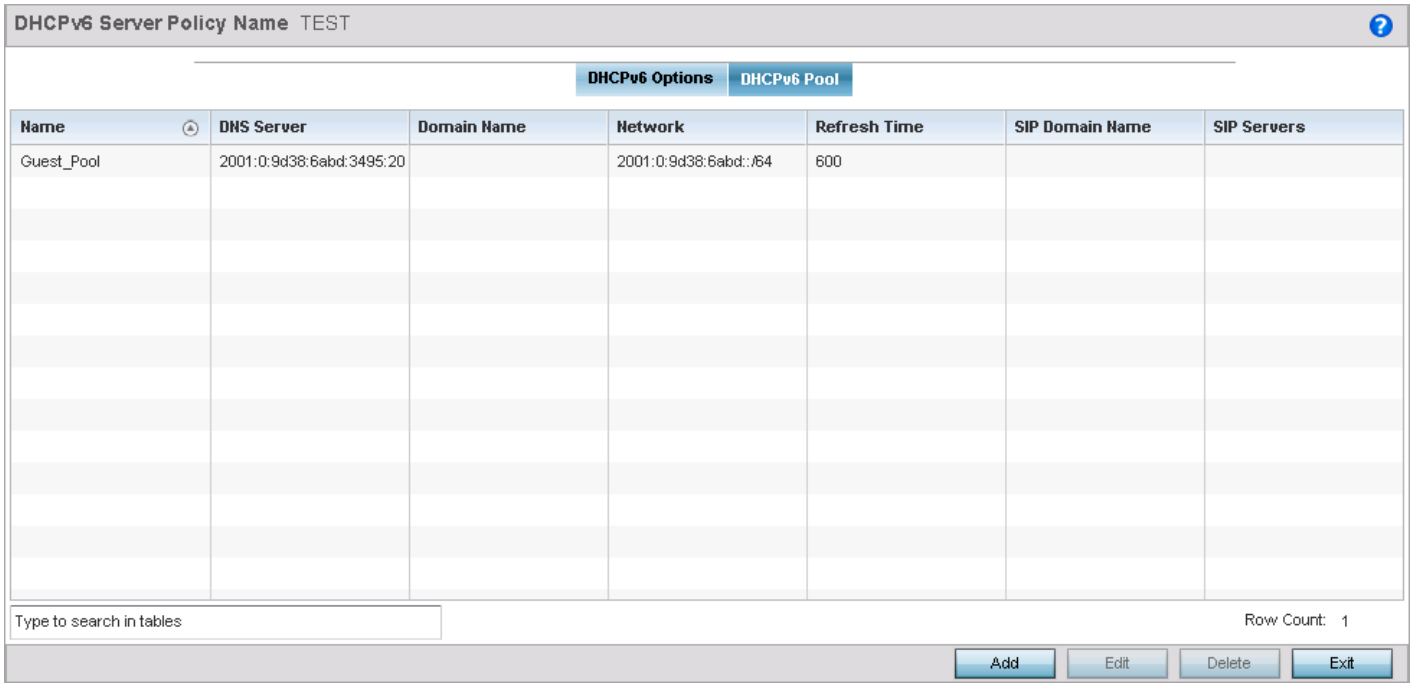


Figure 25: DHCP Server Policy - DHCPv6 Pool tab

6 Set the following parameters within the **Configuration** field:

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 or edit screen.
Refresh Time	Displays the time, in seconds, between refreshes of the DHCPv6 address pool.
SIP Domain Name	Displays the domain name associated with the *Session Initiation Protocol* (SIP) server which 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.

7 Select **Add** to create a new DHCPv6 pool configuration or **Edit** to modify the policy's properties of a selected DHCPv6 pool. Select a configuration item and click **Delete** to delete it.

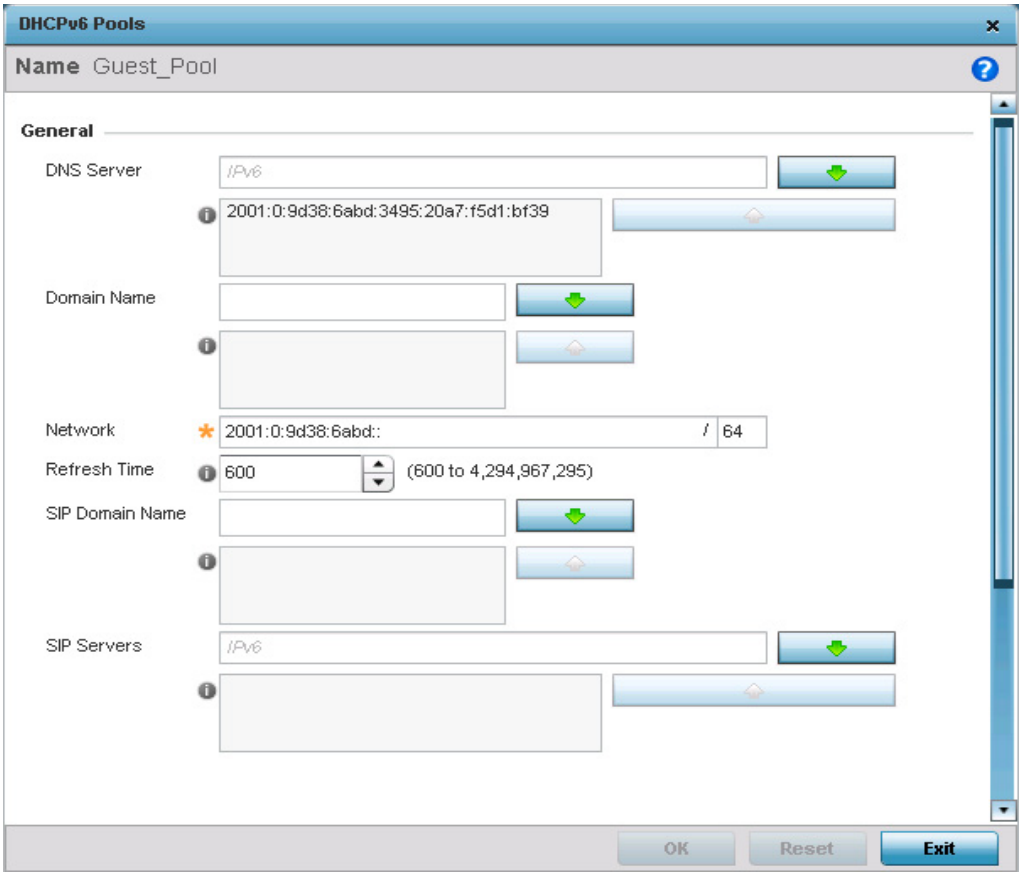


Figure 26: DHCP Server Policy - DHCPv6 Pool - Add/Edit screen

8 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.
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 Domain Name	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.

9 If 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.

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

Setting the RADIUS Configuration

"Services 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 to the access point managed network. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the access point's 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 a RADIUS supported access point, the access point sends the authentication request to the RADIUS server. The authentication and encryption of communications between the access point and server 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.

WiNG managed access points have an internal RADIUS server resource. However, AP6521 model does not have an onboard RADIUS server resource and an external resource must be used.

The access point allows the enforcement of user-based policies. User policies include dynamic VLAN assignment and access based on time of day. The access point uses a default trustpoint. A certificate is required for EAP TTLS,PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

To view RADIUS configurations:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Select 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"
- "Defining User Pools"
- "Configuring the RADIUS Server"

Creating RADIUS Groups

"Setting the RADIUS Configuration"

The access point's RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in the access point's local database. The user ID in the received access request is mapped to the associated wireless group for authentication. Group configurations allow the enforcement of the following policies controlling user access:

- The assignment of a VLAN to the user upon successful authentication
- The creation of a start and end of time in (HH:MM) when a user is allowed to authenticate
- The creation of a list of SSIDs to which a user belonging to this group is allowed to associate
- The ability to set the days of the week a user is allowed to login
- The ability to rate limit traffic

To review existing RADIUS groups and add, modify or delete group configurations:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Select **RADIUS**.

A list of existing groups displays by default.

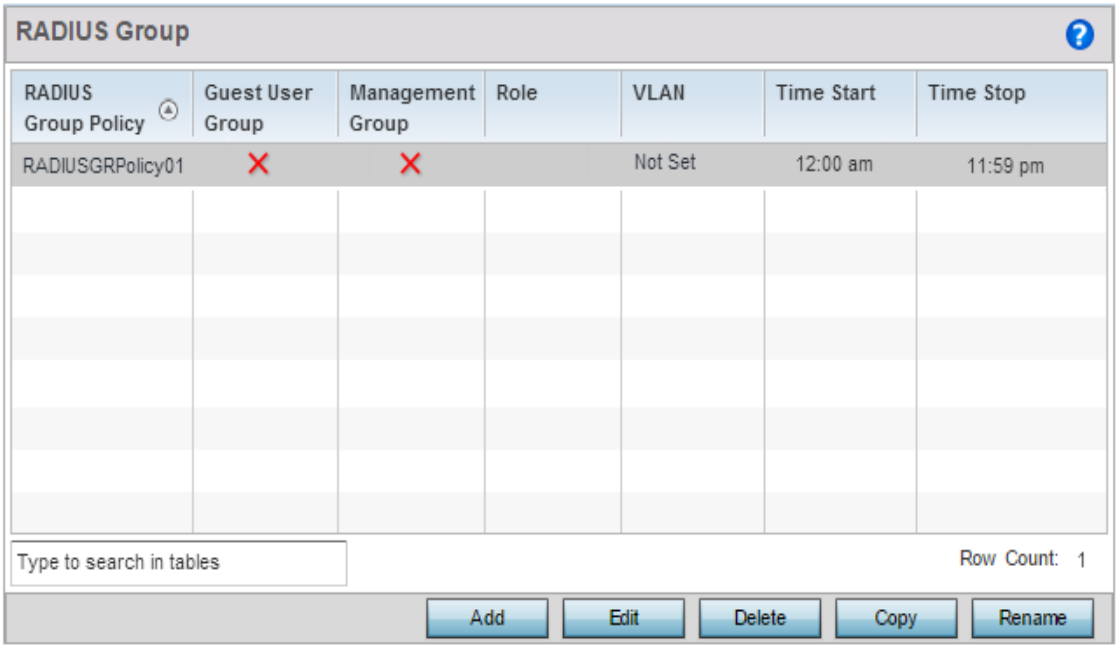


Figure 27: RADIUS Group screen

4 Review the following read-only information for existing groups to determine if a new group requires creation or an existing group requires modification:

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's 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* - Grants full read/write access • *system-admin* - System administrator access • *superuser* - Super user access • *webuser-admin* - Grants rights to manage captive portal users • *vendor-admin* - Grants rights to manage device onboarding
VLAN	Displays the VLAN ID used by the group. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the access point managed 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.

5 Select **Add** to create a new group. To modify the settings of an existing group, select the group and click the **Edit** button. To delete an obsolete group, select the group and click the **Delete** button. Select a group and click **Copy** to make a copy of the group to make further modifications or use **Rename** to rename the existing configuration.

Creating RADIUS Groups

"Creating RADIUS Groups"

To create a RADIUS group:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Select and expand the **RADIUS** menu. Select **Groups** if the RADIUS Group screen is not already displayed by default.

4 Select **Add** to create a new RADIUS group, **Edit** to modify the configuration of an existing group or **Delete** to permanently remove a selected group.

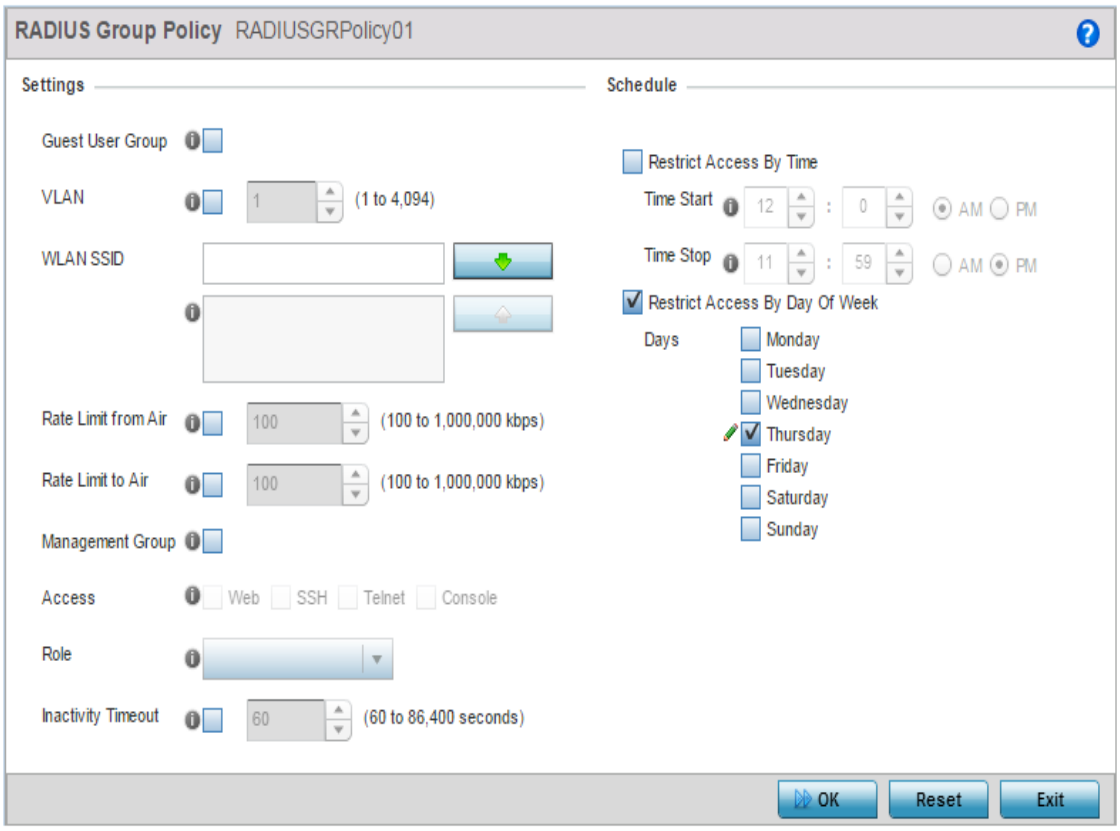


Figure 28: RADIUS Group Policy Add screen

5 Define the following **Settings** to define the user group configuration:

RADIUS Group Policy	If 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. This setting is disabled by default.
VLAN	Select this option (and use the slider) to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (Single VLAN) is enabled for the WLAN for the VLAN to work properly. For more information, see "Configuring WLAN Basic Configuration" on page 529.
WLAN SSID	Assign a list of SSIDs (users) the RADIUS group are allowed to associate to. An SSID cannot exceed 32 characters. Assign WLAN SSIDs representative of users a guest user will need to access. The parameter is not available if this RADIUS group has been defined as a management group.
Rate Limit from Air	Select the check box to set an uplink rate limit for managed clients within this 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 check box to set a downlink rate limit from clients within this 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 the RADIUS group as a management group. If set as management group, assign a role to the members of the group using the Access drop-down menu, allowing varying levels of administrative rights. 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
Role	If a group is listed as a management group, assign a unique role. Available roles include: • *monitor* - Read-only access • *helpdesk* - Helpdesk/support access • *network-admin* - Wired and wireless access • *security-admin* - Grants full read/write access • *system-admin* - System administrator access • *superuser* - Super user access • *webuser-admin* - Grants rights to manage captive portal users • *vendor-admin* - Grants rights to manage device onboarding
Inactivity Timeout	Select 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. The default is 60 seconds.
Session Time	Select the option to enable session timeout. Use the drop-down menu to set a client session time in *Minutes* (5 - 144,000). This is the session time a client is granted upon successful authentication. The RADIUS session is terminated when this time expires.

6 Set the **Schedule** to configure access times and dates. Select **Restrict Access By Time** control to enable time based access.

Time Start	Use the spinner control to set the time (in HH:MM format) RADIUS group members are allowed to login and access 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.

7 Select **Restrict Access By Day Of Week** control to enable access based on the day of the week.

Days	Optionally select the *Restrict Access by Day Of Week* option, and select the days RADIUS group members can access RADIUS resources. This is an additional means of refining the access permissions of RADIUS group members.

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

Defining User Pools

"Setting the RADIUS Configuration"

A user pool defines policies for individual user access to the access point's internal RADIUS resources. User or pools provide a convenient means of providing user access to RADIUS resources based on the pool's unique permissions (either 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** tab from the Web user interface.

2 Select **Services**.

3 Expand the **RADIUS** menu option and select **User Pools**.

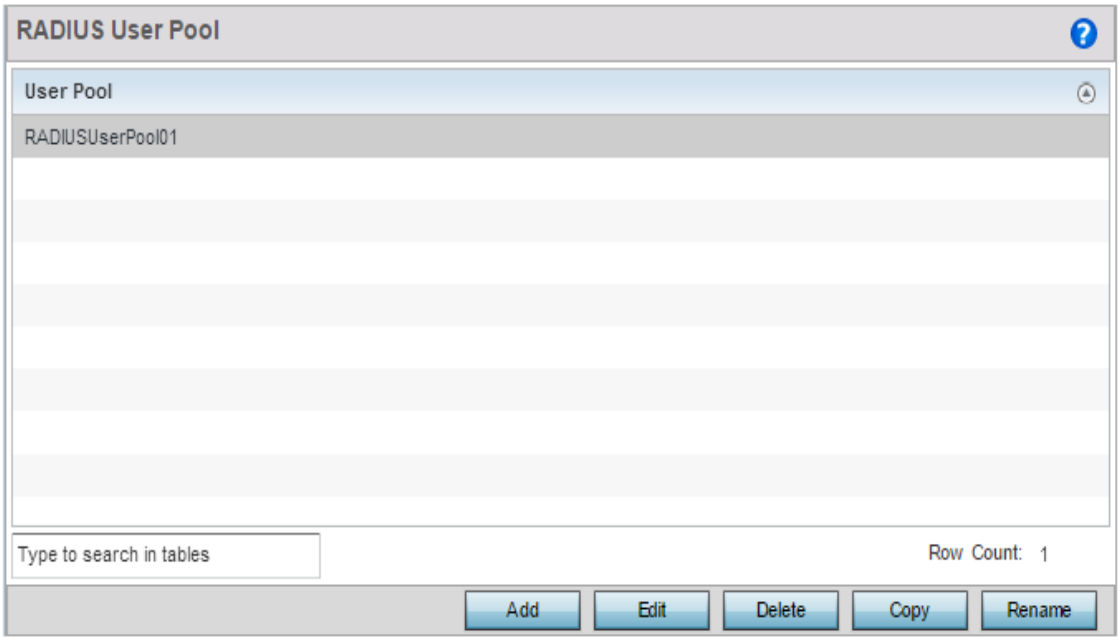


Figure 29: RADIUS User Pool screen

4 Select **Add** to create a new user pool, **Edit** to modify the configuration of an existing pool or **Delete** to remove a selected pool.

5 If creating a new pool, assign it a name up to 32 characters and select **Continue**.

The name should be representative of the users comprising the pool and/or the temporary or permanent access privileges assigned.

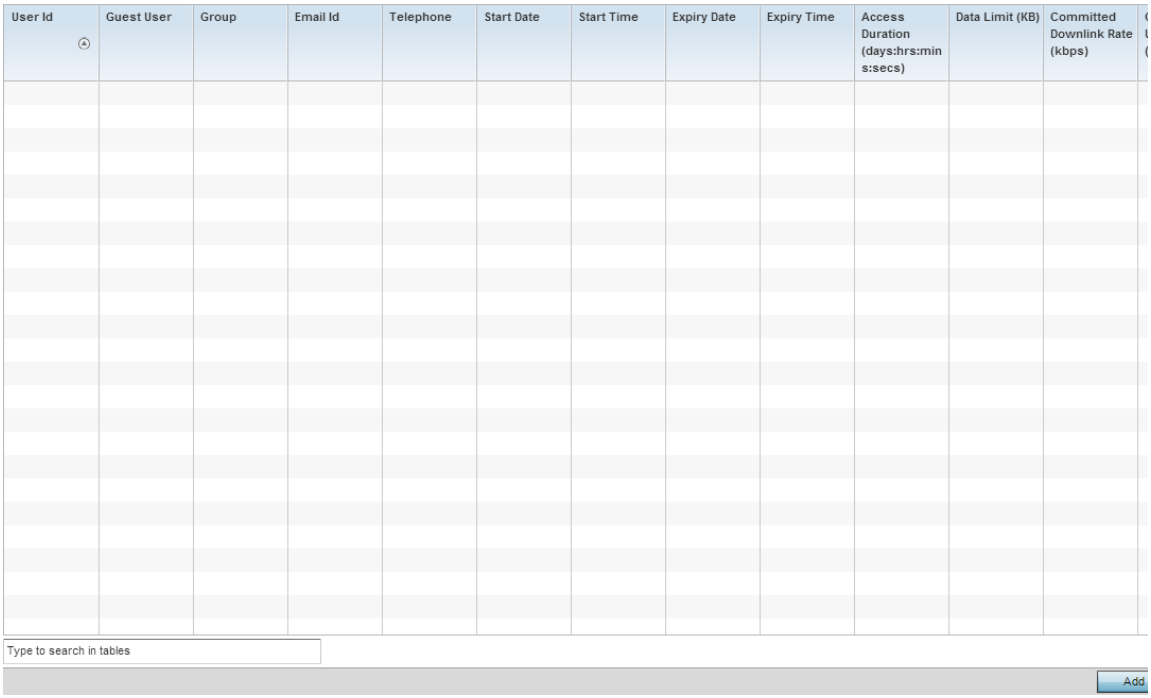


Figure 30: RADIUS User Pool Add screen

6 Refer to the following **User Pool** configurations to discern when specific user IDs have access to the access point's RADIUS resources:

User Id	Displays the unique alphanumeric string identifying this user. This is ID assigned to the user when created and cannot be modified with the rest of the configuration.
Guest User	Specifies (with a green checkmark) that 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	Displays the group name each configured user ID is a member.
Email Id	Displays the configured E-mail ID for this user. This is the address used when communicating with users in this pool.
Telephone	Displays the configured telephone number for this user. This is the number used when communicating with users in this pool.
Start Date	Lists the *month*, *day* and *year* the listed user ID can access the access point's internal RADIUS server resources.
Start Time	Lists the time the listed user ID can access the internal RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.
Expiry Date	Lists the month, day and year the listed user Id can no longer access the internal RADIUS server.
Expiry Time	Lists the time the listed user Id losses access internal RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.

Access Duration (days:hrs:mins:secs)	Lists the total duration of allowed access for guest users. Up to 356 days can be configured.
Data Limit (KB)	Lists the total amount of bandwidth (in KiloBytes) consumable by each guest user.
Committed Downlink Rate (kbps)	Displays 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)	Displays 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)	Displays 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)	Displays 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.

7 Select the **Add** button to add a new RADIUS user, **Edit** to modify the configuration of an existing user or **Delete** to remove an existing user Id. Select a RADIUS user and click **Copy** to make a copy of the user to make further modifications or use **Rename** to rename the existing RADIUS user.

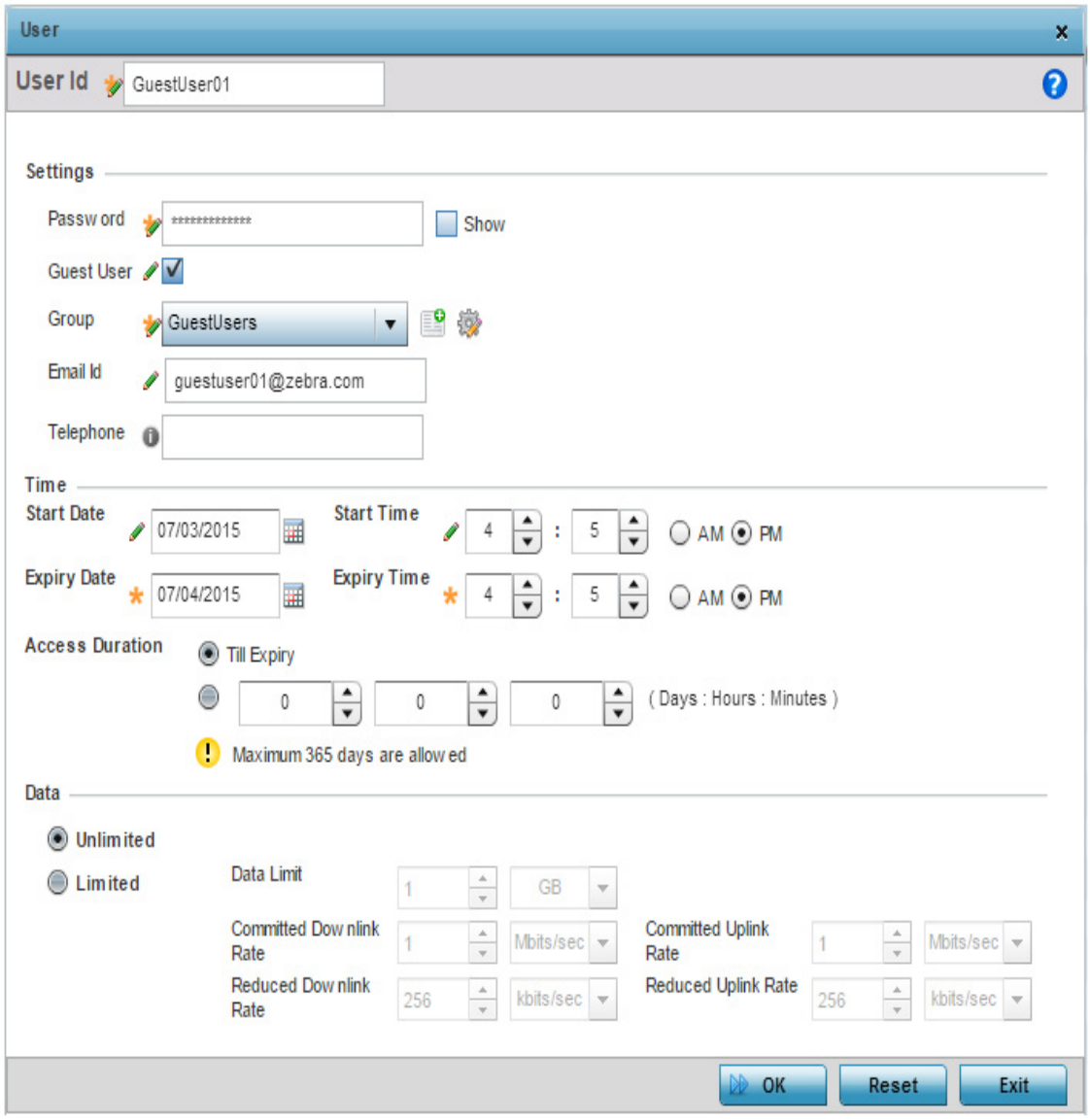


Figure 31: RADIUS - Add User screen

8 Set the following to create a new RADIUS 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. The password cannot exceed 32 characters. Select the Show check box to expose the password's actual character string. Leaving the option unselected displays the password 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 the groups listed are not relevant to the user's intended access, select the *Create* icon and create a new group configuration suitable for the user membership. For more information, see "Creating RADIUS Groups" on page 803.
Email Id	Set the E-mail ID for this user.
Telephone	Configure the telephone number for this user.

9 Set the following **Time** settings for the new user:

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 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, Hours and Minutes the user is allowed access. The Access Duration cannot exceed 365 days.

10 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 (KB)	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 have 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).

11 Select **OK** to save the user group membership configuration. Select Reset to revert to the last saved configuration.

Configuring the RADIUS Server

"Setting the RADIUS Configuration"

A RADIUS server policy is a unique authentication and authorization configuration for receiving user connection requests, authenticating users and returning the configuration information necessary for the RADIUS client to deliver service to the user. An access point's requesting client is the entity with authentication information requiring validation. The access point's local RADIUS server has access to a database of authentication information used to validate client authentication requests.

The RADIUS server ensures the information is correct using authentication schemes like PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information. The access point's RADIUS server policy can also be configured to refer to an external LDAP resource to verify the user's credentials. The creation and utilization of a single RADIUS server policy is supported.

To manage the access point's RADIUS server policy:

1 Select **Configuration** tab from the Web user interface.

2 Select **Services**.

3 Expand the **RADIUS** menu option and select **RADIUS Server**.

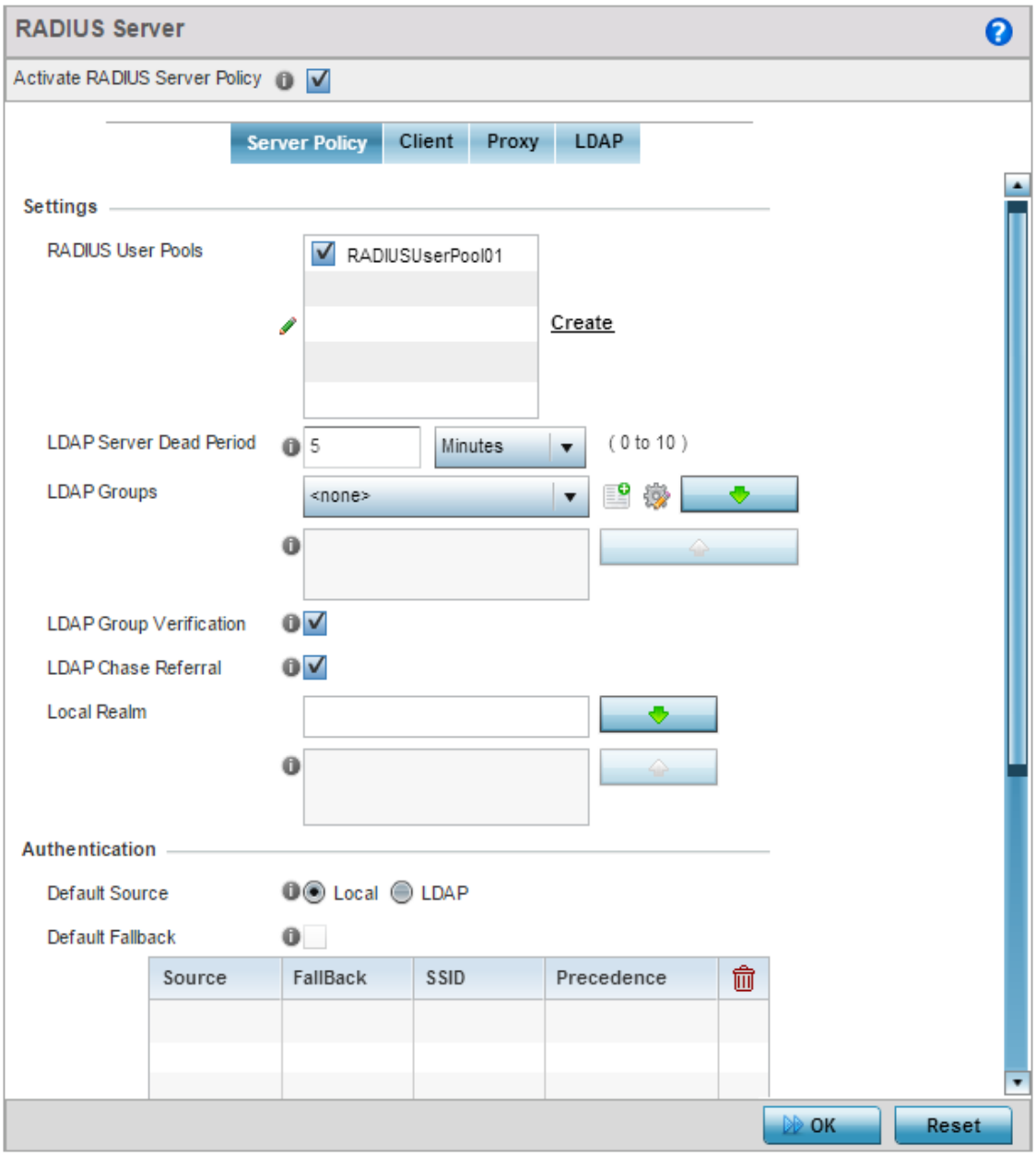


Figure 32: RADIUS Server Policy screen - Server Policy tab

The **RADIUS Server Policy** screen displays with the **Server Policy** tab displayed by default.

4 Select the **Activate RADIUS Server Policy** button to enable the parameters within the screen for configuration. Ensure this option remains selected, or this RADIUS server configuration is not applied to the access point profile.

5 Define the following **Settings** required in the creation or modification of the server policy:

RADIUS User Pools	Select the user pools (groups of existing client users) to apply to this server policy. If there is not an existing user pool configuration suitable for the deployment, select the Create link and define a new configuration. For more information, see "Defining User Pools" on page 806.
LDAP Server Dead Period	Set an interval in either *Seconds* (0 - 600) or *Minutes* (0- 10) during which the access point will not contact its LDAP server resource. A dead period is only implemented when additional LDAP servers are configured and available.
LDAP Groups	Use the drop-down menu to select LDAP groups to apply the server policy configuration. Select the *Create* or *Edit* icons as needed to either create a new group or modify an existing group. Use the arrow icons to add and remove groups as required.
LDAP Group Verification	Select the check box to set the LDAP group search configuration. This setting is enabled by default.
LDAP Chase Referral	Select the check box to set the LDAP referral chase feature. This settings is enabled by default. When enabled, if the LDAP server does not contain the requested information, it indicates to the LDAP client that it does not have the requested information and provides the client with another LDAP server that could have the requested information. It is up to the client to contact the other LDAP server for its information.
Local Realm	Define the LDAP Realm performing authentication using information from an LDAP server. User information includes *user name*, *password*, and the *groups* to which the user belongs.

6 Set the following **Authentication** parameters to define server policy authorization settings.

Default Source	Select the RADIUS resource for user authentication with this server policy. Options include Local for the local user database or LDAP for a remote LDAP resource. The default setting is *Local*.
Default FallBack	Select this option to indicate that fall back from RADIUS to local is enabled incase RADIUS authentication is not available for any reason. This option is only enabled when *LDAP* is selected as the *Default Source*. Use the *Add Row* button to add fallback sources into the *Sources* table. Provide the following information: • *Source* – Select the type of fallback. Select from *LDAP* or *Local* • *Fallback* – Select to enable fallback on this record. • *SSID* – Enter the SSID to fall back on. • *Precedence* – Use the spinner to select the precedence for selection of fallback.
Authentication Type	Use the drop-down menu to select the EAP authentication scheme for local and LDAP authentication. The following EAP authentication types are supported: • *All* – Enables all authentication schemes. • *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. However, when user credentials are stored on an LDAP server, the RADIUS server cannot conduct PEAP-MSCHAPv2 authentication on its own, as it is not aware of the password. Use LDAP agent settings to locally authenticate the user. Additionally, an authentication utility (such as Samba) must be used to authenticate the user. Samba is an open source software used to share services between Windows and Linux machine.

Do Not Verify Username	Only enabled when *TLS* is selected in *Authentication Type*. When selected, user name is not matched but the certificate expiry is checked.
Enable CRL Validation	Select this option to enable a *Certificate Revocation List* (CRL) check. Certificates can be checked and revoked for a number of reasons, including the failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. This option is disabled by default.
Enable EAP Termination	Select this option to enable EAP Termination on the current RADIUS server policy. EAP Termination terminates EAP authentication at the controller.
Bypass CRL Check	Select the option to bypass a *certificate revocation list* (CRL) check when a CRL is not detected. This setting is enabled by default. A CRL is a list of certificates that have been revoked or are no longer valid.
Allow Expired URL	Select this option to allow the use of an expired CRL. This option is enabled by default.



NOTE

When using LDAP as authentication external source, PEAP-MSCHAPV2 authentication type can be used only if the LDAP server returns the password as plain-text. PEAP-MSCHAPv2 authentication is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory Server.

7 If using LDAP as the default authentication source, select **+ Add Row** to set LDAP Agent settings.

When a user's credentials are stored on an external LDAP server, the controller or service platform's local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource using credentials maintained locally.

Username	Enter a128 character maximum username for the LDAP server's domain administrator. This is the username defined on the LDAP server for RADIUS authentication requests.
Password	Enter and confirm the 32 character maximum password (for the username provided above). The successful verification of the password maintained on the controller or service platform enables PEAP-MSCHAPv2 authentication using the remote LDAP server resource.
Retry Timeout	Set the number of *Seconds* (60 - 300) or *Minutes* (1 - 5) to wait between LDAP server access requests when attempting to join the remote LDAP server's domain. The default settings is one minute.
Redundancy	Define the *Primary* or *Secondary* LDAP agent configuration used to connect to the LDAP server domain.
Domain Name	Enter the name of the domain (from 1 - 127 characters) to which the LDAP server resource belongs.

Set the following **Session Resumption/Fast Reauthentication** settings to define how server policy sessions are re-established once terminated and require cached data to resume:

Enable Session Resumption	Select the check box to control volume and the duration cached data is maintained by the server policy upon the termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption. This setting is disabled by default.
Cached Entry Lifetime	Use the spinner control to set the lifetime (1 - 24 hours) cached data is maintained by the RADIUS server policy. The default setting is 1 hour.
Maximum Cache Entries	Use the spinner control to define the maximum number of entries maintained in cache for this RADIUS server policy. The default setting is 128 entries.

8 Select **OK** to save the settings to the server policy configuration. Select **Reset** to revert to the last saved configuration.

9 Select the **Client** tab and ensure the **Activate RADIUS Server Policy** button remains selected.

The access point uses a RADIUS client as a mechanism to communicate with a central server to authenticate users and authorize access.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash to create a 16 octet value used with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS access request packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified access accept packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified access reject message, the username and password are considered incorrect, and the user is not authenticated.

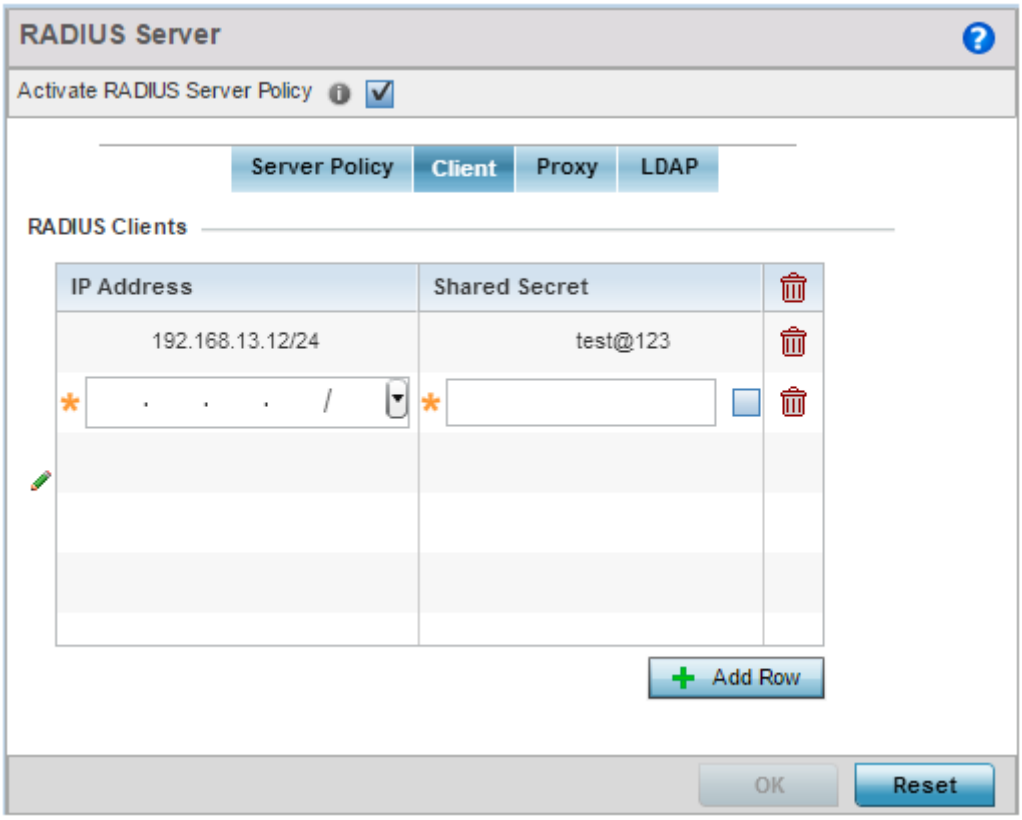


Figure 33: RADIUS Server Policy screen - Client tab

10 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.

11 Specify the **IP Address** and mask of the RADIUS client authenticating with the RADIUS server.

12 Specify a **Shared Secret** for authenticating the RADIUS client.

13 Shared secrets verify RADIUS messages with a RADIUS enabled device configured with the same shared secret. Select the **Show** check box to expose the shared secret's actual character string. Leave the option unselected to display the shared secret as a string of asterisks (*).

14 Select **OK** to save the server policy's client configuration. Select the **Reset** button to revert to the last saved configuration.

15 Select the **Proxy** tab and ensure the **Activate RADIUS Server Policy** button remains selected.

A user's access request is sent to a proxy server if it cannot be authenticated by local RADIUS resources. The proxy server checks the information in the user access request, and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to the NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the access point's RADIUS server receives a request for a user name containing a realm, the server references a table of configured realms. If the realm is known, the server proxies the request to the RADIUS server. The behavior of the proxying server is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove or rewrite requests when they are proxied.

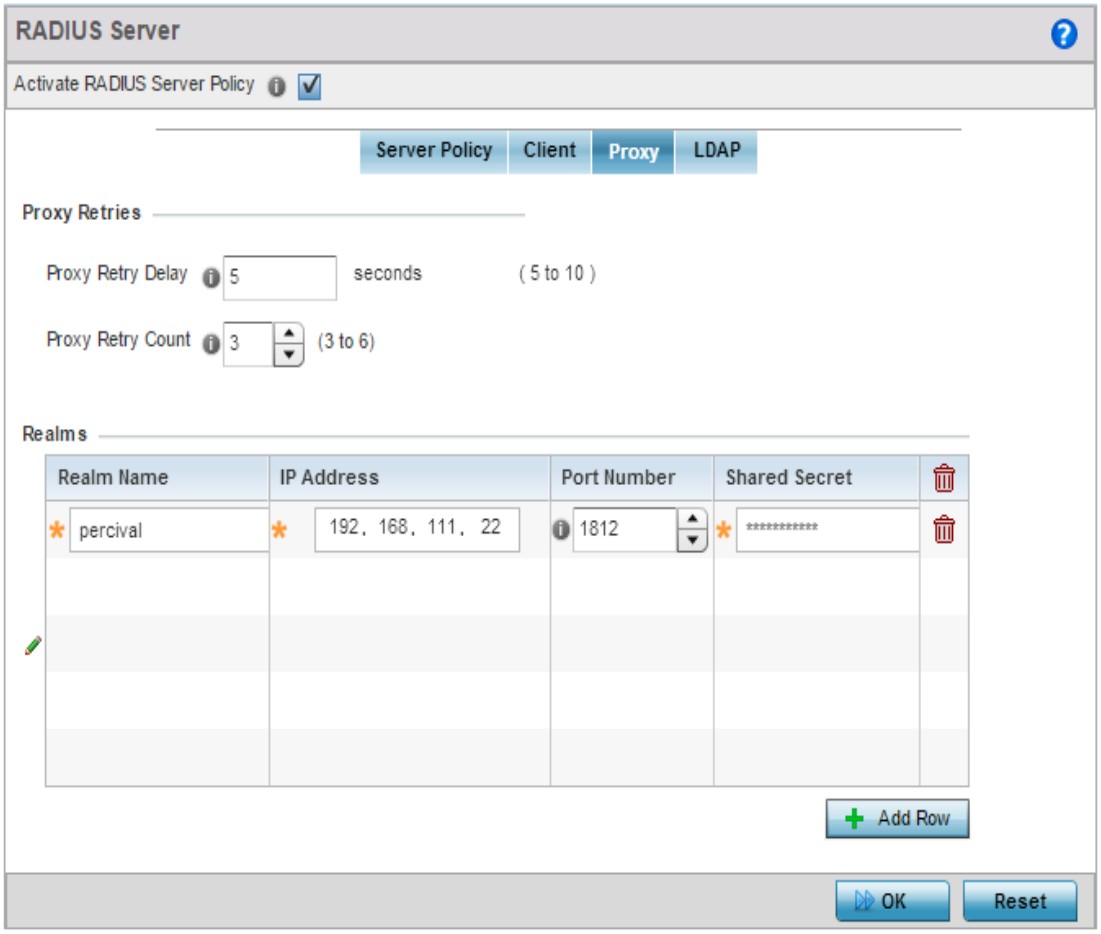


Figure 34: RADIUS Server Policy screen - Proxy tab

16 Enter the **Proxy Retry Delay** as a value in seconds (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.

17 Enter the **Proxy Retry Count** field as a value from 3 - 6. This is the number of retries sent to the proxy server before giving up the request. The default retry count is 3 attempts.

18 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.

19 Enter a 50 character maximum **Realm Name**. When the access point's RADIUS server receives a request for a user name, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

20 Enter the Proxy server's **IP Address**. This is the address of server checking the information in the user access request. The proxy server either accepts or rejects the request on behalf of the RADIUS server.

21 Enter the TCP/IP **Port Number** for the server that acts as a data source for the proxy server. Use the spinner to select a value from 1024 - 65535. The default port is 1812.

22 Enter the RADIUS client's **Shared Secret** for authenticating the RADIUS proxy.

23 Select the **Show** check box to expose the shared secret's actual character string. Leave the option unselected to display the shared secret as a string of asterisks (*).

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

25 Select the **LDAP** and ensure the **Activate RADIUS Server Policy** button remains selected.

Administrators have the option of using the access point's RADIUS server to authenticate users against an external LDAP server resource. An external LDAP user database allows the centralization of user information and reduces administrative user management overhead. Thus, making the RADIUS authorization process more secure and efficient.

RADIUS is not just a database. It is a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location. It is the access point's RADIUS resources that provide the tools to perform user authentication and authorize users based on complex checks and logic. There is no way to perform such complex authorization checks from a LDAP user database alone.

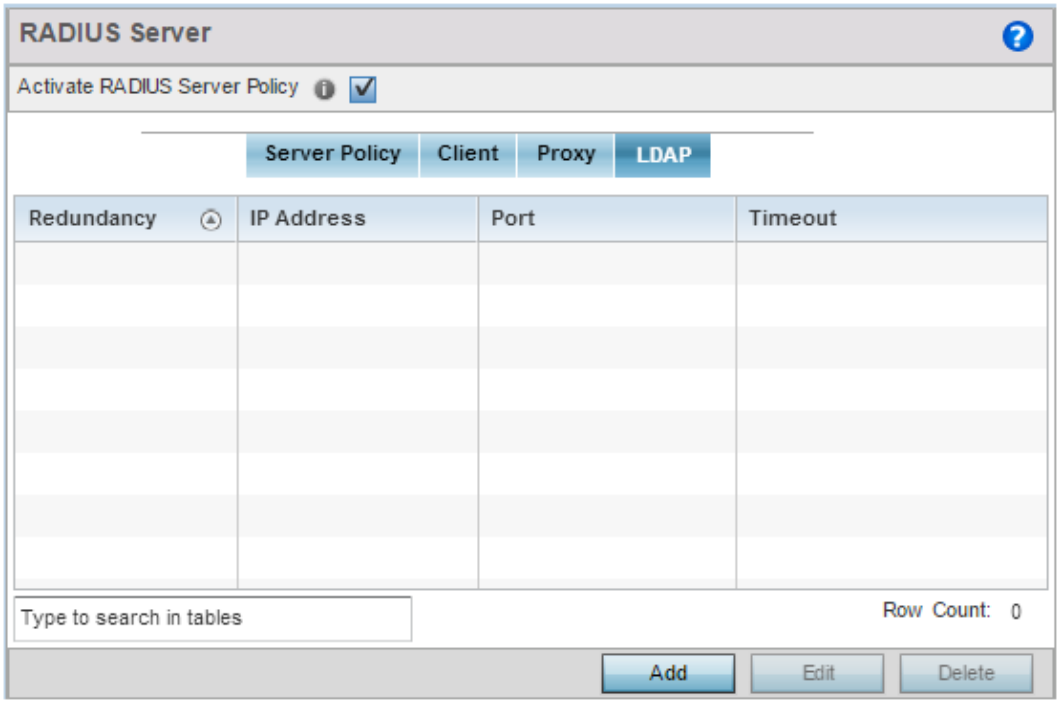


Figure 35: RADIUS Server Policy screen - LDAP tab

26 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:

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 user information is 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 access point's local RADIUS server.
Port	Lists the physical port 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.

27 Select **Add** to add a new LDAP server configuration, **Edit** to modify an existing LDAP server configuration or **Delete** to remove a LDAP server from the list of those available.

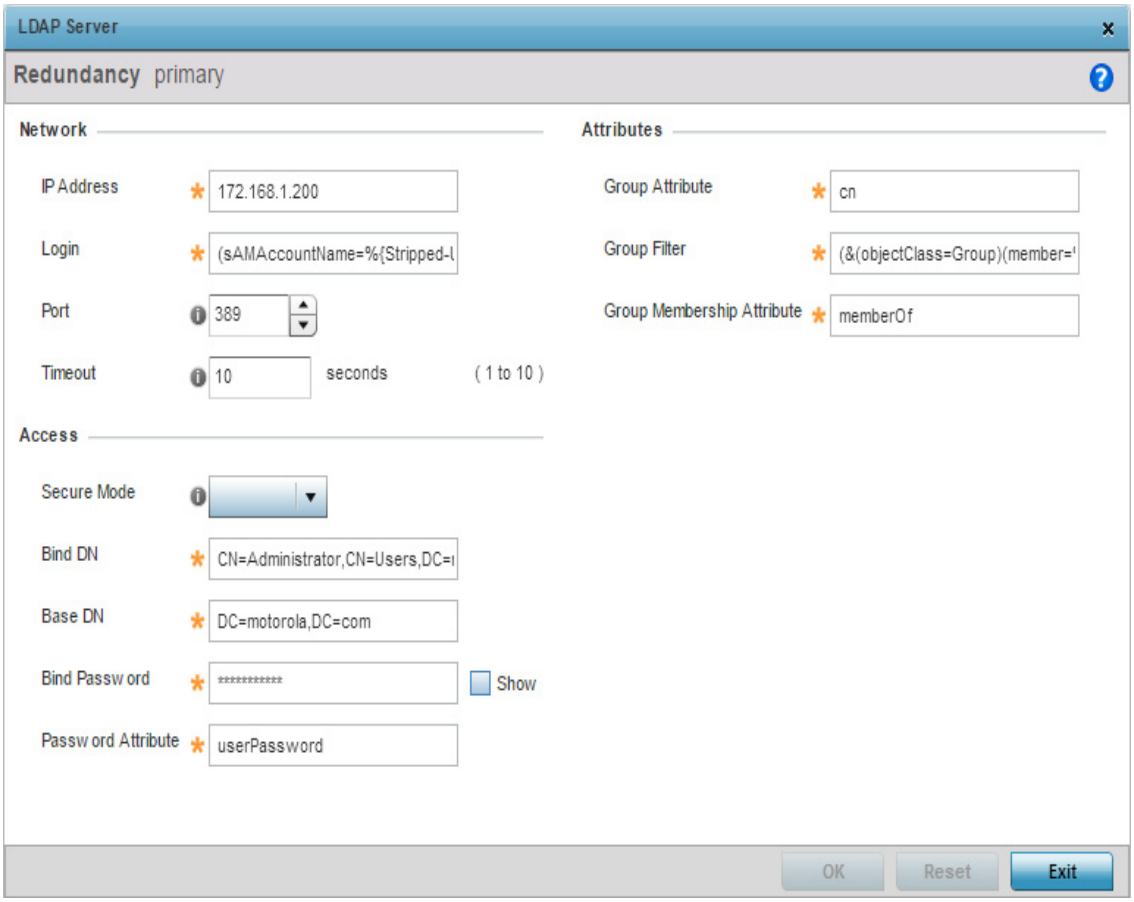


Figure 36: LDAP Server Add screen

28 Set the following **Network** address information required for the connection to the external LDAP server resource:

Redundancy	Define whether this LDAP server is a primary or secondary server resource. Primary servers are always queried for the first connection attempt. 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 to increase the security of the connection between the access point and remote LDAP resource.
Port	Use the spinner control to set the physical port used by the RADIUS server to secure a connection with the remote LDAP server resource. The default port is 389.
Timeout	Set an interval between 1 - 10 seconds the RADIUS server uses as a wait period for a response from the target primary or secondary LDAP server resource. The default setting is 10 seconds.

29 Set the following **Access** information for the connection to the external LDAP server resource:

Secure Mode	Specify the security mode to use when connecting to the external LDAP server. Use *start-tls* or *tls-mode* to connect. The *start-tls* mode offers a way to upgrade a plain text connection to an encrypted connection using TLS.
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). The RDN 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* check box to expose the password's actual character string. Leave the option unselected to display the password as a string of asterisks (*). The password cannot 32 characters.
Password Attribute	Enter the LDAP server password attribute. The password cannot exceed 64 characters.

30 Set the following **Attributes** for LDAP groups to optimally refine group queries:

Group Attribute	LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group, an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.
Group Filter	Specify the group filters used by the LDAP server. The group filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
Group Membership Attribute	Specify the group member attribute sent to the LDAP server when authenticating users.

31 Select the **OK** button to save the changes to the LDAP server configuration. Select **Reset** to revert to the last saved configuration.

Setting the URL List

"Services Configuration"

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 **Configuration** tab from the main menu.

2 Select the **Services** tab from the **Configuration** menu.

3 Select **URL List** from the menu.

The URL Lists screen displays existing policies. New policies can be created, existing policies can be modified, deleted or copied.

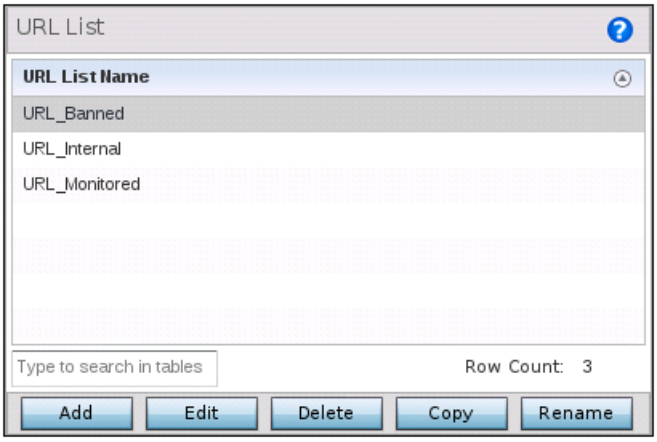


Figure 37: Smart Caching - URL List Name screen

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.

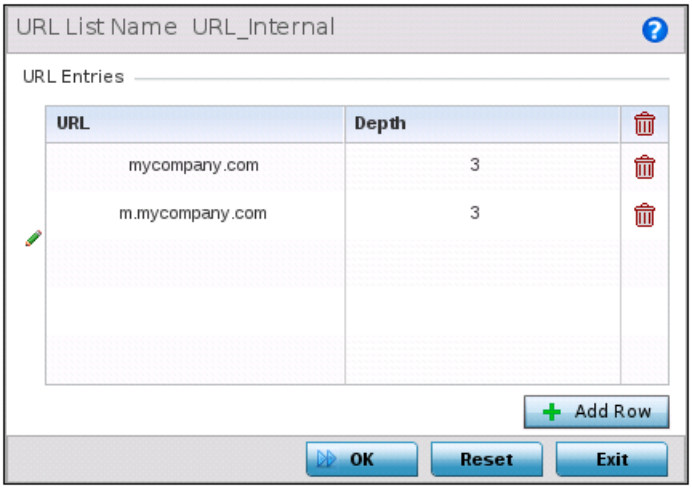


Figure 38: URL List Name - Add/Edit screen

6 Select **+ Add Row** to display configurable parameters for defining a URL and its depth.

7 If creating a new URL lists policy, assign it a **Name**. If editing an existing URL Lists policy, the policy name cannot be modified. The name cannot exceed 32 characters.

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. Since 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.

Services Deployment Considerations

"Services Configuration"

Before defining the access point's configuration using the Services menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- It is recommended that each RADIUS client use a different shared secret password. If a shared secret is compromised, only the one client poses a risk as opposed all the additional clients that potentially share that secret password.
- Consider using an LDAP server as a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location.
- Designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server were to become unavailable.

10 Management Access

The access point uses mechanisms to allow/deny access to the network for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for unique policies. Management Access is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Disable unused and insecure management interfaces as required within different access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources too.



NOTE

The access point utilizes a single Management Access policy, so ensure all the intended administrative roles, access control permissions, authentication settings and SNMP settings are correctly set. If the access point is a Virtual Controller AP, these are the management settings used by adopted access points.

To set Management Access administrative rights, access control permissions, authentication refer to the following:

- "Creating Administrators and Roles"
- "Setting the Access Control Configuration"
- "Setting the Authentication Configuration"
- "Setting the SNMP Configuration"
- "SNMP Trap Configuration"

Refer to "Management Access Deployment Considerations" on page 838 for tips on how to optimize the access point's management access configuration.

Creating Administrators and Roles

- "Management Access"

Use the **Administrators** screen to review existing administrators, their access medium and their administrative role within the access point managed network. New administrators can be added and existing administrative configurations modified or deleted as required.

To create administrators and assign them access types and roles:

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

2 Select **Management** from the top menu.

3 Select **Administrators.**

The **Administrators** screen displays by default.

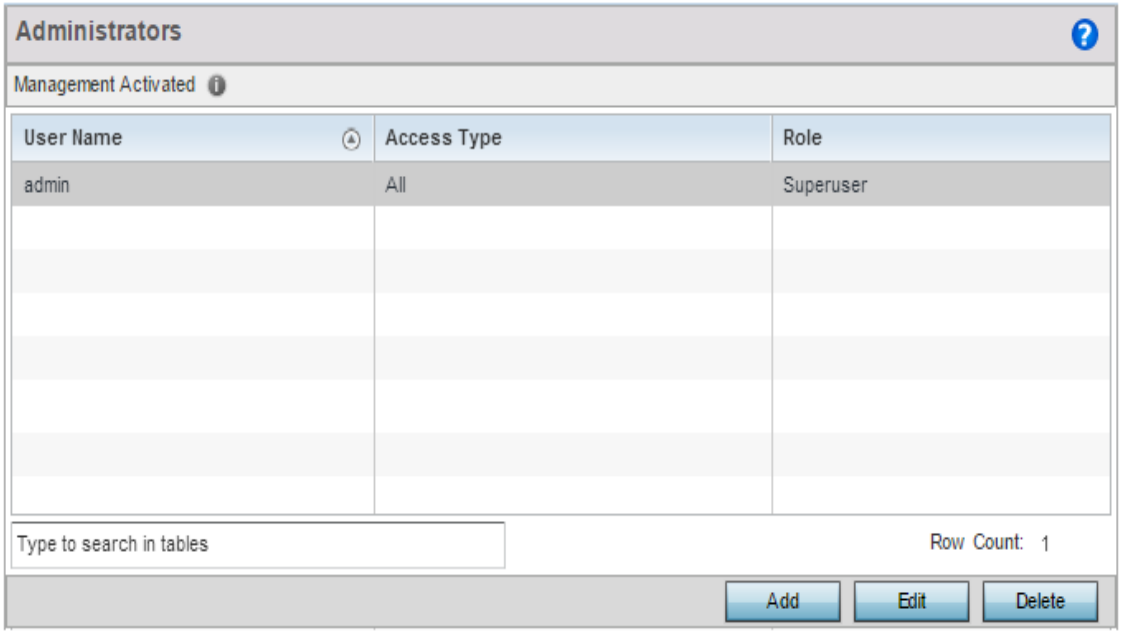


Figure 1: Management Policy - Administrators screen

4 Refer to the following to review existing administrators:

User Name	Displays the name assigned to the administrator upon creation. The name cannot be modified when editing an administrator's configuration.
Access Type	Lists the *Web UI*, *Telnet*, *SSH* or *Console* access assigned to each administrator. A single administrator can have any or all roles assigned.
Role	Lists the *Superuser*, *System*, *Network*, *Security*, *Monitor*, *Help Desk*, *Web User or Device Provisioning* role assigned to each listed administrator. An administrator can only be assigned one role at a time.

5 Select **Add** to create a new administrator configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove an administrator.

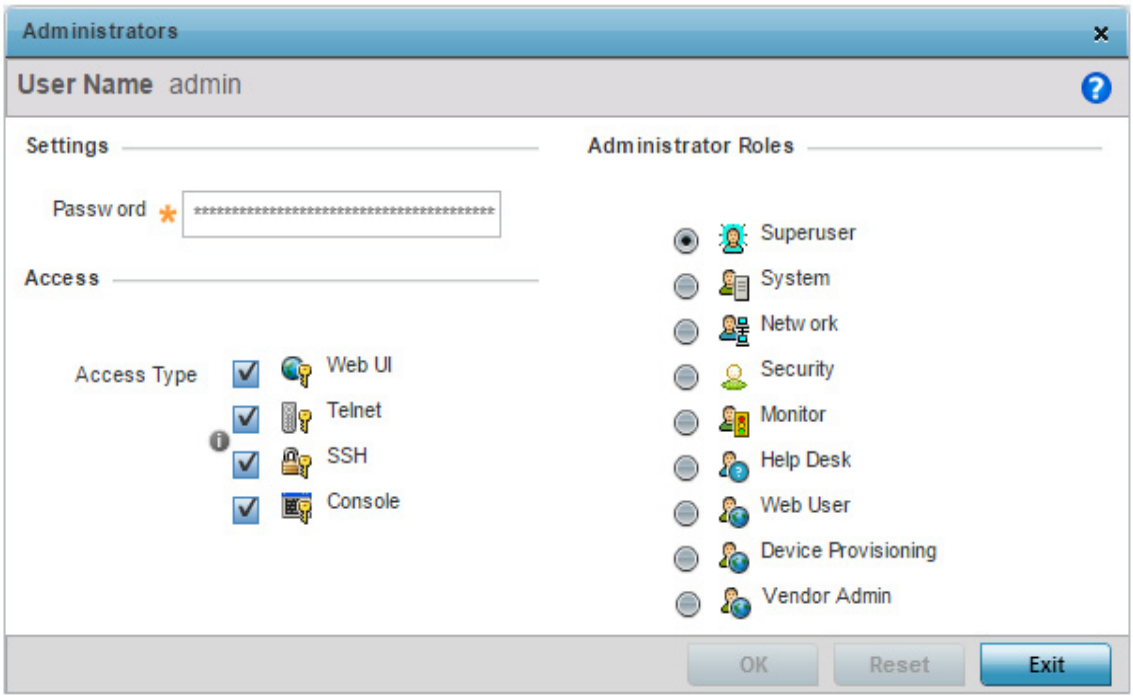


Figure 2: Administrators screen

6 If adding a new administrator, enter the name in the **User Name** field. This is a mandatory field, and cannot exceed 32 characters. Optimally assign a name representative of the user's intended access type and role.

7 Provide a strong administrator password. Once provided, **Reconfirm** the password to ensure its accuracy. This is also a mandatory field.

8 Define protocol **Access** for the user's unique permissions. If required, all four options can be selected and invoked simultaneously.

Web UI	Select this option to enable access to the access point's Web UI.
Telnet	Select this option to enable access to the access point using TELNET.
SSH	Select this option to enable access to the access point using SSH.
Console	Select this option to enable access to the access point's console.

9 Select an **Administrator Role**. Only one role can be assigned.

Superuser	Select this option to assign complete administrative rights to this user. This entails all the roles listed.
System	Select this option to allow the administrator to configure general settings like NTP, boot parameters, licenses, perform image upgrade, auto install, manager redundancy/clustering and control access.
Network	Select this option to allow the user to configure all wired and wireless parameters (IP configuration, VLANs, L2/L3 security, WLANs, radios etc).
Security	Select this option to set the administrative rights for a security administrator allowing the configuration of all security parameters.
Monitor	Select this option to assign permissions without administrative rights. The Monitor option provides read-only permissions.
Help Desk	Assign this option to someone who typically troubleshoots and debugs reported problems. The Help Desk manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the access point.
Web User	Select this option to assign privileges to add users for captive portal authentication. For more information on captive portal access rights and configuration requirements, see "Configuring Captive Portal Policies" on page 759.
Device Provisioning	Select this option 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.
Vendor Admin	Select this option to create a user role group that 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

10 Select **OK** to save the administrator configuration. Select **Reset** to revert to the last saved configuration.

Setting the Access Control Configuration

- "Management Access"

Refer to the **Access Control** screen to allow/deny management access to the network using selected protocols (*HTTP*, *HTTPS*, *Telnet*, *SSH* or *SNMP*). Access options can be either enabled or disabled as required. Disable unused interfaces to reduce 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.

The following table demonstrates some interfaces provide better security than others and are more desirable:

Access Type	Encrypted	Authenticated	Default State
Telnet	No	Yes	Disabled
HTTP	No	Yes	Disabled
HTTPS	Yes	Yes	Disabled
SSHv2	Yes	Yes	Disabled

To set user access control configurations:

1 Select **Configuration.**

2 Select **Management.**

3 Select **Access Control** from the list of Management Policy options in the upper, left-hand, side of the UI.

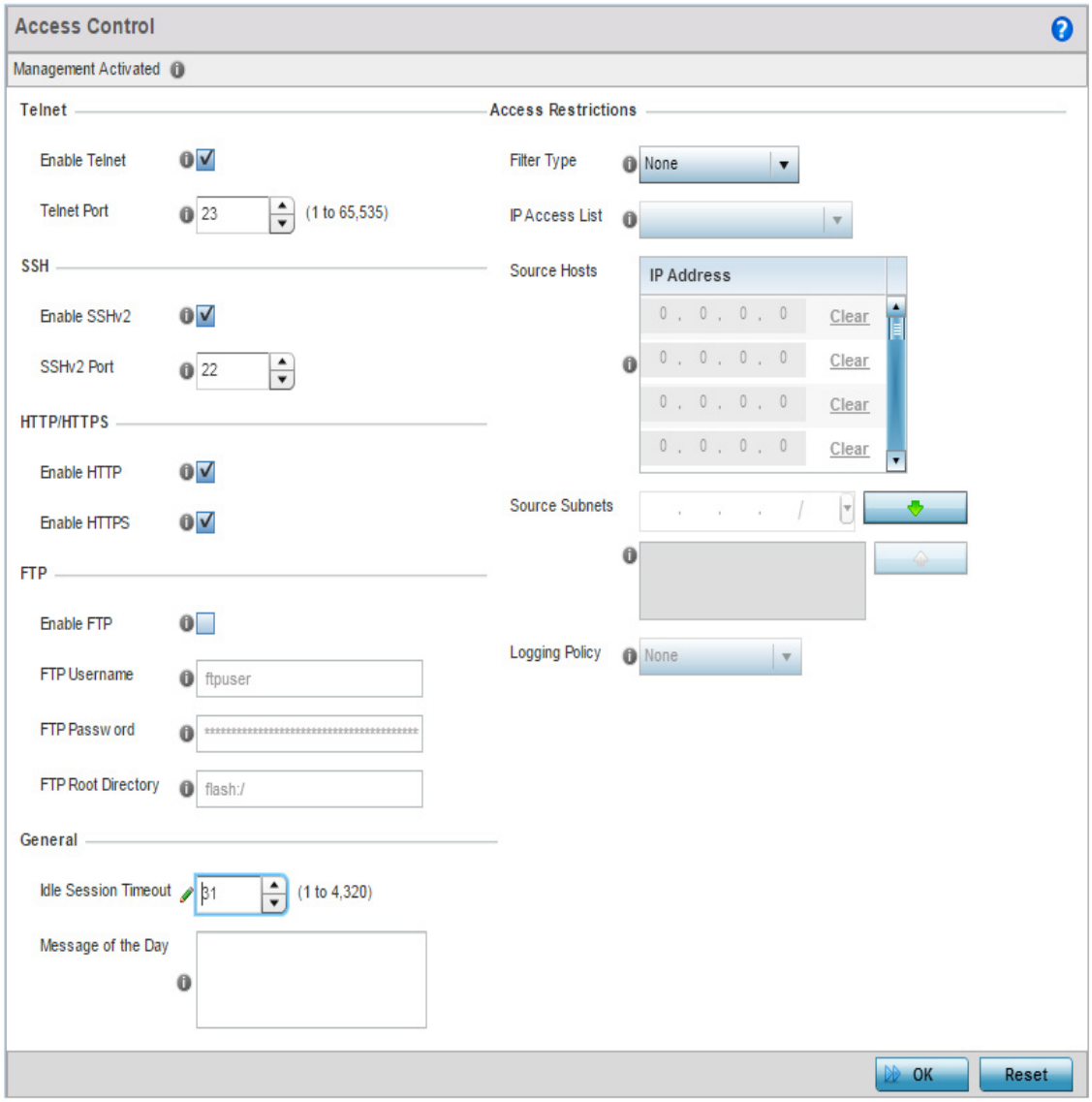


Figure 3: Management Policy - Access Control screen

4 Set the following parameters required for **Telnet** access:

Enable Telnet	Select the check box 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 or by entering the port number in the field.

5 Set the following parameters required for **SSH** access:

Enable SSHv2	Select the check box 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 or by entering the port number in the field.

6 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 an AP6521's external RADIUS server is not reachable, HTTPS or SSH management access to the access point may be denied. Those models do not have an onboard RADIUS resource and are reliant on an external RADIUS resource for authentication.

7 Set the following FTP parameters:

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:/

8 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.

9 Set the following **Access Restrictions**:

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*.

10 Select **OK** to save the Access Control configuration. Select **Reset** to revert to the last saved configuration.

Setting the Authentication Configuration

"Management Access"

As part of the access point's Management Policy, define how client authentication requests are validated using either an *external* or *internal* authentication resource:

To configure an authentication resource:

1 Select **Configuration**.

2 Select **Management**.

3 Select **Authentication** from the list of Management Policy options in the upper, left-hand, side of the UI.

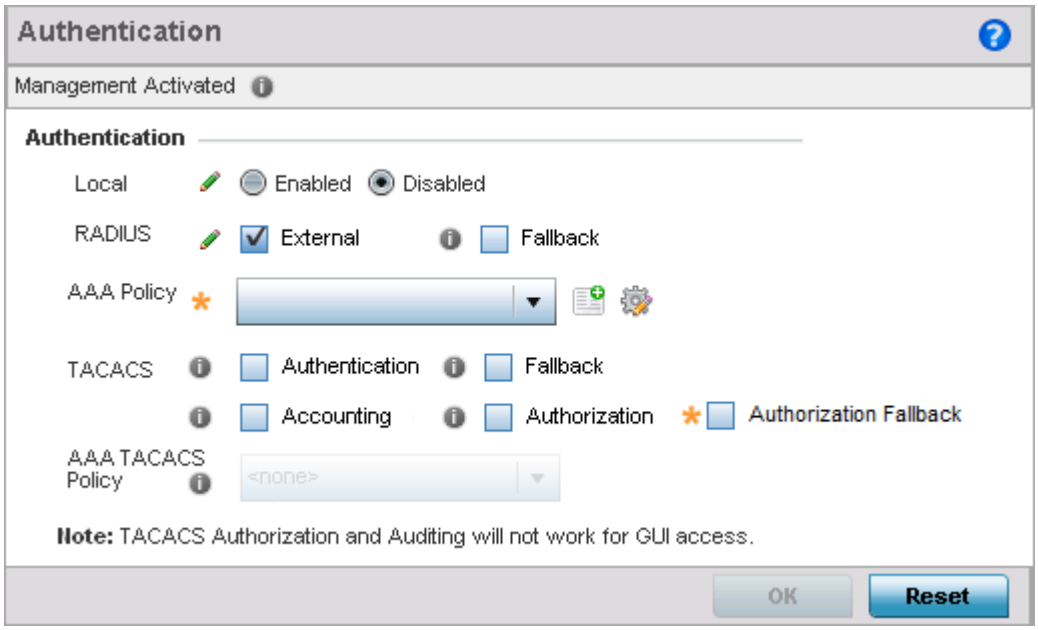


Figure 4: Management Policy - Authentication screen

4 Set the following to authenticate access requests to the access point managed network:

Local	Define whether the access point's internal RADIUS resource (if supported) is used to validate authentication requests. The default setting is Enabled. When enabled, network address information is not required for an external RADIUS resource. AP6521 model has no local resource however and must use an external RAIDUS server.
RADIUS	If local is disabled, an external RADIUS resource is used as the authentication service. *External* and *Fallback* are not available if the access point's local RADIUS resource is enabled.

5 Use the drop-down menu to specify to select the **AAA Policy** to use with an external RADIUS resource.

An AP6521 model access point (or a model that is 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. For more information on defining the configuration of a AAA policy, see "AAA Policy" on page 663.

6 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.

7 Configure the **AAA TACACS Policy** to use with this authentication policy. Use the drop-down to select a configured AAA TACACS policy.

8 Select **OK** to update the configuration. Select **Reset** to revert to the last saved configuration.

Setting the SNMP Configuration

"Management Access"

The access point can use *Simple Network Management Protocol* (SNMP) to interact with wireless devices. SNMP is an application layer protocol that facilitates the exchange of management information. SNMP enabled devices listen on port 162 (by default) for SNMP packets from their 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 statistical data 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
SNMPv2	No	No	Enabled
SNMPv3	Yes	Yes	Enabled

To define SNMP management values:

1 Select **Configuration** > **Management**.

2 Select **SNMP** from the list of Management Policy options in the upper, left-hand, side of the UI.

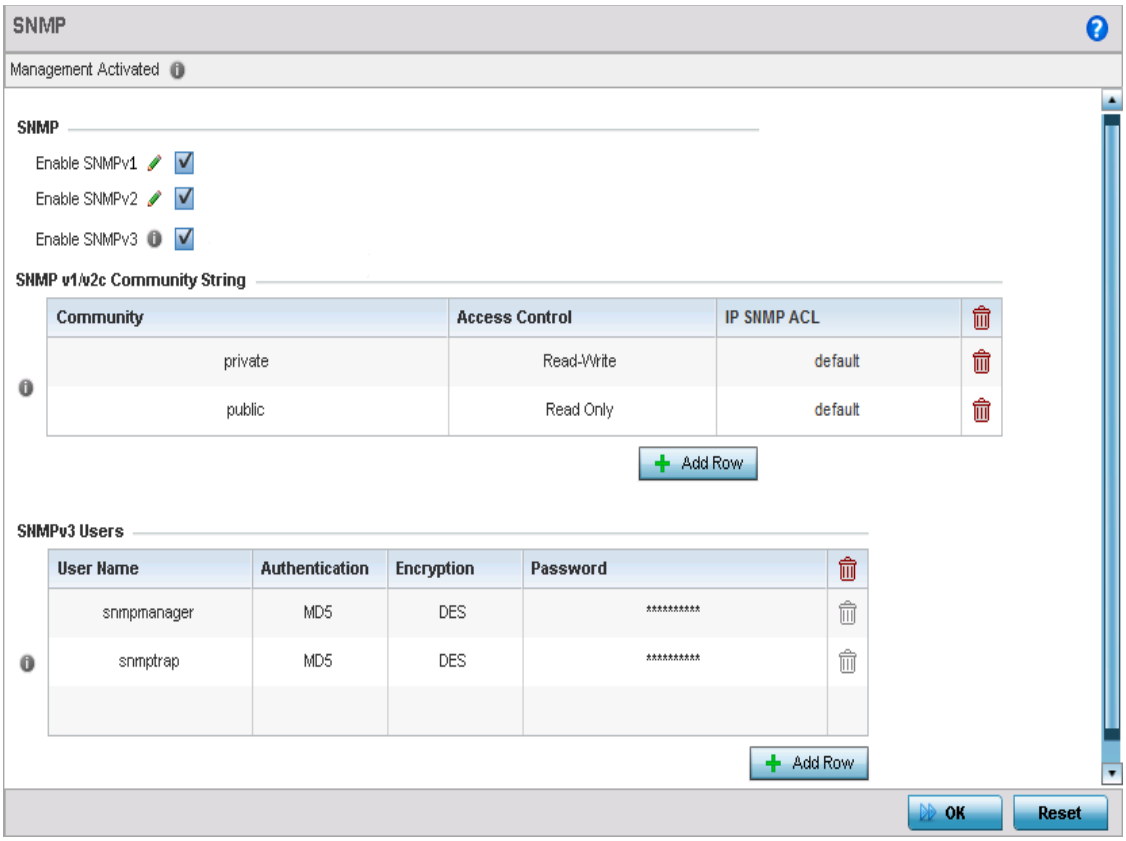


Figure 5: Management Policy screen - SNMP tab

3 Enable or disable SNMPv1, SNMPv2 and SNMPv3.

Enable SNMPv1	Select the check box to enable SNMPv1 support. SNMPv1 provides device management using a hierarchical set of variables. SNMPv1 uses *Get*, *GetNext*, and *Set* operations for data management. SNMPv1 is enabled by default.
Enable SNMPv2	Select the check box 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 check box 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.

4 Set the **SNMP v1/v2c 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. The 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 to be used along with this community string. Use the drop-down menu to select an existing ACL. Use the *Create* icon to create and add a new ACL. Select an existing ACL and use the *Edit* icon to edit an existing ACL.

5 Set the **SNMPv3 Users** configuration. Use the **+ Add Row** function as needed to add additional SNMPv3 user configurations, or select a SNMP user's radio button and select the **Delete** icon to remove the user.

User Name	Use the drop-down menu to define a user name of either 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 are permitted access.
Encryption	Displays the encryption scheme used with the listed SNMPv3 user. The listed encryption scheme ensures data is protected when forwarded over insecure interfaces like HTTP.
Password	Provide the user's password in the field provided. Select the *Show* radio button to display the actual character string used in the password. Leaving the radio button unselected protects the password and displays each character as "*".

6 Select **OK** to update the SNMP configuration. Select **Reset** to revert to the last saved configuration.

SNMP Trap Configuration

"Management Access"

An access point can use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions) on devices, and are therefore an important fault management tool.

A SNMP trap receiver is the SNMP message destination. 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 **Configuration** > **Management**.

2 Select **SNMP Traps** from the list of Management Policy options in the upper, left-hand, side of the UI.

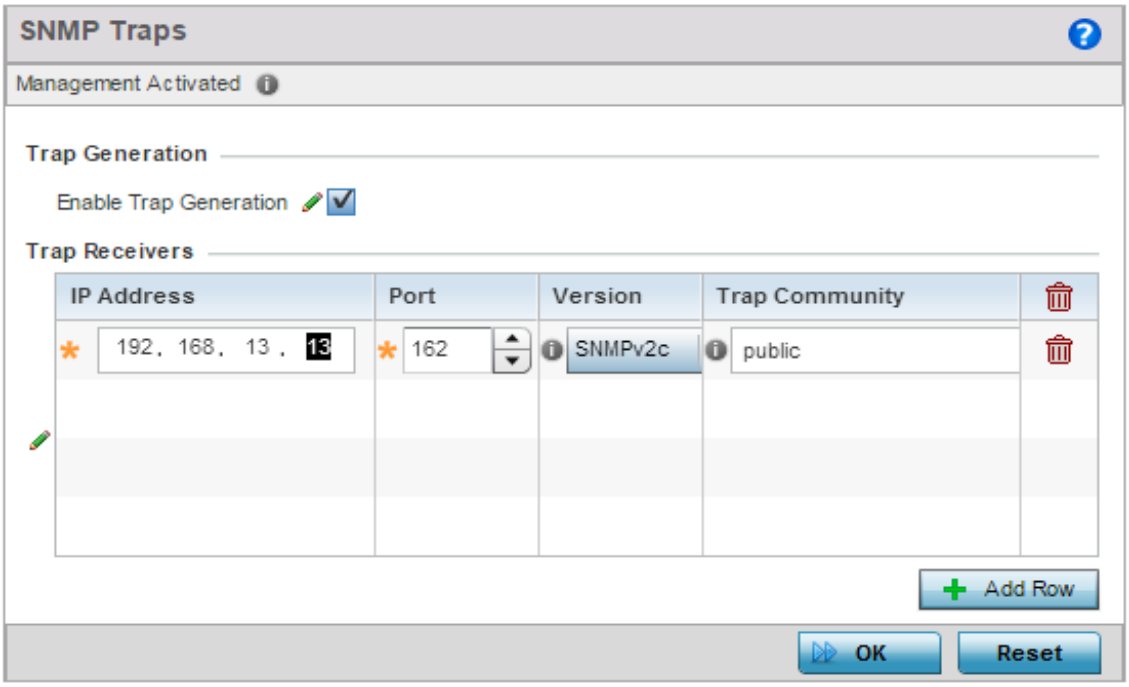


Figure 6: Management Policy screen - SNMP Traps tab

3 Select the **Enable Trap Generation** check box to enable trap creation using the trap receiver configuration defined in the lower portion of the screen. This feature is disabled by default.

4 Refer to the **Trap Receiver** table to set the configuration of the external resource receiving trap information. Select **Add Row +** as required to add additional trap receivers. Select the **Delete** icon to permanently remove a trap receiver.

IP Address	Set the IP address of the external server resource receiving SNMP traps on behalf of the access point.
Port	Set the server port dedicated to receiving traps. The default port is 162.
Version	Set the SNMP version for sending SNMP traps. SNMPv2c 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 access point resources. If the community string is correct, the access point provides with the requested information. If the community string is incorrect, the 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*.

5 Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

Management Access Deployment Considerations

Before defining an access control configuration as part of a Management Access policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Unused management protocols should be disabled to reduce a potential attack.
- 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.
- 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. Our legacy devices may use other community strings by default.
- It is recommended that SNMPv3 be used for device management, as it provides both encryption, and authentication.
- Enabling SNMP traps can provide alerts for isolated attacks at both small radio deployments or distributed attacks occurring across multiple sites.

11 Diagnostics

An access point's resident diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting network performance. Performance and diagnostic information is collected and measured for anomalies causing a key processes to potentially fail.

Numerous tools are available within the Diagnostics menu. Some allow event filtering, some enable log views and some allow you to manage files generated when hardware or software issues are detected.

Diagnostic capabilities include:

- "Fault Management"
- "Crash Files"
- "Advanced"

Fault Management

- "Diagnostics"

Fault management enables users administering multiple sites to assess device performance and issues effecting the network. Use the Fault Management screens to view and administrate errors generated by an access point or a connected wireless client.

To conduct fault management on an access point:

1 Select **Diagnostics**.

2 Select **Fault Management.**

The *Filter Events* screen displays by default. Use this screen to configure how events are tracked and managed. By default, all events are enabled, and an administrator has to turn off events if they don't require tracking.

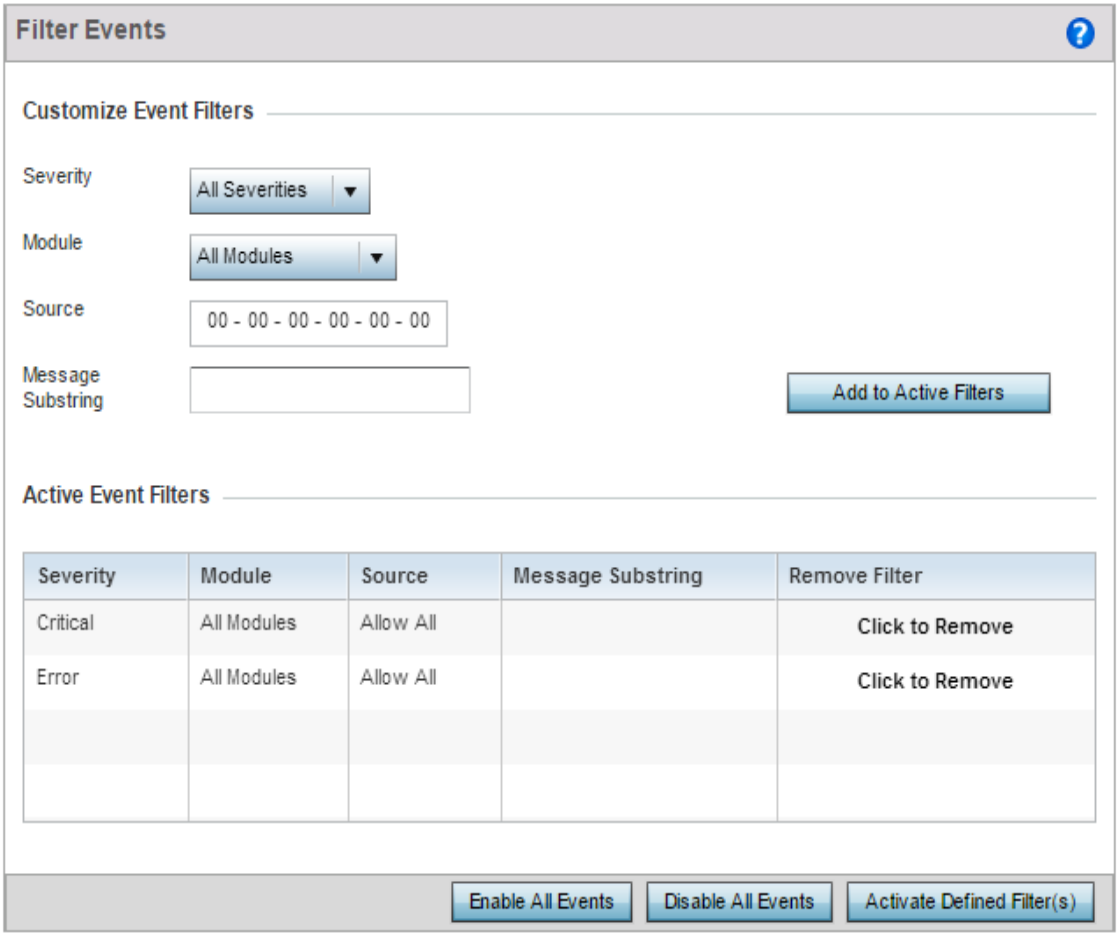


Figure 1: Fault Management - Filter Events screen

Use the *Filter Events* screen to create filters for managing events. Events can be filtered based on severity, module received, source MAC of the event, device MAC of the event and MAC address of the wireless client.

3 Define the following **Customize Event Filters**:

Severity	Set the severity of the event being filtered. Select from the following: • *All Severities* – All events are displayed irrespective of their severity • *Critical* – Only critical events are displayed • *Error* – Only errors are displayed • *Warning* – Only warnings are displayed • *Informational* – Only informational events are displayed
Module	Select the module from which events are tracked. When a single 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 being tracked. Setting a MAC address of 00:00:00:00:00:00 allows all devices to be tracked.
Message Substring	Set the error message search string. This filters out any error message or event message that does not contain the string being searched.



NOTE

Leave the Source, Device and Mobile Unit fields at the default setting of 00:00:00:00:00:00 to allow 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 configuration defined in the Customize Event Filters field.

5 Refer to the **Active Event Filters** 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.

6 Select View Events from the upper, left-hand, side of the Fault Management browser.

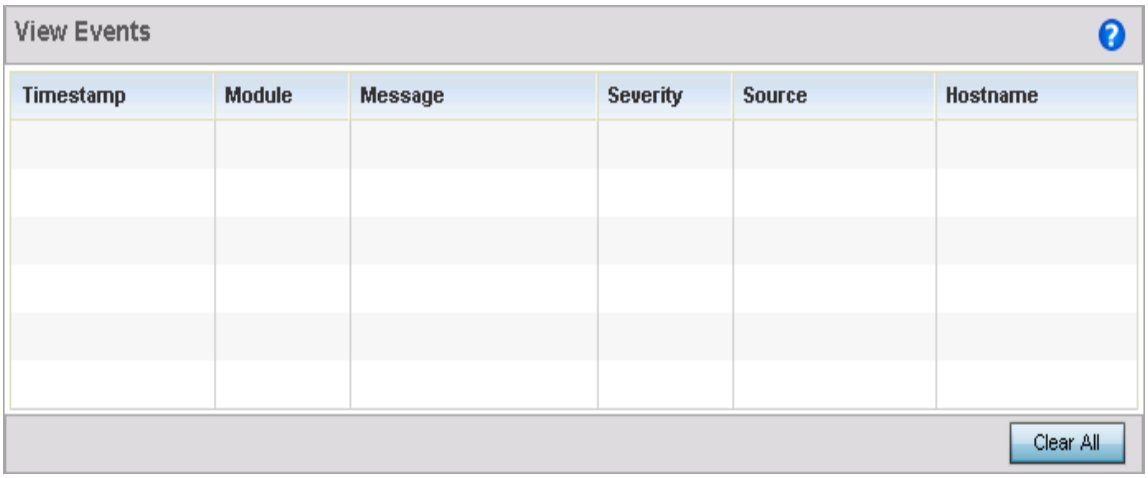


Figure 2: Fault Management - View Events screen

Use the *View Events* screen to track and troubleshoot events using source and severity levels defined in the configure events screen.

7 Refer to the following event parameters to assess nature and severity of the displayed event:

Timestamp	Displays the timestamp (time zone specific) when the event occurred.
Module	Displays the module used to track the event. Events detected by other modules 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 regardless of their severity • *Critical* – Only critical events are displayed • *Error* – Only errors are displayed • *Warning* – Only warnings are displayed • *Informational* – Only informational 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.

8 Select **Clear All** to clear the events displayed on this screen and begin a new event data collection.

9 Select **Event History** from the upper, left-hand, side of the Fault Management browser.

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.

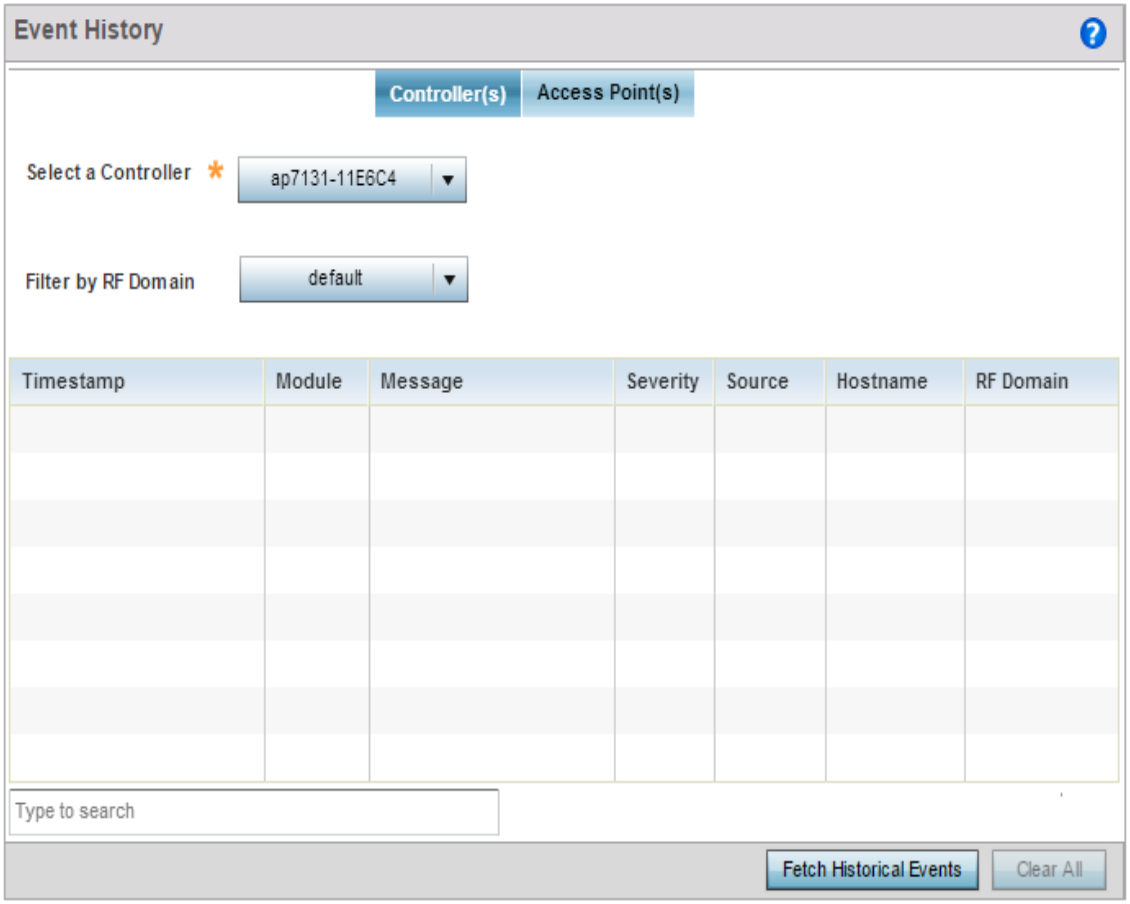


Figure 3: Fault Management - Event History screen

10 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.

11 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.,

12 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 message for each event.
Severity	Displays event severity as defined for tracking from the Configuration screen. Severity options include: • *All Severities* – All events are displayed regardless of severity • *Critical* – Only critical events are display • *Error* – Only errors display • *Warning* – Only warnings display • *Informational* – Only informational events display, no critical events, errors or warnings.
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.

13 Select **Clear All** to clear the event table and begin a new data collection for the specified device.

Crash Files

"Diagnostics"

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.**

2 Select **Crash Files.**

The crash files screen displays a list of device MAC addresses impacted by core dumps.

3 Select a device from those displayed in the lower, left-hand, side of the UI.

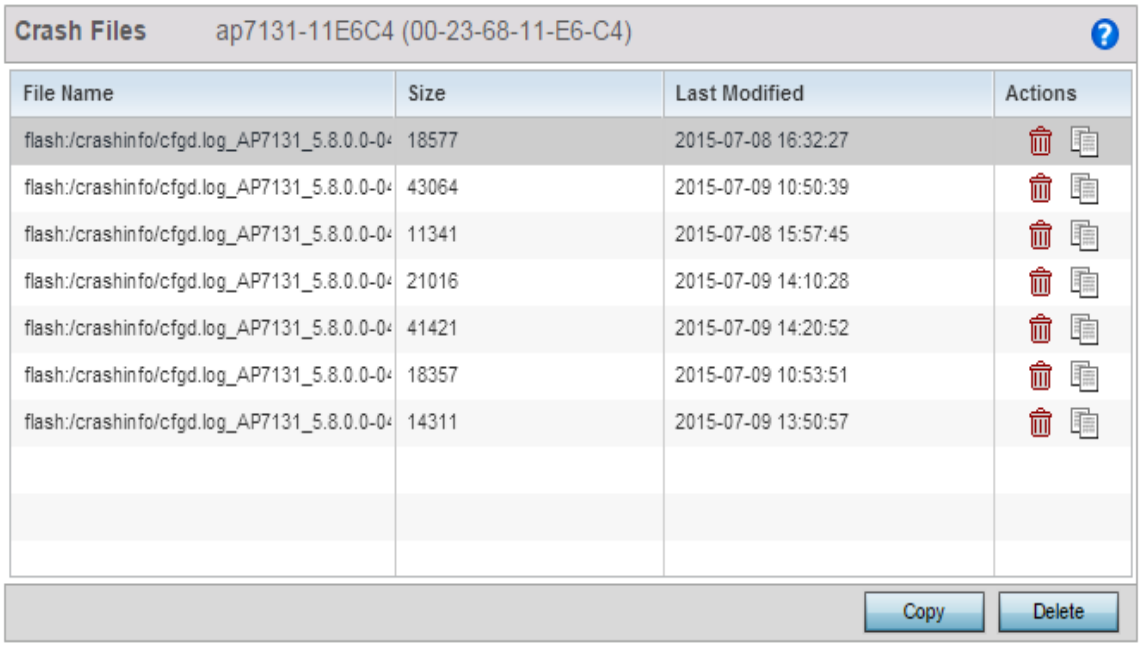


Figure 4: Crash Files screen

The screen displays the following for each reported crash file:

File Name	Displays the name of the file generated when a crash event occurred. This is the file available to copy to an external location for archive and administration.
Size	Lists the size of the crash file, as this information is often needed when copying files to a location external to the access point.
Last Modified	Displays the time stamp of the crash file's most recent update.
Actions	Displays the action taken by the access point in direct response to the detected crash event.

4 Select a listed crash file and select the **Copy** button to display a screen used to copy (archive) the file to an external location.

5 To remove a listed crash file from those displayed, select the file and select the **Delete** button.

Advanced

"Diagnostics"

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"

- "View UI Logs"
- "View Sessions"

UI Debugging

- "Advanced"

Use the **UI Debugging** screen to view debugging information for a selected device.

To review device debugging information:

1 Select **Diagnostics.**

2 Select **Advanced** to display the UI Debugging menu options. By default, **NETCONF Viewer** is selected.

Once a target ID is selected, its debugging information displays within the **NETCONF Viewer** screen.

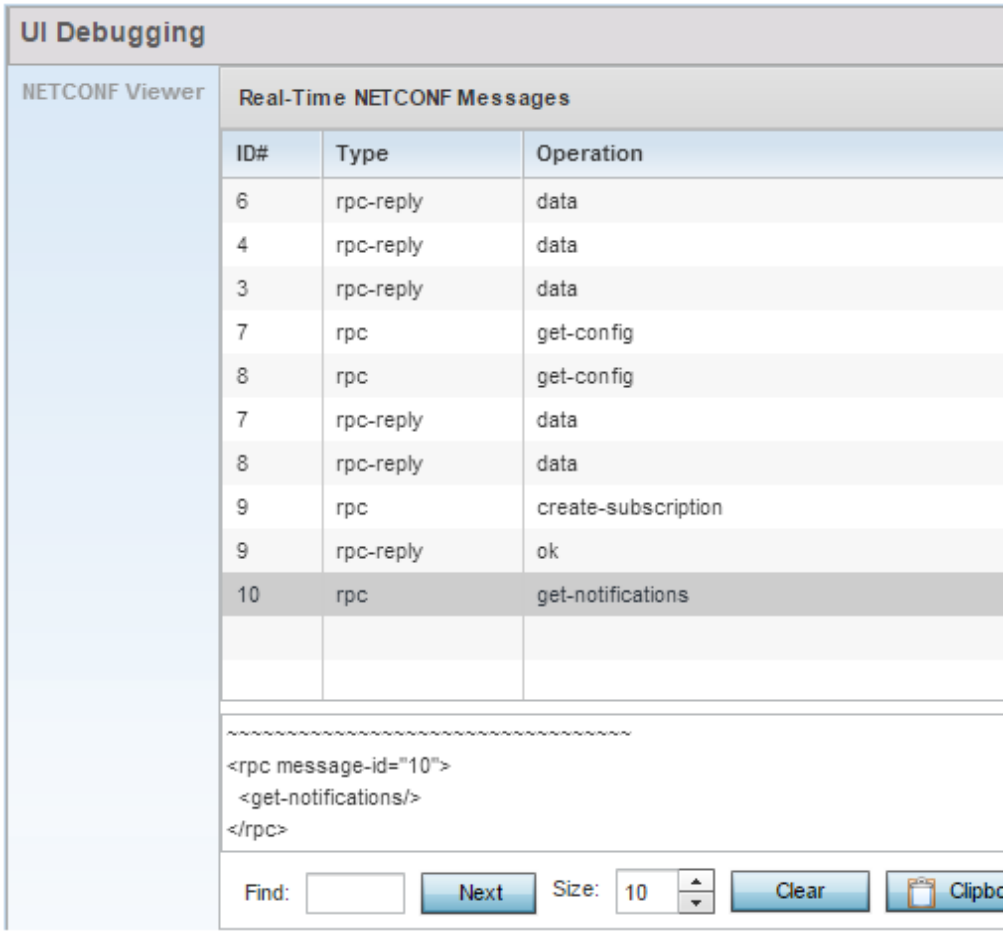


Figure 5: UI Debugging screen - NETCONF Viewer

3 Use **NETCONF Viewe**r 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.

View UI Logs

"Advanced"

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.**

2 Select **Advanced** to display the UI Debugging menu options.

3 Select the **View UI Logs** menu item to display the logs. By default, the *Flex Logs* screen displays.

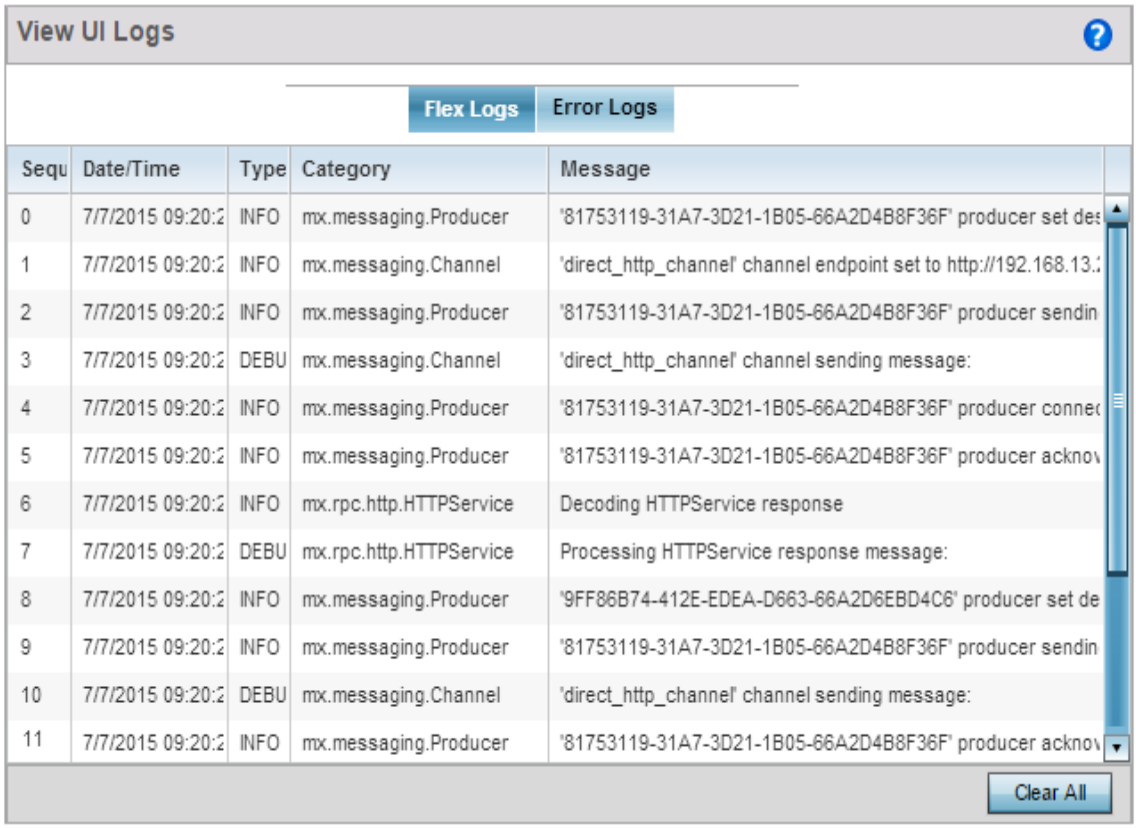


Figure 6: View UI Logs - Flex Logs tab

The Sequence (order of occurrence), Date/Time, Type, Category and Message items display for each log option selected.

Use the **Clear All** button to clear all logs shown in this screen.

4 Select the **Error Logs** tab to display the error logs for this device.

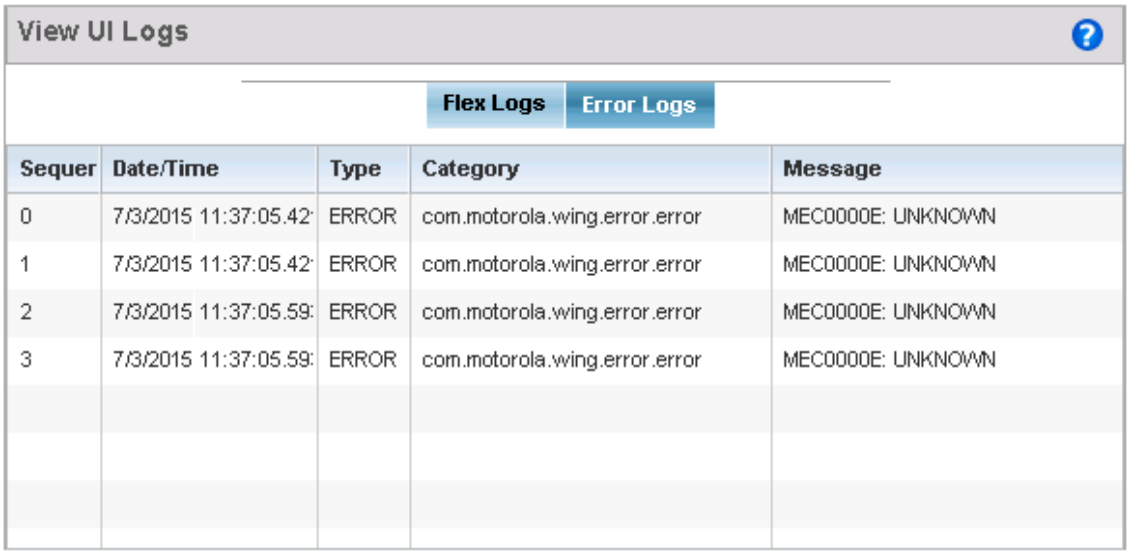


Figure 7: View UI Logs - Error Logs tab

The Sequence (order of occurrence), Date/Time, Type, Category and Message items display for each log option selected.

View Sessions

"Advanced"

The **View Sessions** screen 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**.

2 Select **Advanced** to display the UI Debugging menu options.

3 Select the **View Sessions** menu item to display the users sessions on this device.

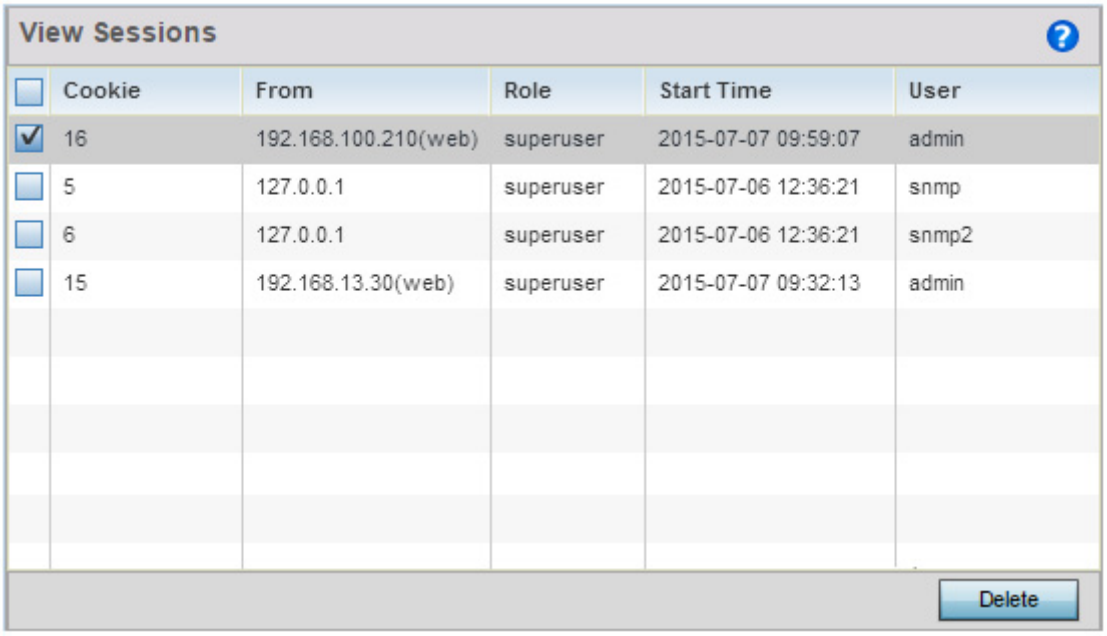


Figure 8: Advanced - View Sessions screen

4 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.

5 To remove a listed session, select the check box before session, then select **Delete**.

12 Operations

The functions supported within the **Operations** menu allow the administration of firmware, configuration files and certificates for managed devices.

A certificate links identity information with a public key enclosed in the certificate. Device certificates can be imported and exported to a secure remote location for archive and retrieval as they are required for application to other managed devices.

Self Monitoring At Run Time RF Management (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements. The Smart RF functionality scans the RF network to determine the best channel and transmit power for each managed access point radio.

For more information, refer to the following:

- "Devices"
- "Certificates"
- "Smart RF"

Refer to "Operations Deployment Considerations" on page 925 for tips on how to optimize the access point's configuration

Devices

- "Operations"

Periodically, releases of updated device firmware and configuration files are uploaded 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, it is recommended to update to the latest firmware version for full functionality and utilization. Additionally, selected devices can either have a primary or secondary firmware image applied or fallback to a selected firmware image if an error were to occur in the update process.

Device update activities include:

- "Managing Firmware and Configuration Files"
- "Rebooting the Device"
- "Locating a Device"
- "Upgrading Device Firmware"
- "Viewing Device Summary Information"
- "Adopted Device Upgrades"
- "File Management"
- "Adopted Device Restart"
- "Captive Portal Pages"

- "Re-elect Controller"

NOTE

AP upgrades can only be performed by access points in Virtual Controller AP mode, and cannot be initiated by Standalone APs. Additionally, upgrades can only be performed on access points of the same model as the Virtual Controller AP.

These tasks can be performed on individual access points and wireless clients.

Managing Firmware and Configuration Files

"Devices"

Firmware and configuration files are viewed and managed from the device browser.



Figure 1: Device Browser

Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

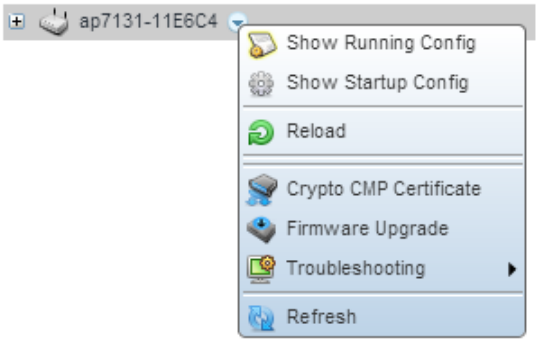


Figure 2: Device Browser - Options for an AP7131

Refer to the drop-down menu on the lower, left-hand side, of the UI. The following tasks and displays are available in respect to device firmware for the selected device:

Show Running Config	Select this option to display the running configuration of the selected device. The running configuration is displayed in a separate window. Select *Execute* to perform the function. For more information on viewing and managing the running configuration, see "Managing Running Configuration" on page 853.
Show Startup Config	Select this option to display the startup configuration of the selected device. The startup configuration is displayed in a separate window. Select *Execute* to perform the function. For more information on viewing and managing the startup configuration, see "Managing Startup Configuration" on page 856.
Reload	Select this option to reload the selected device. Clicking this option reboots the selected device.
Crypto CMP Certificate	Select this option to manage Crypto CMP Certificates on this device. For more information on this, see "Managing Crypto CMP Certificates" on page 860.
Firmware Upgrade	Select this option to upgrade the selected device's firmware. For information on conducting a device firmware upgrade, see "Upgrading Device Firmware" on page 861.
Troubleshooting	Select this option to expand a sub-menu with various option to troubleshoot this device. For more information on the troubleshooting menu, see "Troubleshooting the Device" on page 864.
Refresh	Select this option to refresh the information displayed in the screen being displayed.

For information on conducting a device firmware upgrade, see "Upgrading Device Firmware" on page 861. For information on file transfers, see "File Management" on page 889.

Managing Running Configuration

"Managing Firmware and Configuration Files"

Running configuration is the current configuration of the selected device. To view and manage the running configuration:

1 Select a target device from the left-hand side of the UI.



Figure 3: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

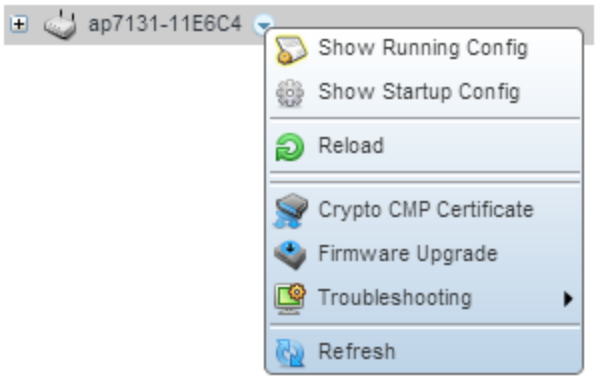


Figure 4: Device Browser - Options for a device

3 Select **Show Running Config** to display the *Running Configuration* window.

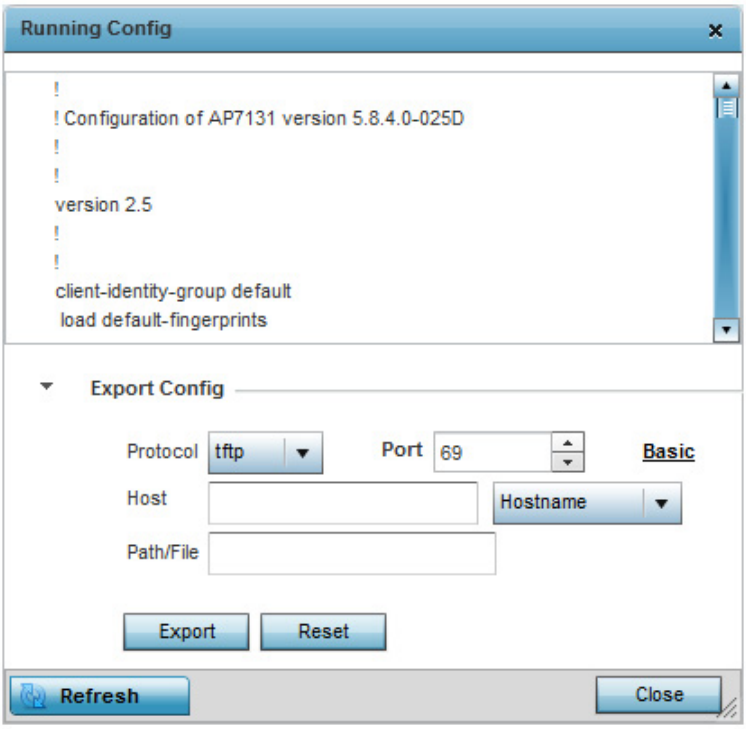


Figure 5: Operations - Manage Running Configuration

4 Use the **Export Config** field to configure the parameters required to export the running configuration to an external server. Refer to the following to configure the export parameters:

Protocol	Select the protocol used for exporting the running configuration. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4 • *local*
Port	Use the spinner control or manually enter the value to define the port used by the protocol for exporting the running configuration. This option is not valid for *cf*, *usb1*, *usb2, usb3* and *usb4*.
Host	Enter IP address or the hostname of the server used to export the running configuration to. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*.
Path/File	Specify the path to the folder to export the running configuration to. Enter the complete relative path to the file on the server.
User Name	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*
Password	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*

5 Select **Export** button to export the running configuration using the settings configured in the **Export Config** field.



NOTE

Another way to export the running configuration to the device used to view the configuration is to click in the area that displays the running configuration and use the [ctrl]+a keyboard combination to select all the contents of the text area into the OS's clipboard memory. Open a text editor, paste the copied content and save the file.

6 To update the screen with the latest changes made to the running configuration, select the **Refresh** button located to the bottom right of the screen.

Managing Startup Configuration

"Managing Firmware and Configuration Files"

Startup configuration is the configuration that will be loaded the next time the device is booted. To view and manage the startup configuration:

1 Select a target device from the left-hand side of the UI.



Figure 6: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

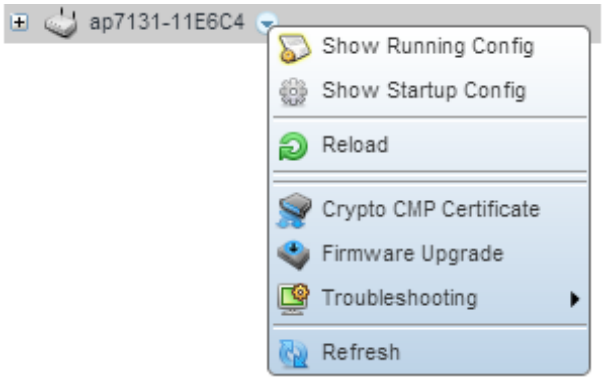


Figure 7: Device Browser - Options for a device

3 Select **Show Startup Config** to display the *Startup Configuration* window.

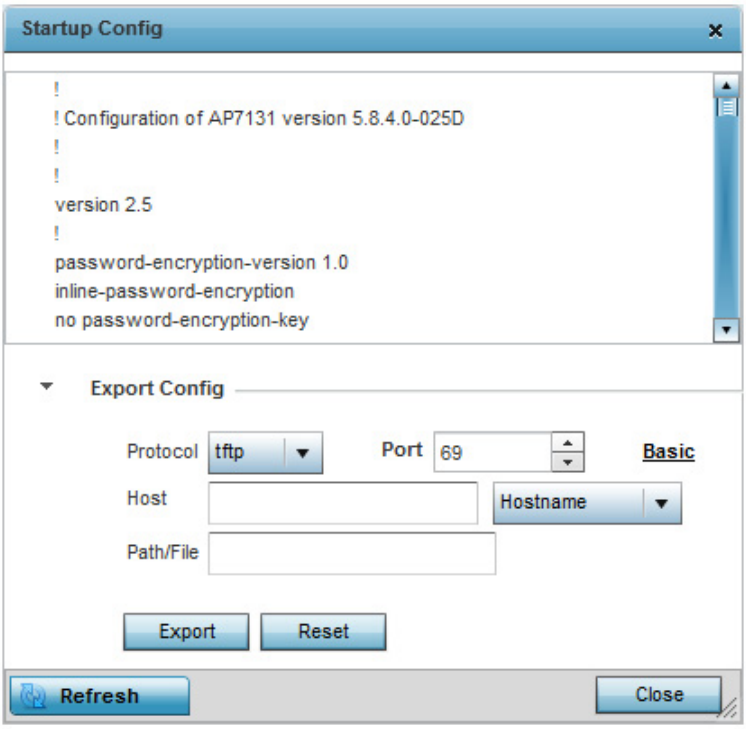


Figure 8: Operations - Manage Startup Configuration

4 Use the **Import/Export Config** field to configure the parameters required to export or import the startup configuration to or from an external server. Refer to the following to configure the remote server parameters:

Protocol	Select the protocol used for exporting or importing the startup configuration. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4 • local
Port	Use the spinner control or manually enter the value to define the port used by the protocol for exporting or importing the startup configuration. This option is not valid for *cf*, *usb1*, *usb2, usb3* and *usb4*.
Host	Enter IP address or the hostname of the server used to export or import the startup configuration to. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*. Use the drop-down to select the type of host information. Host can be one of *Host Name* or *IP Address.*
Path/File	Specify the path to the folder to export or import the startup configuration to. Enter the complete relative path to the file on the server.
User Name	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*
Password	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*

5 Select **Export** button to export the startup configuration using the settings configured in the **Import/Export Config** field. Similarly, Select **Import** button to import the startup configuration.



NOTE

Another way to export the running configuration to the device used to view the configuration is to click in the area that displays the running configuration and use the [ctrl]+a keyboard combination to select all the contents of the text area into the OS's clipboard memory. Open a text editor, paste the copied content and save the file.

6 To update the screen with the latest changes made to the startup configuration, select the **Refresh** button located to the bottom right of the screen.

Rebooting the Device

“Devices”

To force the device to restart:

1 Select a target device from the left-hand side of the UI.



Figure 9: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

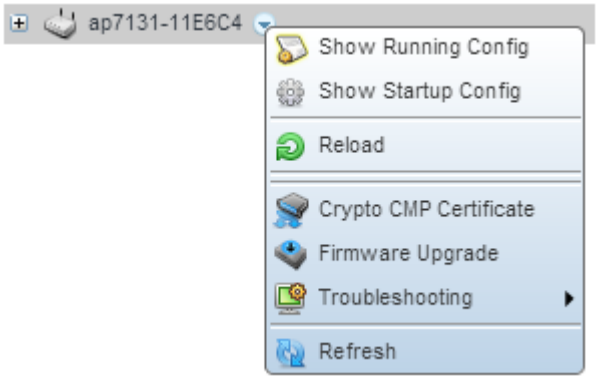


Figure 10: Device Browser - Options for a device

3 To reboot the device, select the **Reload** item.

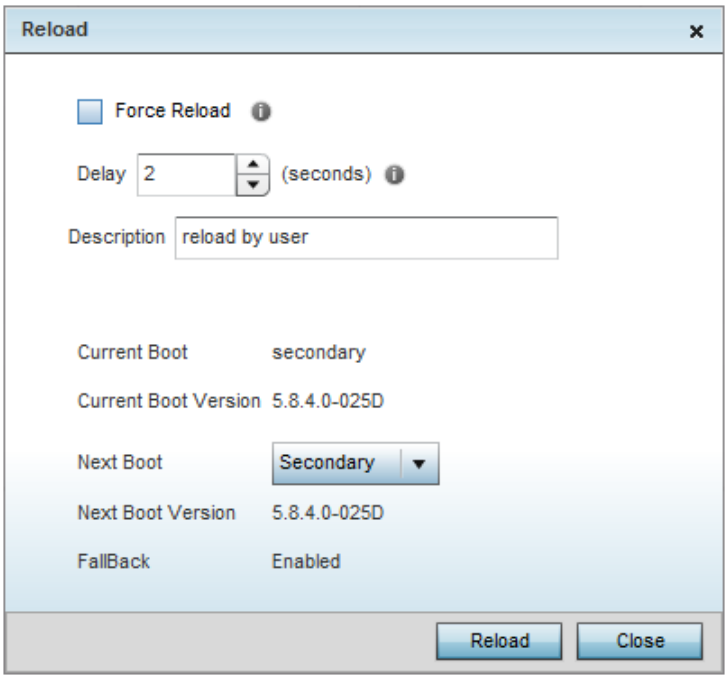


Figure 11: Device - Reload screen

4 Refer the following for more information on this screen:

Force Reload	Select this option to force this device to reload. Use this option for devices that are unresponsive and do not reload normally.
Delay	Use the spinner to configure a delay in seconds before the device is reloaded. Set this value to 0 to reload the device immediately.
Description	Use the text box to provide a brief description detailing the reason to reload this device.
Current Boot	Displays the current running firmware. Displays either *primary* or *secondary*.
Current Boot Version	Displays the firmware version number for the running firmware.
Next Boot	Displays the firmware that will be loaded on next boot.
Next Boot Version	Displays the firmware version number that will be loaded on next boot.
Fallback	Displays the status of Fallback. Displays *Enabled* or *Disabled*.

Managing Crypto CMP Certificates

"Managing Firmware and Configuration Files"

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.

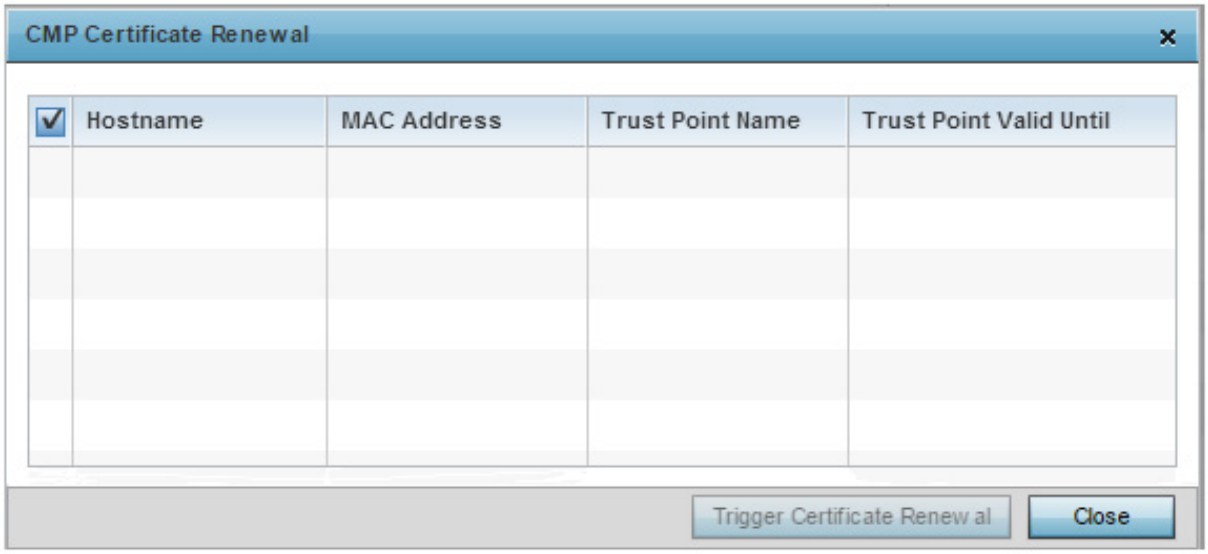


Figure 12: Crypto CMP Certificate Management screen

Use the *Crypto Certificate Renewal* screen to view and if required, trigger certificate renewal for CMP 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	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.

Upgrading Device Firmware

- "Devices"

To update the firmware of an access point:

1 Select a target device from the left-hand side of the UI.

2 Select the down arrow next to the device to view a set of operations that can b performed on the selected device.

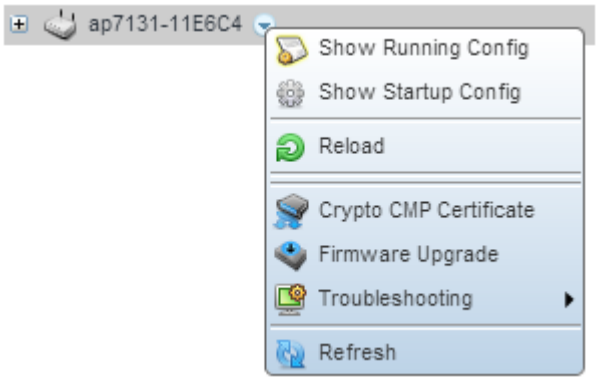


Figure 13: Device Browser - Options for a device

3 Select the **Firmware Upgrade** button to upgrade the device's firmware.

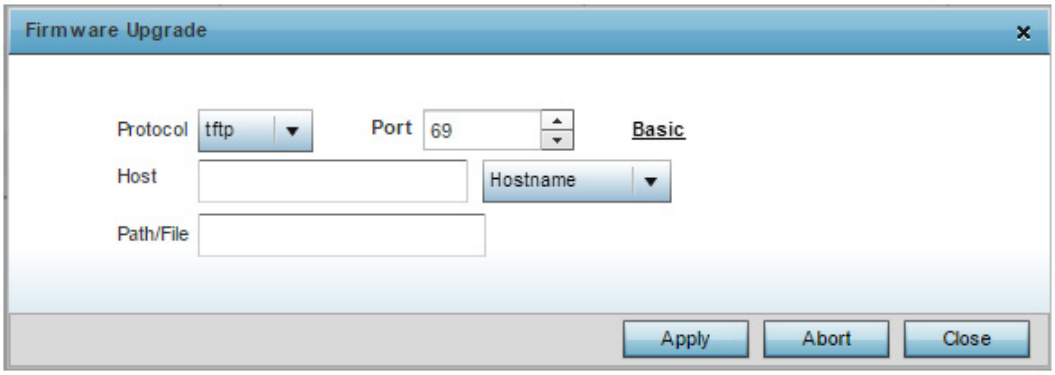


Figure 14: Firmware Upgrade screen

4 Provide the following information to accurately define the location of the target device's firmware file:

Protocol	Select the protocol used for updating the firmware. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4 • local
Port	Use the spinner control or manually enter the value to define the port used by the protocol for importing the firmware upgrade file. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*.
Host	Enter IP address or the hostname of the server used to import the firmware file. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*. Use the drop-down to select the type of host information. The host can be either an IP address or hostname.
Path/File	Specify the path to the firmware file. Enter the complete relative path to the file on the server.
User Name	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*
Password	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*

5 Select **Apply** to start the firmware update. Select **Abort** to terminate the firmware update. Select **Close** to close the upgrade popup. The upgrade continues in the background.

6 The **Basic** link on the screen displays a simple interface with a text box to provide a **URL** to the upgrade file. Enter the complete relative path to the file on a remote server in the **URL** field. Click **Apply** to start the firmware update.

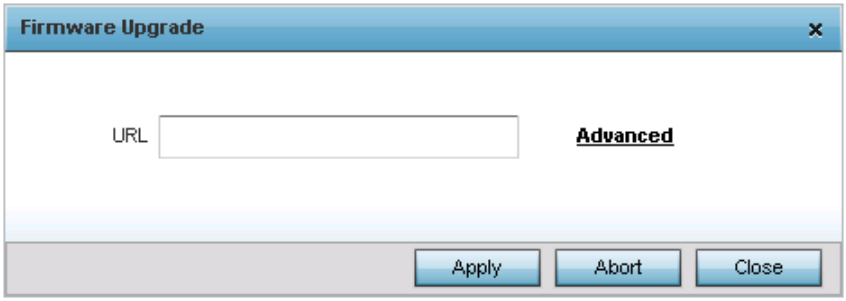


Figure 15: Firmware Upgrade - Basic screen

Troubleshooting the Device

"Managing Firmware and Configuration Files"

The Troubleshooting menu is a list of the functions that can be performed on the device to resolve any issues with the device. The following options are available:

- "Managing Crash Dump Files"
- "Copy Crash Info"
- "Copy Tech Support Dump"
- "Locating a Device"
- "Debugging Wireless Clients"
- "Debug Captive Portal Clients"
- "Packet Capture"

Managing Crash Dump Files

"Troubleshooting the Device"

Crash files are generated when the device encounters a critical error that impairs the performance of the device. When a critical error arises, information about the state of the device at that moment is written to a text file. This file is used by the Support Center to debug the issue and provide a solution to correct the error condition.

To view and manage the crash information files:

1 Select a target device from the left-hand side of the UI.



Figure 16: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

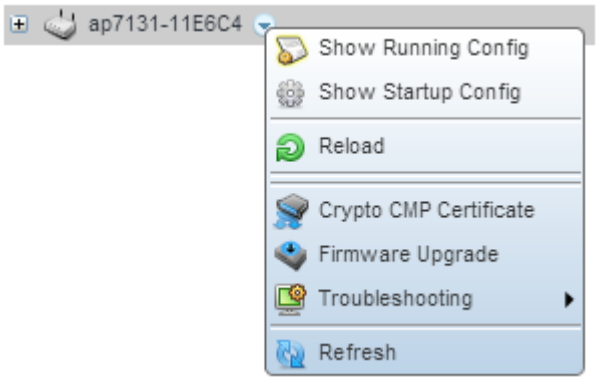


Figure 17: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

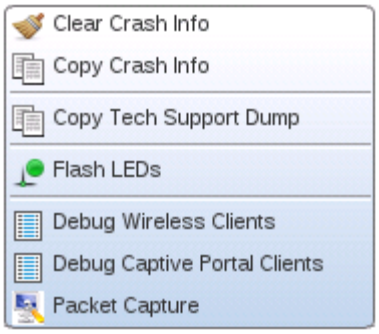


Figure 18: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Clear Crash Info** to display the *Clear Crash Info* window.

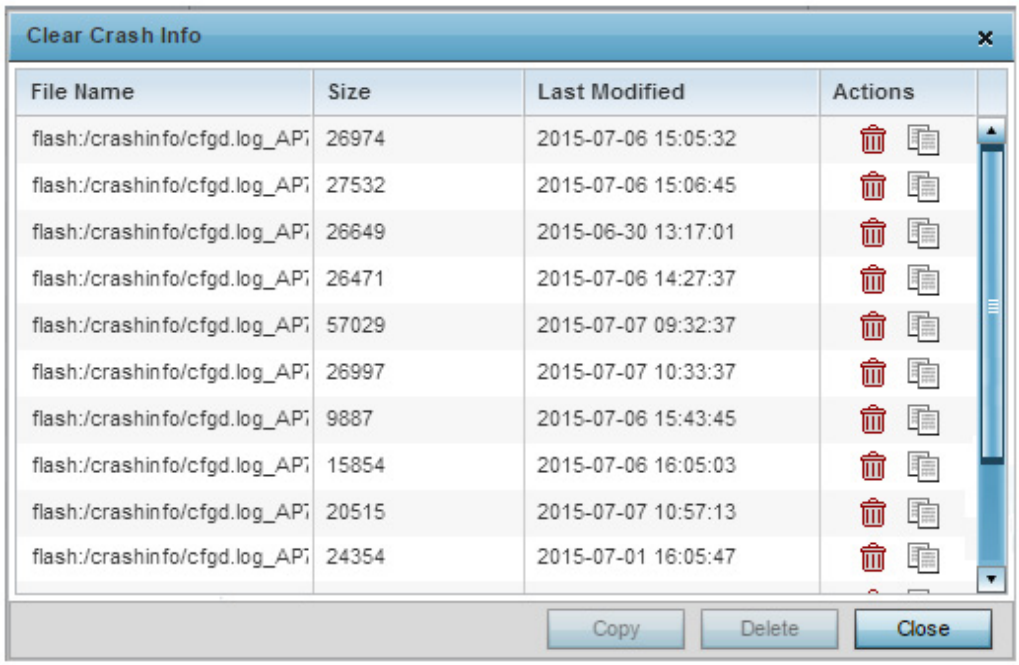


Figure 19: Clear Crash Info screen

5 Refer to the following for more information on the *Clear Crash Info* screen.

File Name	Displays the full path to the crash file
Size	Displays the size of the crash information file in kilobytes.
Last Modified	Displays the timestamp the crash information file was modified last.
Action	Displays icons for the actions that can be performed on the selected crash information file. Use the *Trash* icon to delete the selected crash info file. Use the *Copy* icon to copy the file to a remote location.

6 Use the **Copy** button at the bottom to copy the selected file to a remote location. Use the **Delete** button to delete the selected crash info file.

Copy Crash Info

"Troubleshooting the Device"

Crash files are generated when the device encounters a critical error that impairs the performance of the device. When a critical error arises, information about the state of the device at that moment is written to a text file. This file is used by the Support Center to debug the issue and provide a solution to correct the error condition.

Use the Copy Crash Info screen to copy the crash files to a remote device using *ftp* or *tftp*.

To use the Copy Crash Info screen:

1 Select a target device from the left-hand side of the UI.



Figure 20: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

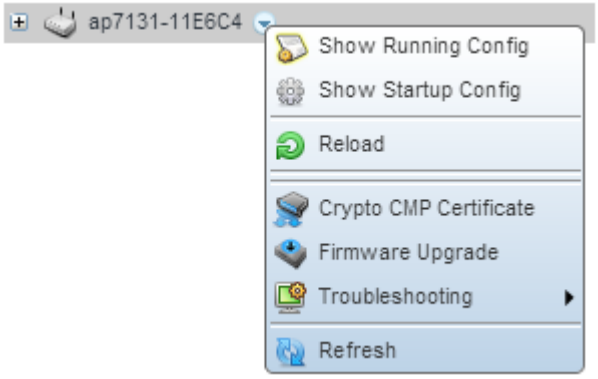


Figure 21: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

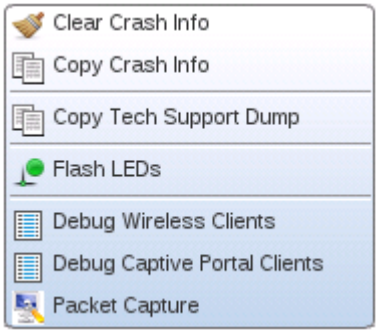


Figure 22: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Copy Crash Info** to display the *Copy Crash Info* window.

Use the **Area** and the **Floor** fields to provide more information about the location of the access point when exporting the crash information.

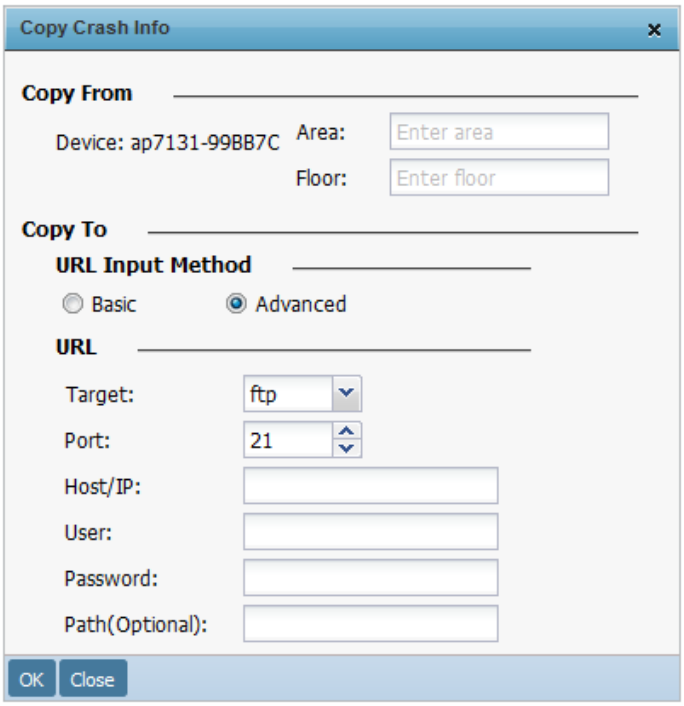


Figure 23: Copy Crash Info screen

5 The crash dump files on this device can be copied to another device for further analysis. Files can be transferred using either the *ftp* or *tftp* protocols.

Provide the following information when transferring files using the *ftp* protocol.

Target	This is the protocol used for file transfer. Select *ftp*.
Port	This is the port used by the FTP server. The default and standard port is 21. If the FTP server uses a non standard port, use the spinner to select it.
Host/IP	Use this field to provide the hostname or the IP address of the FTP server.
User	Use this field to provide the user credentials to authenticate on the FTP server.
Password	Use this field to provide the authentication password for the user credentials provided in the *User* field.
Path (Optional)	Optionally, provide the complete path to the directory on the FTP server where the crash files have to be placed.

Provide the following information when transferring files using the *tftp* protocol.

Target	This is the protocol used for file transfer. Select *tftp.*
Port	This is the port used by the TFTP server. The default and standard port is 69. If the TFTP server uses a non standard port, use the spinner to select it.
Host/IP	Use this field to provide the hostname or the IP address of the TFTP server.
Path (Optional)	Optionally, provide the complete path to the directory on the TFTP server where the crash files have to be placed.

6 Use the **OK** button to begin file transfer. Use the **Close** to exit this screen.

Copy Tech Support Dump

"Troubleshooting the Device"

To troubleshoot some issues, the Support Center might require that some files be supplied to it. These files are compressed as a *.tar.gz* file. This file must be sent to the Support Center on request.

To retrieve the Tech Support Dump files, do the following:

1 Select a target device from the left-hand side of the UI.



Figure 24: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

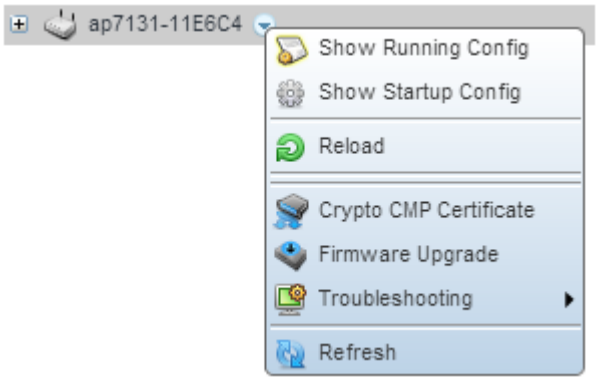


Figure 25: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

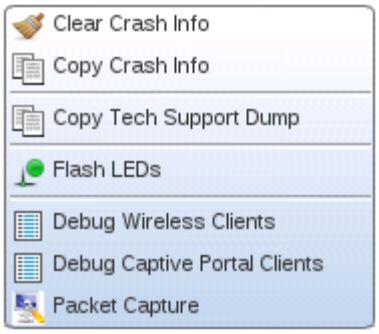


Figure 26: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Copy Tech Support Dump** to display the *Copy Tech Support Dump* window.

Use the **Area** and the **Floor** fields to provide more information about the location of the access point when exporting the crash information.

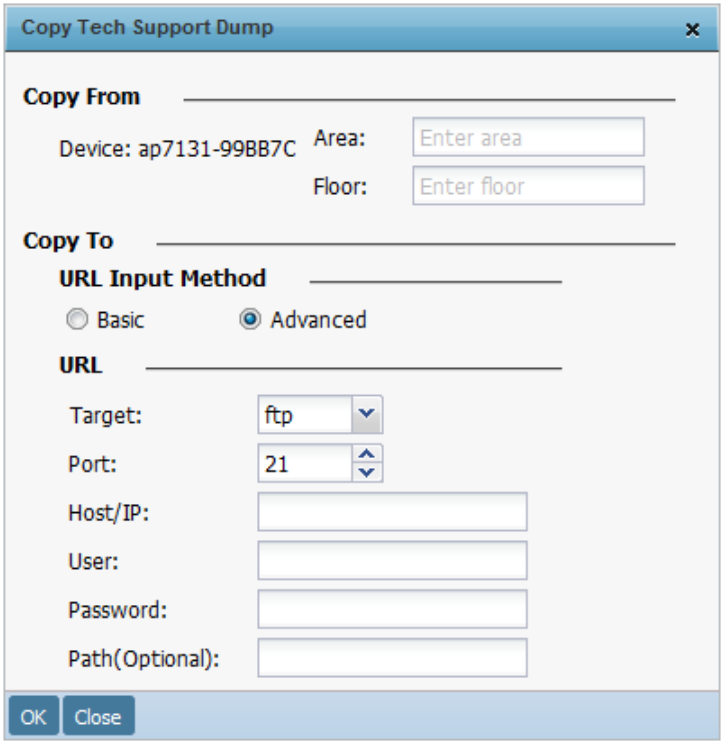


Figure 27: Copy Tech Support Dump screen

5 The Tech Support Dump file can be sent using *ftp* or *tftp*.

Provide the following information when transferring files using the *ftp* protocol.

Target	This is the protocol used for file transfer. Select *ftp*.
Port	This is the port used by the FTP server. The default and standard port is 21. If the FTP server uses a non standard port, use the spinner to select it.
Host/IP	Use this field to provide the hostname or the IP address of the FTP server.
User	Use this field to provide the user credentials to authenticate on the FTP server.
Password	Use this field to provide the authentication password for the user credentials provided in the *User* field.
Path (Optional)	Optionally, provide the complete path to the directory on the FTP server where the Tech Support Dump file is to be placed.

Provide the following information when transferring files using the *tftp* protocol.

Target	This is the protocol used for file transfer. Select *tftp*.
Port	This is the port used by the TFTP server. The default and standard port is 69. If the TFTP server uses a non standard port, use the spinner to select it.
Host/IP	Use this field to provide the hostname or the IP address of the TFTP server.
Path (Optional)	Optionally, provide the complete path to the directory on the TFTP server where the Tech Support Dump file is to be placed.

6 Use the **OK** button to begin file transfer. Use the **Close** to exit this screen.

Locating a Device

"Troubleshooting the Device"

In large deployments with a large number of devices, it is very hard to identify a specific device. Use the device's locator feature to find the device. Once configured, the device blinks its LEDs in a color that enables it to be identified amongst all other deployed devices.

To locate a device:

1 Select the target device from the left-hand side of the UI.



Figure 28: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

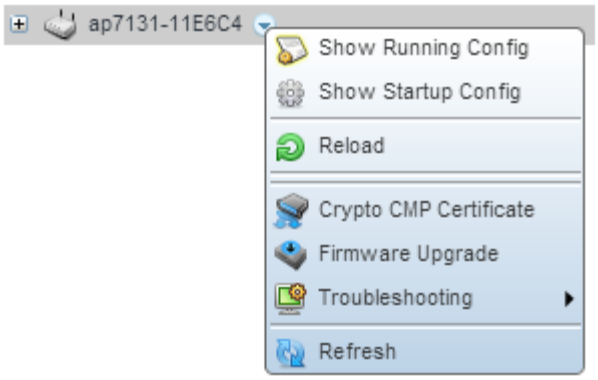


Figure 29: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

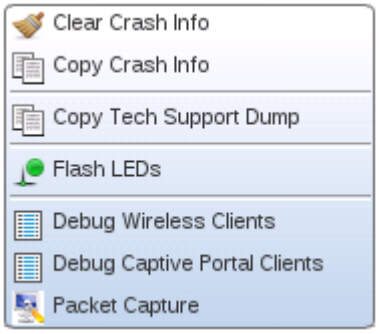


Figure 30: Device Browser - Options for a device - Troubleshooting sub-menu

4 To locate the device, click the **Flash LEDs** item. The following windows displays:

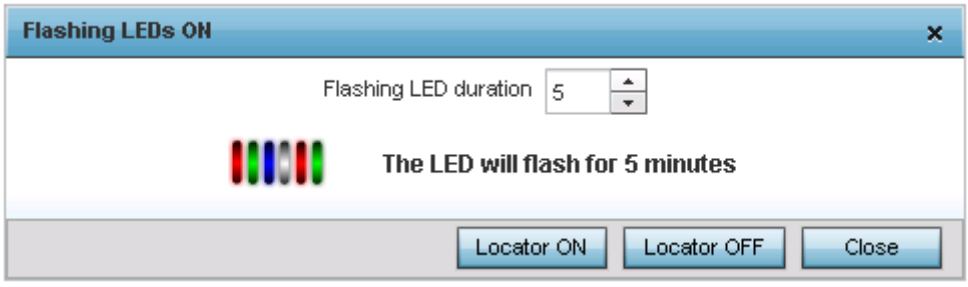


Figure 31: Device Pane - Locator screen

5 Use the spinner to set a value for **Flash LED Duration.** This is the duration, in minutes, the device will flash its LEDs. Once this duration expires, the LEDs starts operating normally.

6 Click **Locator ON** to start flashing the LEDs. Click **Locator OFF** to stop the LEDs from flashing and resume normal operation. Click **Close** to close this window.

Debugging Wireless Clients

"Troubleshooting the Device"

Use the **Debug Wireless Clients** screen to assess whether a connection to a wireless client is proper and is working as intended. To view the **Debug Wireless Clients** screen:

1 Select the target device from the left-hand side of the UI.



Figure 32: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

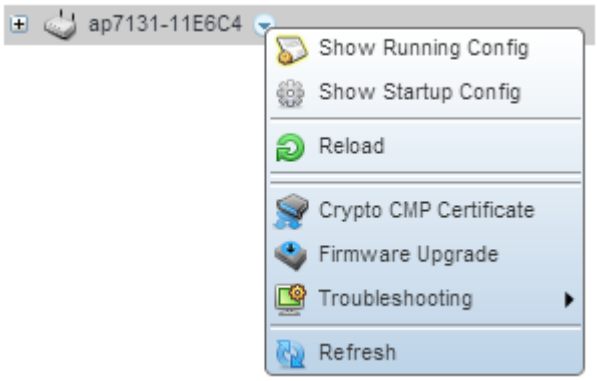


Figure 33: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

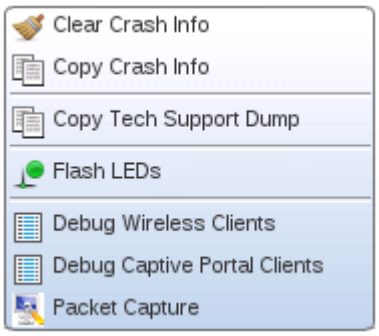


Figure 34: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Debug Wireless Clients**.

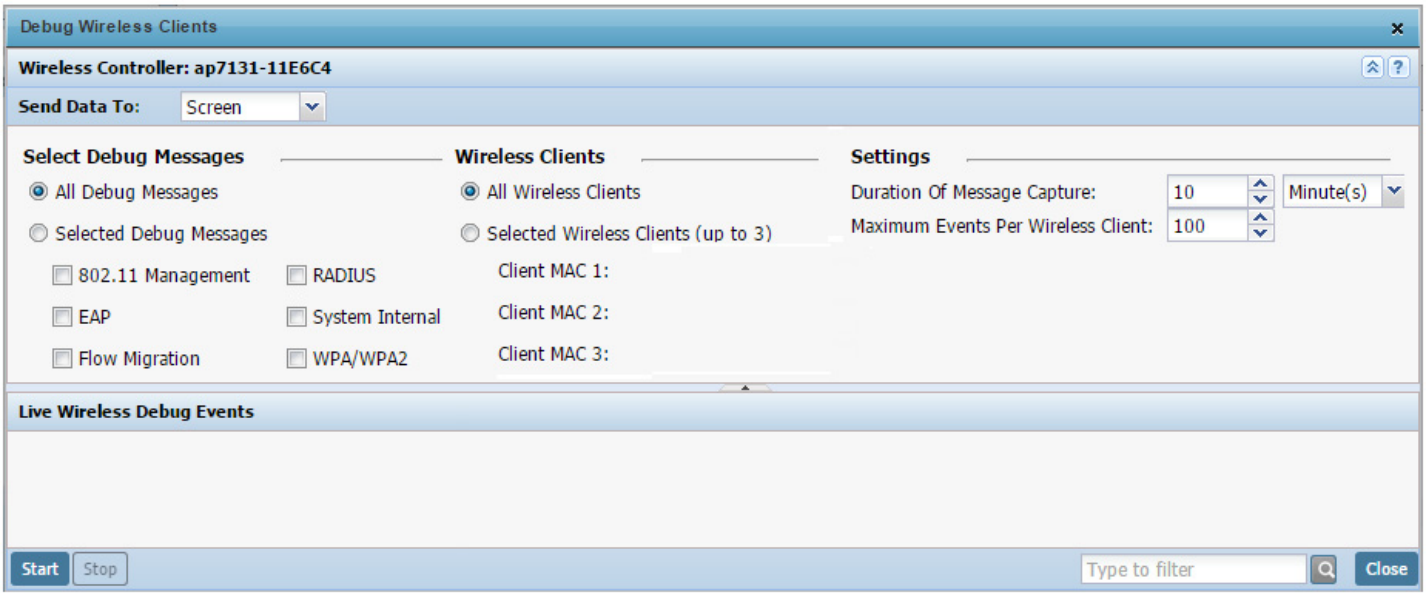


Figure 35: Device Browser - Options for Devices - Troubleshooting menu - Debug Wireless Clients screen

5 Use the **Send Data To** drop-down to select the destination for the debug events. Select from *Screen* or *File*.

When *File* is selected, the captured debug events are stored on a file and then saved to a remote location using either the *FTP* or *TFTP* protocols. Use the screen to provide the appropriate information to save the file on the remote server.

6 When in the RF Domain context, use the **Edit Devices List** to select the device to view the debug information for.

7 Refer to the following **Select Debug Messages** fields to configure the debug messages that are displayed.

All Debug Messages	Select this to display all debug messages generated by the device.
Selected Debug Messages	Select this to display only selected debug messages. The list of debug messages that can be selected are: • 802.11 Management – Displays all 802.11 management debug messages. • EAP – Displays all debug messages related to EAP. • Flow Migration – Displays all debug messages related to flow migration. • RADIUS – Displays all debug messages related to RADIUS server. • System Internal – Displays all debug messages related to system internals. • WPA/WPA2 – Displays all debug messages related to WPA/WPA2.

8 Refer to the following **Wireless Clients** fields to configure the display of debug messages from wireless clients.

All Wireless Clients	Select this to display all debug messages generated by all the wireless clients associated with this device.
Selected Wireless Clients (up to 3)	Select this to display debug messages from up to 3 wireless clients whose MAC addresses are specified. The MAC addresses must be entered in the fields *Client MAC 1*, *Client MAC 2* and *Client MAC 3.*

9 Refer to the following **Settings** fields.

Duration of Message Capture	Use the spinner to set the maximum duration of message capture in *Hours*, *Minutes* and *Seconds*. The default is 10 minutes.
Maximum Events Per Wireless Client	Use the spinner control to set the maximum number of events that is received from a wireless client. The default value is 100 messages.

10 Use the **Start** button to start capture of debug messages. Use **Stop** to stop the capture. Use the **Type to filter** text area to filter debug messages.

11 Use **Close** to close this screen.

Debug Captive Portal Clients

"Troubleshooting the Device"

An administrator can select a 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 the target device from the left-hand side of the UI.



Figure 36: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

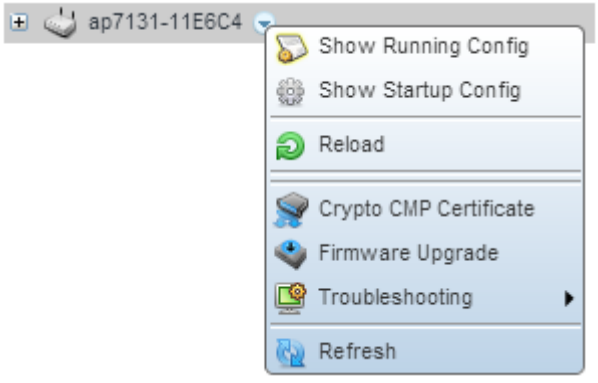


Figure 37: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

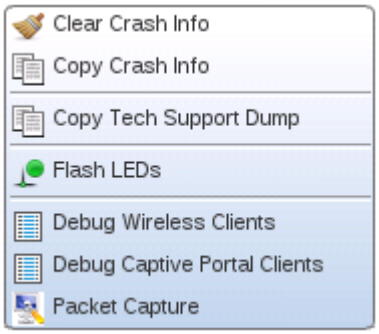


Figure 38: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Debug Captive Portal Clients.**

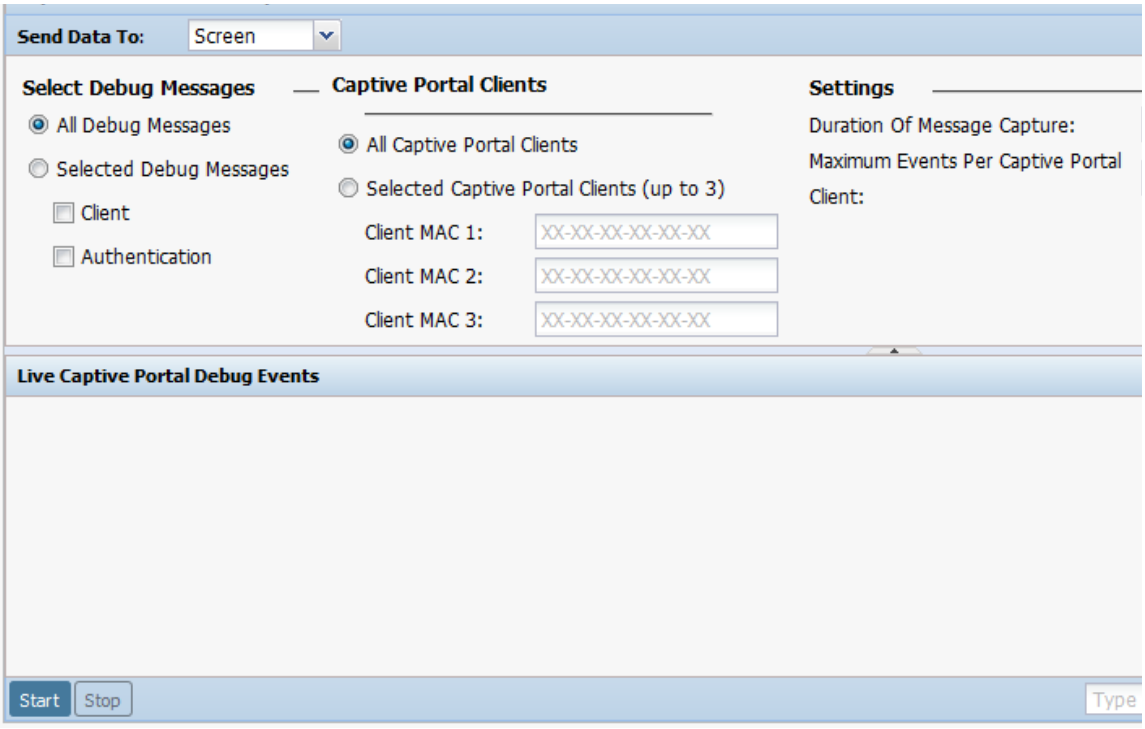


Figure 39: Debug Captive Portal Clients screen

5 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.

6 Select **Debug Message** settings to 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	Choose *Selected Debug Messages* 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.

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

All Captive Portal Clients	Select *All Captive Portal Clients* 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.

8 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.

9 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 wish to end the capture early, select **Stop**.

Packet Capture

"Troubleshooting the Device"

Use the **Packet Capture** screen to capture packets to troubleshoot network issues. To view the **Packet Capture** screen:

1 Select the target device from the left-hand side of the UI.



Figure 40: Device Browser

2 Select the down arrow next to the device to view a set of operations that can be performed on the selected device.

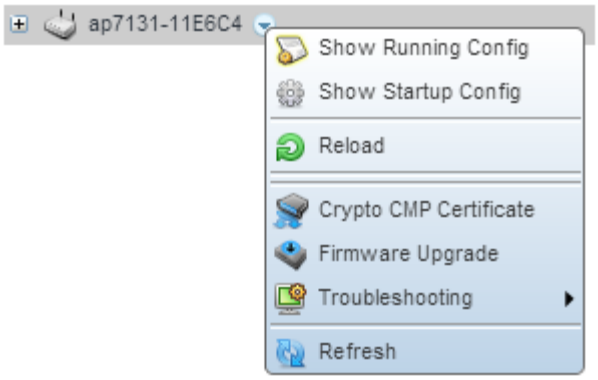


Figure 41: Device Browser - Options for a device

3 Select **Troubleshooting** to expand its sub-menu.

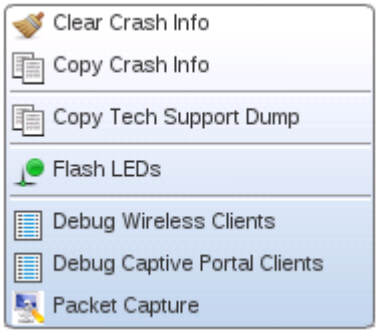


Figure 42: Device Browser - Options for a device - Troubleshooting sub-menu

4 Select **Packet Capture**.

NOTE

The maximum packet capture data limit is 15 MB.

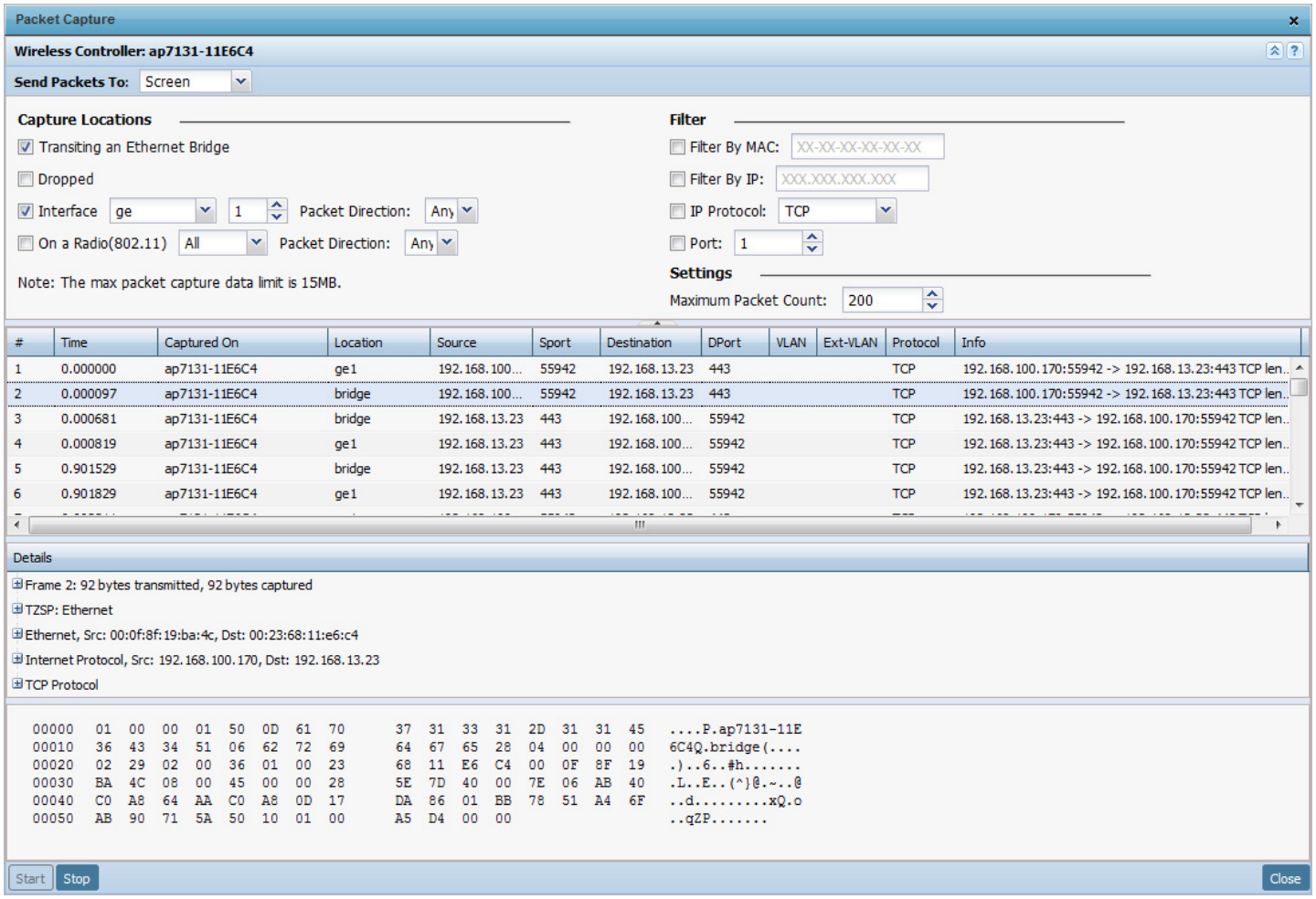


Figure 43: Device Browser - Options for Devices - Troubleshooting menu - Packet Capture screen

5 Use the **Send Data To** drop-down to select the destination for the captured packets. Select from *Screen* or *File*.

When *File* is selected, the captured debug events are stored on a file and then saved to a remote location using either the *FTP* or *TFTP* protocols. Use the screen to provide the appropriate information to save the file on the remote server.

6 Refer to the following **Capture Locations** options:

Transiting an Ethernet Bridge	Select this to enable capture of packets traversing an ethernet bridge.
Dropped	Select this to enable to capture dropped packets.
Interface	Select this to enable capture packets on specific interfaces. The interfaces can be select from the drop-down list. Select the interface number from the spinner control. Use the *Packet Direction* drop-down to configure the direction the packet traverses.
On a Radio (802.11)	Select this option to enable capture packets on specific radios. Depending on the device, the number of radios available for selection will differ. Select from *All*, *Radio 1*, *Radio 2* or *Radio 3*. Use the *Packet Direction* drop-down to configure the direction the packet traverses.

7 Refer to the following **Filter** options:

Filter by MAC	Select this to enable filtering the capture of packets based on the MAC address of a device.
Filter by IP	Select this to enable filtering the capture dropped packets based on the IP address of a device.
IP Protocol	Select this to enable filtering the capture packets on specific protocols. The protocols can be select from the drop-down list. The default protocol is *TCP*.
Port	Select this option to enable filtering capture packets on specific ports. Use the spinner to set the port number. The default port number is 1.

8 Refer to the following **Setting** options:

Maximum Packet Count	Use the spinner control to set the maximum number of packets to be captured. Packet capture is stopped once this number of packets are captured. The default value is 200.

9 Use the Start button to start packet capture. Use Stop to stop the capture.

10 Use **Close** to close this screen.

Viewing Device Summary Information

▸ "Devices"

Use the **Summary** screen to assess whether a device's firmware or configuration file requires an update to the latest feature set and functionality. To view the **Summary** screen:

1 Select **Operations.**

2 Select **Devices.**

3 Use the navigation pane on the left to navigate to the device to manage the firmware and configuration files on and select it.

The **Device Details Summary** screen displays by default. when **Operations** menu item is selected from the main menu.

NOTE

When displaying the Summary screen at the RF Domain level of the UI's hierarchal tree, the screen does not display a field for a device's Primary and Secondary firmware image. At the RF Domain level, the Summary screen just lists the *Hostname, MAC Address*, *Online* status, *Device Type* and *Is Controller* designations for the devices comprising the selected RF Domain. A RF Domain must be selected from the hierarchal tree and expanded to list the devices comprising the RF Domain. From there, individual controllers, service platforms and access points can be selected and their properties modified.

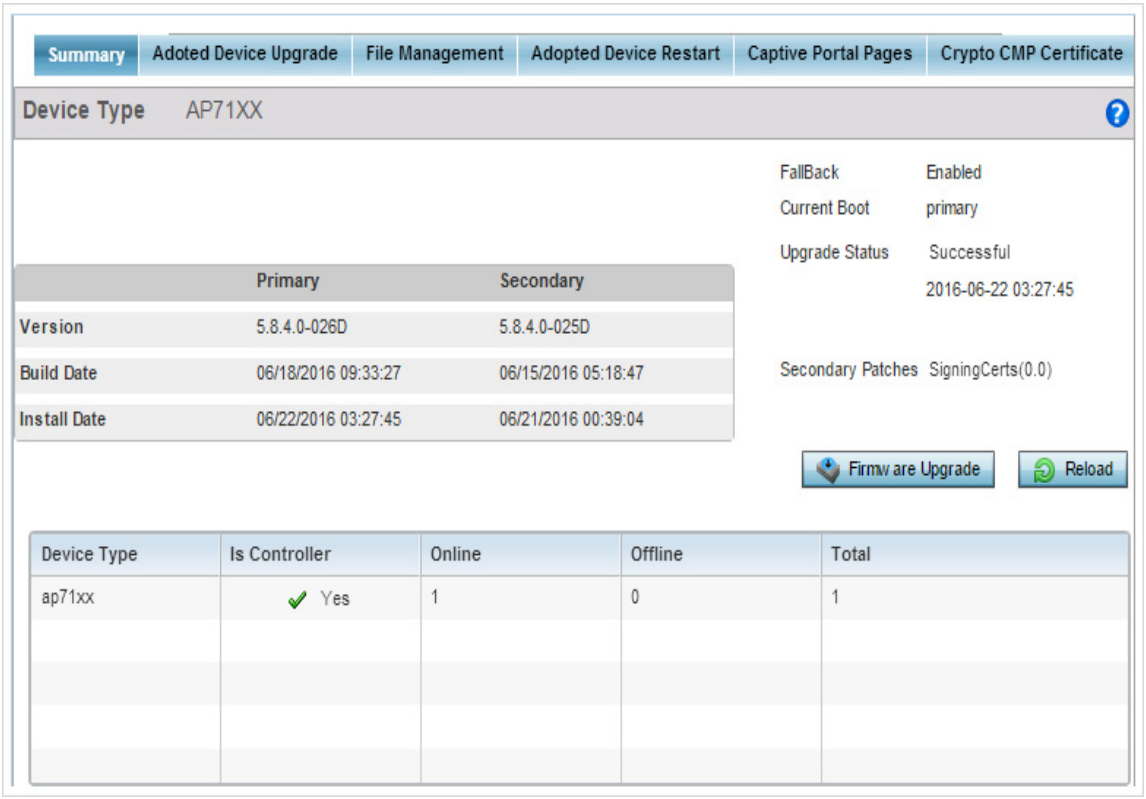


Figure 44: Device Details screen

4 Refer to the following to determine whether a firmware image needs requires an update:

Version	Displays the *Primary* and *Secondary* firmware image version currently utilized by the selected access point.
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 on the access point.
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 whether the primary or secondary firmware image is to be applied the next time the device boots.
Upgrade Status	Displays the status of the last firmware upgrade. For information on upgrading device firmware, see "Upgrading Device Firmware" on page 861.

5 Select **Firmware Upgrade** to upgrade the device's firmware to display the *Firmware Upgrade* screen. For more information, see "Upgrading Device Firmware" on page 861.

6 Select **Reload** to restart the device.

Adopted Device Upgrades

- "Devices"

To configure an access point upgrade:



NOTE

AP upgrades can only be performed by access points in Virtual Controller AP mode, and cannot be initiated by Standalone APs. Additionally, upgrades can only be performed on access points of the same model as the Virtual Controller AP.

1 Select **Operations** from the main menu.

2 Select **Devices.**

3 Use the navigation pane on the left to navigate to the device to manage the firmware and configuration files on and select it.

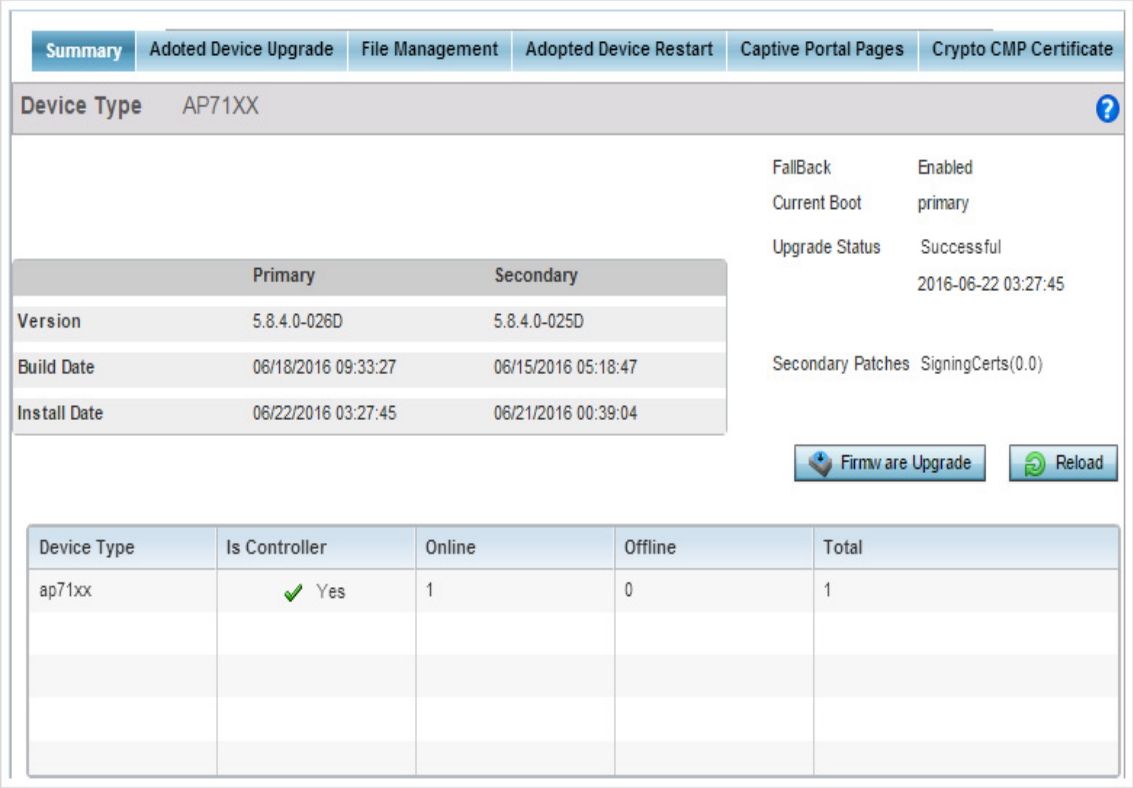


Figure 45: Device Summary screen

4 Select **Adopted Device Upgrade** tab.

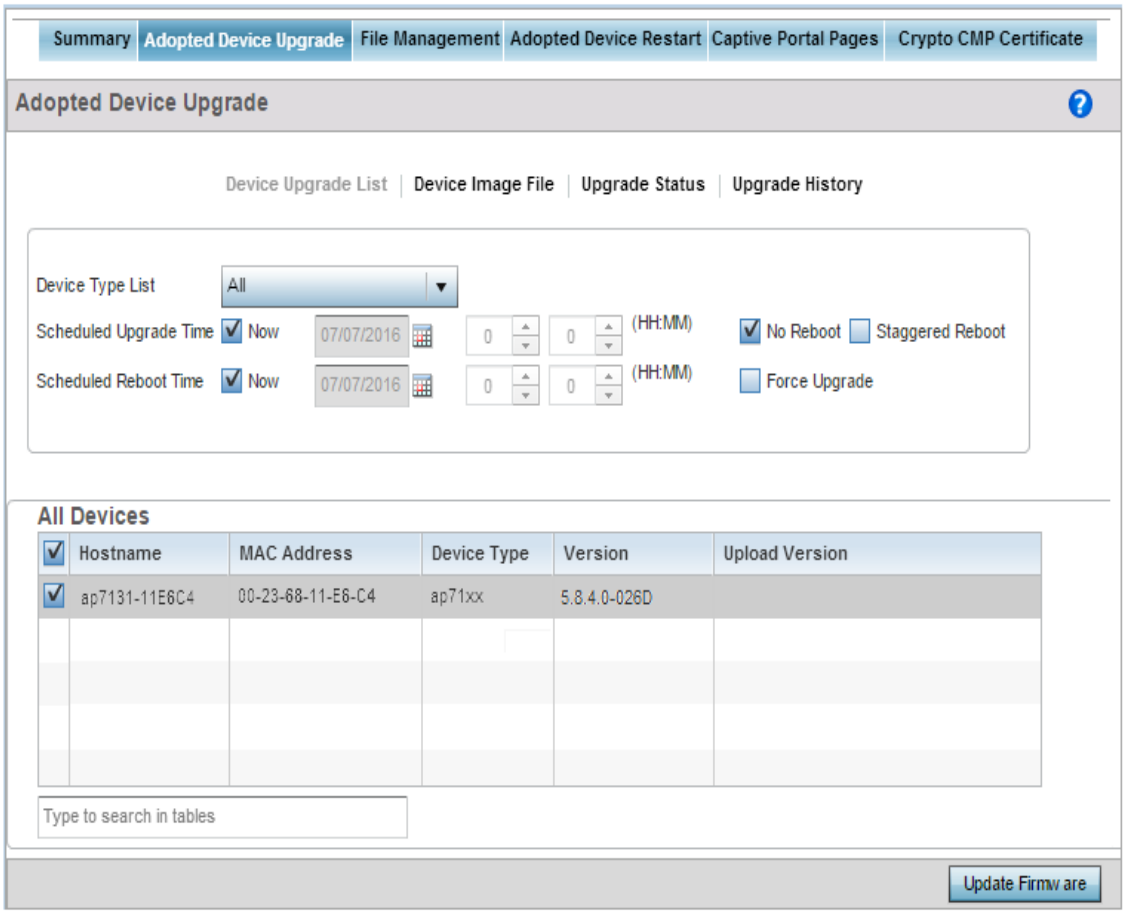


Figure 46: Devices - Adopted AP Upgrade screen



NOTE

If selecting the *Device Upgrade* screen from the RF Domain level of the UI, there is an additional Upgrade from Controller option to the right of the Device Type List drop-down menu. Select this option to provision selected device models within the same RF Domain from this RF Domain manager controller. If expanding a RF Domain and selecting a member device, the upgrade tab is entitled Adopted Device Upgrade, as an upgrade is made from an elected RF Domain Manager device. There is also an additional *Device Image File* screen to select the device image type and set the transfer protocol.

5 Refer to the following to configure the required AP upgrade parameters:

Device Type List	Select the access point model to specify which model is available to upgrade by the Virtual Controller AP. Upgrades can only be made to the same access point model. For example, an AP6532 firmware image cannot be used to upgrade an AP7131 model access point. For that reason, the drop-down menu will only display the model deployed.
Scheduled Upgrade Time	To perform the upgrade immediately, select *Now*. To schedule the upgrade to take place at a specified time, enter a date and time. Select whether you require an immediate reboot once the AP is updated. If you would like a reboot later, schedule the time accordingly. The AP must be rebooted to implement the firmware upgrade. Select *No Reboot* to ensure the access point remains in operation with its current firmware. This option is useful to ensure the access point remains operational until ready to take it offline for the required reboot.
Schedule Reboot Time	To reboot a target access point immediately, select *Now*. To schedule the reboot to take place at a specified time in the future, enter a date and time. This feature is helpful when wishing to upgrade an access point's firmware, but wish to keep in operation until the reboot does not impact its current client support and operation.
No Reboot	Select this option to prevent upgraded access points from being rebooted. This ensures that the access point remains in operation with its current firmware. This option is useful to ensure the access point remains operational until ready to take it offline for the required reboot.
Staggered Reboot	Select this option to do a staggered rebooting of upgraded access points. When selected, upgraded access points are not rebooted simultaneously bringing down the network. A few access points at a time are rebooted to preserve network availability.
Force Upgrade	Select this option to force upgrade for the selected access point. When selected, the access points are upgraded even if they have the same firmware as the upgrading wireless controller or service platform or access point.



NOTE

The Scheduled Upgrade Time and Scheduled Reboot Time are your local system's time. They are not the access point or wireless controller or service platforms or VX time and is not synchronized with the device.

6 Refer to the All Devices table for information about all the access points adopted by this device. Refer to the following for more information:

Hostname	Displays the access point's hostname if configured.
MAC Address	Displays the access point's MAC address.
Device Model	Displays the access point's model and type.
Version	Displays the firmware version installed on the access point,
Upload Version	Displays the firmware version of the image uploaded to the access point.

7 Click the option in the first column for each access point that needs to be updated.

8 Select the **Device Image File** tab to specify the model and network address information to the file used in the access point upgrade operation.

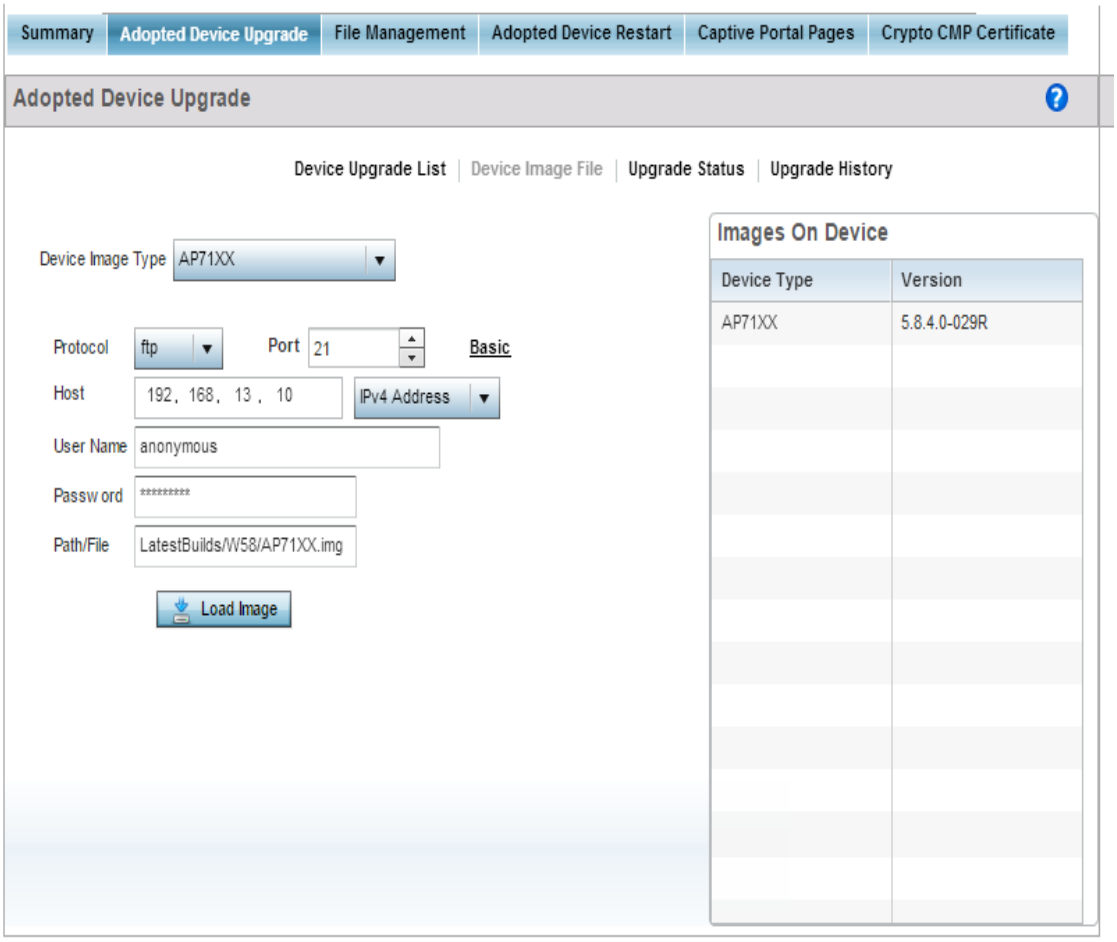


Figure 47: AP Upgrade screen - AP Image File

9 Select the **Device Image File** tab and refer to the following configuration parameters:

Device Image Type	Select the access point model to specify which model should be available to upgrade. Upgrades can only be made to the same access point model. For example, an AP6532 firmware image cannot be used to upgrade an AP7131 model access point. For that reason, the drop-down menu will only display the model deployed.
URL	Enter a URL pointing to the location of the image file.
Advanced/Basic	Select *Advanced* to list additional options for the image file location including protocol, host and path. Additional options display based on the selected protocol. Select *Basic* to display only the URL field.
Protocol	Select the protocol to retrieve the image files. Available options include: • *tftp* - Select this option to specify a file location using *Trivial File Transfer Protocol*. A port and IP address or hostname are required. A path is optional. • *ftp* - Select this option to specify a file location using *File Transfer Protocol*. A port, IP address or hostname, username and password are required. A path is optional. • *sftp* - Select this option to specify a file location using *Secure File Transfer Protocol*. A port, IP address or hostname, username and password are required. A path is optional. • *http* - Select this option to specify a file location using *Hypertext Transfer Protocol*. A hostname or IP address is required. Port and path are optional • *cf* - Select this option to specify a file location on a Compact Flash card installed on the device. This option might not be available on all devices. • *usb1/usb2/usb3/usb4* - Select this option to specify the file location on one of the USB 1, USB 2, USB 3 or USB 4 ports of the device. This option might not be available on all devices.
Port	Use the spinner control or manually enter the value to define the port used by the protocol for importing the firmware upgrade file. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*.
Host	Enter IP address or the hostname of the server used to import the firmware file. This option is not valid for *local, cf*, *usb1*, *usb2, usb3* and *usb4*. Use the drop-down to select the type of host information. Host can be one of *Host Name* or *IP Address.*
Path/File	Specify the path to the firmware file. Enter the complete relative path to the file on the server.
User Name	Define the user name used to access either a FTP or SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*
Password	Specify the user account password to access the FTP or a SFTP server. This field is only available if the selected protocol is *ftp* or *sftp.*

10 When the AP Image Type and appropriate file location and protocol have been specified, select the **Load Image** button to load all available images to the **Type** and **Version** table.

The table now displays available images and their corresponding versions.

11 Select the **Upgrade Status** tab to review a list of devices being upgraded by this access point.

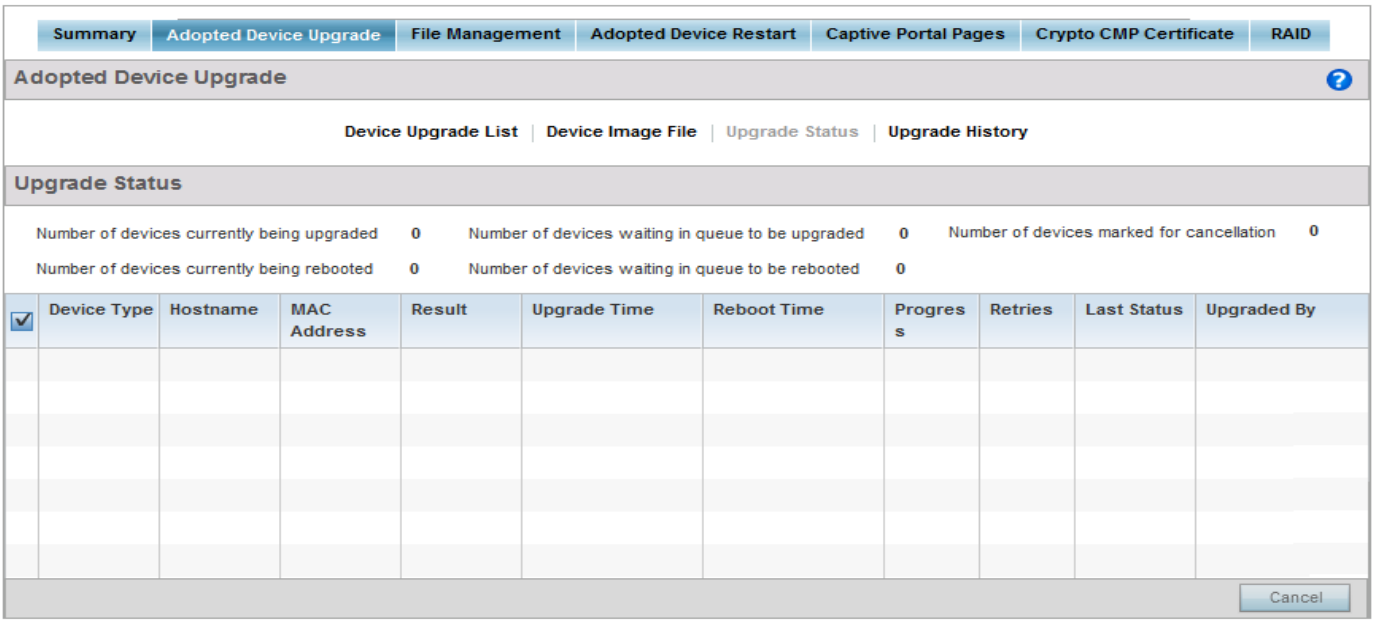


Figure 48: AP Upgrade screen - Upgrade Status screen

12 Refer to the following fields to understand the status of the number of device being updated:

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 rebooted	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 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 rebooted	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 the 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 cancellation	Displays the total number of device upgrades that have been manually cancelled during the upgrade operation.

13 Refer to the following fields for more information:

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 the upgrade is immediate or set by an administrator for a specific time. This is helpful to ensure a sufficient number of devices remain in service at any given time.
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.
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 the image to the listed device.

14 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 are selected for cancellation.

15 Select the **Upgrade History** tab to review an Upgrade History of access point upgrade operations.

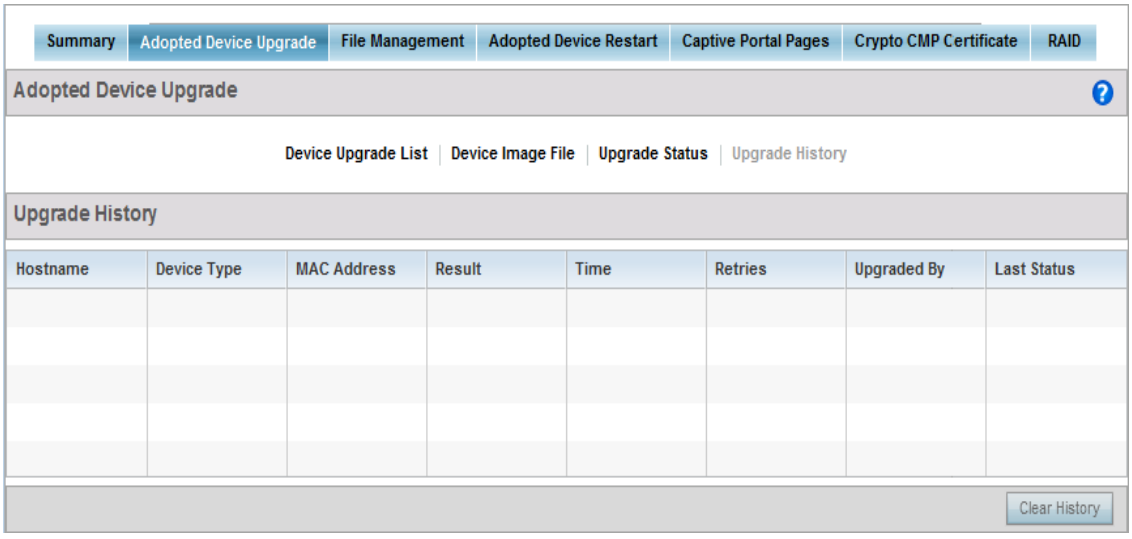


Figure 49: AP Upgrade screen - Upgrade History screen

16 Refer to the following to assess devices impacted by upgrade operations and their upgrade status:

Hostname	Displays the hostname of the access point, if configured.
Device Model	Displays the type of access point upgraded.
MAC Address	Displays the primary MAC (or hardware identifier) for each device impacted by an upgrade operation.
Result	Displays the current upgrade status for each listed access point. Possible states include: • Waiting • Downloading • Updating Scheduled • Reboot • Rebooting Done • Cancelled • Done • No Reboot
Time	Displays the time when the device was upgraded.
Retries	Displays the number of retries, if any, during the upgrade. If this number is more than a few, the upgrade configuration should be revisited.
Upgraded By	Displays the hostname of the device that upgraded this device.
Last Status	Displays the time of the last status update for access points that are no longer upgrading.
Clear History	Selecting the *Clear History* button clears the history log page for each access point.
Cancel	Clicking the *Cancel* button will cancel the upgrade process for any selected access points that are upgrading.

17 Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

File Management

"Devices"

The access point maintains a File Browser enabling the administration of files currently residing on any internal or external memory location. 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 manage files stored on the device:

1 Select **Operations** from the main menu.

2 Select **Devices.**

3 Use the navigation pane on the left to navigate to the device to manage the files on and select it.

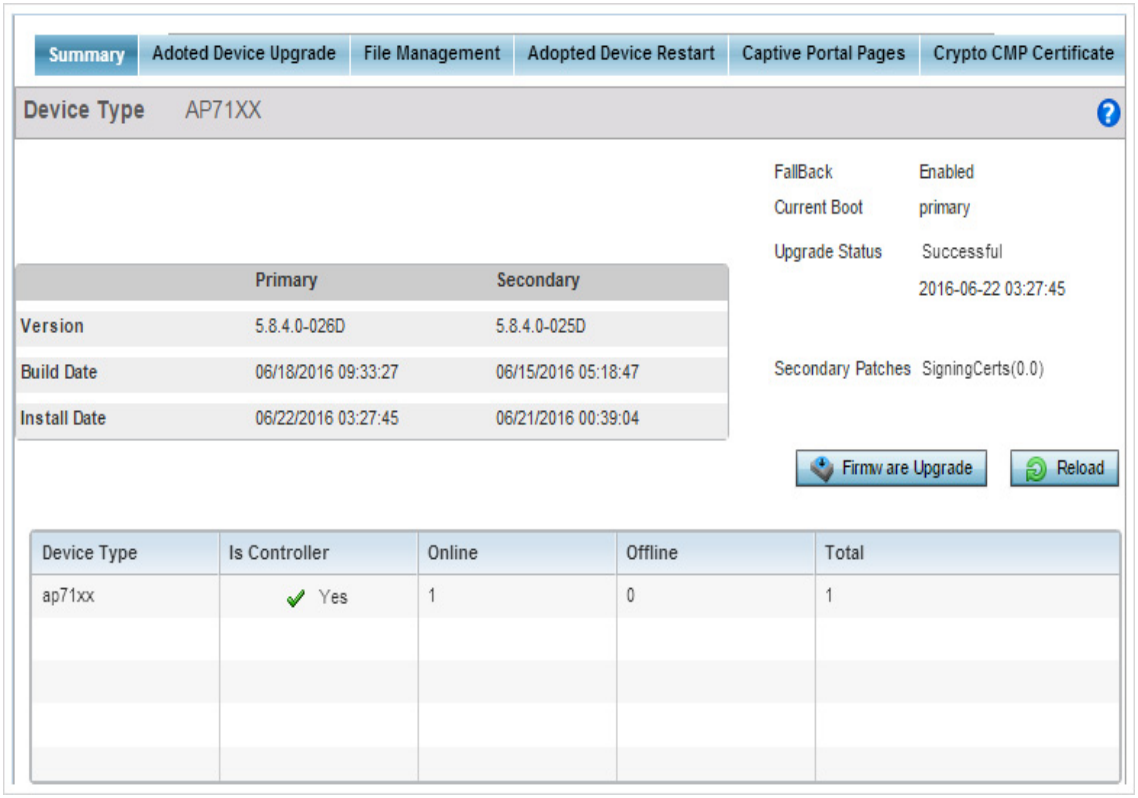


Figure 50: Device Summary screen

4 Click **File Management**.

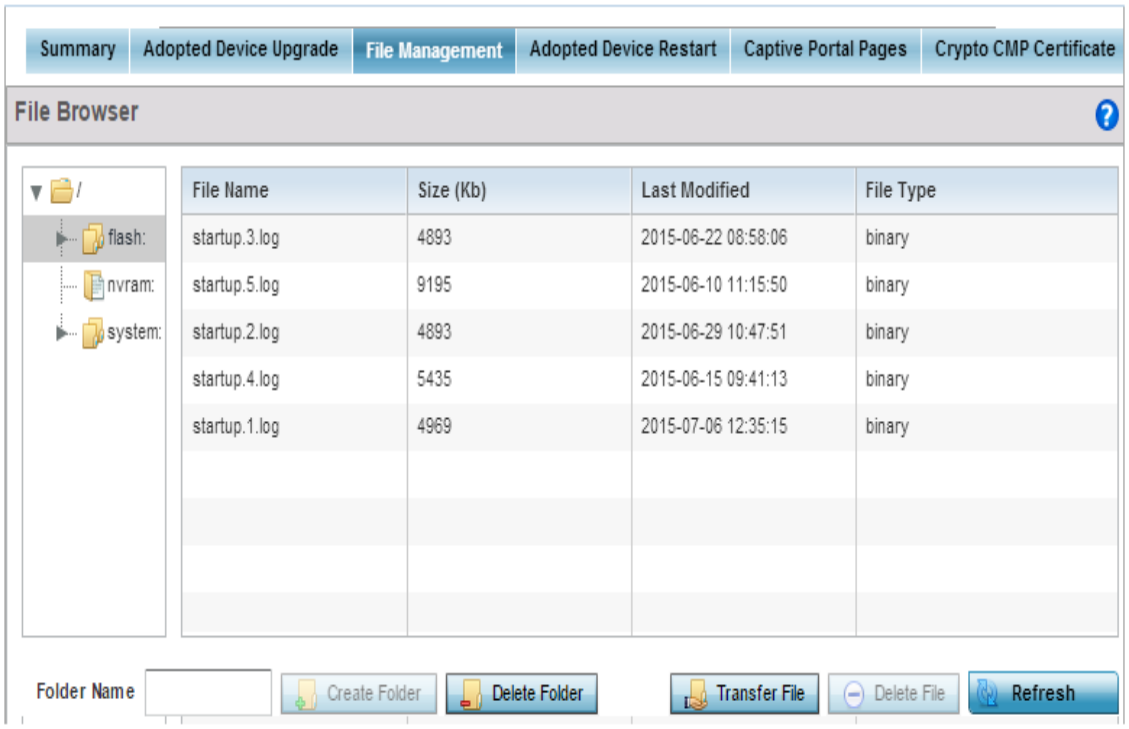


Figure 51: Devices - File Management screen

5 The pane on the left of the screen displays the directory tree for the selected device. Use this tree to navigate around the device's directory structure. When a directory is selected, all files in that directory is listed in the pane on the right.

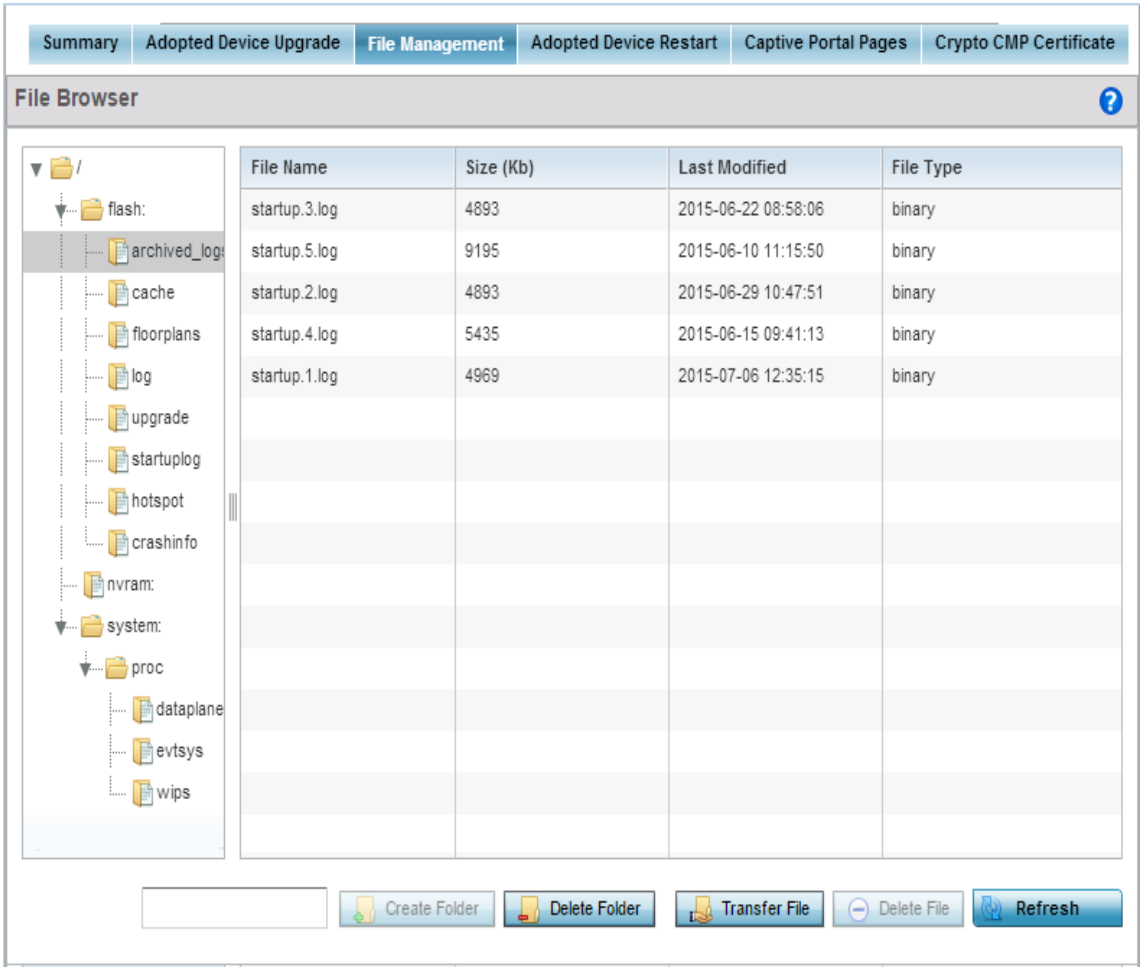


Figure 52: Devices - File Management screen

6 Refer to the following for more information:

File Name	Displays the name of the file.
Size (Kb)	Displays the size of the file in kilobytes.
Last Modified	Displays the timestamp for the last modification made to the file.
File Type	Displays the type of file. File type can be *binary, empty* or *text*.

7 To create a folder, select the parent folder in the directory tree on the left. Enter the directory name in the **Folder Name** text box. Click the **Create Folder** button to create the new folder. Click the **Refresh** button to refresh the view in the screen.

8 To delete a folder, select the folder in the directory tree on the left. Click **Delete Folder** button. The following popup displays:

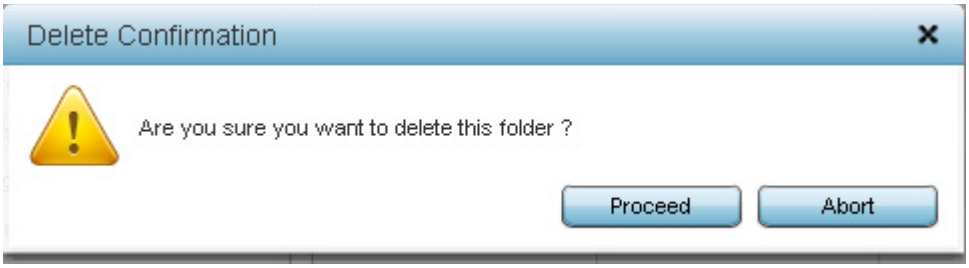


Figure 53: Devices - File Management - Delete Confirmation screen

Click **Proceed** to delete the directory. All files in the selected directory also get deleted. Click **Abort** to exit without deleting the directory.

9 Click **Transfer File** to transfer files between the device and a remote server. The following window displays:

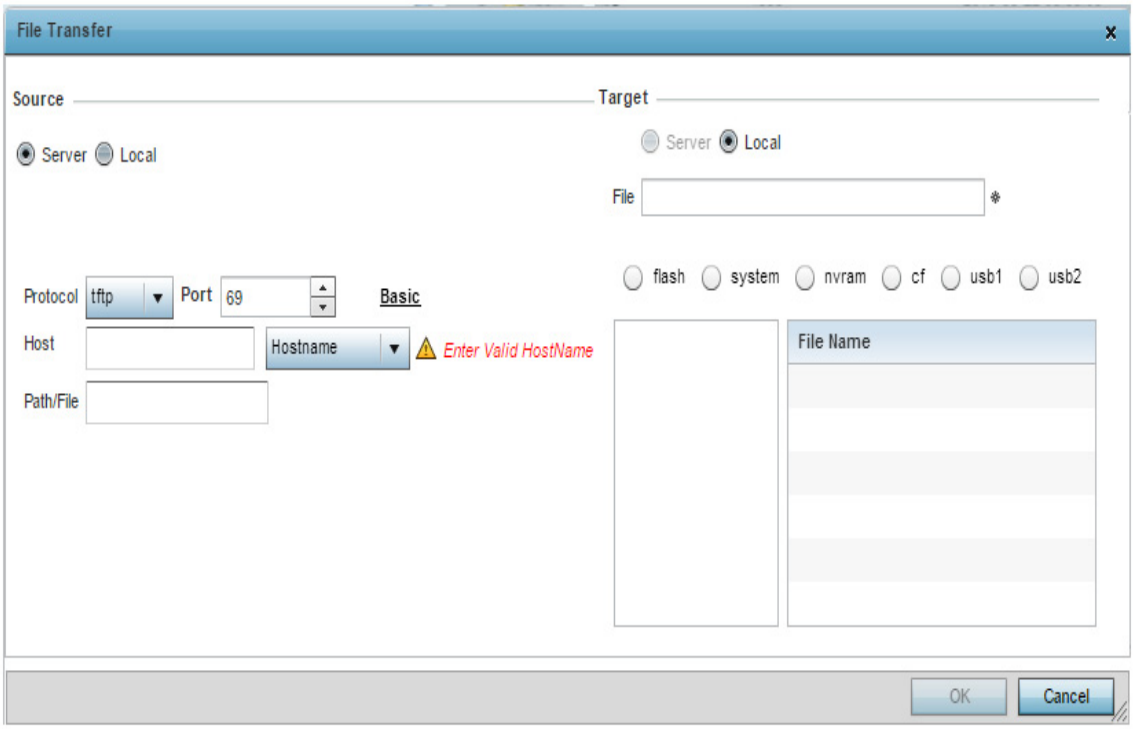


Figure 54: File Management - File Transfer Dialog

Use this dialog to transfer files between the device and a remote location. The transfer can be done as follows:

- *From remote server to the device*
- *From device to remote server*
- *From a location on the device to another location on the same device.*

10 Set the following file management source and target directions as well as the configuration parameters of the required file transfer activity:

Source	• Select *Server* to indicate the source of the file is a remote server. • Select *Local* to indicate the file is on the access point itself.
File	If the source is *Local*, enter the name of the file to be transferred.
Protocol	If *Advanced* is selected, choose the protocol for file management. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4 This parameter is required only when *Server* is selected as the *Source* and *Advanced* is selected.
Port	If *Advanced* is selected, specify the port for transferring files. This option is not available for *cf*, *usb1*, *usb2, usb3* and *usb4*. Enter the port number directly or use the spinner control. This parameter is required only when *Server* is selected as the *Source*.
IP Address	If *Advanced* is selected, specify the IP address of the server used to transfer files. This option is not valid for *cf*, *usb1*, *usb2, usb3* and *usb4*. If IP address of the server is provided, a *Hostname* is not required. This parameter is required only when *Server* is selected as the *Source*.

Hostname	If needed, specify a Hostname of the server transferring the file. This option is not valid for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. If a hostname is provided, an *IP Address* is not needed. This field is only available when *Server* is selected in the *From* field.
Path/File	If *Advanced* is selected, 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*.
User Name	If *Advanced* is selected, provide a user name to access a FTP or SFTP server. This parameter is required only when *Server* is selected as the *Source*, and the selected protocol is *ftp* or *sftp*.
Password	If *Advanced* is selected, 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*.
Target	If *Advanced* is selected, set the target destination to transfer the file using FTP or SFTP. • Select *Server* if the destination is a remote server, then provide a URL to the location of the server resource or select *Advanced* and provide the same network address information described above. • Select Access Point if the destination is an access point.

11 Select **Ok** to begin the file transfer. Selecting **Cancel** reverts the screen to its last saved configuration.

12 To delete a file, select the file to be deleted and click **Delete File** button. The file is deleted immediately.

Adopted Device Restart

"Devices"

Use the *Adopted Device Restart* screen to restart one or more of the access points adopted by this AP. To view the Adopted Device Restart screen:



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.

1 Select **Operations** from the main menu.

2 Select **Devices.**

3 Use the navigation pane on the left to navigate to the device to manage the files on and select it.

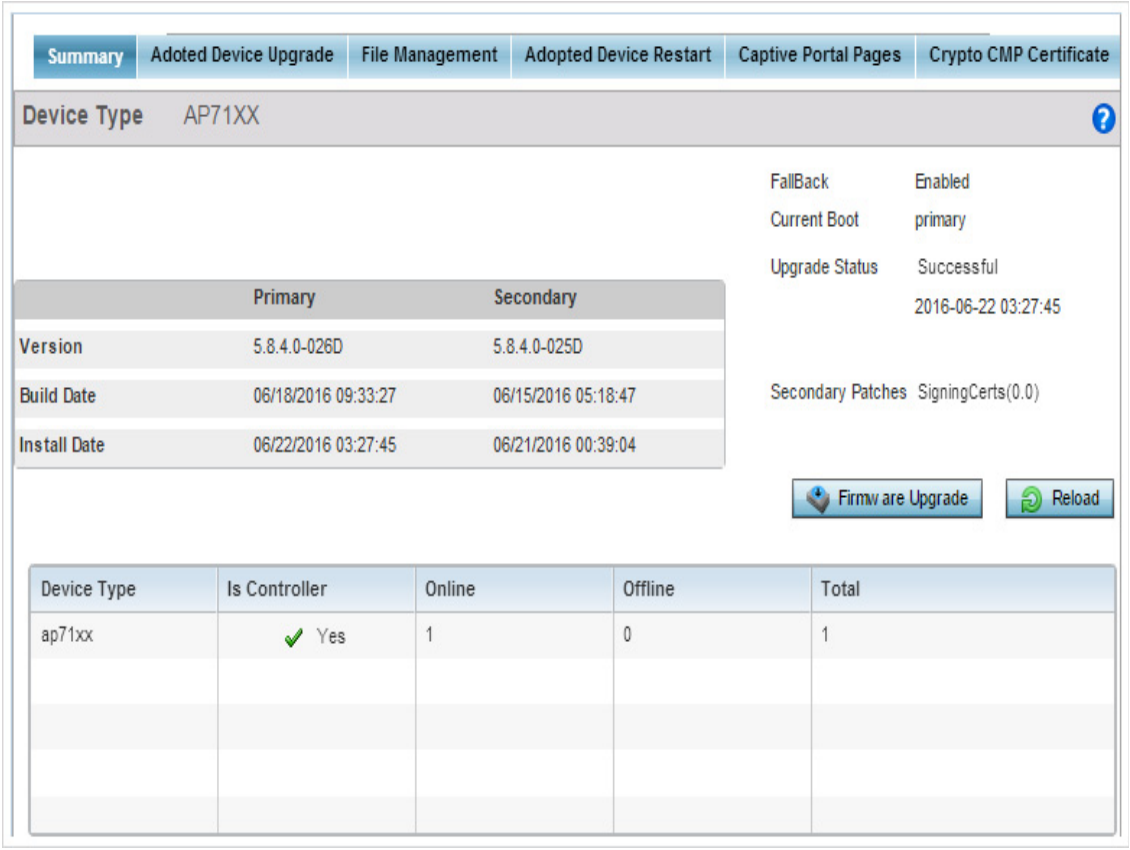


Figure 55: Device Summary screen

4 Select **Adopted Device Restart**.

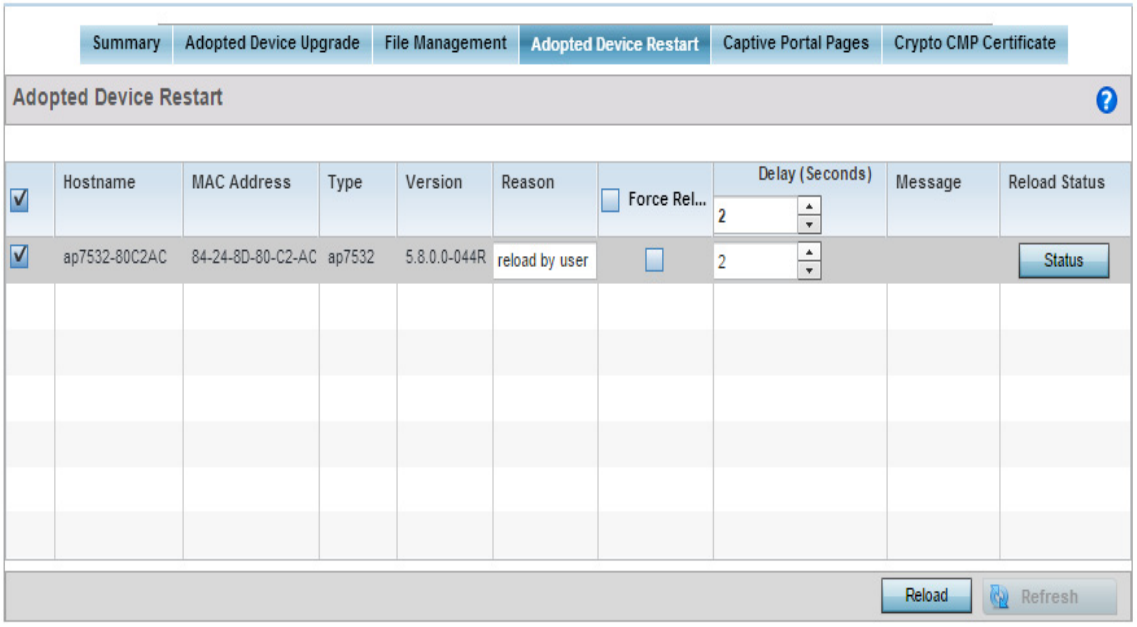


Figure 56: Devices - Adopted Device Restart screen

5 From the list of adopted devices, select the access point from the list and select **Reload**.

6 Select **Refresh** to refresh the list of adopted access points on the screen.

Captive Portal Pages

"Devices"

A *captive portal* is an access policy that provides temporary and restrictive access to the access point managed wireless network.

A captive portal policy 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 the wireless network. Once logged into the captive portal, additional *Terms and Conditions*, *Welcome* and *Fail* pages provide the administrator with a number of options on screen flow and appearance.

Captive portal authentication is used primarily for guest or visitor access to the network, 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.

Each supported access point model can support up to 32 captive portal policies, with the exception of AP6521 model, which can only support 16 captive portal policies.

The *Captive Portal Pages* screen enables the management of the configured captive portal pages and their transfer to the adopted access points.

To manage captive portal pages:

1 Select **Operations** from the main menu.

2 Select **Devices.**

3 Use the navigation pane on the left to navigate to the device to manage the files on and select it.

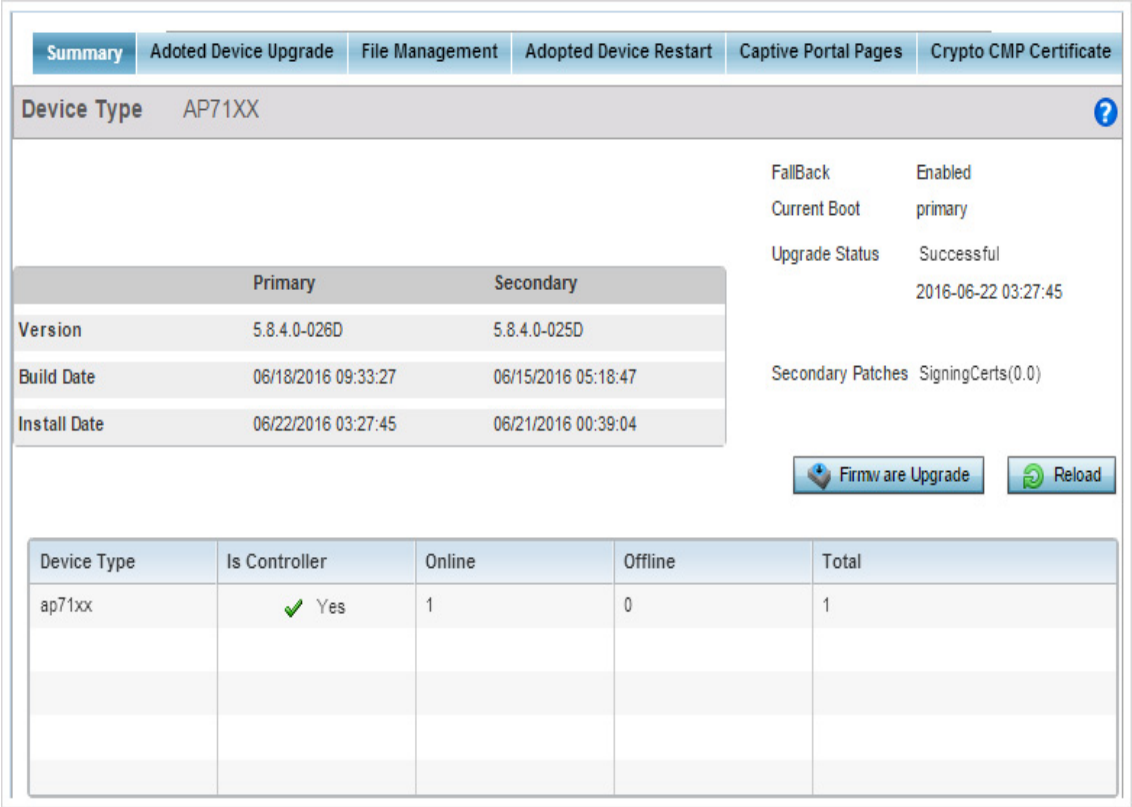


Figure 57: Device Summary screen

4 Select **Captive Portal Pages**.

NOTE

If selecting the Captive Portal Pages screen from the RF Domain level of the UI's hierarchal tree, there is an additional Upload from Controller option to the right of the Captive Portal List drop-down menu. Select this option to upload captive portal page support from this device's managing controller.

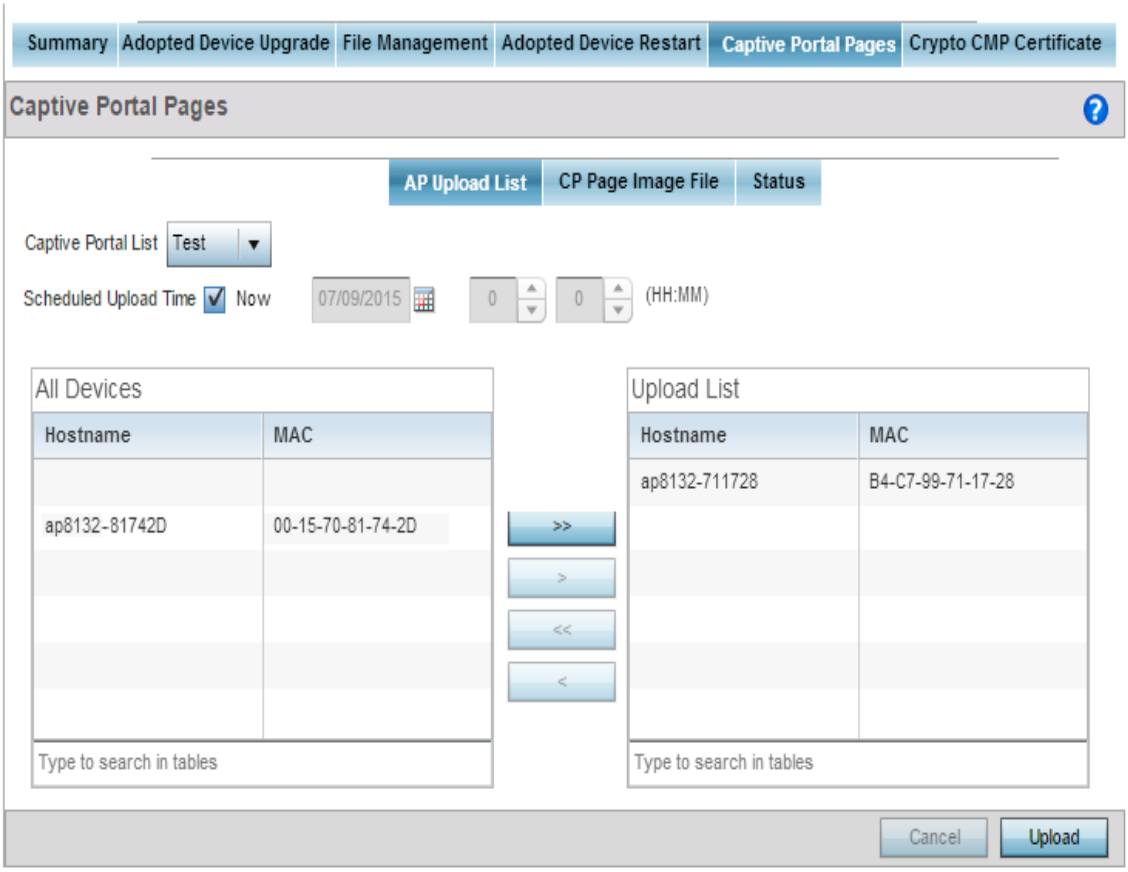


Figure 58: Devices Captive Portal Pages - AP Upload List screen

5 Use the **Captive Portal List** drop-down list to select the captive portal configuration to upload to the adopted access points.

6 Use the **Scheduled Upload Time** field to configure the time of the captive portal pages update. Select **Now** option to immediately start the process of the update. Use the date, hour fields to configure a specific date and time for upload.

NOTE

The Scheduled Upload Time is your local system's time. It is not the access point or wireless controller or service platforms or VX time and is not synchronized with the device.

7 The **All Devices** table lists the hostname and MAC address of all devices adopted by this access point. Use the arrow buttons to move selected devices from the **All Devices** table to the **Upload List** table. The **Upload List** table lists the devices to which the captive portal pages are updated.

8 Select **Upload Pages** to upload the captive portal pages to the selected devices.

9 Select the **CP Pages Image File** tab.

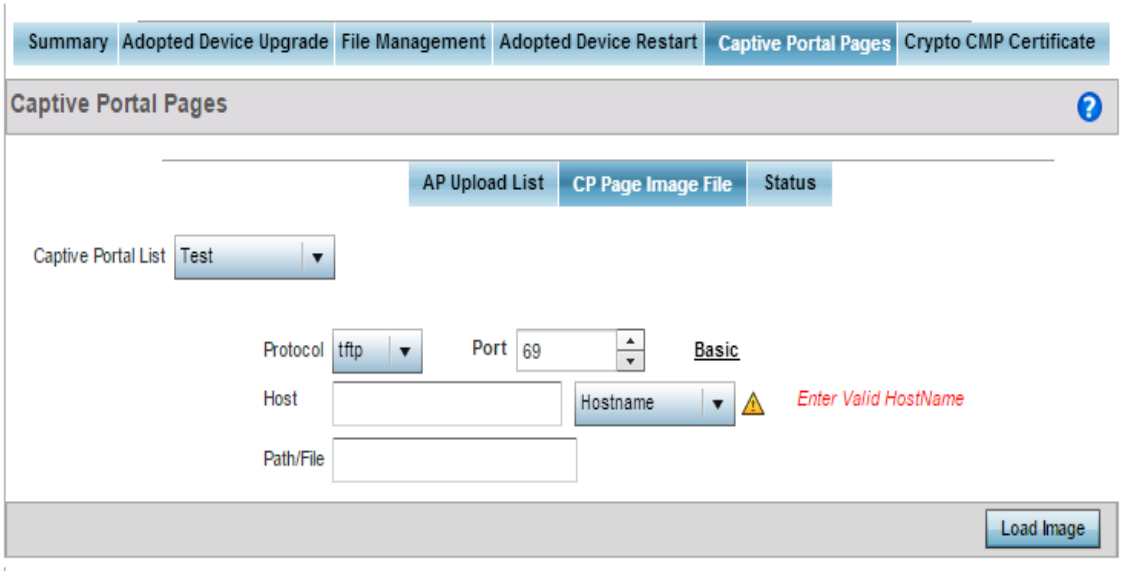


Figure 59: Devices Captive Portal Pages - CP Page Image File screen

10 Use the **Captive Portal List** drop-down list to select the captive portal configuration to upload to the adopted access points.

11 Set the following file transfer configuration parameters of the required file transfer activity:

Protocol	If *Advanced* is selected, choose the protocol for file management. Available options include: • tftp • ftp • sftp • http This parameter is required only when Server is selected as the Source and Advanced is selected.
Port	If *Advanced* is selected, specify the port for transferring files. This option is not available for *cf*, *usb1*, *usb2*, *usb3* and *usb4*. Enter the port number directly or use the spinner control.

IP Address	If *Advanced* is selected, specify the IP address of the server used to transfer files. This option is not valid for *cf*, *usb1*, *usb2, usb3* and *usb4*. If IP address of the server is provided, a *Hostname* is not required.
Hostname	If needed, specify a Hostname of the server transferring the file. This option is not valid for *cf*, *usb1*, *usb2, usb3* and *usb4*. If a hostname is provided, an *IP Address* is not needed. This field is only available when *Server* is selected in the *From* field.
Path/File	If *Advanced* is selected, define the path to the file on the server. Enter the complete relative path to the file.
User Name	If *Advanced* is selected, provide a user name to access a FTP or SFTP server. This parameter is required only when the selected protocol is *ftp* or *sftp*.
Password	If *Advanced* is selected, provide a password to access the FTP or SFTP server. This parameter is required only when the selected protocol is *ftp* or *sftp*.

12 Select **Load Image** to start loading the captive portal pages image file.

13 Optionally, refer to the **Load Image Status** field to view the status of the current upload.

14 Select **Status** tab.

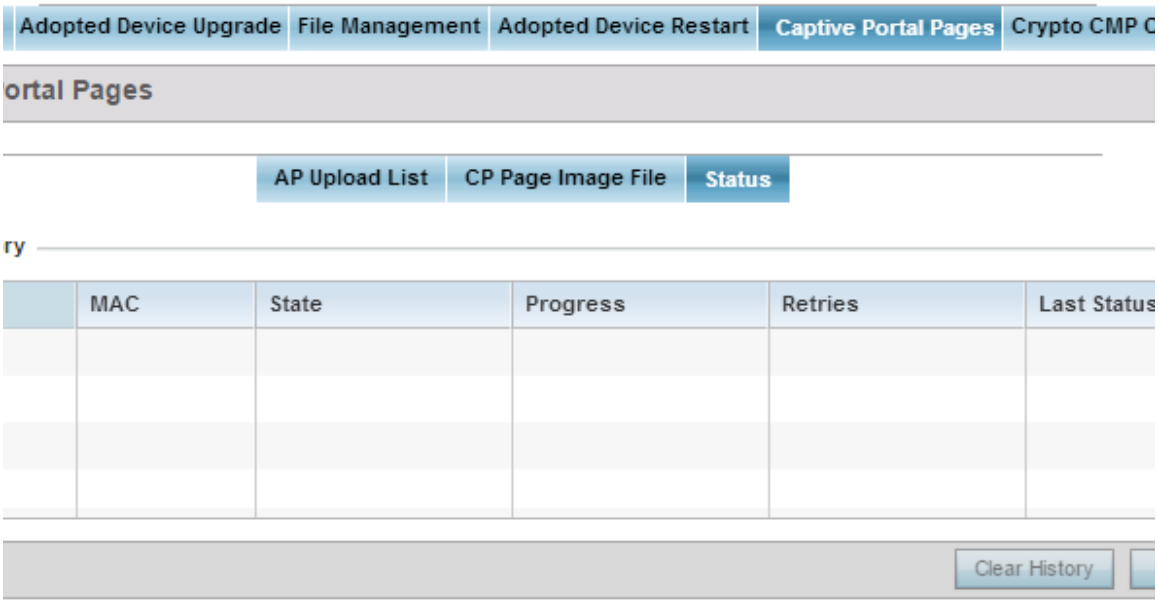


Figure 60: Devices Captive Portal Pages - Status screen

15 Refer to the **Status** tab to view the history of captive portal pages upload.

Hostname	Displays the hostname of the target device.

MAC	Displays the factory assigned MAC address of the target device.
State	Displays the target device's state.
Progress	Displays the progress of the upload to the target device.
Retries	Displays the number of retires attempted for upload to the target device.
Last Status	Displays the last known status of the upload to the target device.

16 Select **Clear History** to clear the history displayed in the **Status** tab.

Managing Crypto CMP Certificates

"Devices"

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.

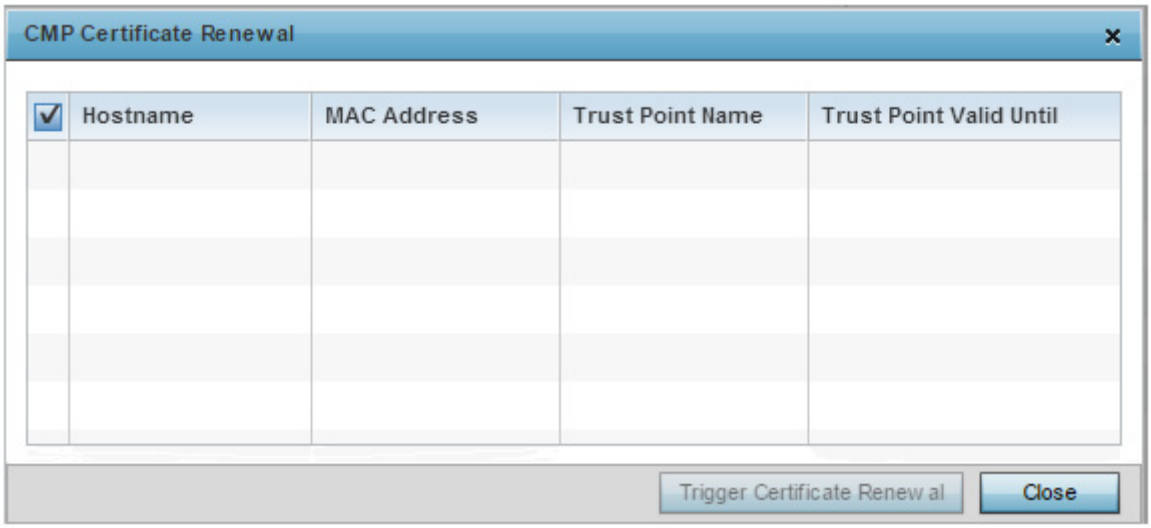


Figure 61: Crypto CMP Certificate Management screen

Use the Crypto Certificate Renewal screen to view and if required, trigger certificate renewal for CMP 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	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.

Re-elect Controller

- "Devices"

Use the **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:



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 access points.

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.

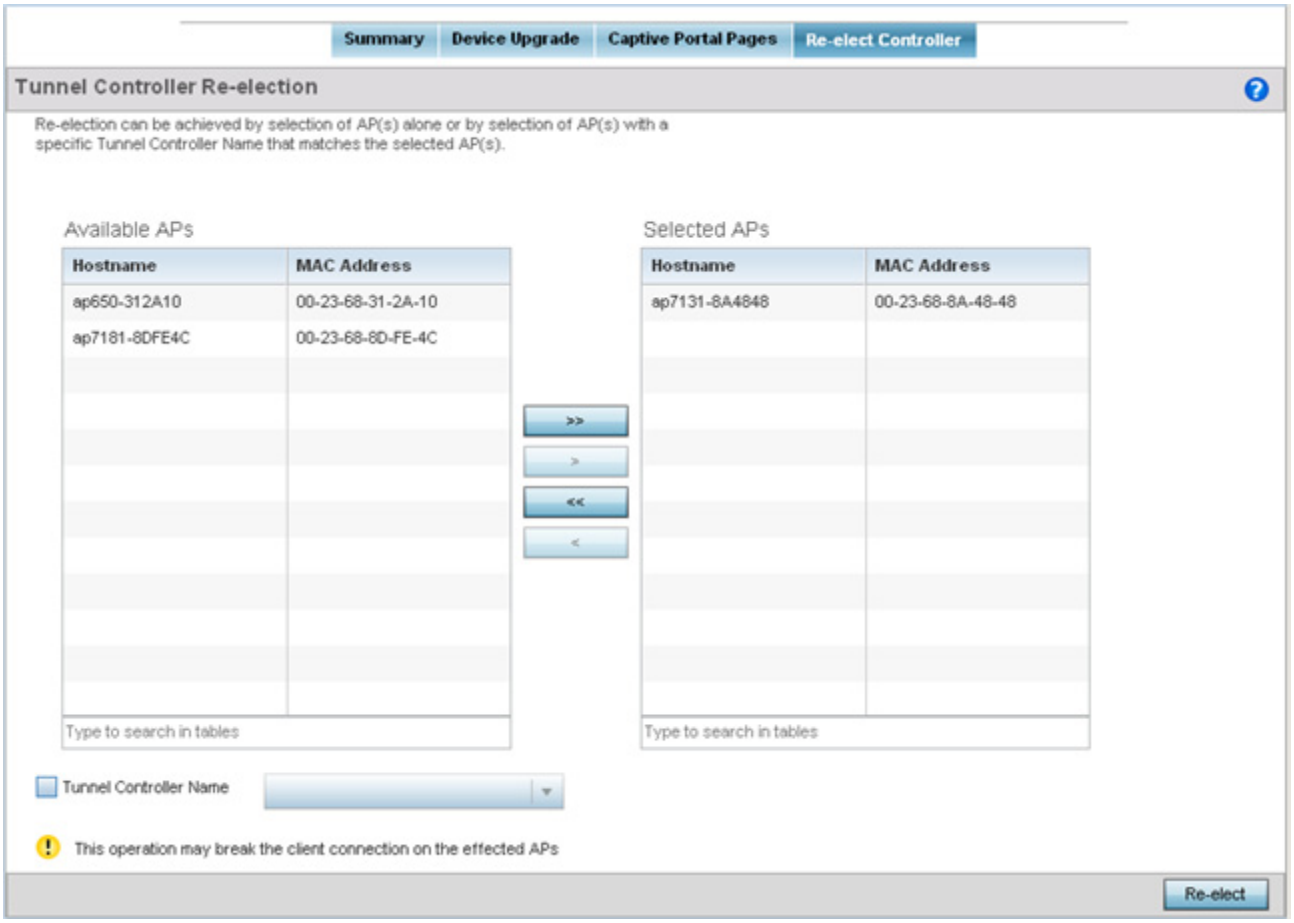


Figure 62: Re-elect Controller screen

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

"Operations"

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 resources, if properly configured. A RSA key pair must be generated on the client.

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

- "Certificate Management"
- "RSA Key Management"
- "Certificate Creation"
- "Generating a Certificate Signing Request (CSR)"

Certificate Management

- "Certificates"

If not wanting to use an existing certificate or key with a selected device, an existing *stored* certificate can be leveraged from a different device for use with the target device. 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**.

2 Select **Certificates.**

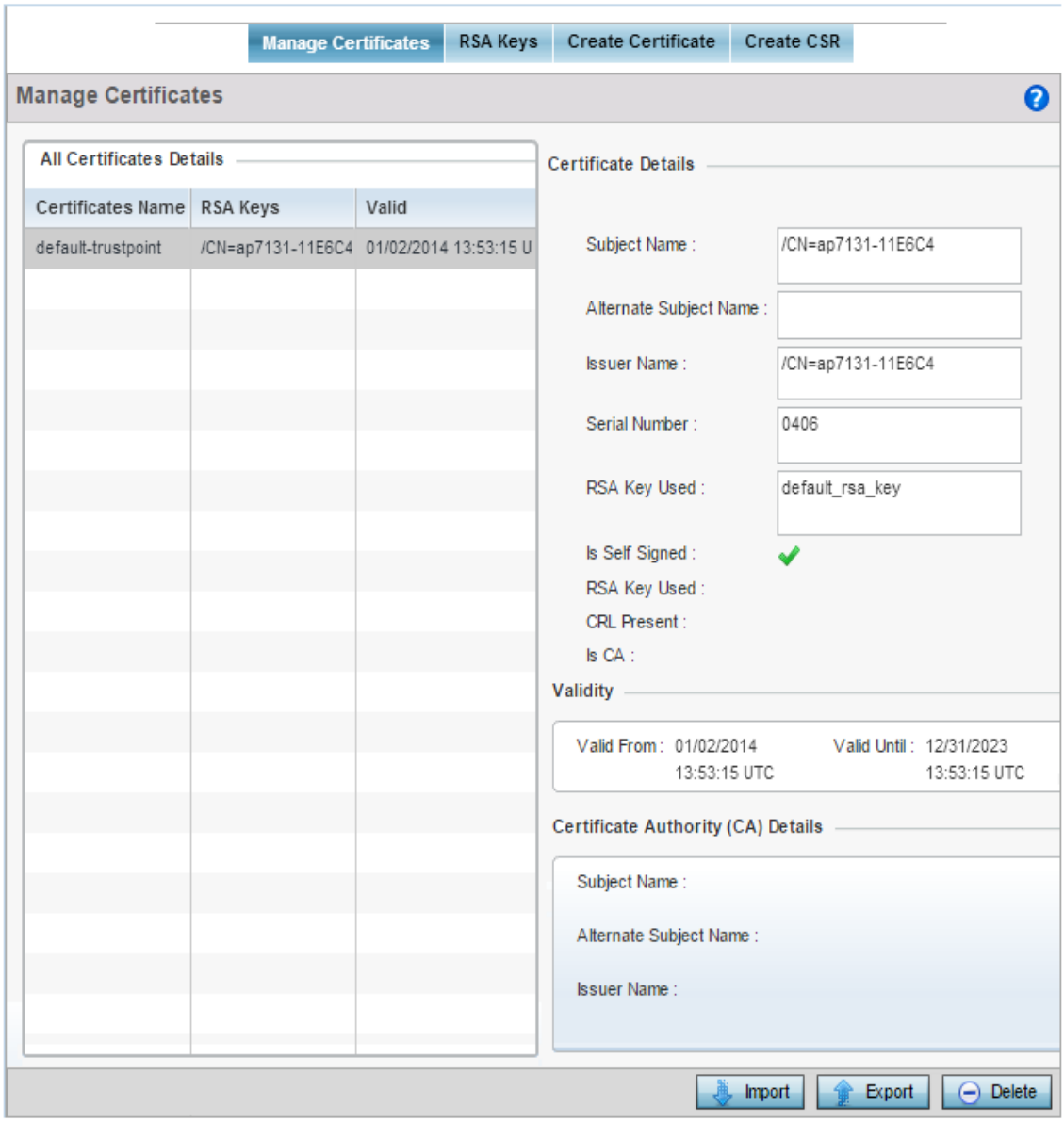


Figure 63: Certificate Management -Trustpoints screen

The **Trustpoints** screen displays for the selected MAC address.

3 Refer to the **Certificate Details** to review certificate properties, self-signed credentials, validity period and CA information.

4 Select the **Import** button to import a certificate.

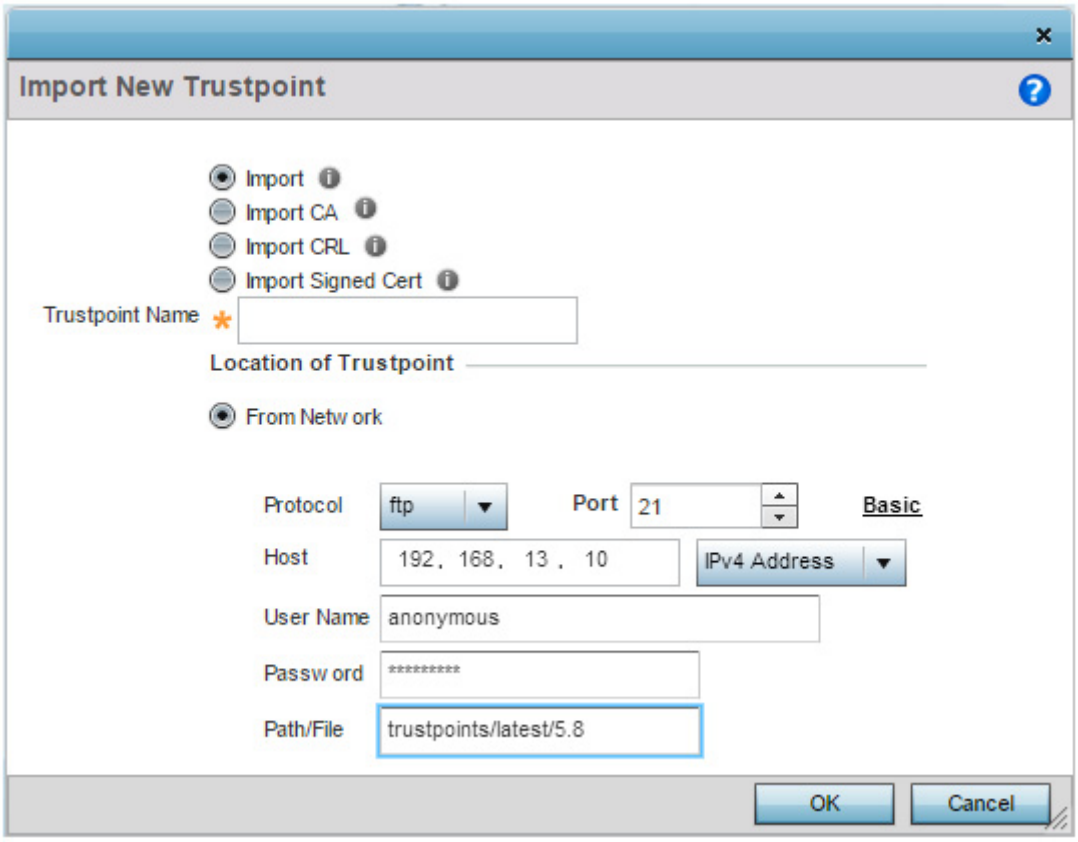


Figure 64: Certificate Management - Import New Trustpoint screen

5 Define the following configuration parameters required for the **Import** of the Trustpoint:

Import	Select the type of Trustpoint to import. The following Trustpoints can be imported: • *Import* – Select to import any trustpoint. • *Import CA* – Select to import a *Certificate Authority* (CA) certificate on to the access point. • *Import CRL* – Select to import a *Certificate Revocation List* (CRL), CRLs are used to identify and remove those installed certificates that have been revoked or are no longer valid. • *Import Signed Cert* – Select to import a self signed certificate.
Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.

A *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*.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A *certificate revocation list* (CRL) is a list of revoked certificates, or certificates no longer valid. A certificate can be revoked if the CA improperly issued a certificate, or if a

private key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

6 Define the following configuration to import the Trustpoint from a location on the network. To do so, select **From Network** and provide the following information.

URL	Provide the complete URL to the location of the trustpoint. This option is available by default. Click the *Advanced* link next to this field to display more fields to provide detailed trustpoint location information.
Protocol	If using *Advanced* settings, select the protocol used for importing the target trustpoint. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If using *Advanced* settings, use the spinner control to set the port. This option is not valid for *cf* and *usb1 - 4.*
IP Address	If using *Advanced* settings, enter IP address of the server used to import the trustpoint. This option is not valid for *cf* and *usb1 - 4.*
Hostname	Provide the hostname or numeric IP4 or IPv6 formatted IP address of the server used to import the trustpoint. 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. Providing a host is not required for cf and usb1-4. If using Advanced settings, provide the hostname of the server used to import the trustpoint. This option is not valid for cf and usb1 - 4.
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If using *Advanced* settings, specify the path to the trustpoint. Enter the complete path to the file on the server.

7 Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

8 To optionally export a trustpoint to a remote location, select the **Export** button from the Trustpoints screen.

Once a certificate has been generated on the authentication server, export the self signed certificate. A digital CA certificate is different from a self signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an Active Directory Group Policy for automatic root certificate deployment.

Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication servers, export the certificate and do not generate a second key unless you want to deploy two root certificates.

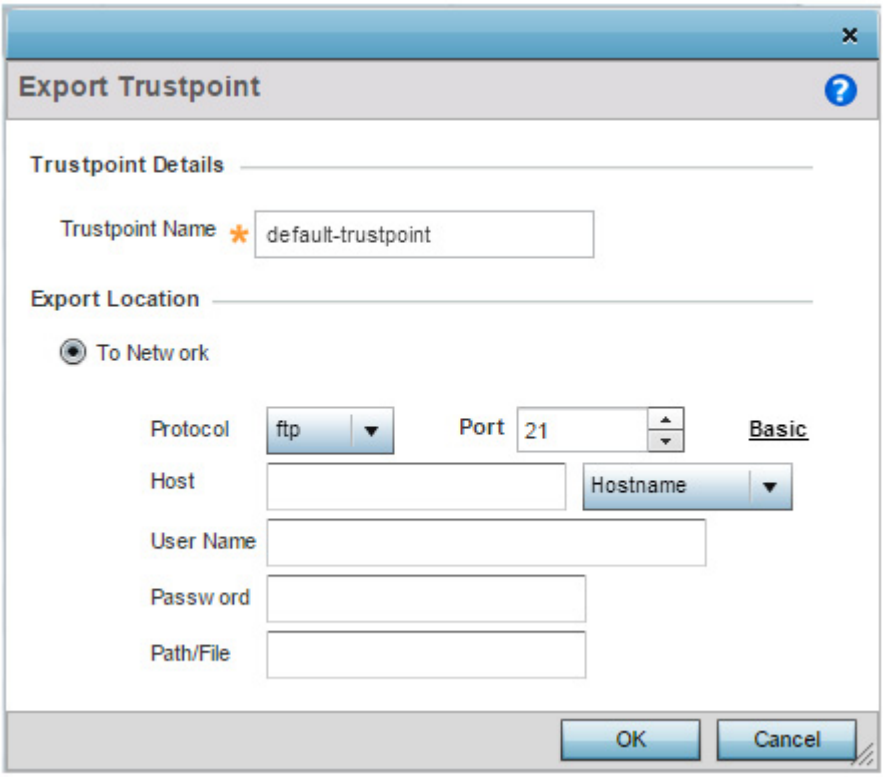


Figure 65: Certificate Management - Export Trustpoint screen

9 Define the following configuration parameters required for the **Export** of the trustpoint:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
URL	Provide the complete URL to the location of the trustpoint. If needed, select Advanced to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol.
Protocol	Select the protocol used for exporting the target trustpoint. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	If using *Advanced* settings, use the spinner control to set the port. This option is not valid for *cf* and *usb1 - 4.*
IP Address	If using *Advanced* settings, enter IP address of the server used to export the trustpoint. This option is not valid for *cf* and *usb1 - 4.*
Hostname	Provide the hostname or numeric IP4 or IPv6 formatted IP address of the server used to export the trustpoint. 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. Providing a host is not required for cf and usb1-4. If using *Advanced* settings, provide the hostname of the server used to export the trustpoint. This option is not valid for *cf* and *usb1 - 4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If using *Advanced* settings, specify the path to the trustpoint. Enter the complete relative path to the file on the server.

10 Select **OK** to export the trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

11 To optionally delete a trustpoint, select the **Delete** button from the Trustpoints screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select the **Delete RSA Key** option to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the last saved configuration.

RSA Key Management

"Certificates"

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 or export an existing key to and from a remote location.

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. it is an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Select **Operations**.

2 Select **Certificates.**

3 Select **RSA Keys**.

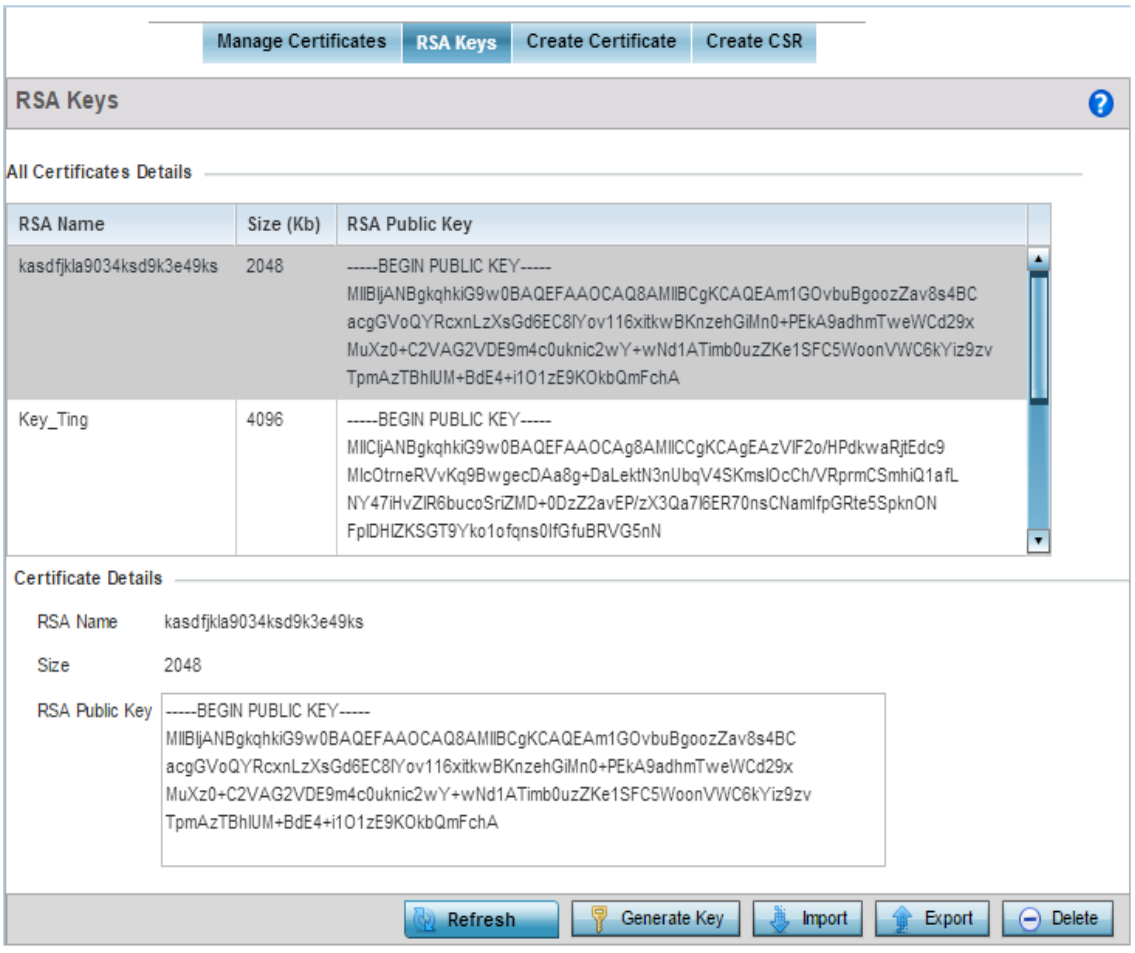


Figure 66: Certificate Management - RSA Keys screen

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

4 Select **Generate Key** to create a new key with a defined size.

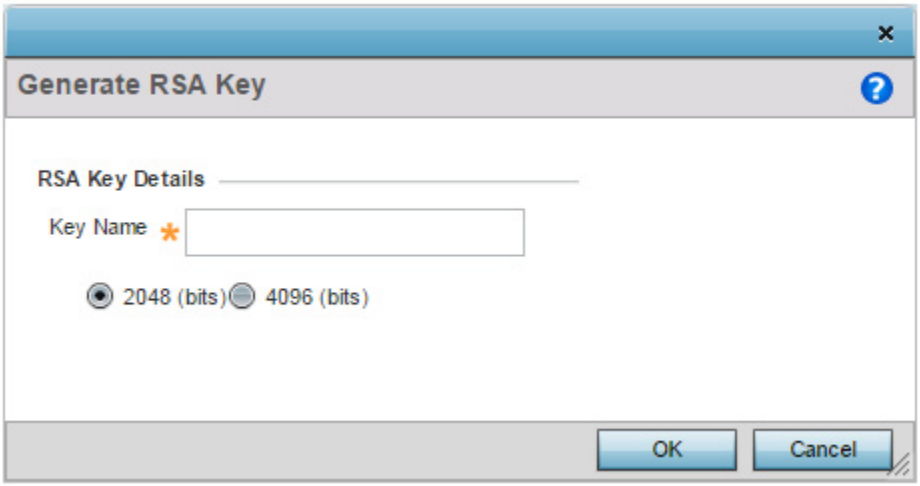


Figure 67: Certificate Management - Generate RSA Key screen

5 Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

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 (between 1,024 - 2,048 bits). It is recommended leaving this value at the default setting of 1024 to ensure optimum functionality.

6 To optionally import a RSA Key, select the **Import** button from the RSA Keys screen.

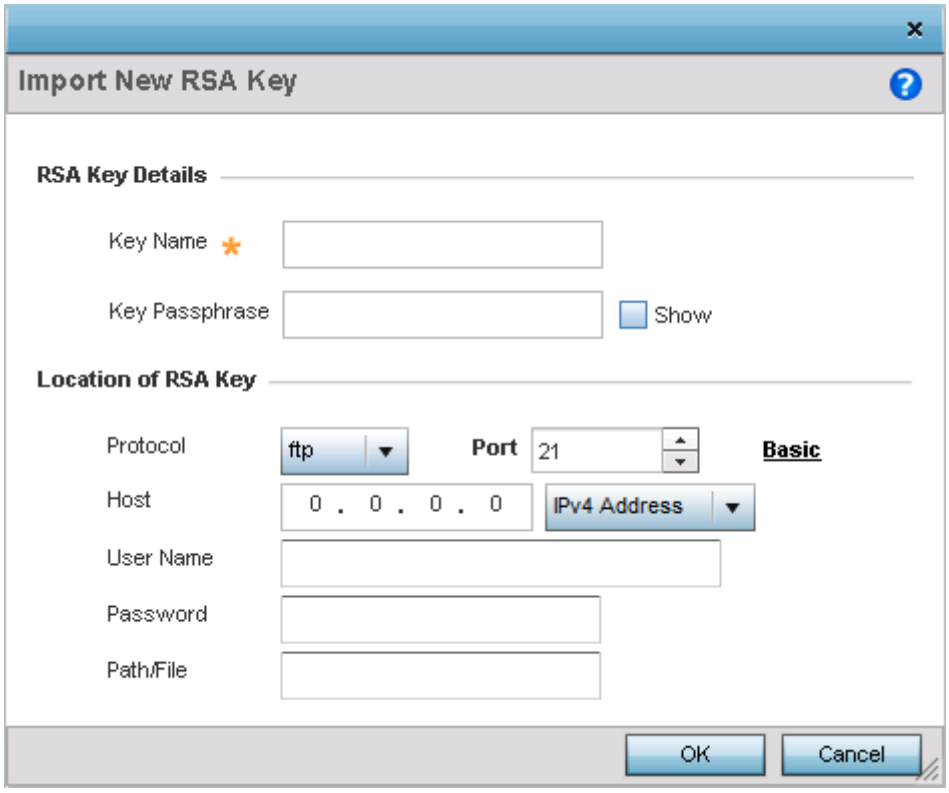


Figure 68: Certificate Management - Import New RSA Key screen

7 Define the following configuration 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 the server (or repository) of the target RSA key. Select the *Show* textbox to expose the actual characters used in the passphrase. Leaving the option unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the RSA key. If needed, select *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 importing the target key. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1 - 4.*
IP Address	Enter IP address of the server used to import the RSA key. This option is not valid for *cf* and *usb1 - 4.*
Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to import the RSA key. 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. Providing a host is not required for cf and usb1-4.
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

8 Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

9 To optionally export a RSA key to a remote location, select the **Export** button from the RSA Keys screen.

10 Export the key to a redundant RADIUS server so it can be imported without generating a second key. If there are more than one RADIUS authentication servers, export the certificate and do not generate a second key unless you want to deploy two root certificates.

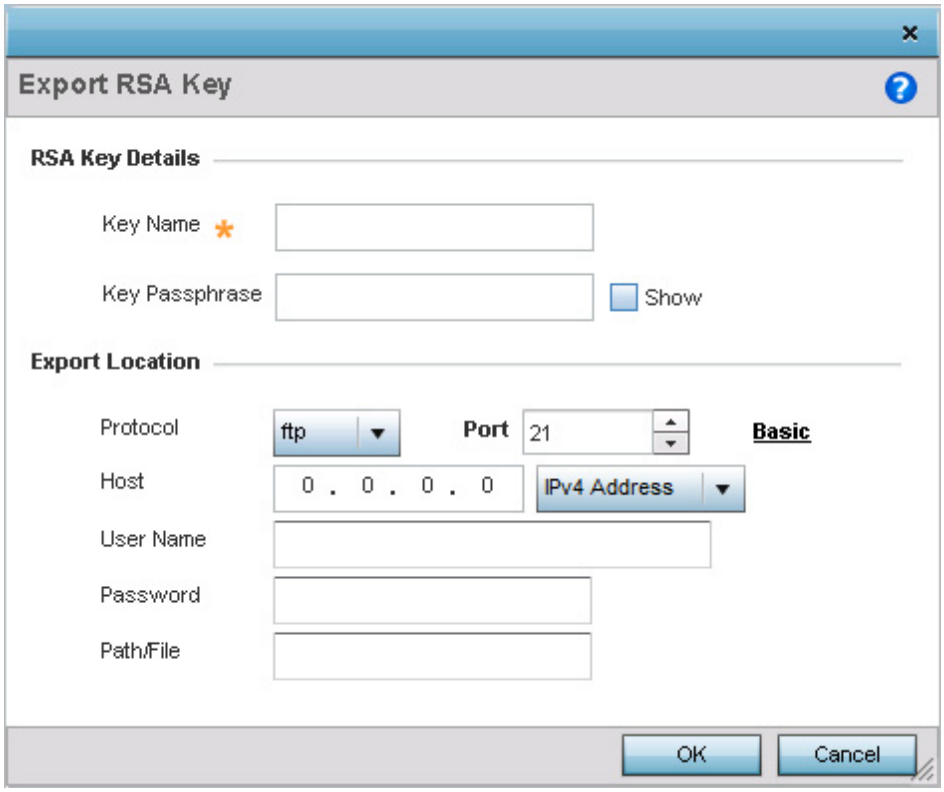


Figure 69: Certificate Management - Export RSA Key screen

11 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 passphrase used by the server. Select the *Show* textbox to expose the actual characters used in the passphrase. Leaving the option unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the key. If needed, select *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 also dependent on the selected protocol.
Protocol	Select the protocol used for exporting the RSA key. Available options include: • tftp • ftp • sftp • http • cf • usb1 • usb2 • usb3 • usb4

Port	If using *Advanced* settings, use the spinner control to set the port. This option is not valid for *cf* and *usb1 - 4.*
IP Address	If using *Advanced* settings, enter IP address of the server used to export the RSA key. This option is not valid for *cf* and *usb1 - 4.*
Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to export the RSA key. 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. Providing a host is not required for cf and usb1-4. If using *Advanced* settings, provide the hostname of the server used to export the RSA key. This option is not valid for *cf* and *usb1 - 4.*
Username/Password	These fields are enabled if using *ftp* or *sftp* protocols. Specify the username and the password for that username to access the remote servers using these protocols.
Path/File	If using *Advanced* settings, specify the path to the key. Enter the complete relative path to the key on the server.

12 Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to the last saved configuration.

13 To optionally delete a key, select the **Delete** button from within the RSA Keys screen. Provide the key name within the Delete RSA Key screen and select the **Delete Certificates** option to remove the certificate the key supported. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the last saved configuration.

Certificate Creation

"Certificates"

The Certificate Management screen provides the facility for creating new self-signed certificates. Self signed certificates (often referred to as root certificates) do not use public or private CAs. A self signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate that can be applied to a device:

1 Select **Operations.**

2 Select **Certificates**.

3 Select **Create Certificate**.

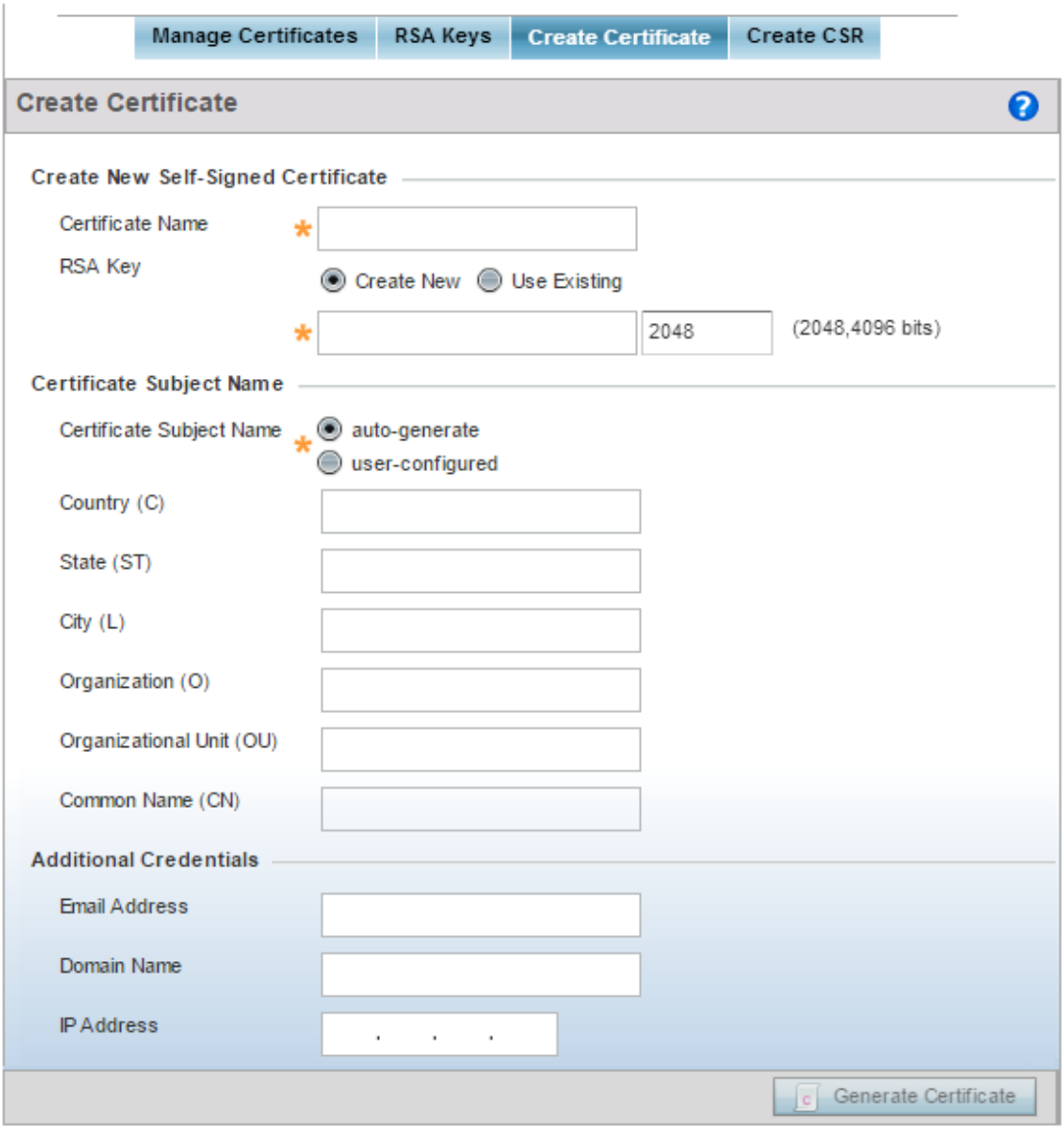


Figure 70: Certificate Management - Create Certificate screen

4 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: Create New	To create a new RSA key, select the radio button to define 32 character name used to identify the RSA key. Use the spinner control to set the size of the key (between 2,048 - 4,096 bits). Leave this value at the default setting of 2048 to ensure optimum functionality. For more information on creating a new RSA key, see "RSA Key Management" on page 910.
RSA Key: Use Existing	Select the radio button and use the drop-down menu to select the existing key used by both the access point and the server (or repository) of the target RSA key.

5 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or select *user-configured* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the *Country* used in the certificate. This is a required field and must not exceed a 2 character country code.
State (ST)	Enter a State/Prov. for the state or province name used in the certificate. This is a required field.
City (L)	Enter a City to represent the city name used in the certificate. This is a required field.
Organization (O)	Define an Organization for the organization used in the certificate. This is a required field.
Organizational Unit (OU)	Enter an Organizational Unit for the name of the organization unit used in the certificate. This is a required field.
Common Name (CN)	If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here.

6 Select the following **Additional Credentials** required for the generation of the self signed certificate:

Email Address	Provide an E-mail address used as the contact address for issues relating to this certificate request.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. A 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.

7 Select the **Generate Certificate** button at the bottom of the Create Certificate screen to produce the certificate.

Generating a Certificate Signing Request (CSR)

"Certificates"

A *certificate signing request* (CSR) is a message from a requestor to a certificate authority to apply for a digital identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional. The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 Select **Operations.**

2 Select **Certificates**.

3 Select **Create CSR.**

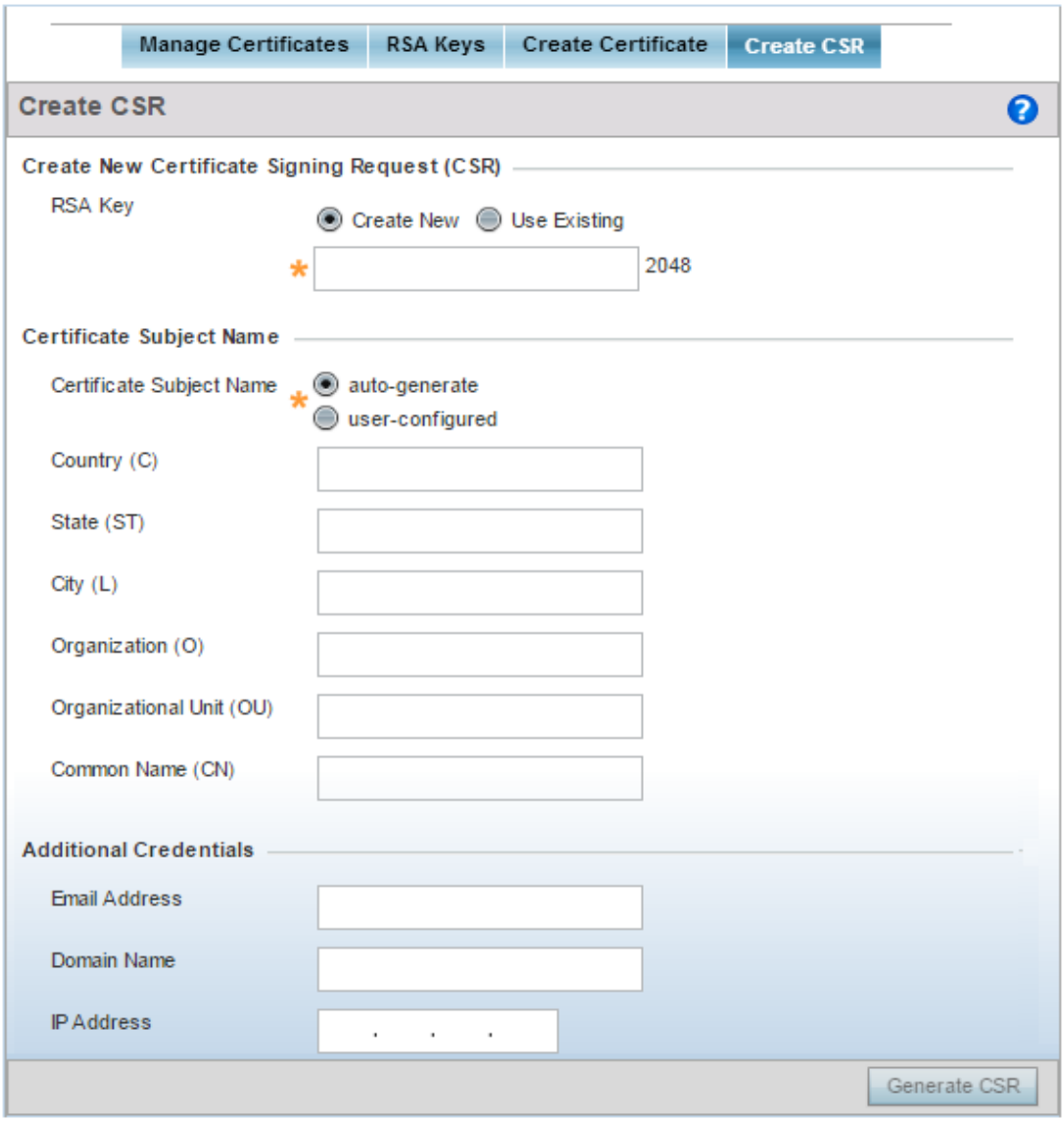


Figure 71: Certificate Management - Create CSR screen

4 Define the following configuration parameters required to **Create New Certificate Signing Request (CSR)**:

RSA Key: Use Existing	Select the radio button and use the drop-down menu to select the existing key used by both the access point and the server (or repository) of the target RSA key.
RSA Key: Create New	To create a new RSA key, select Create Key to define a 32 character maximum name used to identify the RSA key. The key size is always set to 2,048 bit key length. To use an existing key, select Use Existing and select a key from the drop-down menu. For more information, see "RSA Key Management" on page 910.

5 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or select *user-configured* to manually enter the credentials of the self signed certificate. The default setting is 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 a State/Prov. for the state or province name used in the CSR. This is a required field.
City (L)	Enter a City to represent the city name used in the CSR. This is a required field.
Organization (O)	Define an Organization for the organization used in the CSR. This is a required field.
Organizational Unit (OU)	Enter an Organizational Unit for the name of the organization unit used in the CSR. This is a required field.
Common Name (CN)	If there is a common name (IP address) for the organizational unit issuing the certificate, enter it here.

6 Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an E-mail address used as the contact address for issues relating to this CSR.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: 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.

7 Select the **Generate CSR** button at the bottom of the screen to produce the CSR.

Smart RF

"Operations"

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 RF network to determine the best channel and transmit power for each access point radio.

Smart RF also provides self recovery functions by monitoring the 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, that otherwise require manual reconfiguration to resolve.

Within the Operations node, Smart RF is managed 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 a RF Domain

"Smart RF"

When calibration is initiated, Smart RF instructs adopted radios 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 as well as signals from external, un-managed radios. Access point to access point distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

To conduct Smart RF calibration:

1 Select **Operations.**

2 Select **Smart RF**.

The Smart RF screen populates with information specific to the devices within the RF Domain with updated data from the last interactive calibration.

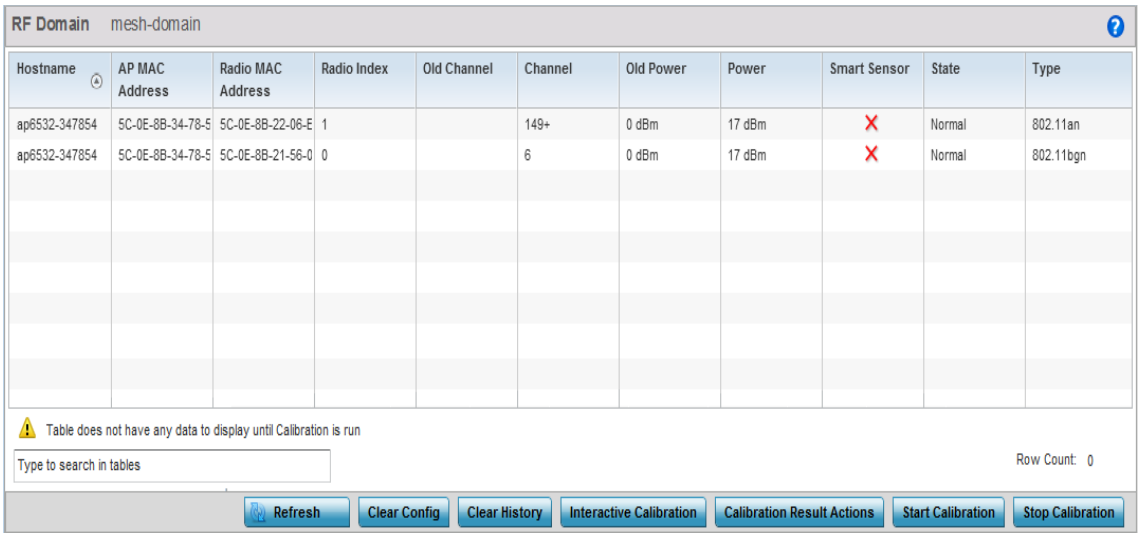


Figure 72: Smart RF screen

3 Refer to the following to determine whether Smart RF calibrations or interactive calibration is required:

Hostname	Displays the user friendly hostname assigned to each access point within the RF Domain. This value cannot be modified as a part of calibration activity.
AP MAC Address	Displays the hardware encoded MAC address assigned to each access point within the 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 RF Domain. This value cannot be modified as past 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 the 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 within the RF Domain. This value may have been changed as part an Interactive Calibration process applied to the 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 the RF Domain.
Old Power	Lists the transmit power assigned to each listed access point within the RF Domain. The power level may have been increased or decreased as part an Interactive Calibration process applied to the 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 after an Interactive Calibration resulted in an 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 RF Domain.

4 Select the **Refresh** button to (as required) to update the contents of the Smart RF screen and the attributes of the devices within the RF Domain.



CAUTION

Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections.

Select the **Interactive Calibration** button to initiate a Smart RF calibration using the access points within the 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 Smart RF module. Expand the screen to display the Event Monitor to track the progress of the Interactive Calibration.

5 Select **Calibration Result Actions** to define the actions taken based on the results of an 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.

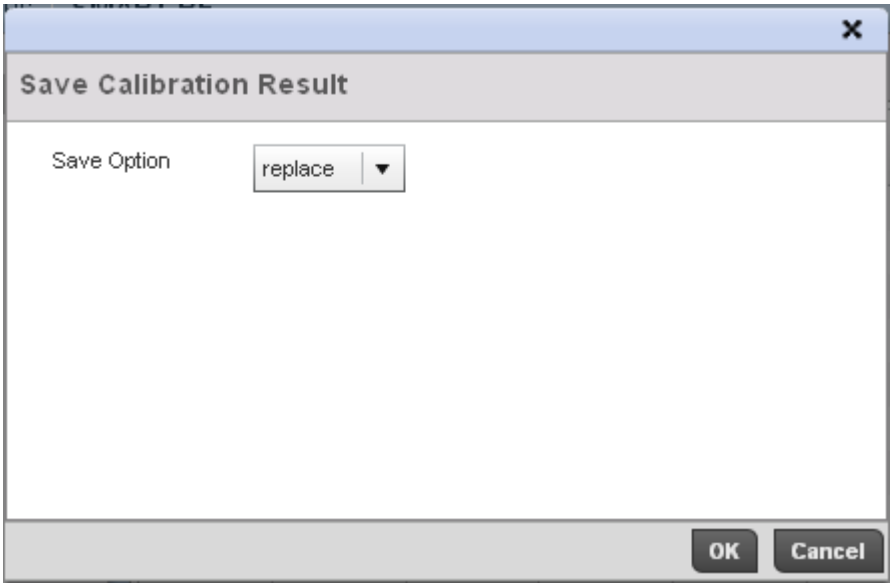


Figure 73: Save Calibration Result screen

- *Replace* - Only overwrites the current channel and power values with the 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.
- *Commit* - Commits the Smart RF module Interactive Calibration results to their respective access point radios.

6 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.

The calibration process can be stopped by selecting the **Stop Calibration** button.

Operations Deployment Considerations

Before defining the access point's configuration using the Operations menu, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- If an access point's (or its associated device's) firmware is older than the version on the support site, update to the latest firmware version for full functionality and utilization.
- An access point must be rebooted to implement a firmware upgrade. Take advantage of the reboot scheduling mechanisms available to the access point to ensure its continuously available during anticipated periods of heavy wireless traffic utilization.
- Within a well planned RF Domain, any associated radio should be reachable by at least one other radio. Keep this in mind when utilizing the Smart RF feature to record signals from neighboring access points. Access point to access point distance is recorded in terms of signal attenuation.

13 Statistics

This chapter describes statistics displayed by the *graphical user interface* (GUI). Statistics are available for access point and their managed devices.

A Smart RF statistical history is available to assess adjustments made to device configurations to compensate for detected coverage holes or device failures.

Statistics display detailed information about peers, health, device inventories, wireless clients associations, adopted AP information, rogue APs and WLANs. Access point statistics can be exclusively displayed to validate connected access points, their VLAN assignments and their current authentication and encryption schemes.

Wireless client statistics are available for an overview of client health. Wireless client statistics includes RF quality, traffic utilization and user details. Use this information to assess if configuration changes are required to improve network performance.

For more information, see:

- "System Statistics"
- "RF Domain Statistics"
- "Access Point Statistics"
- "Wireless Client Statistics"

System Statistics

- "Statistics"

The **System** screen displays information supporting managed devices. Use this information to asses the overall state of the devices comprising the system. Systems data is organized as follows:

- "Health"
- "Inventory"
- "Adopted Devices"
- "Pending Adoptions"
- "Offline Devices"
- "Device Upgrade"
- "WIPS Summary"

Health

- "System Statistics"

The *Health* screen displays the overall performance of the managed network (system). This includes device availability, overall RF quality, resource utilization and network threat perception.

To display the health of the network:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Health** from the left-hand side of the UI.

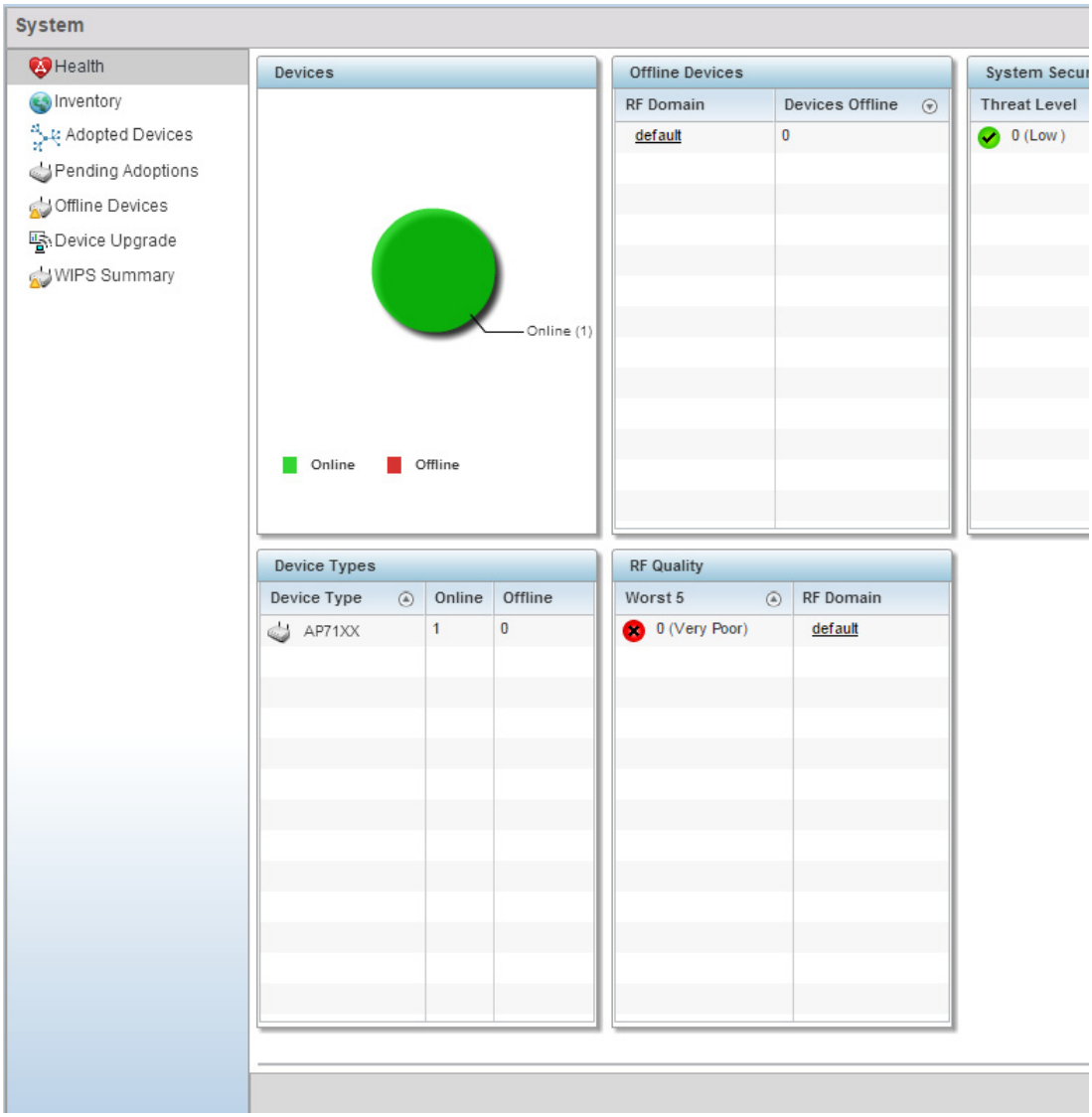


Figure 1: System - Health screen

4 The **Devices** field displays the total number of devices in the 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 network.

5 The **Offline Devices** table displays a list of detected devices in the network that are currently offline but available as potential managed resources.

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.

The **Device Types** table displays the kinds of devices detected within the system. Each device type displays the number currently online and offline.

6 Use the **RF Quality** table to isolate poorly performing radio devices within specific RF Domains. This information is a starting point to improving the overall quality of the network.The **RF Quality** area displays the RF Domain performance. Quality indices are:

- 0 – 50 (Poor)
- 50 – 75 (Medium)
- 75 – 100 (Good).

The RF Quality field displays the following:

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.

7 The **System Security** table defines a Threat Level as an integer value indicating a potential threat to the system. It is an average of the threat indices of all the RF Domains managed by the wireless controller.

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.

8 Select **Refresh** at any time to update the statistics counters to their latest values.

Inventory

"System Statistics"

The *Inventory* screen displays information about the physical hardware managed within the system by its members. Use this information to assess the overall performance of wireless devices.

To display the inventory statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Inventory** from the left-hand side of the UI.

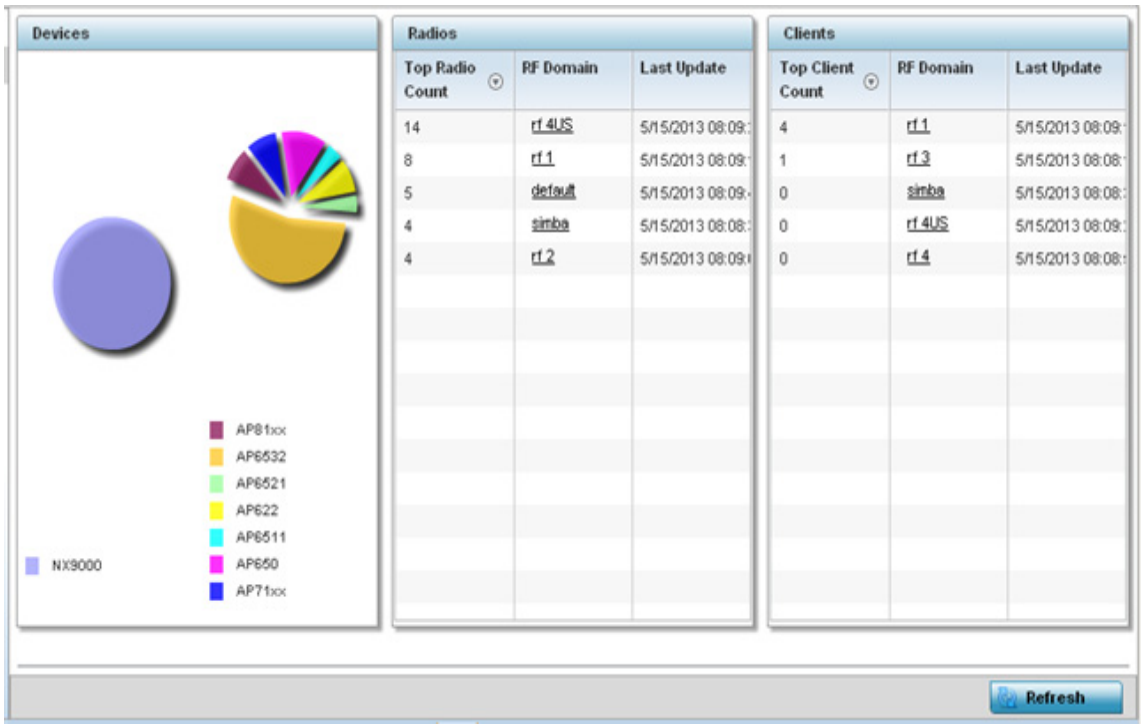


Figure 2: System - Inventory screen

4 The **Devices** field displays an exploded pie chart depicting controller, service platform and access point device type distribution by model. Use this information to assess whether these are the correct models for the original deployment objective.

5 The **Radios** table displays radios deployed within the network. This area displays the total number of managed radios and top 5 RF Domains in terms of radio count. The **Total Radios** value is the total number of radios in this system.

Top Radio Count	Displays the radios index of each listed top radio.
RF Domain	Displays the name of the RF Domain the listed radios belong. The RF Domain displays as a link that can be selected to display configuration and network address information in greater detail.
Last Update	Displays the UTC timestamp when each listed client was last seen on the network.

6 The **Clients** table displays the total number of wireless clients managed by the access point. This **Top Client Count** table lists the top 5 RF Domains, in terms of the number of wireless clients adopted:

Top Client Count	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 timestamp when the client count was last reported.

7 Select **Refresh** to update the statistics counters to their latest values.

Adopted Devices

"System Statistics"

The *Adopted Devices* screen displays a list of devices adopted to the network (entire system). Use this screen to view a list of devices and their current status.

To view adopted AP 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.

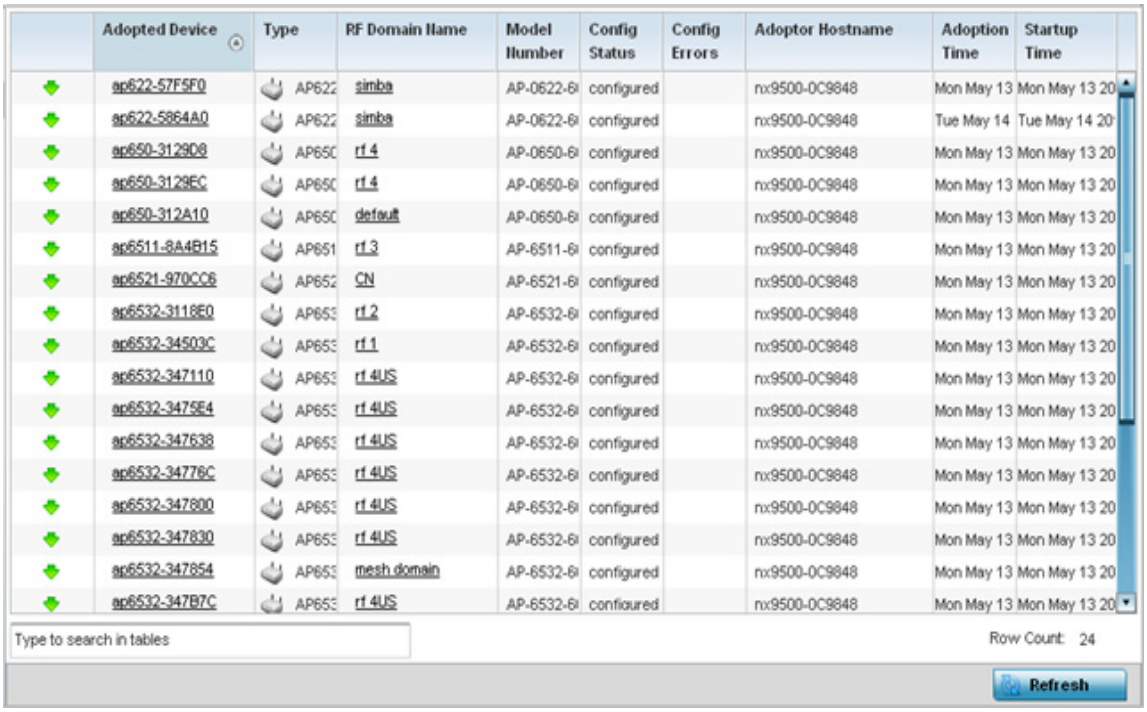


Figure 3: System - Adopted Devices screen

The **Adopted Devices** screen provides the following:

Adopted Device	Displays administrator assigned hostname of the adopted device. Select the adopted device 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 to. Select the RF Domain to display configuration and network address information in greater detail.
Model Number	Lists the model number of each AP that's 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 or service platform.
Adoption Time	Displays a timestamp for each listed device that reflects when the device was adopted by the controller or service platform.
Startup Time	Provides a date stamp when the adopted device was restarted post adoption.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Pending Adoptions

"System Statistics"

The *Pending Adoptions* screen displays those devices detected within the network coverage area, but have yet to be adopted. Review these devices to assess whether they could provide radio coverage to wireless clients needing support.

To view pending AP adoptions to the controller or service platform:

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.

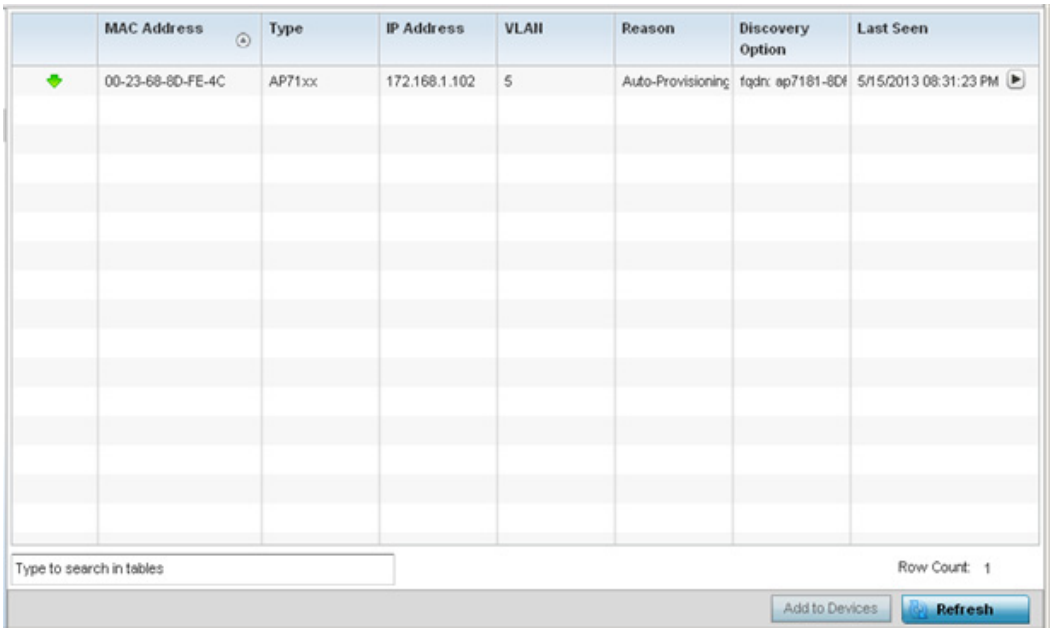


Figure 4: System - Pending Adoptions screen

The **Pending Adoptions** screen displays the following:

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 AP type.
IP Address	Displays the current IP Address of the device pending adoption.
VLAN	Displays the VLAN the device pending adoption will use as a virtual interface with its adopting controller or service platform.
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.
Refresh	Click the *Refresh* button to update the list of pending adoptions.

Offline Devices

"System Statistics"

The *Offline Devices* screen displays a list of devices in the network or RF Domain that are currently offline. Review the contents of this screen to help determine whether an offline status is still warranted.

To view offline device 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.

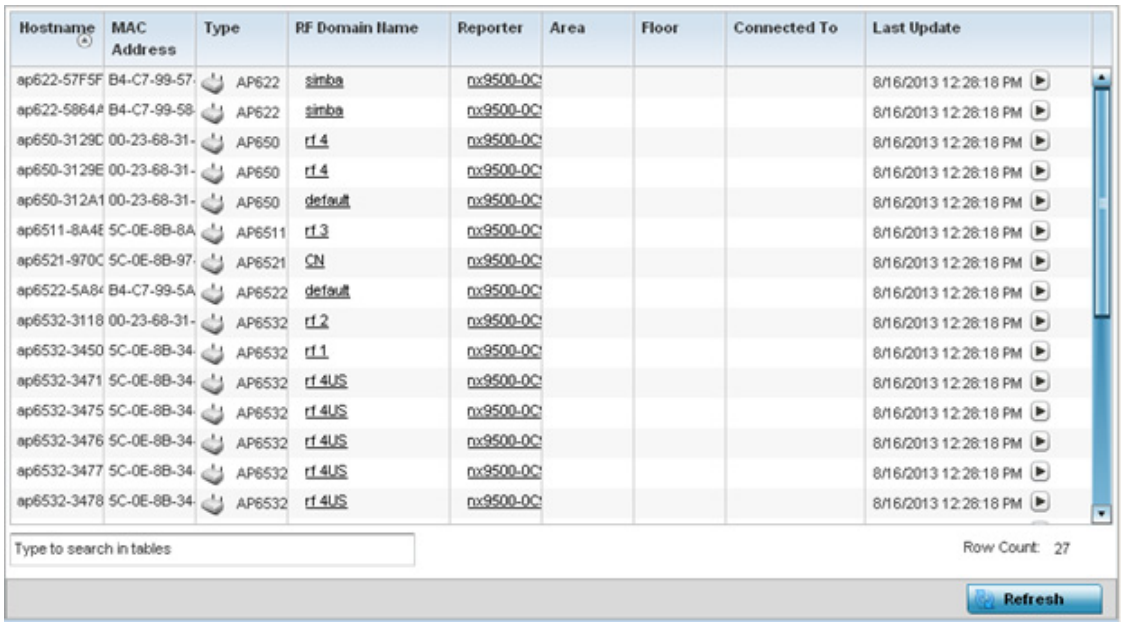


Figure 5: System - Offline Devices screen

The **Offline Devices** screen provides the following:

Hostname	Lists the administrator assigned hostname provided when the device was added to the network.
MAC Address	Displays the factory encoded MAC address of each listed offline device.
Type	Displays the offline access point's model type.
RF Domain Name	Displays the name of the offline device's RF Domain membership, if applicable. Select the RF Domain to display configuration and network address information in greater detail.
Reporter	Displays the hostname of the device reporting the listed device as offline. Select the reporting device name to display configuration and network address information in greater detail.
Area	Lists the administrator assigned deployment area where the offline device has been detected.
Floor	Lists the administrator assigned deployment floor where the offline device has been detected.
Connected To	Lists the offline's 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 network. Click the *arrow* next to the date and time to toggle between standard time and UTC.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Device Upgrade

"System Statistics"

The *Device Upgrade* screen displays available licenses for devices within a cluster. It displays the total number of AP licenses.

To view a licenses statistics within the network:

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.

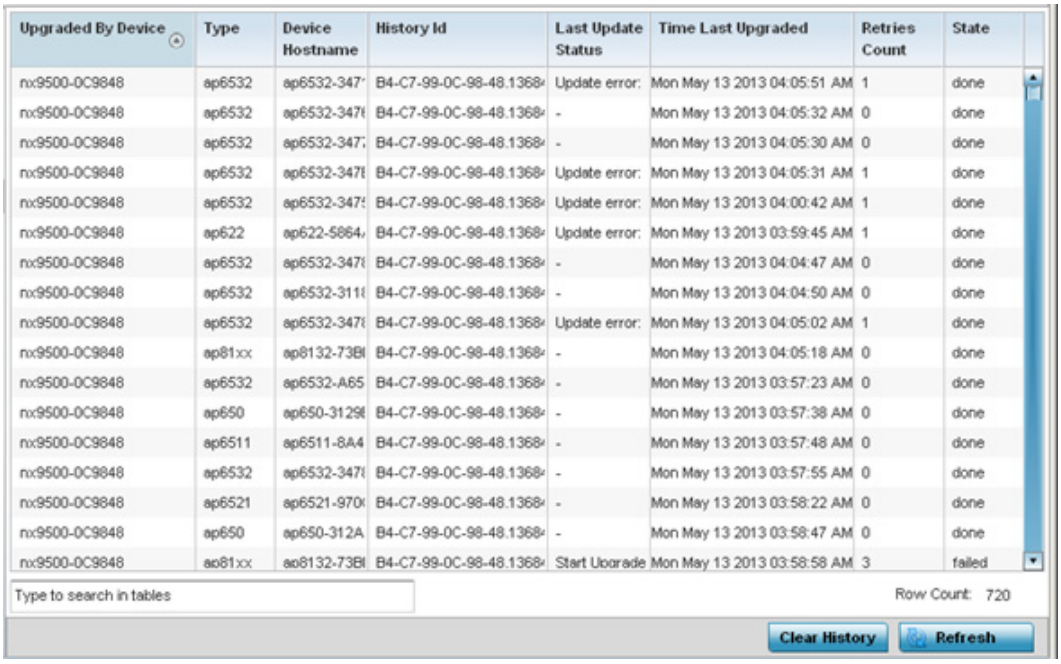


Figure 6: System - Device Upgrade screen

4 Select **Device Upgrade** from the left-hand side of the UI:

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 type of the adopting controller, service platform or access point. An updating access point must be of the same model as the access point receiving the update.
Device Hostname	List the administrator assigned hostname of the device receiving an 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	Lists the date and time of each upgrade operation.
Retries Count	Displays the number of retries required in an update operation.
State	Displays the done or failed state of an upgrade operation.
Clear History	Select *Clear History* to clear the screen of its current status and begin a new data collection.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

WIPS Summary

"System Statistics"

The *Wireless Intrusion Protection System* (WIPS) 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 lockdown 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 access points, as well as the occurrence of WIPS events within the controller or service platform's 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.

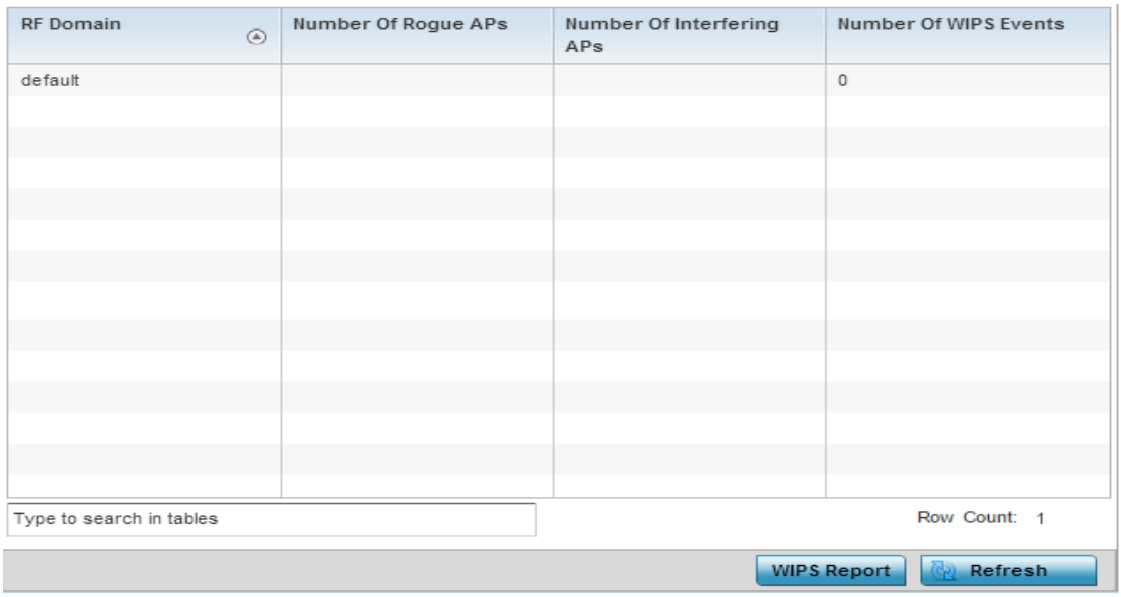


Figure 7: System - WIPS Summary screen

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 access point 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 access points versus the other RF Domains within the controller, service platform or access point 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 or service platform 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.

Use the available options to select the type of WIPS report to generate. Select **Generate Report** button to generate the report and save it locally on the device used to access the WiNG user interface.

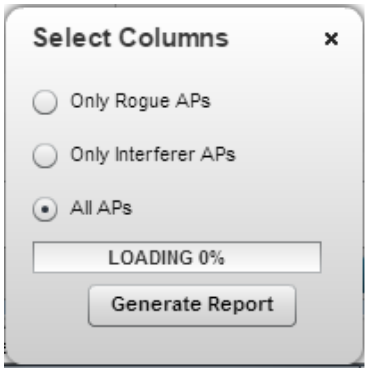


Figure 8: System - WIPS Summary screen

6 Select **Refresh** to update the screen's statistics counters to their latest values.

RF Domain Statistics

"Statistics"

The RF Domain screens display status for a selected RF domain. This includes the RF Domain *health* and *device inventory, wireless clients* and *Smart RF* functionality. 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.

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"
- "Wireless Clients"
- "Device Upgrade"
- "Wireless LANs"
- "Radios"
- "Bluetooth"
- "Mesh"
- "Mesh Point"
- "SMART RF"
- "WIPS"
- "Captive Portal"
- "Coverage Hole Detection"

Health

"RF Domain Statistics"

The *Health* screen displays general status information for a selected RF Domain, including data polled from all its members.

To display the health of an access point's RF Domain:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Health** from the **RF Domain** menu.

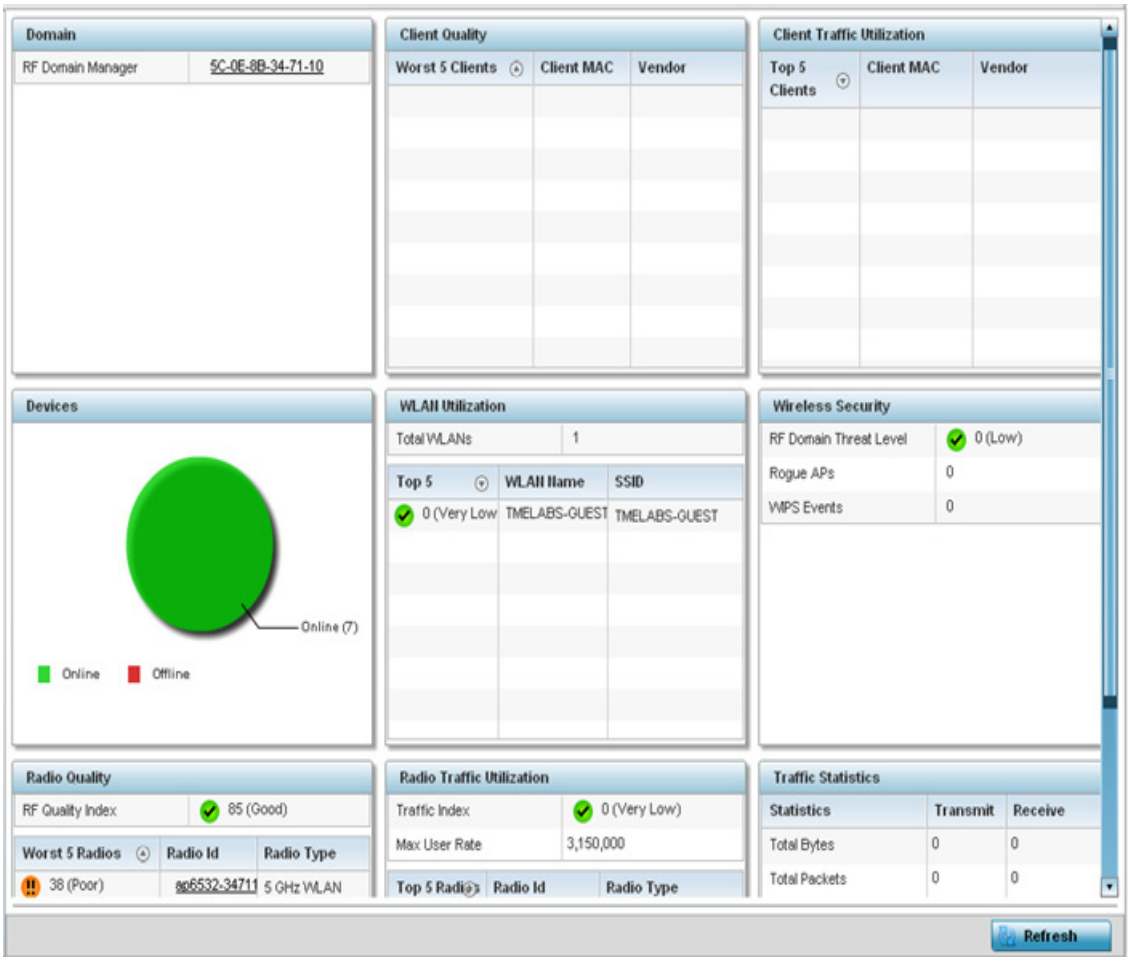


Figure 9: RF Domain - Health screen

4 The **Domain** field 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.

5 The **Devices** field displays the total number of online versus offline devices in the RF Domain, and an exploded pie chart depicts their status.

6 The **Radio Quality** field 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 in the RF Domain.

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.

7 Refer to the **Client Quality** table 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.

8 Refer to the **WLAN Utilization** field to assess the following:

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.

9 The **Radio Traffic Utilization** area displays the following:

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.

10 Refer to the **Client Traffic Utilization** table:

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.

11 The **Wireless Security** area 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 the wireless clients trying to find network vulnerabilities within the access point RF Domain. The threat level is represented by an integer.
Rogue APs	Lists the number of unauthorized access points detected by RF domain member devices.
WIPS Events	Lists the number of WIPS events generated by RF Domain member devices.

The **Traffic Statistics** statistics table displays the following information for transmitted and received packets:

Total Bytes	Displays the total bytes of data transmitted and received within the access point RF Domain.
Total Packets	Lists the total number of data packets transmitted and received within the access point RF Domain.
User Data Rate	Lists the average user data rate within the access point RF Domain.
Bcast/Mcast Packets	Displays the total number of broadcast/multicast packets transmitted and received within the access point RF Domain.
Management Packets	This is the total number of management packets processed within the access point RF Domain.
Tx Dropped Packets	Lists total number of dropped data packets within the access point RF Domain.
Rx Errors	Displays the number of errors encountered during data transmission within the access point RF Domain. The higher the error rate, the less reliable the connection or data transfer.

Inventory

"RF Domain Statistics"

The *Inventory* screen displays an inventory of RF Domain member access points, connected wireless clients, wireless LAN utilization and radio availability.

To display RF Domain inventory statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Inventory** from the **RF Domain** menu.

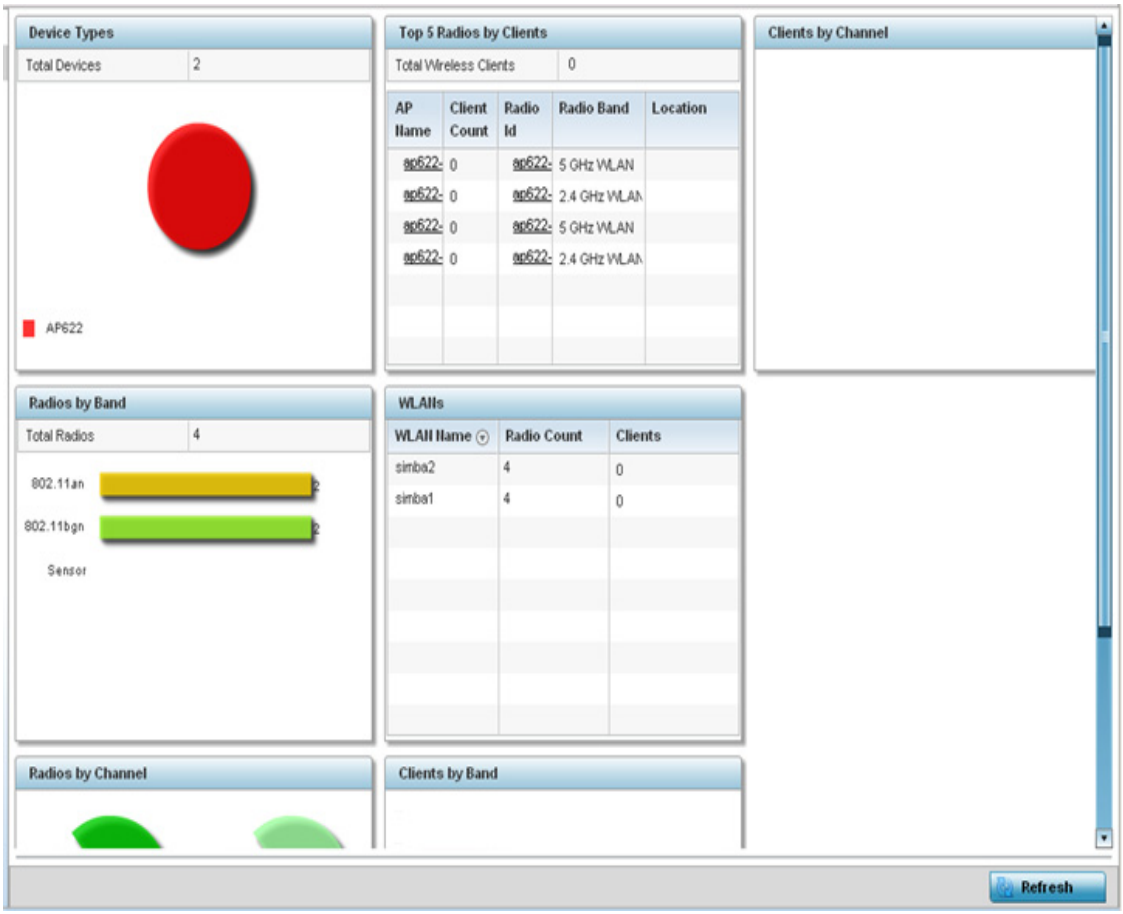


Figure 10: RF Domain - Inventory screen

The **Device Types** table displays the total members in the RF Domain. The exploded pie chart depicts the distribution of RF Domain members by controller and access point model type.

The **Radios by Band** field 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.

The **Radios by Channel** field 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.

The **Top 5 Radios by Clients** table 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 access point. The name displays as a link that can be selected to display access point data in greater detail.
Client Count	List the number of connected clients to each listed RF Domain member access point.
Radio	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 etc.).
Radio Band	Lists each client's operational radio band.
Location	Displays system assigned deployment location for the client.

4 Refer to the **WLANs** 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.

5 The **Clients by Band** bar graph displays the total number of RF Domain member clients by their IEEE 802.11 radio type.

6 The **Clients by Channel** pie charts displays the channels used by RF Domain member clients using 5GHz and 2.4GHz radios.

7 Periodically select **Refresh** to update the contents of the screen to their latest values.

Devices

"RF Domain Statistics"

The **Devices** screen displays RF Domain member hardware data, connected client counts, radio data and network IP address.

To display RF Domain member device statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Devices** from the **RF Domain** menu.

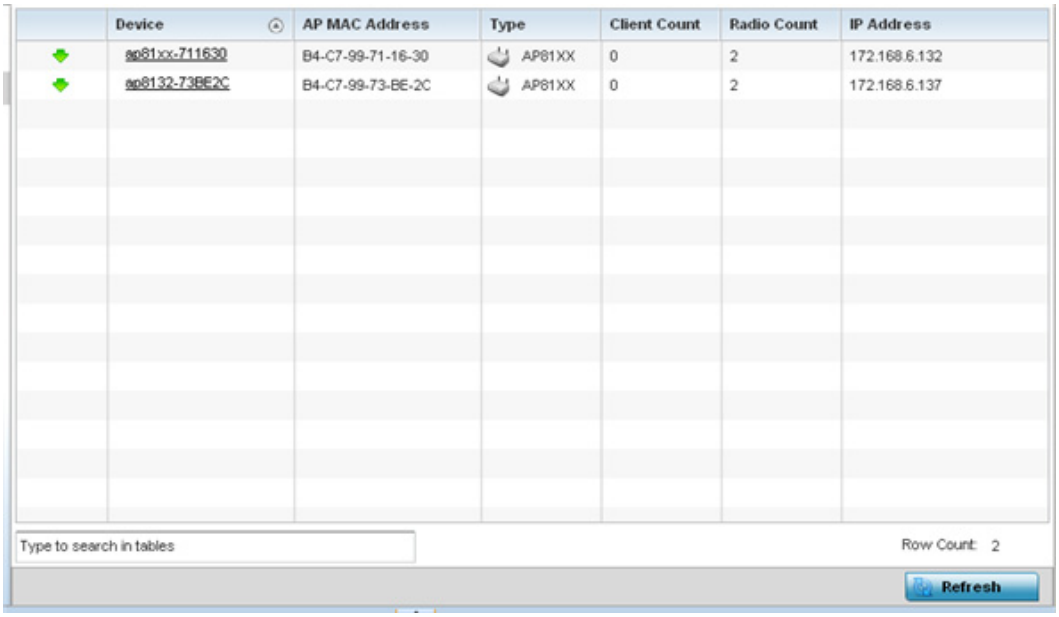


Figure 11: RF Domain - Devices screen

Device	Displays the system assigned name of each device that's a member of the RF Domain. The name displays as a link that can be selected to display configuration and network address information in greater detail.
AP MAC Address	Displays each device's factory encoded MAC address as its hardware identifier.
Type	Displays each device model within the selected RF Domain.
Client Count	Displays the number of clients connected with each listed device. AP6532, AP6522, AP6562, AP71xx, AP8132 and AP8232 models can support up to 256 clients per access point. AP6521 model can support up to 128 clients per access point.
Radio Count	Displays the number of radios on each listed device. AP6532, AP6522, AP6562, AP71xx, AP8132 and AP8232 models have two radios. AP6521 model has one radio.
IP Address	Displays the IP address each listed device is using a network identifier.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

AP Detection

"RF Domain Statistics"

The *AP Detection* screen displays information about detected access points that are not members of a RF Domain. They could be authorized devices or potential rogue devices.

To view device information on detected access points:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **AP Detection** from the **RF Domain** menu.

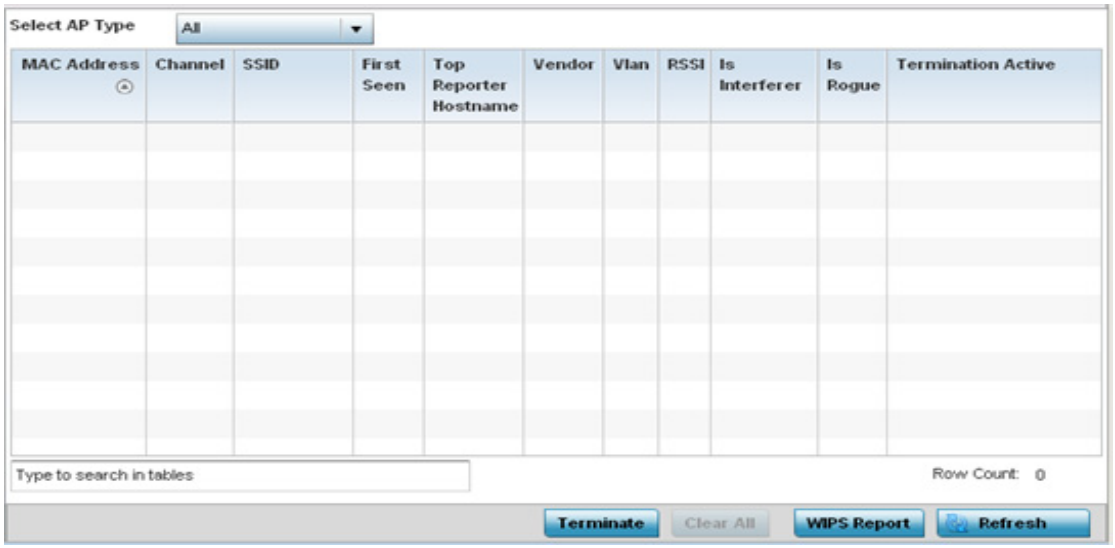


Figure 12: RF Domain - AP Detection screen

The **AP Detection** screen displays the following:

Select AP Type	Displays detected access point 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 access point detected by a RF Domain member device. The MAC address is set at the factory and cannot be modified via the management software.
Channel	Displays the channel of operation used by the detected access point. The channel must be utilized by both the access point and its connected client and be approved for the target deployment country.
SSID	Displays the *Service Set ID* (SSID) of the network to which the detected access point belongs.
First Seen	Provides a timestamp when the detected access point was first detected by a RF Domain member device.
Top Reporter Hostname	Lists the administrator assigned hostname of the top performing RF Domain member detecting the listed access point MAC address. Consider this top performer the best resource for information on the detected access point and its potential threat.
Vendor	Lists the manufacturer of the detected access point as an additional means of assessing its potential threat to the members of this RF Domain.
Vlan	Lists the numeric VLAN ID (virtual interface) the detected access point was detected on by members of this RF Domain
RSSI	Displays the *Received Signal Strength Indicator* (RSSI) of the detected access point. 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 access point 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 access point. 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. Air Termination is disabled by default.
Terminate	Terminates access points based on the option selected from the *Select AP Type* drop-down menu. For example, if the *Select AP Type* is 'All', the system terminates all access points. And if the *Select AP Type* is 'Rogue', the system terminates all rogue access points.
Clear All	Select *Clear All* to reset the statistics counters to zero and begin a new data collection.
WIPS Report	Select *WIPS Report* launch a subscreen to save a WIPS report (in PDF format) to a specified location. This is a recommended practice to capture RF Domain member access point client connection terminations in a format that can be archived externally.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Wireless Clients

"RF Domain Statistics"

The *Wireless Clients* screen displays device information for wireless clients connected to RF Domain member access points. Review this content to determine whether a client should be removed from access point 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 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Wireless Clients** from the **RF Domain** menu.

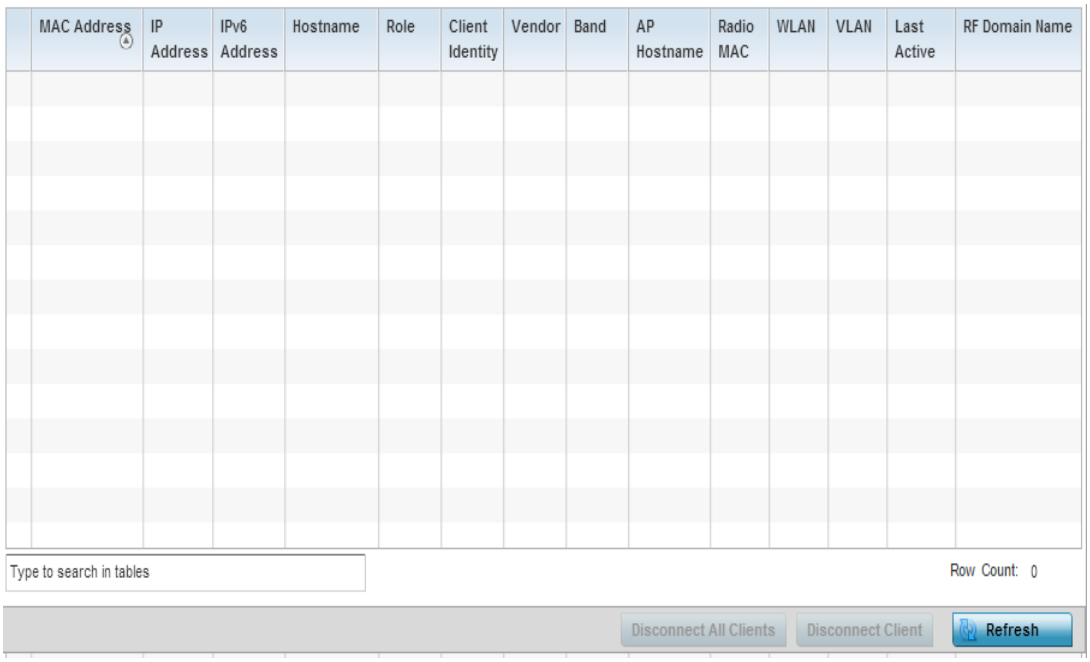


Figure 13: RF Domain - Wireless Clients screen

The **Wireless Clients** screen displays the following:

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 can be selected to display 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's configuration was originally set.
Role	Lists the role assigned to each controller, service platform or access point managed client.
Client Identity	Lists the client's operating system vendor identity (Android, Windows etc.)
Vendor	Displays the vendor (or manufacturer) of the wireless client.
Band	Lists the 2.4 or 5 GHz radio band the listed client is currently utilizing with its connected access point within the RF Domain.
AP Hostname	Displays the administrator assigned hostname of the access point to which the client is connected.
Radio MAC	Lists the hardware encoded MAC address of the access point 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 interoperation within the RF Domain.
VLAN	Displays the VLAN ID the client's connected access point has defined for use as a virtual interface.

Last Active	Displays the time when this wireless client was last detected by a RF Domain member.
RF Domain Name	Lists each client's RF Domain membership as defined by its connected access point.
Disconnect All Clients	Select the *Disconnect All* Clients button to terminate each listed client's connection and RF Domain membership.
Disconnect Client	Select a specific client MAC address and select the Disconnect Client button to terminate this client's connection and RF Domain membership.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Device Upgrade

"RF Domain Statistics"

The *Device Upgrade* screen reports information about devices receiving updates the RF Domain member provisioning the device. Use this screen to assess version data and upgrade status.

To view wireless device upgrade data for RF Domain members:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Device Upgrade** from the **RF Domain** menu.

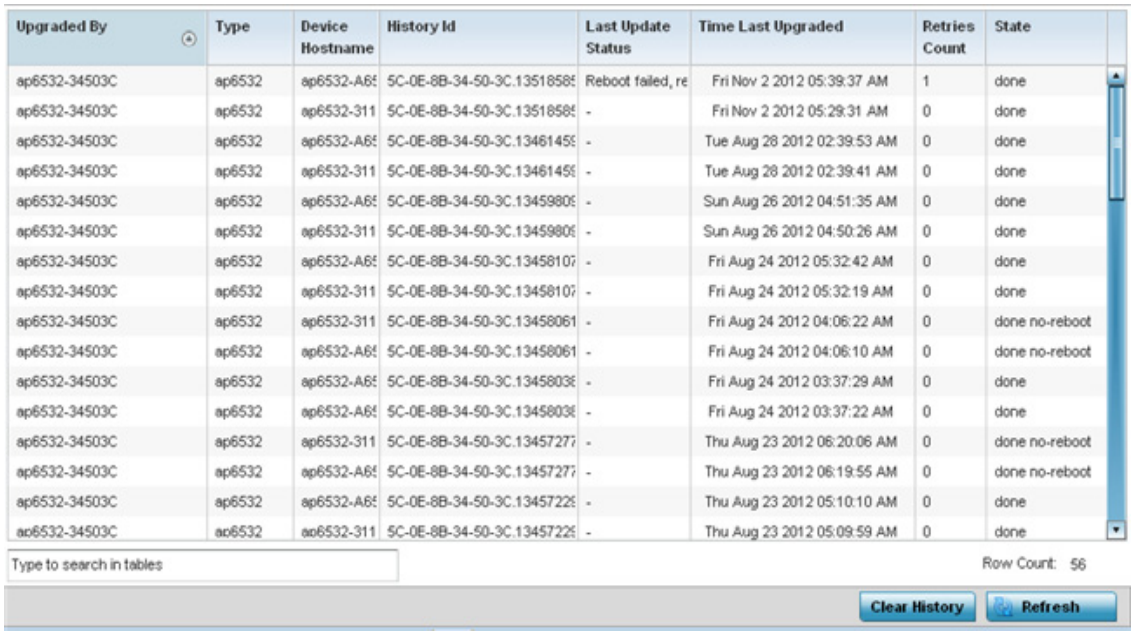


Figure 14: RF Domain - Device Upgrade screen

The **Device Upgrade** screen displays the following for RF Domain member devices:

Upgraded By	Lists the name of the device performing an update on behalf of a peer device.
Type	Displays the model of the device receiving an update. An updating access point must be of the same model as the access point receiving the update.
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 Upgrade	Displays a timestamp for the last successful upgrade.
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 and whether an update was made without a device reboot.
Clear History	Select *Clear History* to remove the upgrade records for RF Domain member devices. Unlike the Refresh function (that updates existing data), Clear History removes the update record from the screen.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Wireless LANs

"RF Domain Statistics"

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 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Wireless LANs** from the **RF Domain** menu.

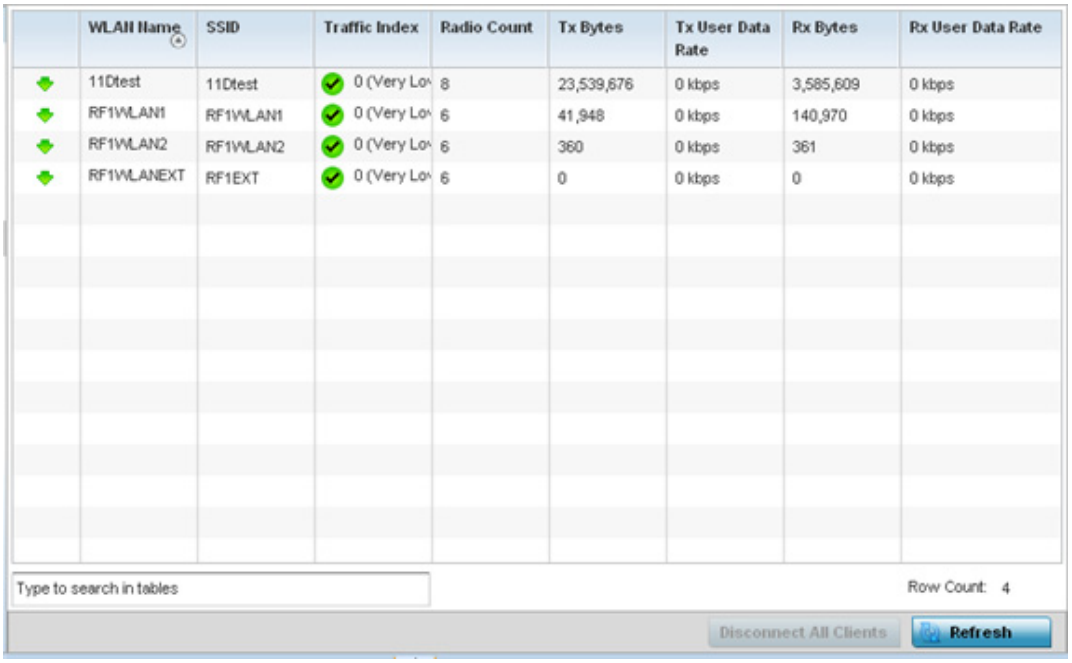


Figure 15: RF Domain - Wireless LANs screen

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name assigned to each WLAN upon its creation within the network.
SSID	Displays the *Service Set ID* (SSID) assigned to the WLAN upon its creation within the network.
Traffic Index	Displays the traffic utilization index of each listed WLAN, which measures how efficiently the traffic medium is used. It is 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), and 60 and above (high utilization).
Radio Count	Displays the number of radios deployed in each listed WLAN by RF Domain member devices.
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.
Disconnect All Clients	Select the *Disconnect All* Clients button to terminate each listed client's WLAN membership from this RF Domain.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Radios

- "RF Domain Statistics"

The **Radio** screens displays information on RF Domain member access point radios. Use these screens to troubleshooting radio issues negatively impacting RF Domain performance.

For more information, refer to the following:

- "Status"
- "RF Statistics"
- "Traffic Statistics"

Status

- "Radios"

To view the RF Domain radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Expand **Radios** from the **RF Domain** menu and select **Status.**

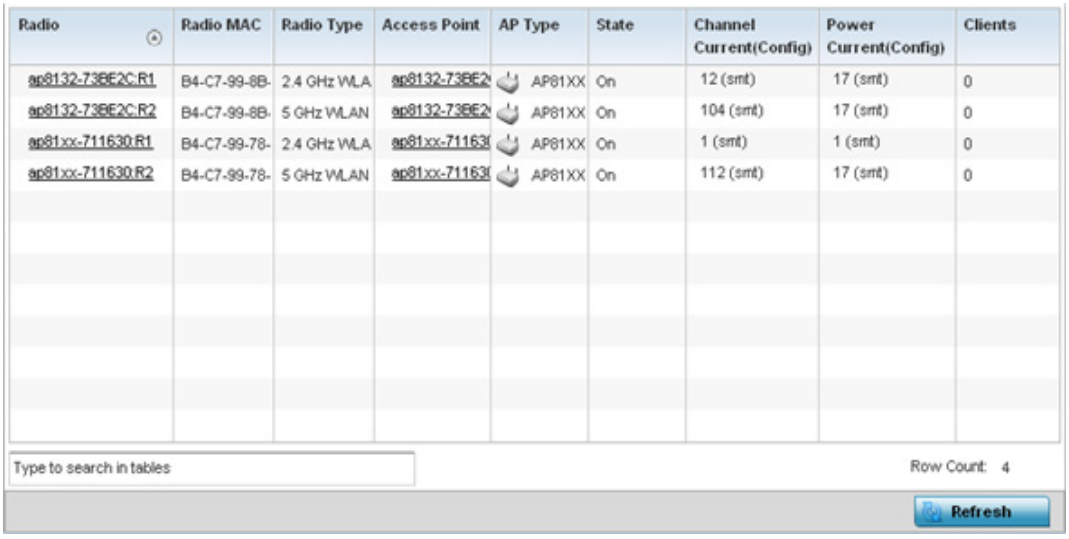


Figure 16: RF Domain - Radio Status screen

The **Radio Status** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that can be selected to display radio information in greater detail.
Radio MAC	Displays the MAC address as a numerical value factory hard coded to each listed RF Domain member access point 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. AP6532, AP6522, AP6562, AP71xx, AP8132 and AP8232 models have two radios, while AP6521 model has 1 radio.
AP Type	Lists the model type of each RF Domain member access point.
State	Displays the radio's current operational state.
Channel Current (Config)	Displays the current channel each listed RF Domain member access point radio is broadcasting on.
Power Current (Config)	Displays the current power level the radio is using for its transmissions.
Clients	Displays the number of clients currently connected to each listed RF Domain member access point radio. AP6532, AP6522, AP6562, AP71xx, AP8132, AP8232 models can support up to 256 clients per radio. AP6521 model can support up to 128 clients per radio.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

RF Statistics

"Radios"

To view the RF Domain radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Expand **Radios** from the **RF Domain** menu and select **RF Statistics.**

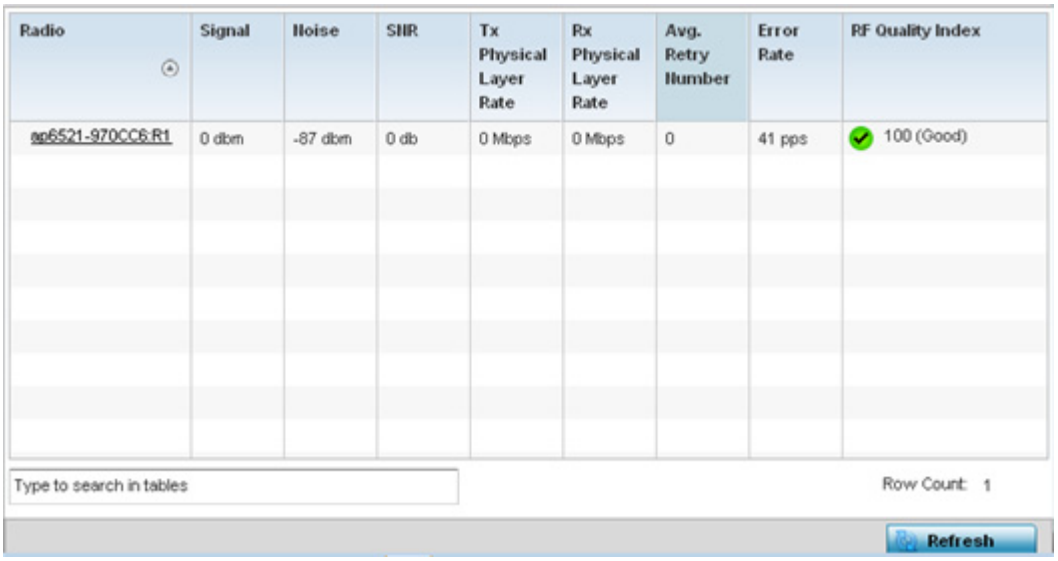


Figure 17: RF Domain - Radio RF Statistics screen

The **RF Statistics** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member radio. Each name displays as a link that can be selected to display 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 access point.
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)
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Traffic Statistics

"Radios"

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.

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Expand **Radios** from the **RF Domain** menu and select **Traffic Statistics.**

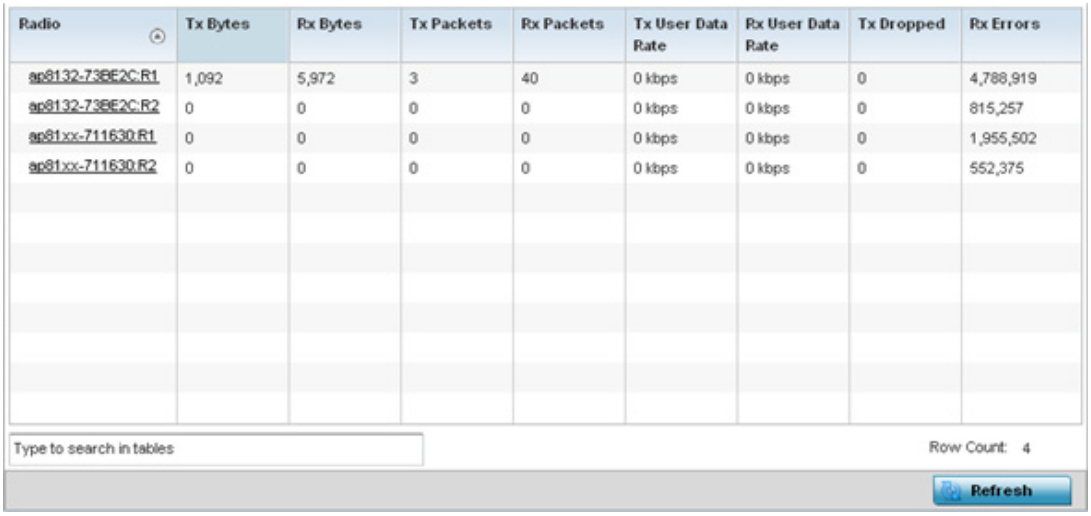


Figure 18: RF Domain - Radio Traffic Statistics screen

The **Radio Traffic** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that can be selected to display radio information in greater detail.
Tx Bytes	Displays the total number of bytes transmitted by each RF Domain member access point 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 access point 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 access point 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 access point 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 access point 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 access point radio. This rate only applies to user data and does not include any management overhead.
Tx Dropped	Displays the total number of transmitted packets which have been dropped by each RF Domain member access point radio. This includes all user data as well as any management overhead packets that were dropped.
Traffic Index	Displays the traffic index which is an index that measures how efficiently how the RF medium is used. This index is the percentage of current throughput relative to the maximum throughput possible.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Bluetooth

"RF Domain Statistics"

AP8432 and AP8533 model access point radios 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 can raise an alarm.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and 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 view Bluetooth radio utilization statistics for RF Domain member access point and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Bluetooth**.

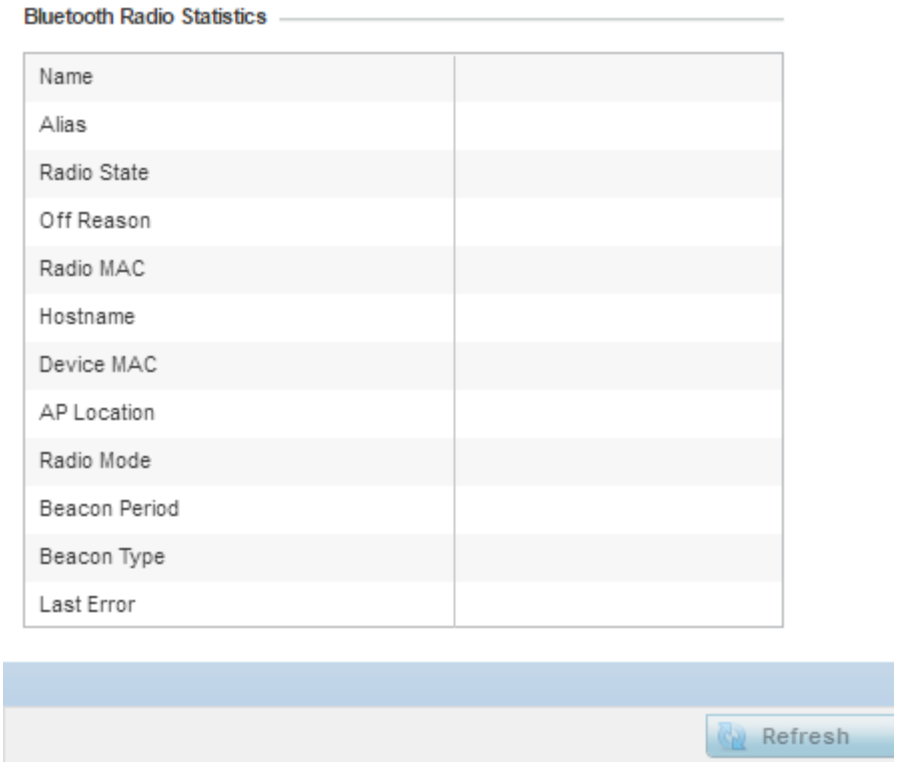


Figure 19: RF Domain - Bluetooth screen

The RF Domain **Bluetooth** screen displays the following:

Name	Lists the administrator assigned name of the access point's Bluetooth radio.
Alias	If an alias has been defined for the access point, 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 access point, it is used in place of the access point's default hostname. 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.
Radio State	Displays the current operational state (On/Off) of the RF Domain member Bluetooth radio.
Off Reason	States an offline access point's reason for bluetooth radio inactivity within the RF Domain.
Radio MAC	Lists the Bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network.
Hostname	Lists the hostname set for the access point as its network identifier. Hostnames cannot include an underscore character.
Device MAC	Lists the access point's factory encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the access point and Bluetooth radio's administrator assigned deployment location.

Radio Mode	Lists an access point's Bluetooth radio functional mode as either *bt-sensor* or *le-beacon*.
Beacon Period	Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds.
Beacon Type	Lists whether this Bluetooth radio is utilizing *eddystone* or *ibeacons* for its RF emissions.
Last Error	Lists descriptive text on any error that is preventing the Bluetooth radio from operating.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

Mesh

"RF Domain Statistics"

Mesh networking enables users to wirelessly access 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 access point and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Mesh**.

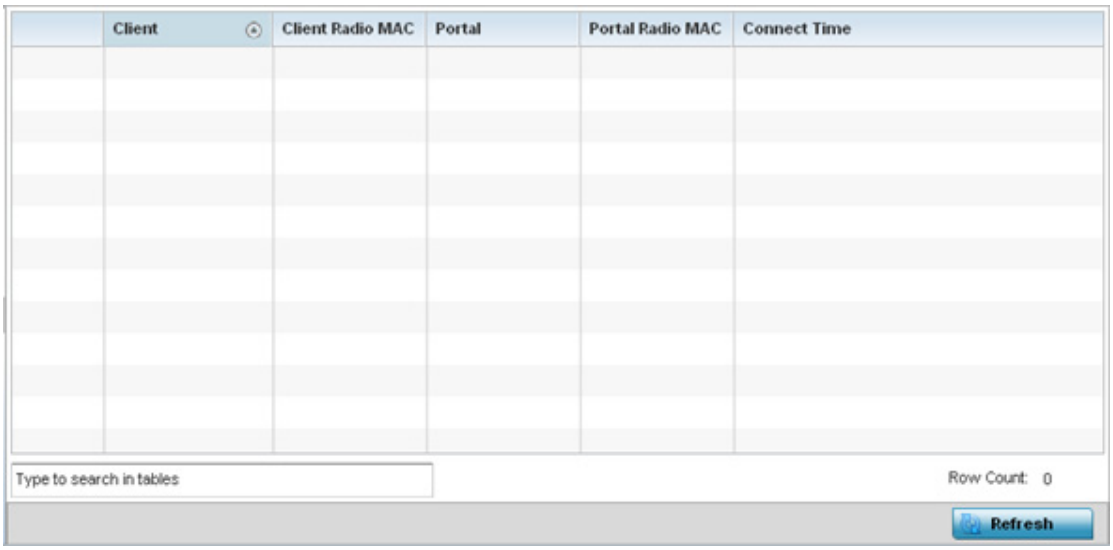


Figure 20: RF Domain - Mesh screen

The RF Domain **Mesh** screen displays the following:

Client	Displays the configured hostname for each mesh client connected to a RF Domain member access point.
Client Radio MAC	Displays the hardware encoded MAC address for each mesh client connected to a RF Domain member access point.
Portal	Displays a numerical portal Index ID for the each mesh client connected to a RF Domain member access point.
Portal Radio MAC	Displays the hardware encoded MAC address for each radio in the RF Domain mesh network.
Connect Time	Displays the total connection time for each listed client in the RF Domain mesh network.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Mesh Point

"RF Domain Statistics"

To view *Mesh Point* statistics for RF Domain member access point and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Mesh Point**.

The **MCX Geographical View** displays by default.

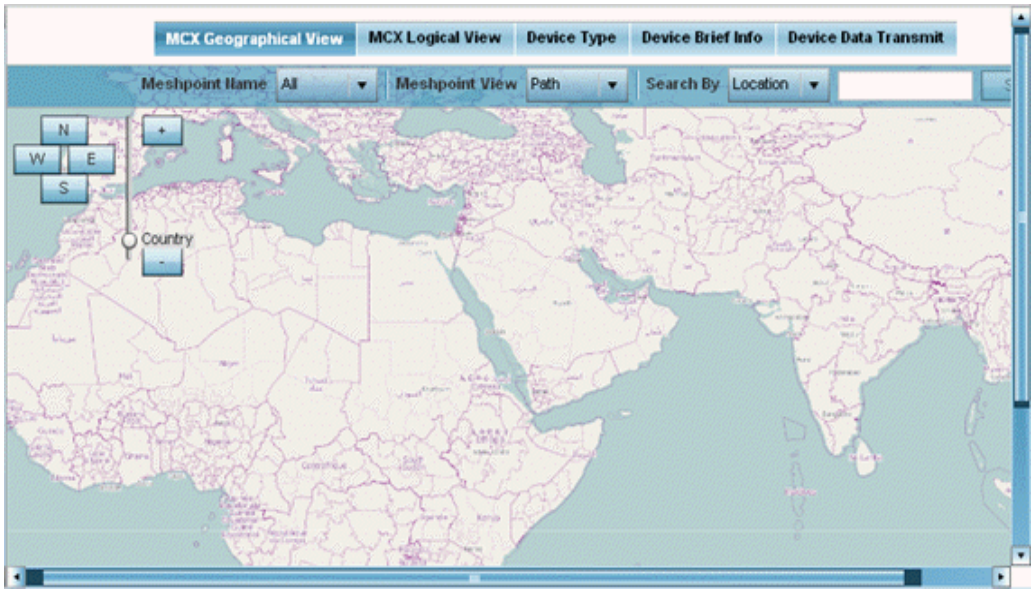


Figure 21: RF Domain - Mesh Point MCX Geographical View screen

The **MCX Geographical View** screen 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.

4 Use the N, E, W and S buttons to move the map in the *North*, *East*, *West* and *South* directions respectively. The slider next to these buttons enables zooming in and out of the view. The available fixed zoom levels are *World*, *Country*, *State*, *Town*, *Street* and *House*.

5 Use the **Maximize** button to maximize this view to occupy the complete screen. Use the **Refresh** button to update the status of the screen.

6 Select the **MCX Logical View** tab to view a logical representation of the mesh point.

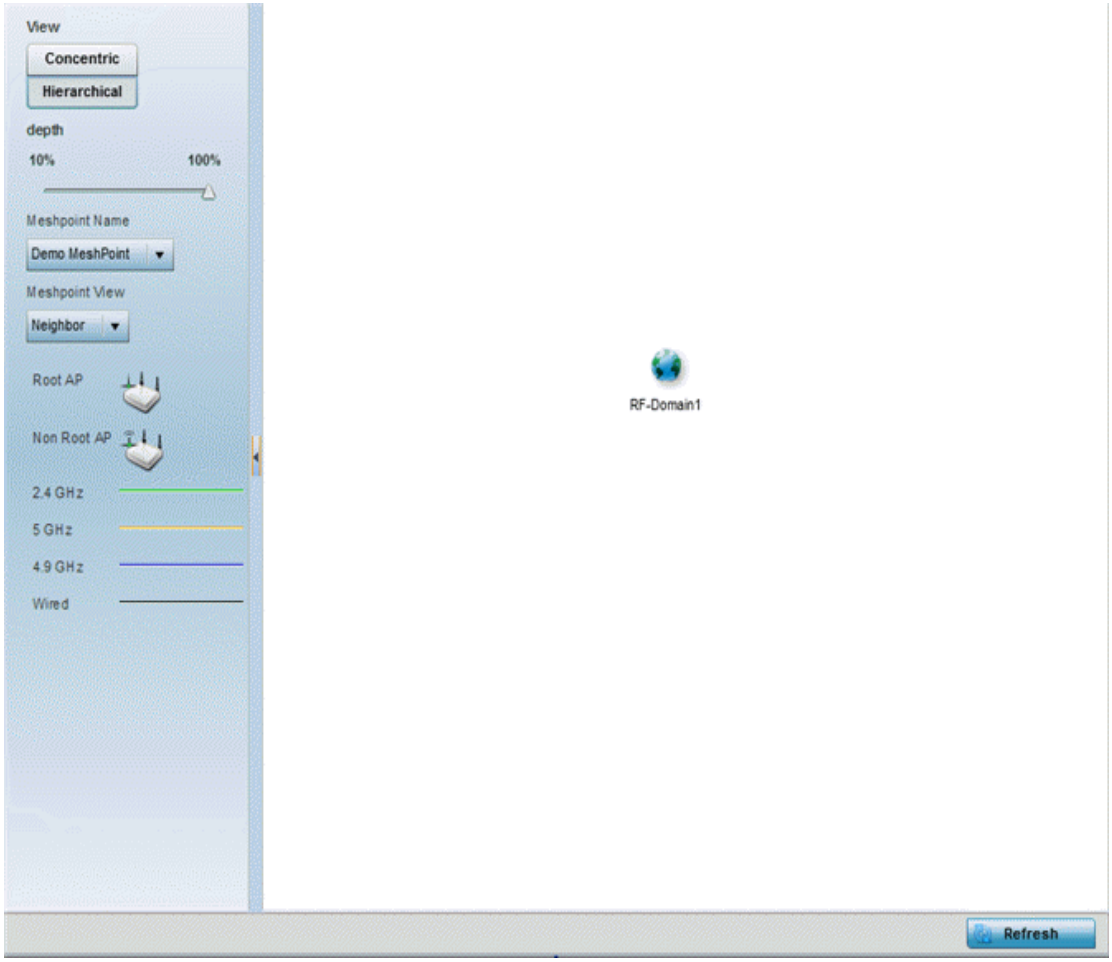


Figure 22: RF Domain - Mesh Point MCX Logical View screen

The **Concentric** and **Hierarchical** buttons define how the mesh point is displayed in the *MCX Logical View* screen. In the *Concentric* mode, the mesh is displayed as a concentric arrangement of devices with the root mesh at the centre and the other mesh device arranged around it.

In the *Hierarchical* arrangement, the root node of the mesh is displayed at the top of the mesh tree and the relationship of the mesh nodes are displayed as such.

Use the **Meshpoint Name** drop down to select a mesh point to see the graphical representation of that mesh point. The view can further be filtered based on the values *Neighbor* or *Path* selected in the **Meshpoint View** field.

7 Select the **Device Type** tab.

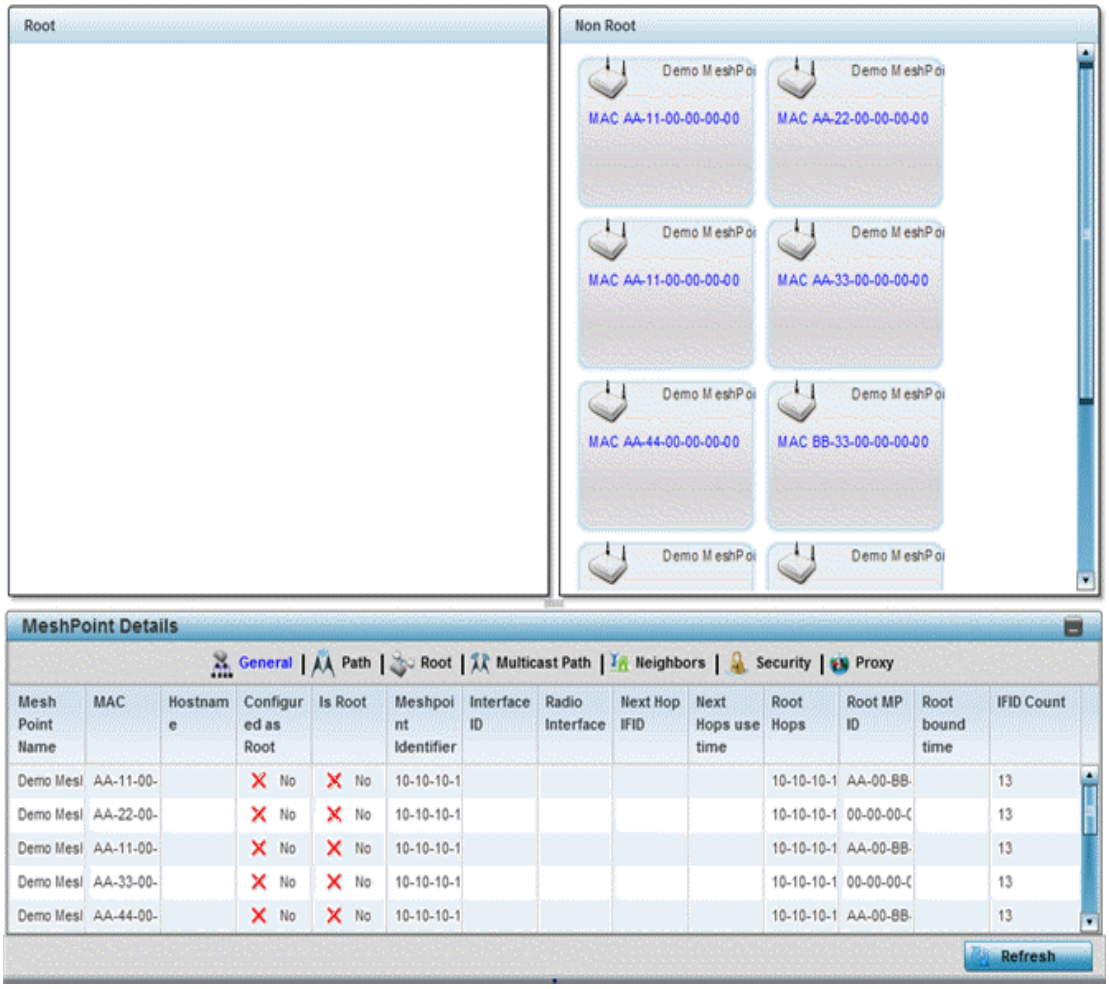


Figure 23: RF Domain - Mesh Point Device Type screen

The **Root** field displays the Mesh ID and MAC Address of the configured root mesh points in the RF Domain.

8 The **Non Root** field 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.

9 The **Mesh Point Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

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.
Radio Interface	Uniquely identifies the radio interface on which the mesh point operates.
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 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	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.

The **Path** tab displays the following:

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.
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 or Invalid.
Binding	Indicates whether the path is bound or unbound.
Timeout	The timeout interval in mili-seconds. 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.

The **Root** tab displays the following:

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 5.0, 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 Preferred Root Interface Index.
Neighbor Bias	This field lists any bias applied because of Preferred Root Next-Hop Neighbor IFID.
Root Bias	This field lists any bias applied because of Preferred Root MPID.

The **Multicast Path** tab displays the following:

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 of 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.

The **Neighbors** tab displays the following:

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 5.0, 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 mili seconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

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 5.0, 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.

The **Proxy** tab displays the following:

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's (MPID) is used to distinguish the neighbor device.
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.

10 Select the **Device Brief Info** tab from the top of the screen.

The *Device Brief Info* screen is divided into 2 fields, **All Roots and Mesh Points** and **MeshPoint Details**.

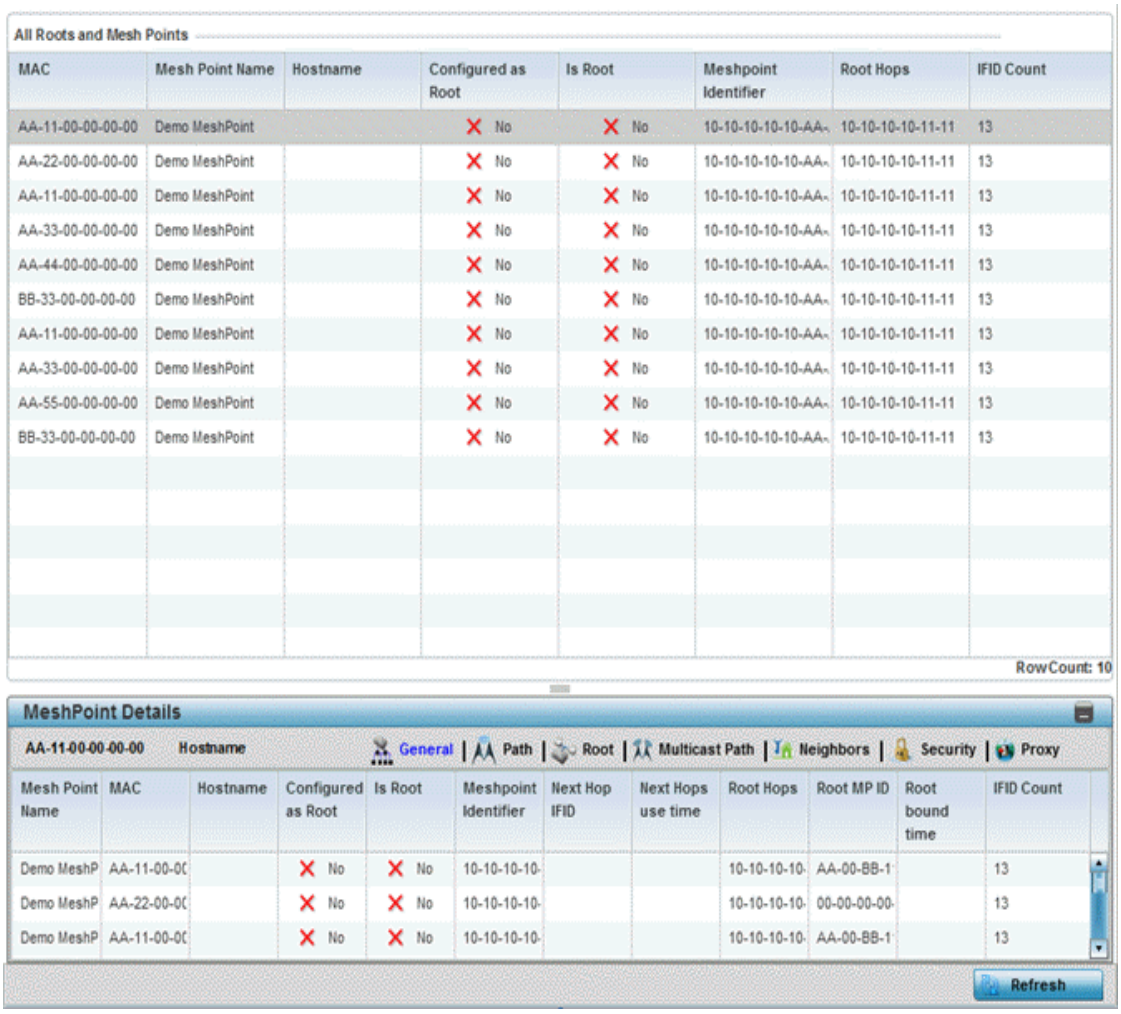


Figure 24: RF Domain - Mesh Point Device Brief Info screen

The **All Roots and Mesh Points** field displays the following:

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 connected to the WAN, providing a wired backhaul to the network (Yes/No).
Is Root	Indicates whether the current mesh point is a root mesh point (Yes/No).
Root Hops	The number of devices between the selected mesh point and the destination device.
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
IFID Count	Displays the number of Interface IDs (IFIDs) associated with all the configured mesh points in the RF Domain.

11 The **MeshPoint Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

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 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	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)
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.
Radio 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 Hops 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 Interface IDs (IFIDs) associated with all the configured mesh points in the RF Domain.

The **Path** tab displays the following:

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 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.

The **Root** tab displays the following:

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 5.0, indicating the frequency of the radio that is used to communicate with the neighbor.
Metric	Displays the computed path metric between the neighbor and their root mesh point.
Interface Bias	This field lists any bias applied because of preferred root Interface Index.
Neighbor Bias	This field lists any bias applied because of preferred root next-hop Neighbor IFID.
Root Bias	This field lists any bias applied because of preferred root MPID.

The **Multicast Path** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
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.

The **Neighbors** tab displays the following:

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 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 *5.0*, 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 mili seconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

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 *5.0*, 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 the local MP acts 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.

The **Proxy** tab displays the following:

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.

12 Select **Device Data Transmit**.

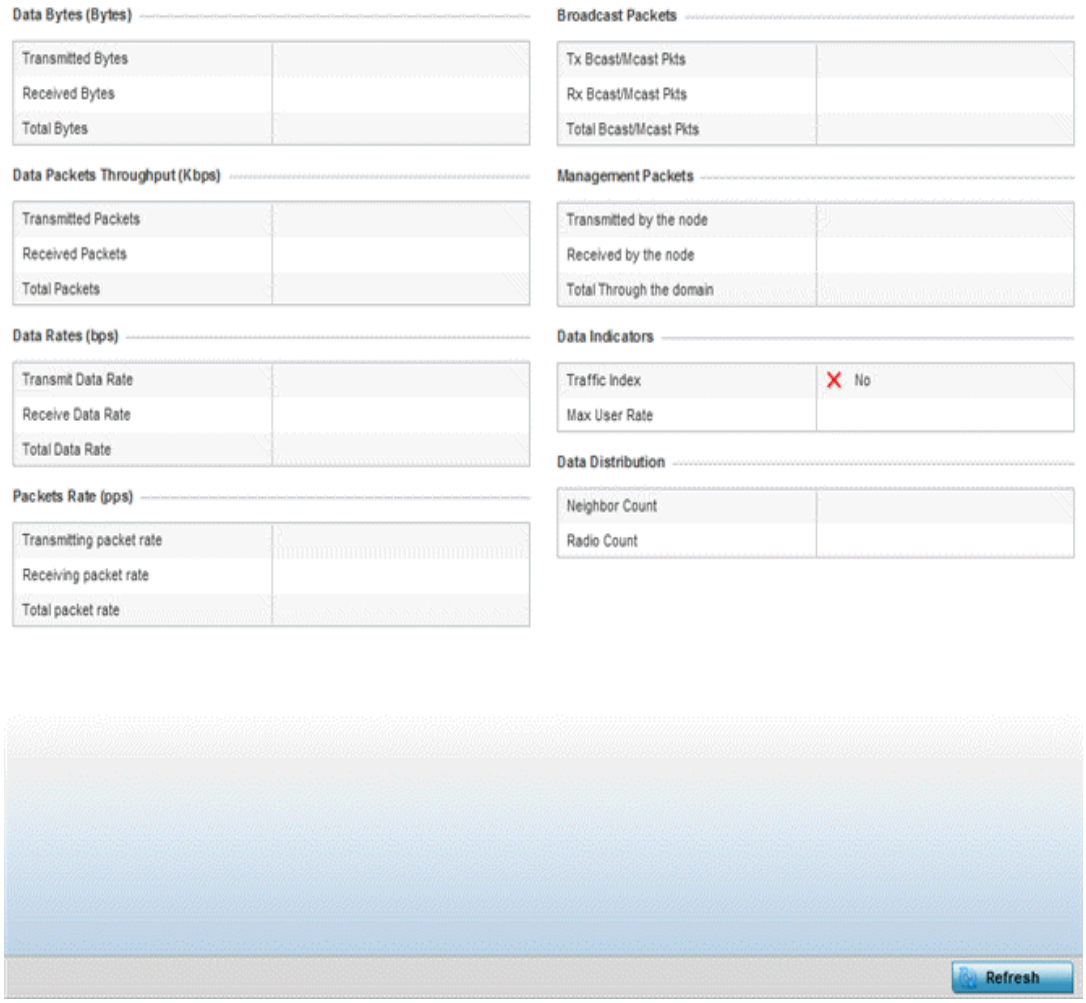


Figure 25: RF Domain - Mesh Point Device Data Transmit screen

Review the following transmit and receive statistics for Mesh nodes:

Data Bytes (Bytes): Transmitted Bytes	Displays the total amount of data, in Bytes, that has been transmitted by mesh points in the RF Domain.
Data Bytes (Bytes): Received Bytes	Displays the total amount of data, in Bytes, that has been received by mesh points in the RF Domain.
Data Bytes (Bytes): Total Bytes	Displays the total amount of data, in Bytes, that has been 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.
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 transmitted through the mesh point node.
Management Packets: Received by the node	Displays the total number of management packets 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 *Yes* or *No* 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: Radio Count	Displays the total number of neighbor radios known to the mesh points in the RF Domain.

SMART RF

"RF Domain Statistics"

When invoked by an administrator, *Self-Monitoring At Run Time* (Smart RF) 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, un-managed 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.

To view the Smart RF summary for RF Domain member access point radios:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **SMART RF** from the **RF Domain** menu.

4 Expand the **SMART RF** menu and select **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.

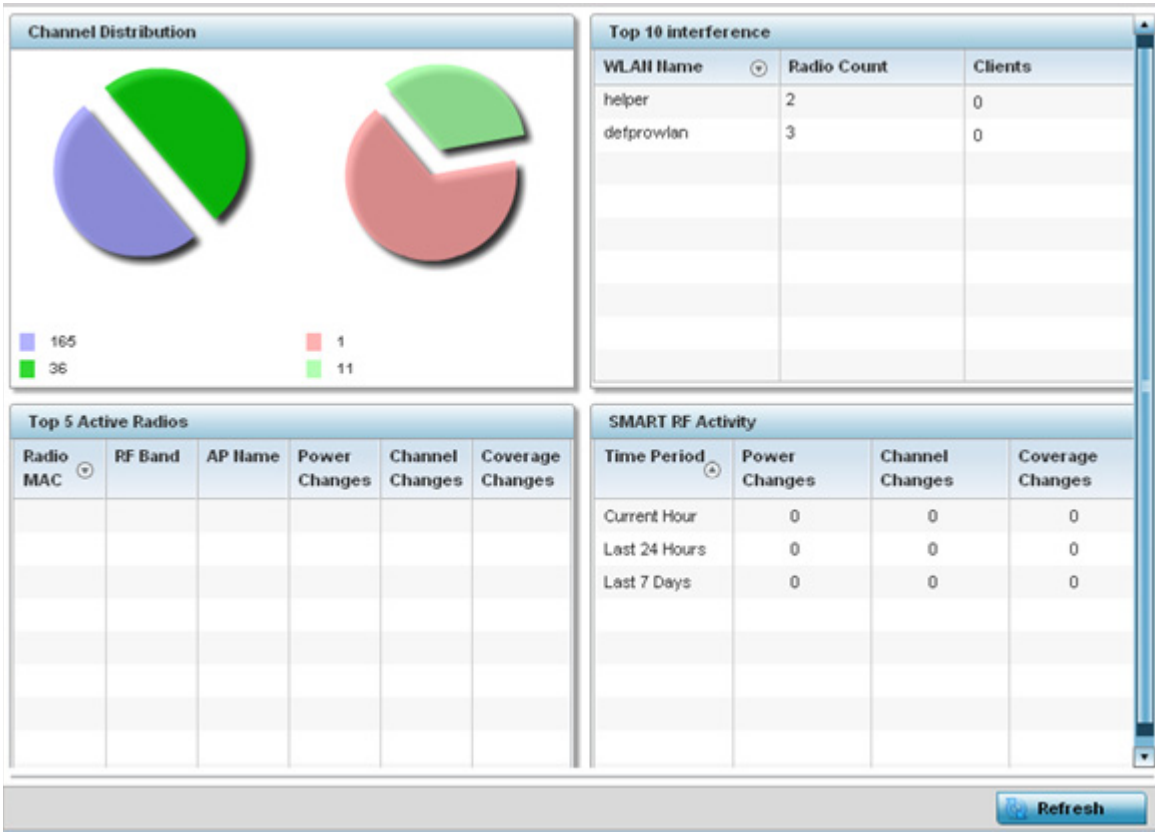


Figure 26: RF Domain - Smart RF Summary screen

5 The **Channel Distribution** field lists how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. 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 WLANs whose radios are contributing the highest levels of detected interference within the RF Domain.

WLAN Name	Lists the WLANs whose member device radios are contributing to the highest levels of interference detected within the RF Domain.
Radio Count	Displays the number of radios within each listed WLAN that are contributing to the RF Domain's high levels of detected interference. These are the radios subject to Smart RF power compensations to reconcile the high levels of interference.
Clients	Lists the number of connected clients detected for the WLAN member device radios.

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 access point name used to differentiate from other RF Domain member access point radios.
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 Select **Refresh** to update the Summary to its latest RF Domain Smart RF information.

10 Select **Details** from the RF Domain menu.

Refer to the **General** field to review or assess the radio's factory encoded hardware MAC address, the radio index assigned by the administrator, the 802.11 radio type, its current operational state, the radio's AP hostname assigned by an administrator, its current operating channel and power.

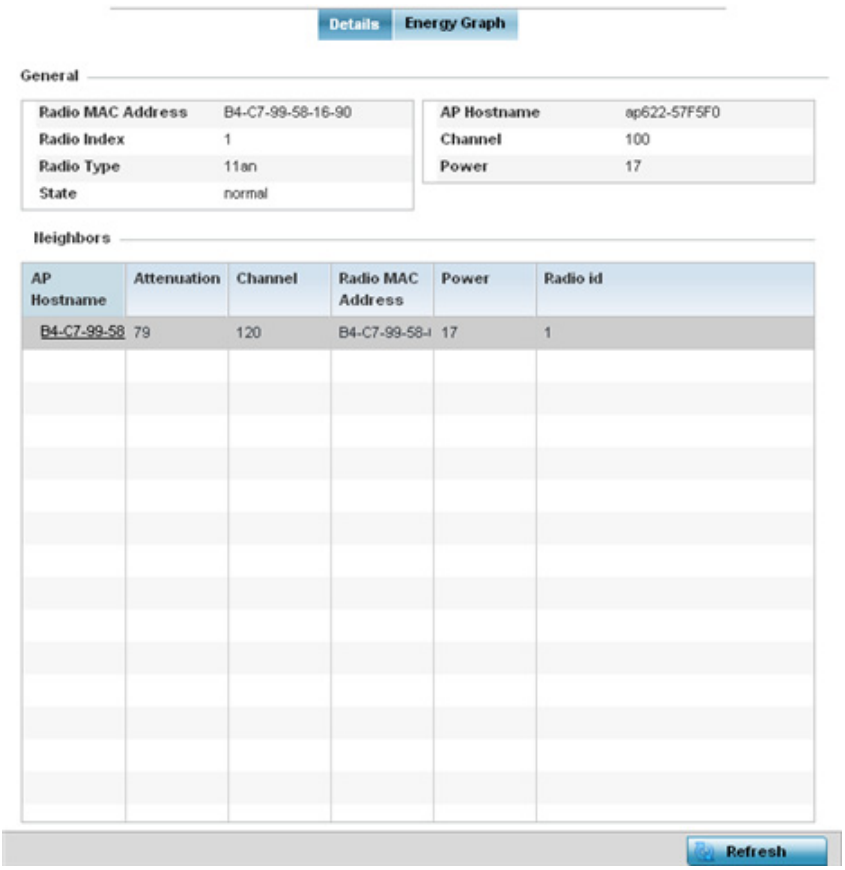


Figure 27: RF Domain - Smart RF Details screen

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. Individual access point hostnames can be selected and the RF Domain member radio can be reviewed in greater detail. *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. Select **Refresh** at any time to update the Details screen to its latest values.

11 Select the **Energy Graph** tab

Use the **Energy Graph** to review the radio's operating channel, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

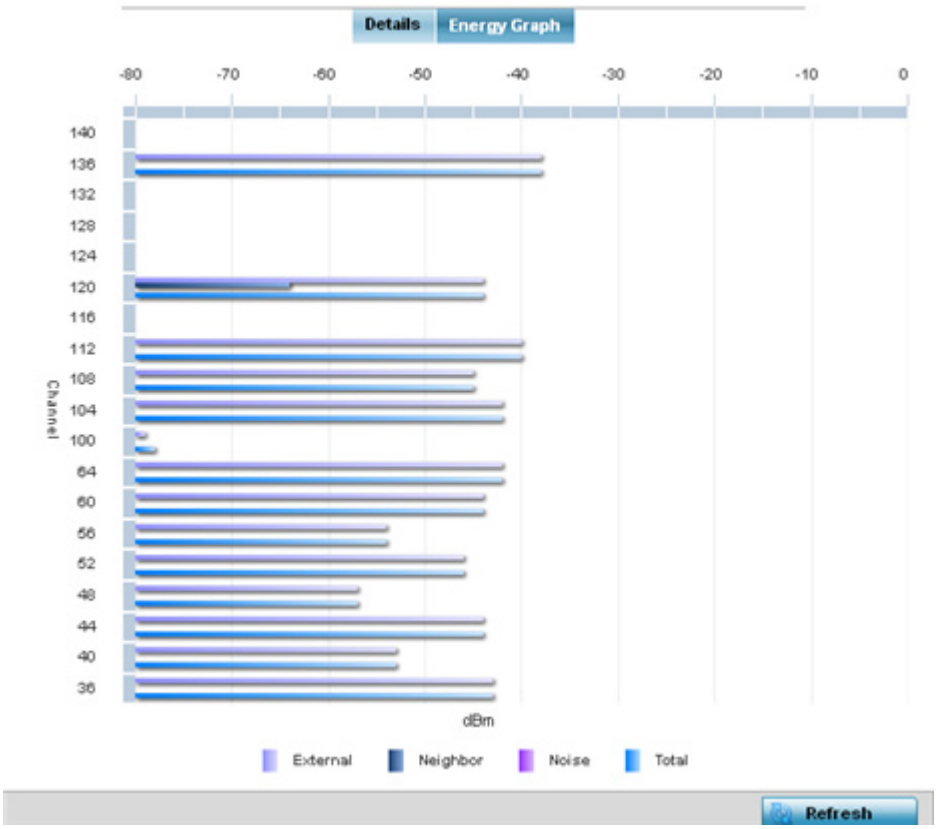
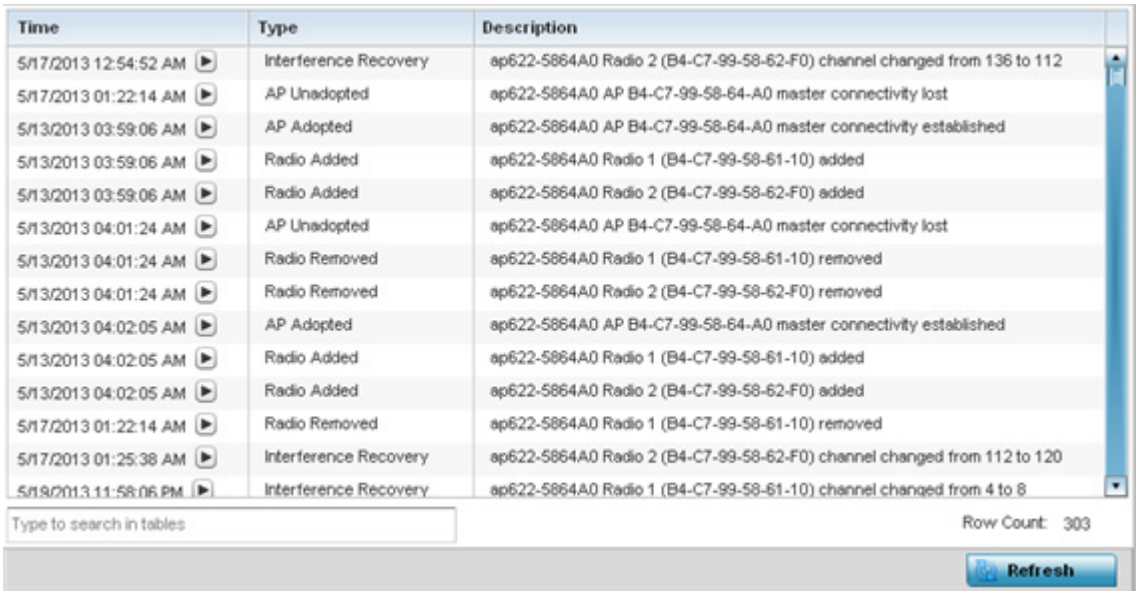


Figure 28: RFDomain - Smart RF Energy Graph

12 Select **Smart RF History** to review the descriptions and types of Smart RF events impacting RF Domain member devices.



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

Type to search in tables

Row Count: 303

Refresh

Figure 29: RF Domain - Smart RF History screen

The **SMART RF History** screen displays the following RF Domain member historical data:

Time	Displays a 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.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

WIPS

"RF Domain Statistics"

Refer to the *Wireless Intrusion Protection Software* (WIPS) screens to review a client blacklist and events reported by a RF Domain member access point.

For more information, see:

- "WIPS Client Blacklist"
- "WIPS Events"

WIPS Client Blacklist

"WIPS"

The *Client Blacklist* displays clients detected by WIPS and removed from RF Domain utilization. Blacklisted clients are not allowed to associate to RF Domain member access point radios.

To view the WIPS client blacklist:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Expand the **WIPS** menu item and select **Client Blacklist**.

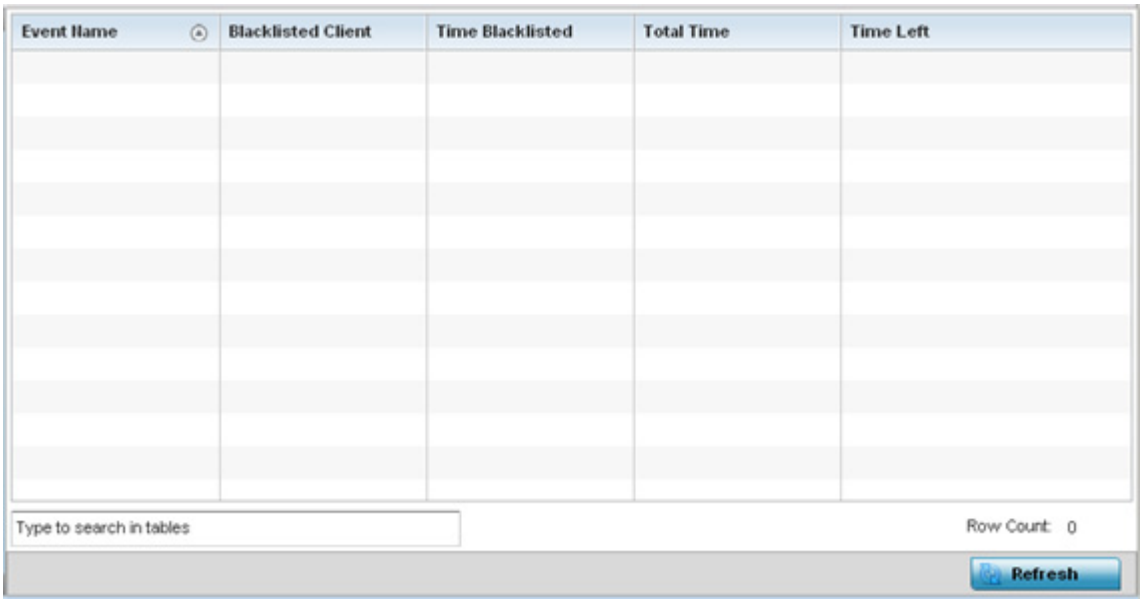


Figure 30: RF Domain - WIPS Client Blacklist screen

The WIPS **Client Blacklist** screen displays the following:

Event Name	Displays the name of the blacklisting wireless intrusion event detected by a RF Domain member access point.
Blacklisted Client	Displays the MAC address 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 access point.
Total Time	Displays the time the unauthorized (now blacklisted) device remained in the RF Domain.
Time Left	Displays the time the blacklisted client remains on the list.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

WIPS Events

"WIPS"

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 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Expand the **WIPS** menu item and select **WIPS Events.**

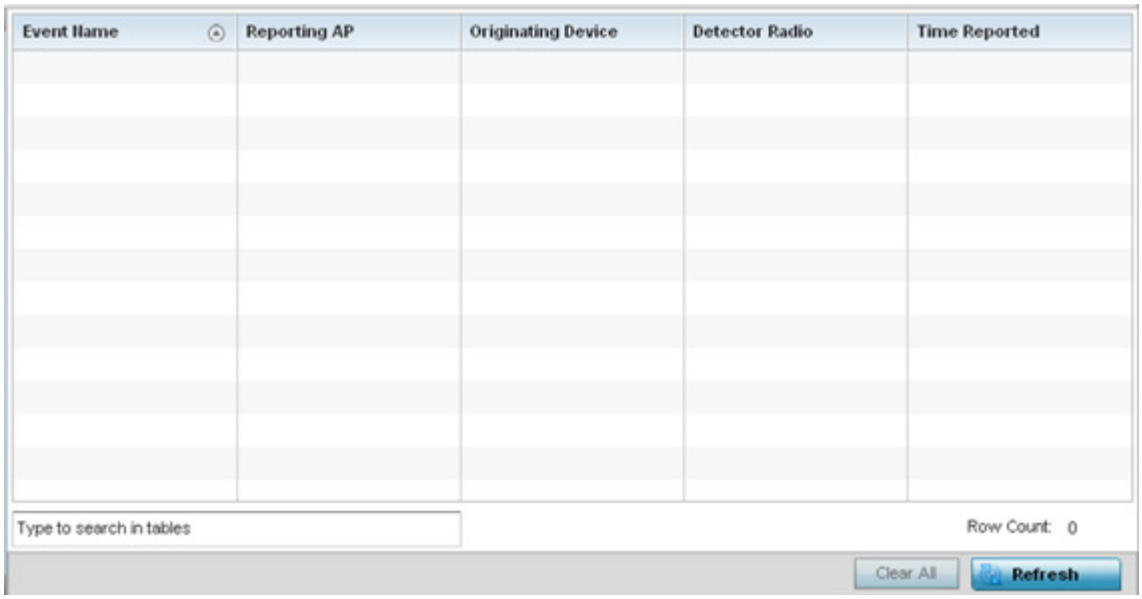


Figure 31: RF Domain - WIPS Events screen

The **WIPS Events** screen displays the following:

Event Name	Displays the event name of the intrusion detected by a RF Domain member access point.
Reporting AP	Displays the MAC address of the RF Domain member access point reporting the event.
Originating Device	Displays the MAC address of the device generating the event.
Detector Radio	Displays access point radio number detecting the event. AP6532, AP6522, AP6562, AP71xx, AP8132 and AP8232 models have 2 radios, while AP6521 model has 1 radio.
Time Reported	Displays a time stamp of when the event was reported by the RF Domain member access point radio.
Clear All	Select the *Clear All* button to clear the statistics counters and begin a new data collection.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Captive Portal

"RF Domain Statistics"

A captive portal is guest access policy for providing guests 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 RF Domain captive portal statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Captive Portal** from the **RF Domain** menu.

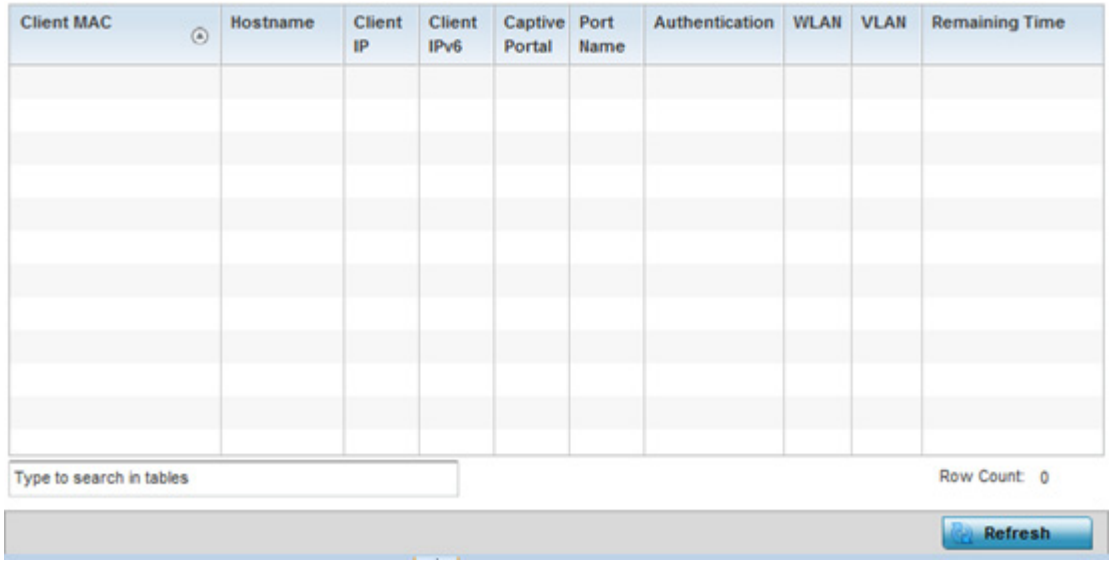


Figure 32: RF Domain - Captive Portal

The screen displays the following **Captive Portal** data for requesting clients:

Client MAC	Displays the MAC address of each listed client requesting captive portal access to the controller or service platform managed network. This address can be selected to display client information in greater detail.
Hostname	Lists the administrator assigned hostname of the device requesting captive portal access to network's RF Domain resources.
Client IP	Displays the IP address of each listed client using its connected RF Domain member access point for captive portal access.
Client IPv6	Displays any IPv6 formatted address of any listed client using its connected RF Domain member access point for captive portal access. 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.
Captive Portal	Lists the name of the RF Domain captive portal currently being utilized by each listed client.
Port Name	Lists the name of the virtual port used for captive portal session direction.

Authentication	Displays the authentication status of requesting clients attempting to connect to the access point via the captive portal.
WLAN	Displays the name of the WLAN the requesting client would use for interoperation with the access point.
VLAN	Displays the name of the VLAN the client would use as a virtual interface for captive portal operation with the access point.
Remaining Time	Displays the time after which a connected client is disconnected from the captive portal.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Coverage Hole Detection

"RF Domain Statistics"

Refer to the *Wireless Intrusion Protection Software* (WIPS) screens to review a client blacklist and events reported by a RF Domain member access point.

Refer to the Coverage Hole Detection screens to review any coverage hole adjustments reported by access points in the selected RF-Domain. When coverage hole recovery is enabled and a deployment area radio coverage hole is detected, Smart RF determines the radio's power increase compensation required based on a reporting client's signal to noise (SNR) ratio. If a client's SNR is above the administrator threshold, its connected Access Point's transmit power is increased until the noise rate falls below the threshold.

For more information, see:

- "Coverage Hole Summary"
- "Coverage Hole Detail"

Coverage Hole Summary

"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 signal to noise (SNR) ratio. If a client's SNR is above the administrator threshold, its connected Access Point's transmit power is increased until the noise rate falls below the threshold.

To view a RF Domain's coverage hole summary:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Coverage Hole Detection** from the **RF Domain** menu and expand this item to display its submenu options.

4 Select **Summary**.

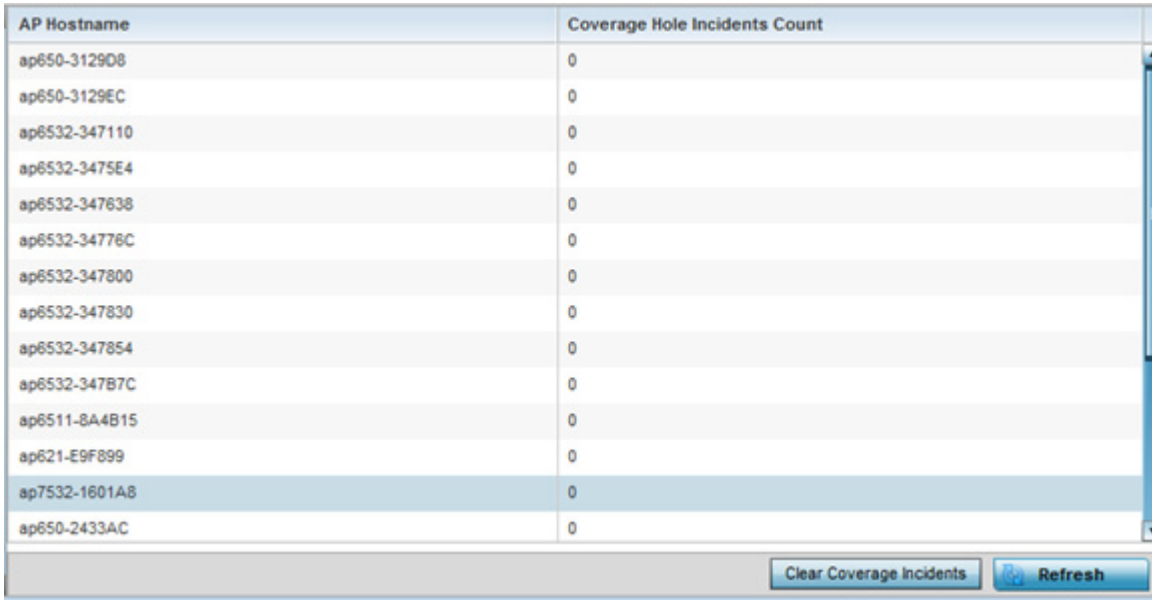


Figure 33: RF Domain - Coverage Hole Summary

The screen displays the following RF Domain coverage hole summarization 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.
Clear Coverage Incidents	Select this option to clear the statistics counters and begin a new coverage hole summary for RF Domain member access point radios.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Coverage Hole Detail

"Coverage Hole Detection"

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 review specific RF Domain member access point coverage hole information:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the **System** node on the top, left-hand side, of the screen.

3 Select **Coverage Hole Detection** from the **RF Domain** menu and expand this item to display its submenu options.

4 Select **Details**.

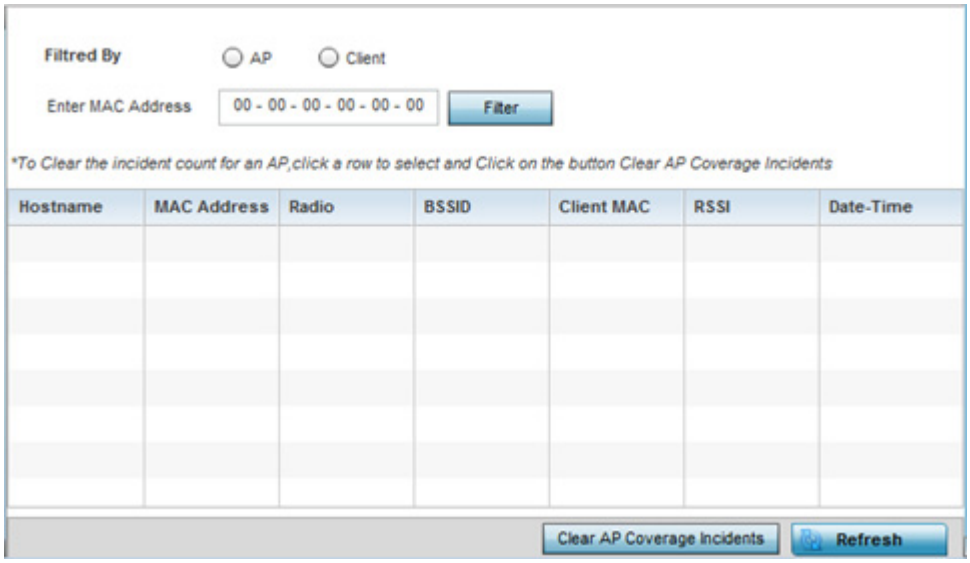


Figure 34: RF Domain - Coverage Hole Details

5 Use the **Filtered By** option to define whether the RF Domain's coverage hole details are provided by a selected access point (*AP*) 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.

6 Refer to the **Enter MAC Address** parameter to define a RF Domain member access point MAC address or Hostname or just a client MAC address. This is the selected device reporting coverage hole details to the listed RF Domain member access point.

7 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.
Radio	Lists the access point radio receiving and reporting coverage hole RSSI data from the listed client MAC. Each supported access point has at least radios, with the exception of AP6521 model which is a single-radio model.
BSSID	Displays the basic service set identifier (BSSID) 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's 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 *Received Signal Strength Indicator* (RSSI) of the detecting access point Radio or client.
Date-Time	Displays the date and time when each listed access point received its coverage hole indecent information.
Clear Coverage Incidents	Select this option to clear the statistics counters and begin a new coverage hole assessment for RF Domain member access point radios.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

Access Point Statistics

- "Statistics"

The access point statistics screens displays controller or service platform connected access point *performance, health, version, client support, radio, mesh, interface, DHCP, firewall, WIPS, sensor, captive portal, NTP* and *load* information. Access point statistics consists of the following:

- "Health"
- "Device"
- "Web-Filtering"
- "Device Upgrade"
- "Adoption"
- "AP Detection"
- "Guest User"
- "Wireless Clients"
- "Wireless LANs"
- "Policy Based Routing"
- "Radios"
- "Mesh"
- "Interfaces"
- "RTLS"
- "PPPoE"
- "Bluetooth"
- "OSPF"
- "L2TPv3 Tunnels"
- "VRRP"
- "Critical Resources"
- "LDAP Agent Status"
- "Mint Links"

- "Guest Users"
- "GRE Tunnels"
- "Dot1x"
- "Network"
- "DHCPv6 Relay & Client"
- "DHCP Server"
- "Firewall"
- "VPN"
- "Certificates"
- "WIPS"
- "Sensor Servers"
- "Bonjour Services"
- "Captive Portal"
- "Network Time"
- "Load Balancing"
- "Environmental Sensors (AP8132 Models Only)"

Health

- "Access Point Statistics"

The *Health* screen displays a selected access point's hardware version and software version. Use this information to fine tune the performance of an access point. This screen should also be the starting point for troubleshooting an access point since it is designed to present a high level display of access point performance efficiency.

To view the access point health:

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 a RF Domain and select one of its connected access points.

3 Select Health.

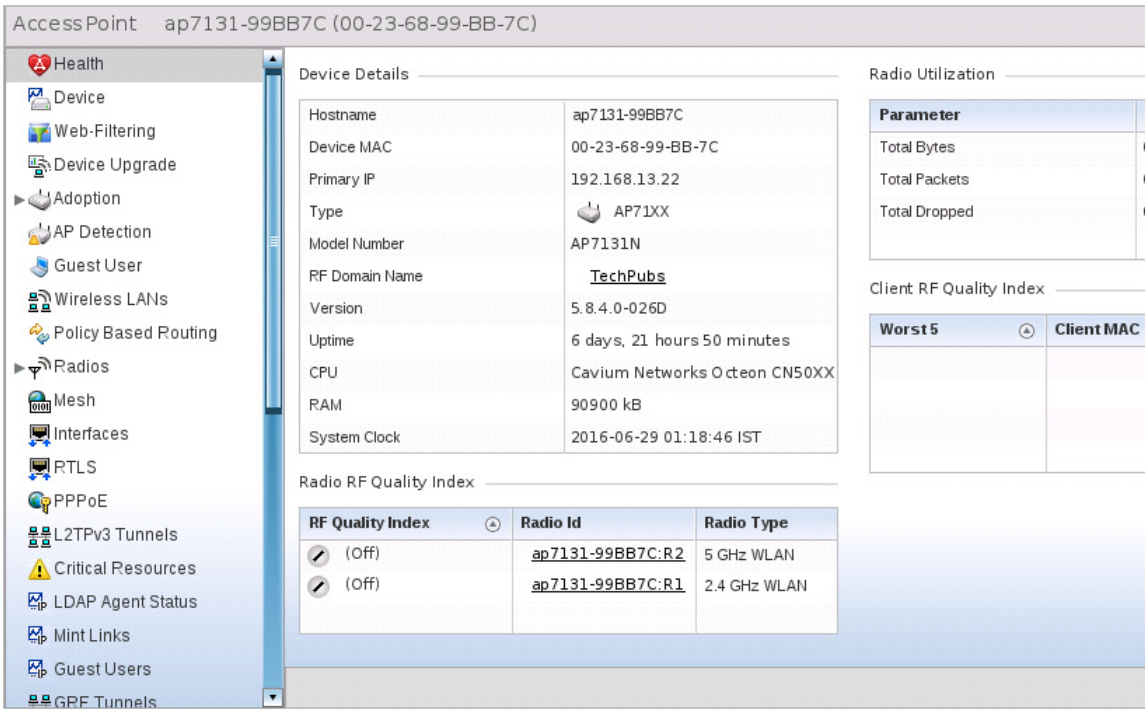


Figure 35: Access Point - Health screen

The Device Details field displays the following information:

Hostname	Displays the AP's unique name as assigned within the 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 AP	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.
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.
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.
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 displays the following:

RF Quality Index	Displays access point radios having very low 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.

4 Select the **Refresh** button as needed to update the screen's statistics counters to their latest values.

Device

"Access Point Statistics"

The *Device* screen displays basic information about the selected access point. Use this screen to gather version information, such as the installed firmware image version, the boot image and upgrade status.

To view the device 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 a RF Domain and select one of its connected access points.

3 Select Device.

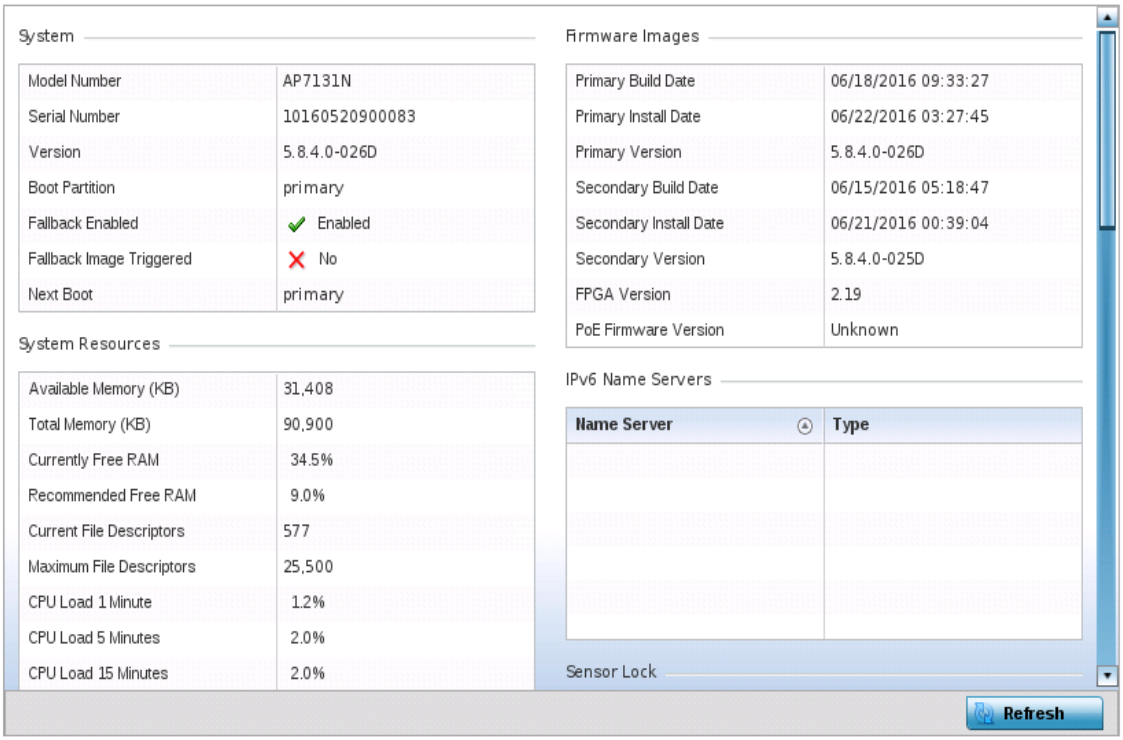


Figure 36: Access Point - Device screen

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.
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 operational software stored in device memory. This allows a user to test a new version of software. If the new version fails, the user can use the old version of the software.
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 it is very low, free up some space by closing some processes.
Recommended Free RAM	Displays the recommended RAM required for routine operation.
Current File Descriptors	Displays the access point's current file descriptors.
Maximum File Descriptors	Displays the access point's maximum file descriptors.
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 this access point.
Speed (Hz)	Displays the fan speed in Hz.

The Temperature field displays the following:

Number	Displays the number of temperature elements used by the access point.
Temperature	Displays the current temperature (in Celsius) to assess a potential access point overheat condition.

The Kernel 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 IPv6 Name Servers field displays the following:

Name Server	Displays the names of the IPv6 name servers designated to provide DNS resources to this access point.
Type	Displays the type of server for each server listed.

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 Sensor Lock field displays the following:

Sensor Lock	Displays whether a lock has been applied to access point sensor capabilities.

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 Delegated Prefixes** table 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.
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.

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.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Web-Filtering

"Access Point Statistics"

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 (whitelist and/or blacklist 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 this controller's Web filter 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 a RF Domain and select one of its connected access points.

3 Select Web-Filtering.

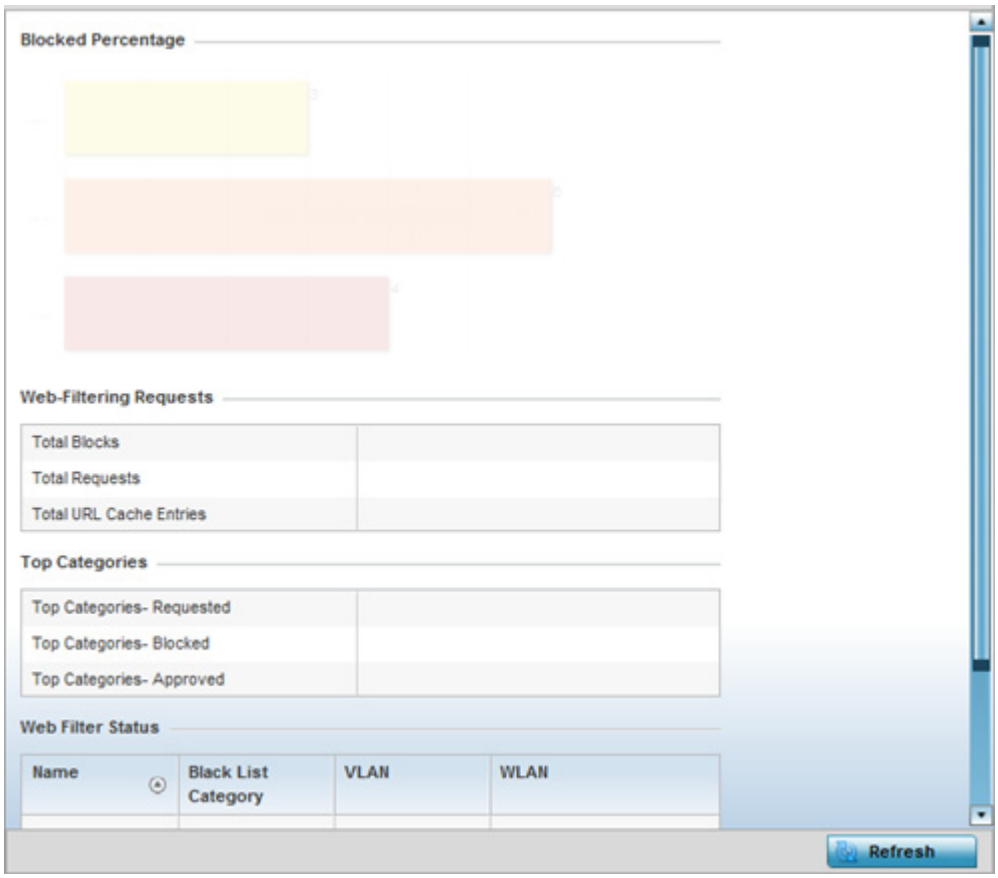


Figure 37: Access Point - Web-Filtering screen

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 chached URL data entries made on this access point on the request of clients requiring URL data managed by the access point and their respective whitelist or blacklist rules.

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 adhere's to your organization's standards for client access.

The Web Filter Status field displays the following information:

Name	Displays the name of Web filter
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.

Periodically select **Refresh** to update this screen to its latest values.

Device Upgrade

"Access Point Statistics"

The *Device Upgrade* screen displays information about devices receiving updates and the devices used to provision them. 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select Device Upgrade.

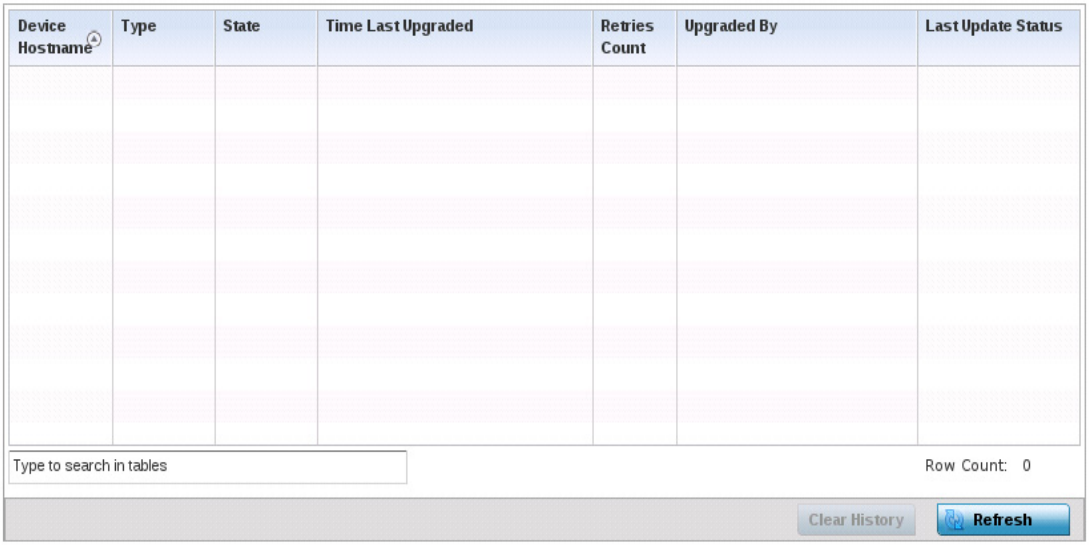


Figure 38: Access Point - Device Upgrade screen

The Device Upgrade screen displays the following

Device Hostname	Displays the administrator assigned hostname of the device receiving the update.
Type	Displays the model of the access point. The updating access point must be of the same model as the access point receiving the update.
State	Displays the current state of the access point upgrade.
Time Last Upgraded	Displays the date and time of the last successful upgrade operation.
Retries Count	Displays the number of retries made in an update operation.
Upgraded By	Displays the device that performed the upgrade.
Last Update Status	Displays the error status of the last upgrade operation.
Clear History	Select the *Clear History* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Adoption

"Access Point Statistics"

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.

For more information, refer to the following:

- "Adopted APs"
- "AP Adoption History"
- "AP Self Adoption History"
- "Pending Adoptions"

Adopted APs

"Adoption"

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 menu from the Web UI.

2 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Expand the Adoption menu item.

4 Select **Adopted APs**.

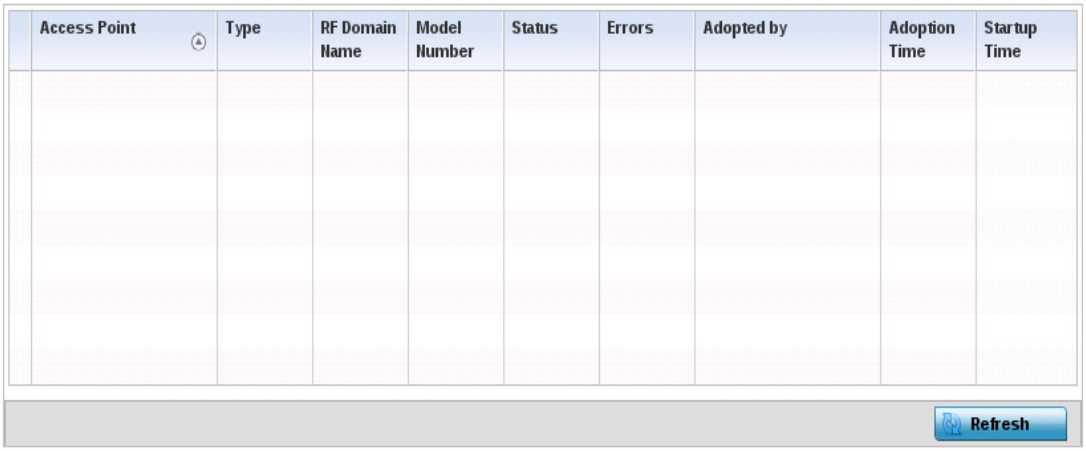


Figure 39: Access Point - Adopted APs screen

The **Adopted APs** screen displays the following:

Access Point	Displays the name assigned to the adopted access point as part of its device configuration.
Type	Lists the each listed access point type adopted by this access point.
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 numeric model (AP6532).
Status	Displays each listed access point's configuration status to help determine its service role.
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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

AP Adoption History

"Adoption"

The *AP Adoption History* screen displays a list of peer access point and their adoption event status.

To review a selected access point's adoption 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 the a RF Domain and select one of its connected access points.

3 Expand the Adoption menu item.

4 Select **AP Adoption History**.

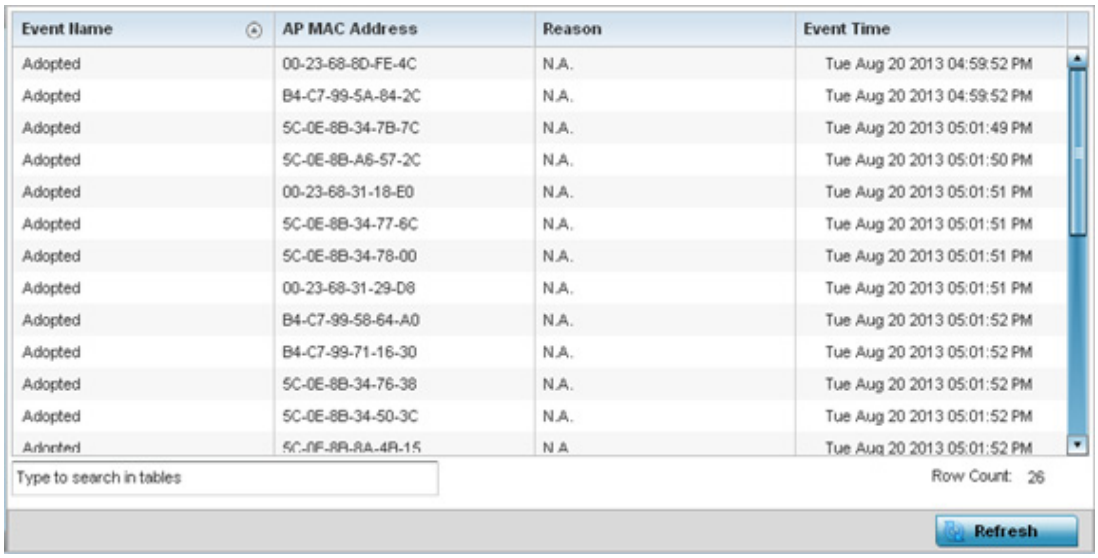


Figure 40: Access Point - AP Adoption History screen

The **Adopted Devices** 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.
Event Time	Displays day, date and time for each access point adoption attempt.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

AP Self Adoption History

"Adoption"

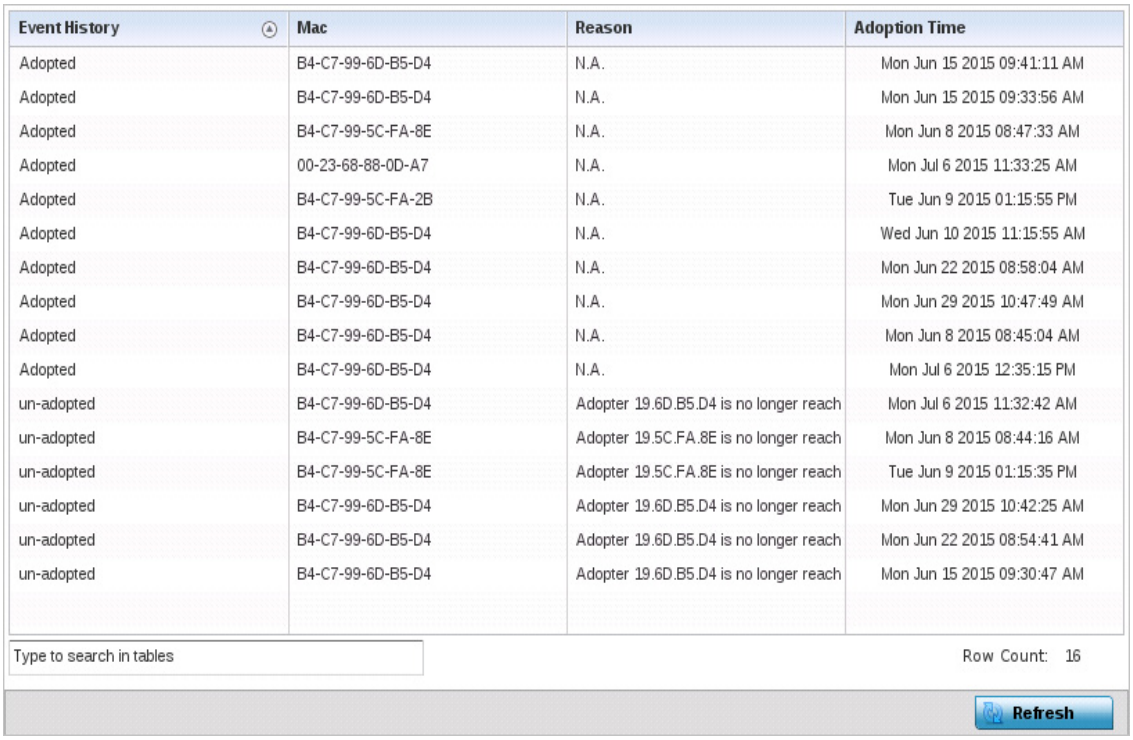
The *AP Self Adoption History* displays an event history of peer access points that have adopted to the selected access point.

1 Select the Statistics menu from the Web UI.

2 Select System from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain and select one of its connected access points.

3 Expand the Adoption menu item.

4 Select **AP Self Adoption History**.



Event History	Mac	Reason	Adoption Time
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jun 15 2015 09:41:11 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jun 15 2015 09:33:56 AM
Adopted	B4-C7-99-5C-FA-8E	N.A.	Mon Jun 8 2015 08:47:33 AM
Adopted	00-23-68-88-0D-A7	N.A.	Mon Jul 6 2015 11:33:25 AM
Adopted	B4-C7-99-5C-FA-2B	N.A.	Tue Jun 9 2015 01:15:55 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Wed Jun 10 2015 11:15:55 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jun 22 2015 08:58:04 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jun 29 2015 10:47:49 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jun 8 2015 08:45:04 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Jul 6 2015 12:35:15 PM
un-adopted	B4-C7-99-6D-B5-D4	Adopter 19.6D.B5.D4 is no longer reach	Mon Jul 6 2015 11:32:42 AM
un-adopted	B4-C7-99-5C-FA-8E	Adopter 19.5C.FA.8E is no longer reach	Mon Jun 8 2015 08:44:16 AM
un-adopted	B4-C7-99-5C-FA-8E	Adopter 19.5C.FA.8E is no longer reach	Tue Jun 9 2015 01:15:35 PM
un-adopted	B4-C7-99-6D-B5-D4	Adopter 19.6D.B5.D4 is no longer reach	Mon Jun 29 2015 10:42:25 AM
un-adopted	B4-C7-99-6D-B5-D4	Adopter 19.6D.B5.D4 is no longer reach	Mon Jun 22 2015 08:54:41 AM
un-adopted	B4-C7-99-6D-B5-D4	Adopter 19.6D.B5.D4 is no longer reach	Mon Jun 15 2015 09:30:47 AM

Figure 41: Access Point - AP Self Adoption History screen

The **AP Self Adoption History** screen describes the following historical data for adopted access points:

Event History	Displays the self adoption status of each access point as either *Adopted* or *un-adopted*.
MAC	Displays the hardware encoded *Media Access Control* (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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Pending Adoptions

"Adoption"

The *Pending Adoptions* screen displays a list of devices yet to be adopted to this peer access point, or access points in the process of adoption.

To view pending access point 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 the a RF Domain and select one of its connected access points.

3 Expand the Adoption menu item.

4 Select **Pending Adoptions**.

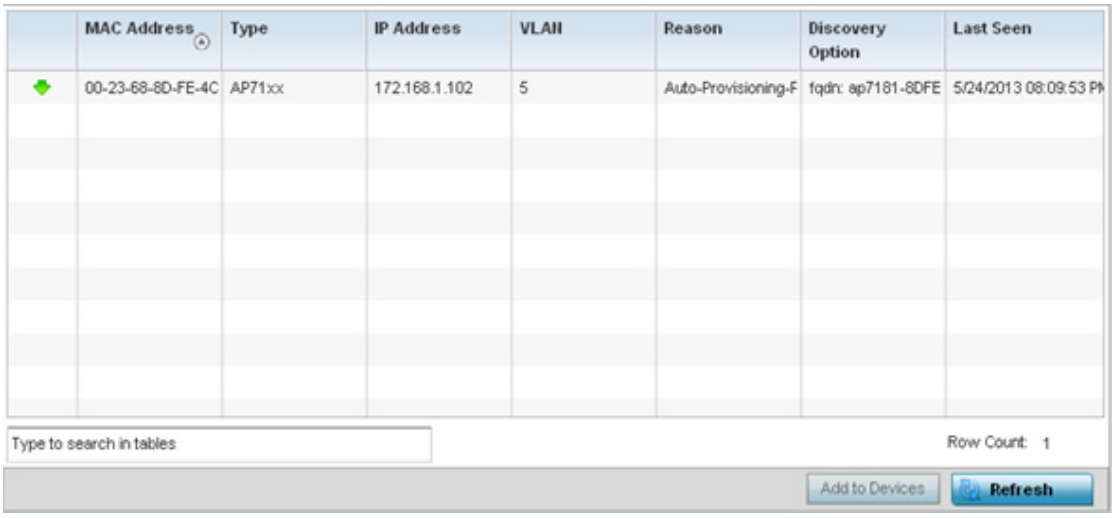


Figure 42: Access Point - Pending Adoptions screen

The **Pending Adoptions** screen provides the following:

MAC Address	Displays the MAC address of the device pending adoption.
Type	Displays the access point's model type.
IP Address	Displays the current network 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 access point 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

AP Detection

"Access Point Statistics"

The *AP Detection* screen displays potentially hostile access points, their SSIDs, reporting AP, and so on. Continuously revalidating 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select AP Detection.

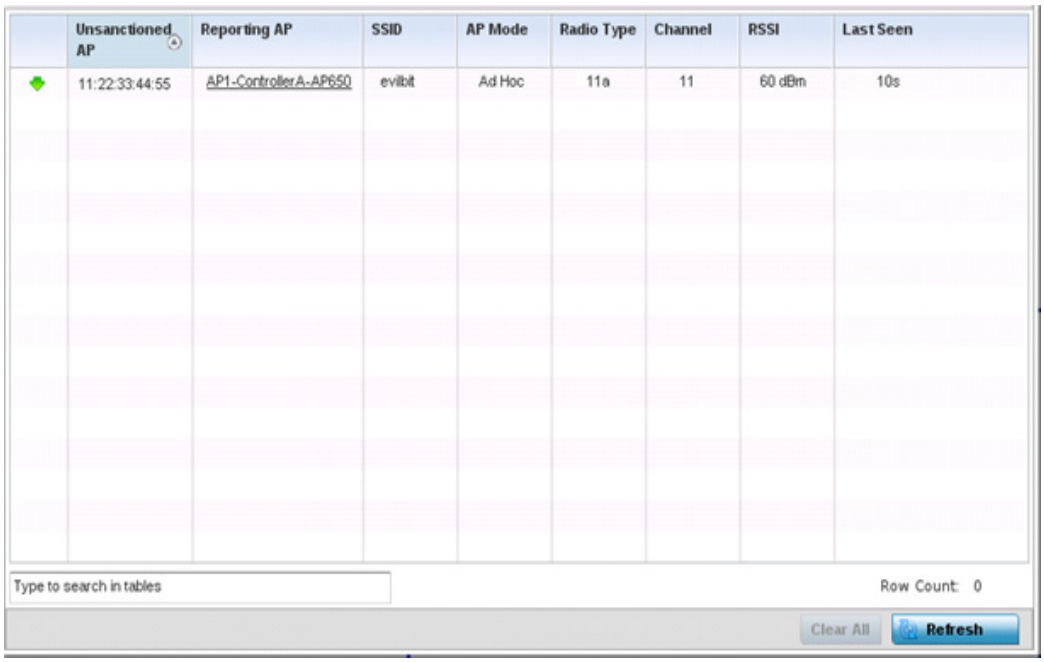


Figure 43: Access Point - AP Detection

The **AP Detection** screen displays the following:

Unsanctioned AP	Displays the MAC address of a detected access point that is 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.
RSSI	Lists a *relative signal strength indication* (RSSI) for a detected (and perhaps unsanctioned) access point.
Last Seen	Displays the time (in seconds) the unsanctioned access point was last seen on the network.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Guest User

"Access Point Statistics"

The *Guest User* 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.

To view guest user 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 a RF Domain and select one of its connected access points.

3 Select Guest User.

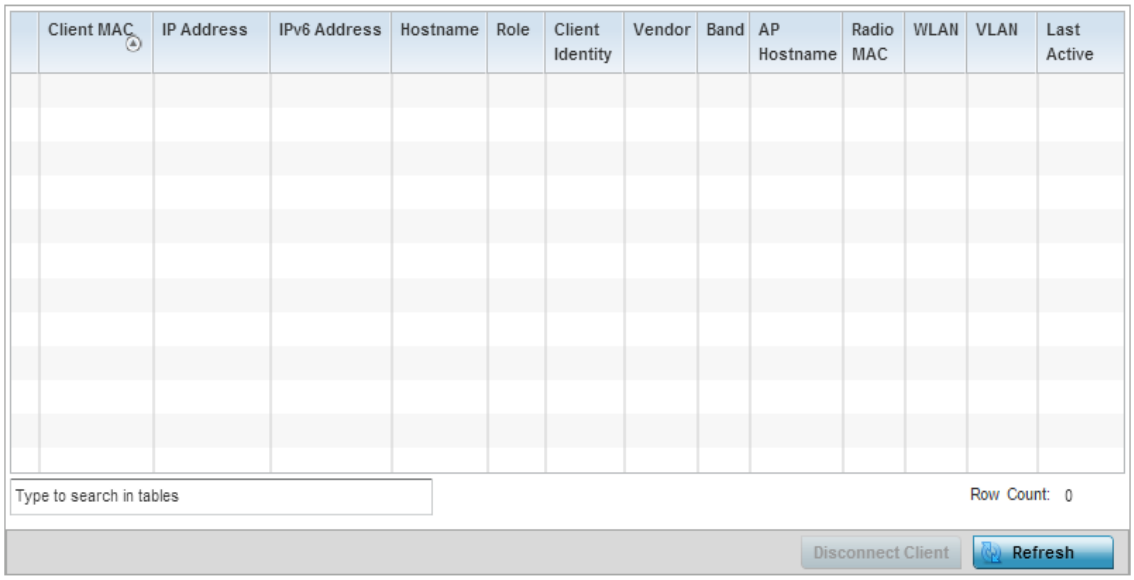


Figure 44: Access Point - Guest User screen

The *Guest User* screen displays the following client information:

Client MAC	Displays the hardcoded MAC address assigned to the guest client at the factory. The address displays as a link that can be selected to display 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 *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 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 access point managed network.
Client Identity	Displays the unique identity of the listed guest client as it appears to its adopting access point.

Vendor	Displays the name of the client vendor (manufacturer).
Band	Displays the 802.11 radio band on which the listed guest client operates.
AP Hostname	Displays the administrator assigned hostname of the access point to which this access point is adopted.
Radio MAC	Displays the MAC address of the radio which the wireless client is using.
WLAN	Displays the name of the WLAN the access point is using with each listed guest 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 guest client is currently mapped to as a virtual interface for access point interoperability.
Last Active	Displays the time when this guest client was last seen (or detected) by a device within the access point managed network.
Disconnect Client	Select a specific client MAC address and select the *Disconnect Client* button to terminate this client's connection to its access point.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Wireless Clients

"Access Point Statistics"

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.

To view wireless 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). Expand a RF Domain and select one of its connected access points.

3 Select Wireless Clients.

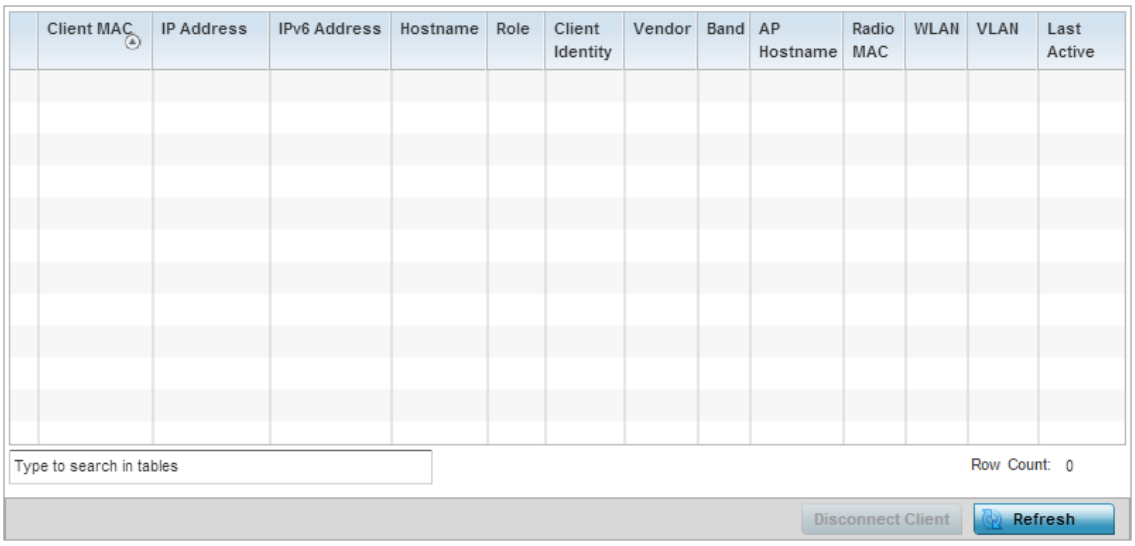


Figure 45: Access Point - Wireless Clients screen

The **Wireless Clients** screen displays the following:

Client MAC	Displays the hardcoded MAC address assigned to the client at the factory. The address displays as a link that can be selected to display 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 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 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 identity of the listed client as it appears to its adopting access point.
Vendor	Displays the name of the client vendor (manufacturer).
Band	Displays the 802.11 radio band on which the listed wireless client operates.
AP Hostname	Displays the administrator assigned hostname of the access point to which this access point is adopted.
Radio MAC	Displays the MAC address of the radio which the wireless client is using.

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 the time when this wireless client was last seen (or detected) by a device within the access point managed network.
Disconnect Client	Select a specific client MAC address and select the Disconnect Client button to terminate this client's connection to its access point.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Wireless LANs

"Access Point Statistics"

The *Wireless LANs* screen displays an overview of access point WLAN utilization. This screen displays access point WLAN assignment, SSIDs, traffic utilization, number of radios the access point is utilizing on the WLAN and transmit and receive statistics.

To review a selected access point's WLAN 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 a RF Domain and select one of its connected access points.

3 Select Wireless LANs.

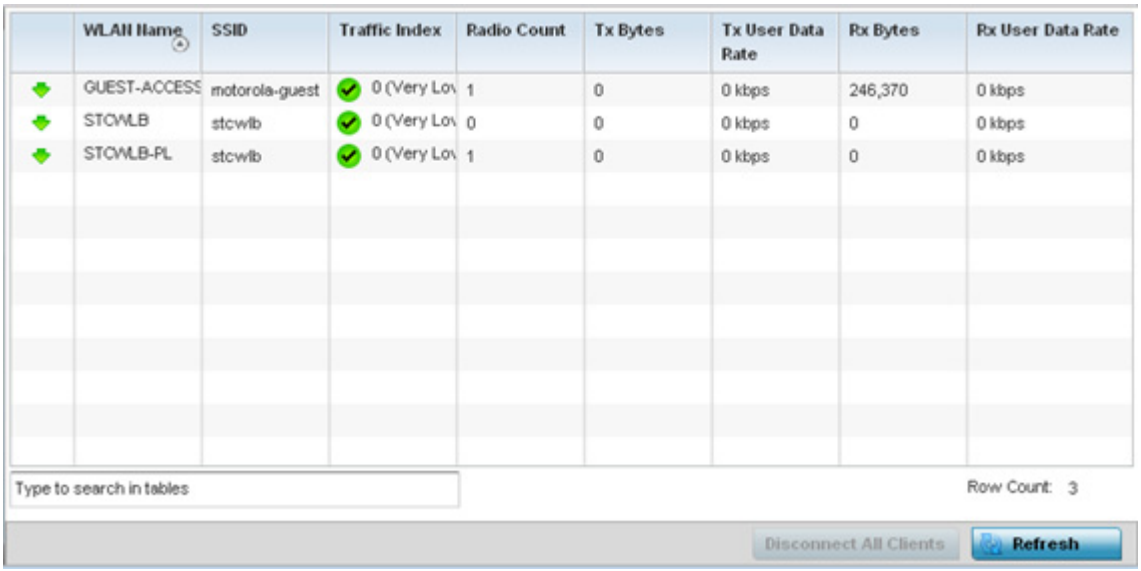


Figure 46: Access Point - Wireless LANs screen

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name of the WLAN the access point is currently using for client transmissions.
SSID	Displays each listed WLAN's *Service Set ID* (SSID) used as the WLAN's network identifier.
Traffic Index	Displays the traffic utilization index, which measures how efficiently the WLAN's traffic medium is used. It is defined as the percentage of current throughput relative to 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 cumulative number of peer access point radios deployed within each listed WLAN.
Tx Bytes	Displays the average number of transmitted bytes sent on each listed WLAN.
Tx User Data Rate	Displays the transmitted user data rate in kbps for each listed WLAN.
Rx Bytes	Displays the average number of packets in bytes received on each listed WLAN.
Rx User Data Rate	Displays the received user data rate on each listed WLAN.
Disconnect All Clients	Select an WLAN then *Disconnect All Clients* to terminate the client connections within that WLAN.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Policy Based Routing

"Access Point Statistics"

The *Policy Based Routing* statistics screen displays statistics for selective path packet redirection. 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 devices.

To review access point PBR 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 a RF Domain and select one of its connected access points.

3 Select Policy Based Routing.

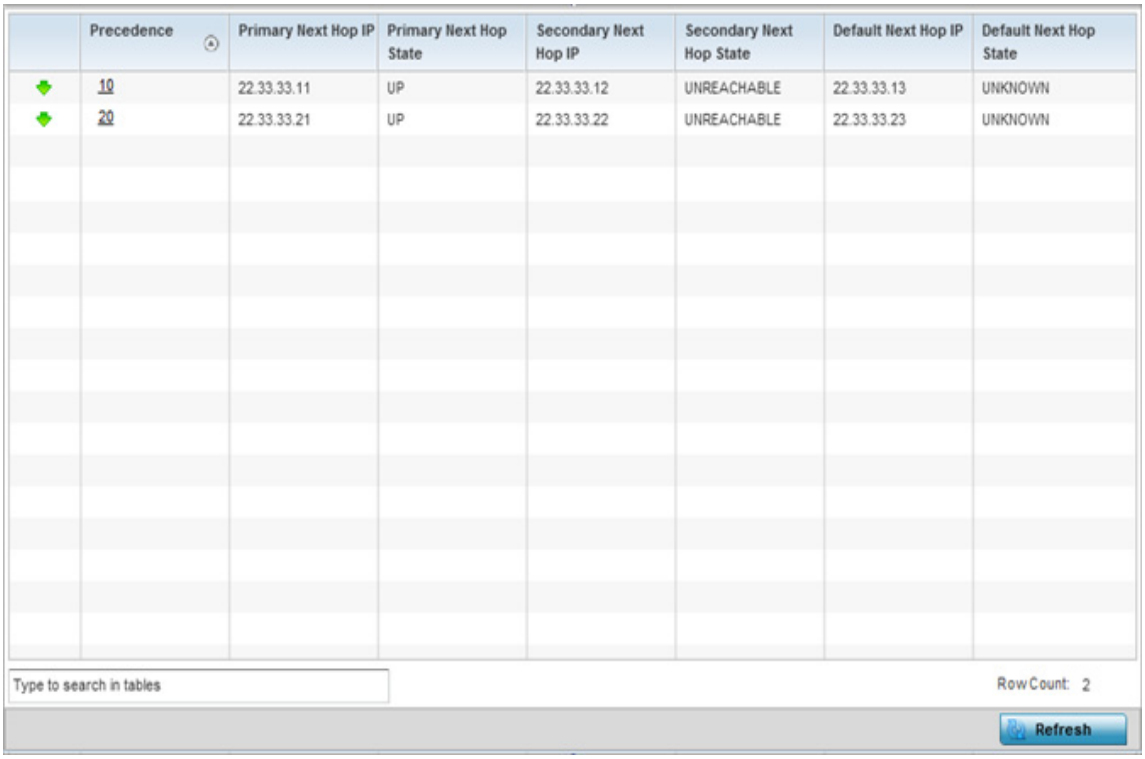


Figure 47: Access Point - Policy Based Routing screen

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 applied to incoming routed packets (UP/ UNREACHABLE).
Secondary Next Hop IP	If the primary hop is unavailable, a 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 applied to incoming routed packets (UP/ UNREACHABLE).
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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Radios

"Access Point Statistics"

The *Radio* statistics screens display information on access point radios. The actual number of radios depend on the access point model and type. This screen displays information on a per radio basis. Use this information to refine and optimize the performance of each radio and therefore improve network performance.

The access point's radio statistics screens provide details about associated radios. It provides radio ID, radio type, RF quality index etc. Use this information to assess the overall health of radio transmissions and access point placement. AP6532, AP6522, AP6562, AP71xx, AP8132 and AP8232 access points are dual radio models and AP6521 model is a single radio model.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- "Status"
- "RF Statistics"
- "Traffic Statistics"

Individual access point radios display as selectable links within each of the three access point radio screens. To review a radio's configuration in greater detail, select the link within the Radio column of either the *Status*, *RF Statistics* or *Traffic Statistics* screens.

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.

Status

"Radios"

Use the *Status* screen to review access point radio stats in detail. Use the screen to assess radio type, operational state, operating channel and current power to assess whether the radio is optimally configured.

To view access point radio 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 a RF Domain and select one of its connected access points.

3 Expand the **Radios** menu item.

4 Select **Status**.

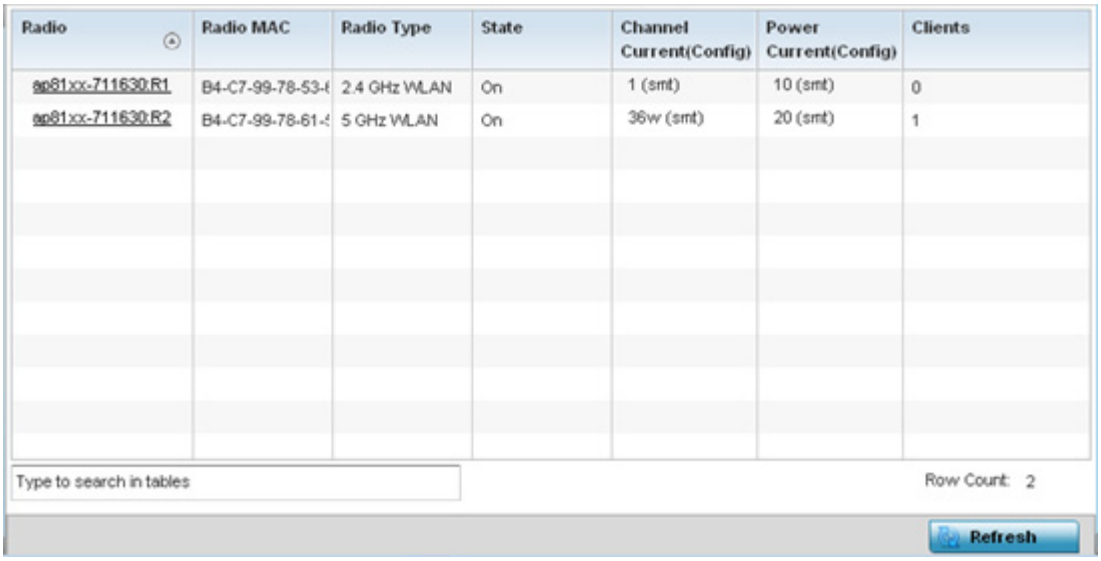


Figure 48: Access Point - Radio Status screen

The radio **Status** screen provides the following information:

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.
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.
Power Current (Config)	Displays the configured power each listed radio is using to transmit and receive.
Clients	Displays the number of connected clients currently utilizing the listed access point radio.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

RF Statistics

"Radios"

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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Expand the **Radios** menu item.

4 Select **RF Statistics**.

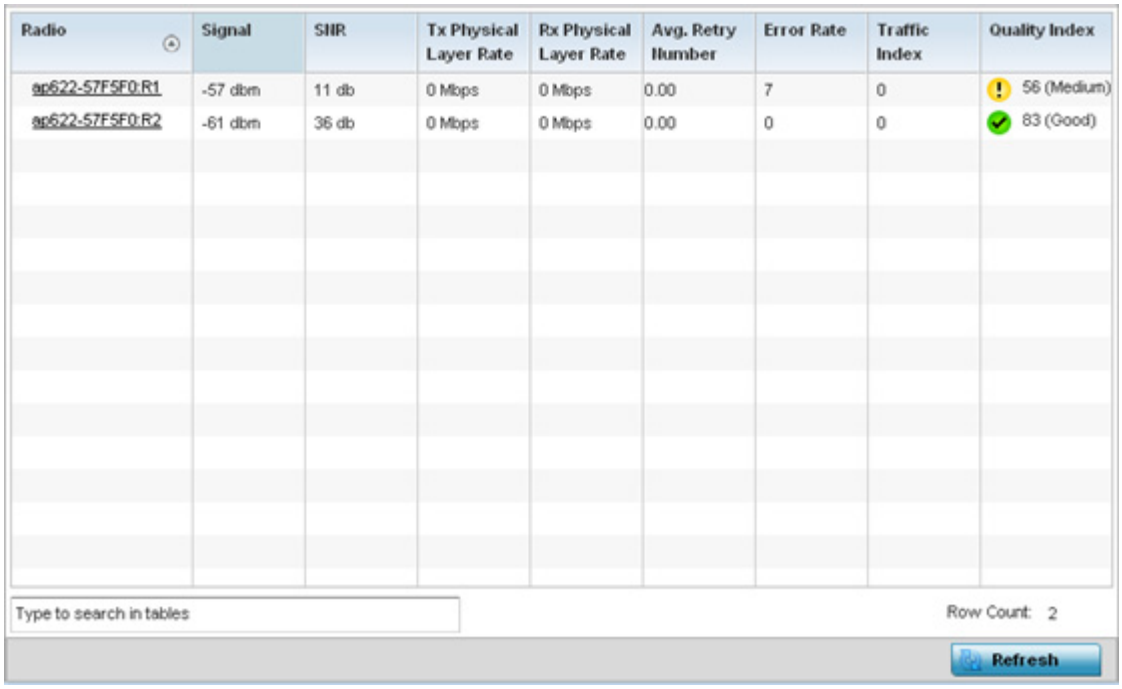


Figure 49: Access Point - Radio RF Statistics screen

The **RF Statistics** screen lists 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 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)
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Traffic Statistics

"Radios"

Refer to the *Traffic Statistics* screen to review access point radio transmit and receive statistics, data rate, and packets dropped during both transmit and receive operations.

To view the access point radio traffic 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 a RF Domain and select one of its connected access points.

3 Expand **Radios**.

4 Select **Traffic Statistics**.

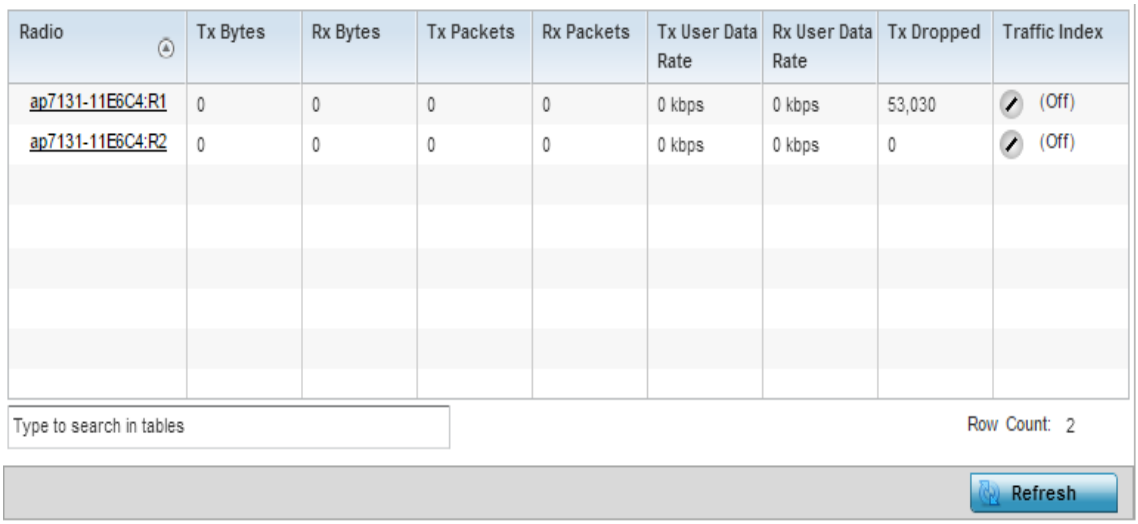


Figure 50: Access Point - Radio Traffic Statistics screen

The **Traffic Statistics** 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.
Traffic Index	Displays the traffic utilization index of each listed radio, which measures how efficiently the traffic medium is used. It is 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), and *60 and above* (high utilization).
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Mesh

"Access Point Statistics"

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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Mesh**.

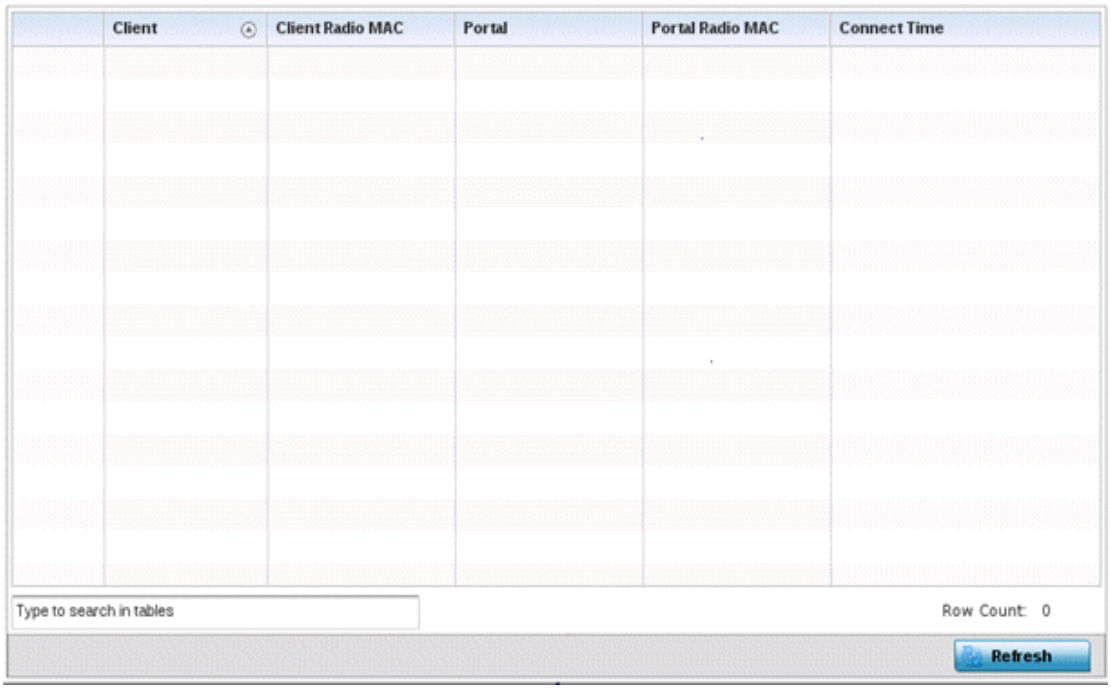


Figure 51: Access Point - Mesh screen

The **Mesh** screen describes the following:

Client	Displays the system assigned name of each member of the mesh network.
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 mesh portals.
Connect Time	Displays the elapsed connection time for each listed client in the mesh network.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Interfaces

"Access Point Statistics"

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.

To review access point interface 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 a RF Domain and select one of its connected access points.

3 Select Interfaces.

4 The General tab displays by default.

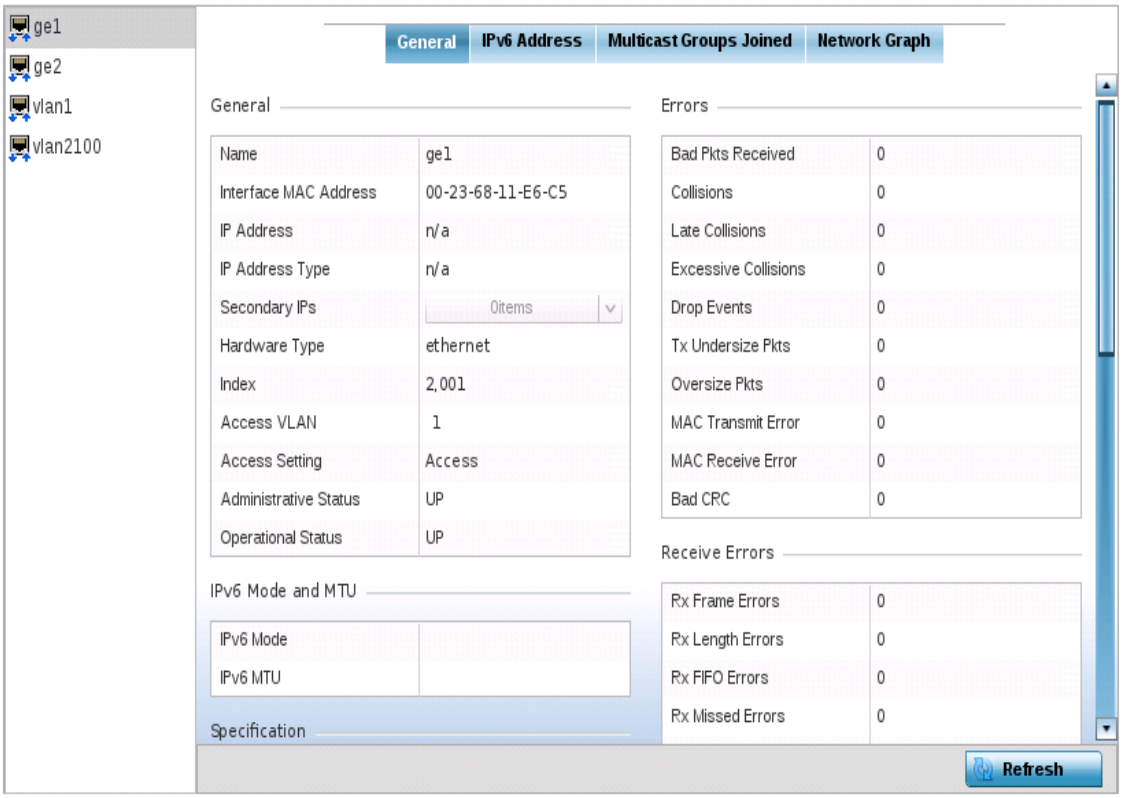


Figure 52: Access Point- General Interface screen

Interface Statistics support the following:

- "General Interface Details"
- "IPv6 Address"
- "Multicast Groups Joined"
- "Network Graph"

General Interface Details

"Interfaces"

The *General* tab provides information on a selected access point interface such as its MAC address, type and TX/RX statistics.

The **General** table displays the following:

Name	Displays the name of the access point interface *ge1*, *vlan1* etc.
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.
Access Setting	Displays the VLAN mode as either *Access* or *Trunk*.
Administrative Status	Displays whether the interface is currently *UP* or *DOWN*.
Operational Status	Displays whether the interface is currently operational. Indicate *UP* or *DOWN*.

The **IPv6 Mode and MTU** table displays the following information:

IPv6 Mode	Displays the IPv6 mode for this interface.
IPv6 MTU	Displays the IPv6 MTU value for 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	Lists whether traffic on the listed port is Layer 2 or Layer 3.
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:

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	Displays the number of good packets transmitted.
Good Pkts 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:

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	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 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:

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 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 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:

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. *First-in First-Out* (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.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

IPv6 Address

"Interfaces"

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 view controller or service platform IPv6 address utilization:

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 a RF Domain and select one of its connected access points.

3 Expand the Interfaces menu from the left-hand side of the UI.

4 Select IPv6 Address.

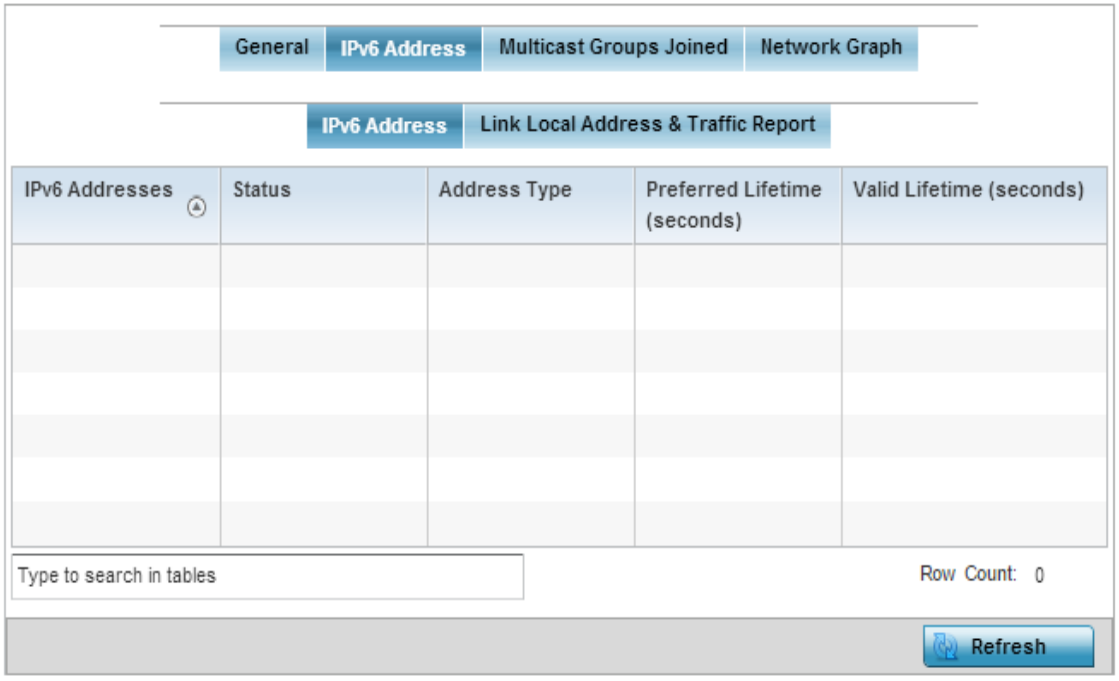


Figure 53: Access Point- Interface IPv6 Address screen

5 The **IPv6 Addresses** table displays the following:

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.

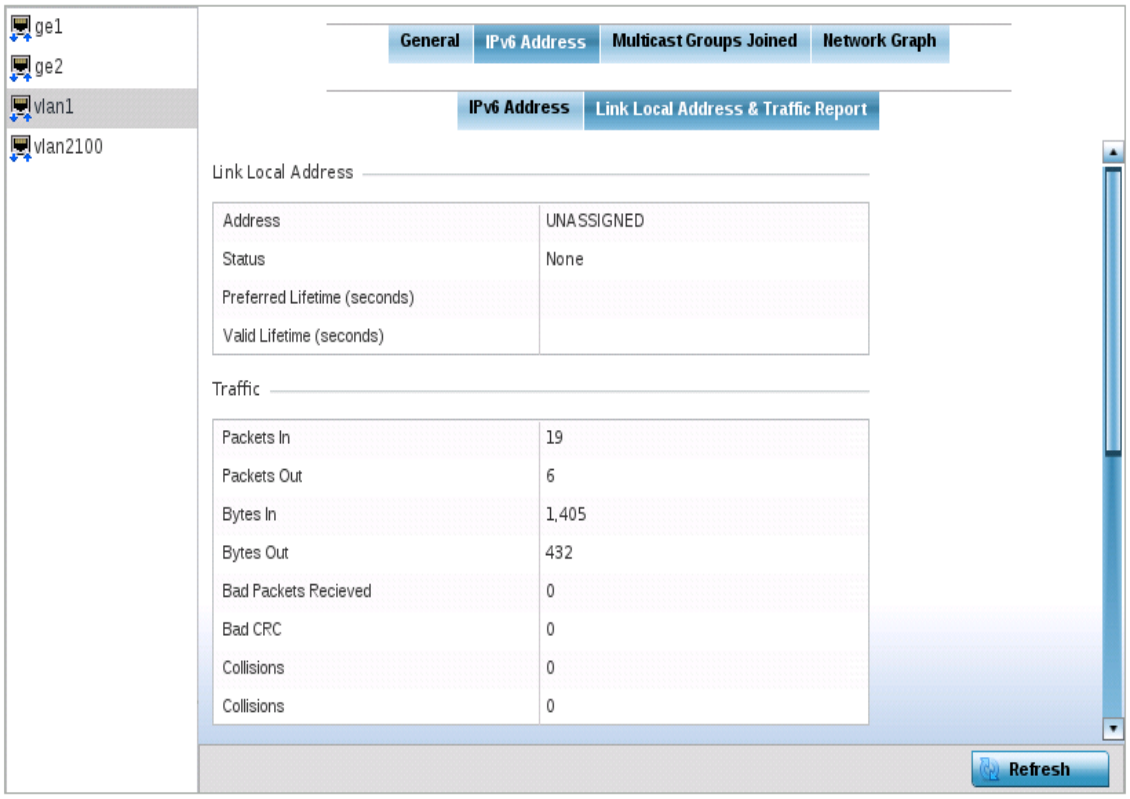


Figure 54: Access Point- Interface IPv6 Address - Link Local Address & Traffic Report screen

6 Verify the following **Link Local Address & Traffic data** data for the IPv6 address:

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.

7 Verify the following IPv6 **Traffic** data:

Packets In	Lists the number of IPv6 formatted data packets received on the selected interface since the screen was last refreshed.
Packets Out	Lists the number of IPv6 formatted data packets transmitted on the selected interface since the screen was last refreshed.
Bytes In	Lists the number of bytes received on the selected interface since the screen was last refreshed.
Bytes Out	Lists the number of bytes sent over the selected interface since the screen was last refreshed.
Bad Packets Received	Displays the number of bad packets received on the selected interface since the screen was last refreshed.
Bad CRC	Displays the number of packets with bad CRC received on the selected interface since the screen was last refreshed.
Collission	Displays the number of packet collisions detected on the selected interface since the screen was last refreshed.
Refresh	Periodically select *Refresh* to update the screen's counters to their latest values.

8 Verify the following IPv6 **Receive Errors** data:

Receive Length Errors	Displays the number of length errors in the received IPv6 packets on the selected interface since the screen was last refreshed.
Receive Over Errors	Displays the number of Receive Over errors on the selected interface since the screen was last refreshed.
Receive Frame Errors	Displays the number of Frame errors in the IPv6 packets received on the selected interface since the screen was last refreshed.
Receive FIFO Errors	Displays the number of FIFO errors in the IPv6 packets received on the selected interface since the screen was last refreshed.
Receive Missed Errors	Displays the number of missed packets received on the selected interface since the screen was last refreshed.

9 Verify the following IPv6 **Transmit Errors** data:

Transmit Errors	Displays the number of transmit errors in the packets sent on the selected interface since the screen was last refreshed.
Transmit Aborted Errors	Displays the number of transmit abort errors on the selected interface since the screen was last refreshed.
Transmit Carrier Errors	Displays the number of transmit carrier errors on the selected interface since the screen was last refreshed.
Transmit FIFO Errors	Displays the number of transmit FIFO errors on the selected interface since the screen was last refreshed.
Transmit Heartbeat Errors	Displays the number of transmit heartbeat errors on the selected interface since the screen was last refreshed.
Transmit Window Errors	Displays the number of transmit window errors on the selected interface since the screen was last refreshed.

Multicast Groups Joined

"Interfaces"

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.

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 view the controller or service platform multicast group memberships on the selected interface:

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 a RF Domain and select one of its connected access points.

3 Expand the Interfaces menu from the left-hand side of the UI.

4 Select Multicast Groups Joined.

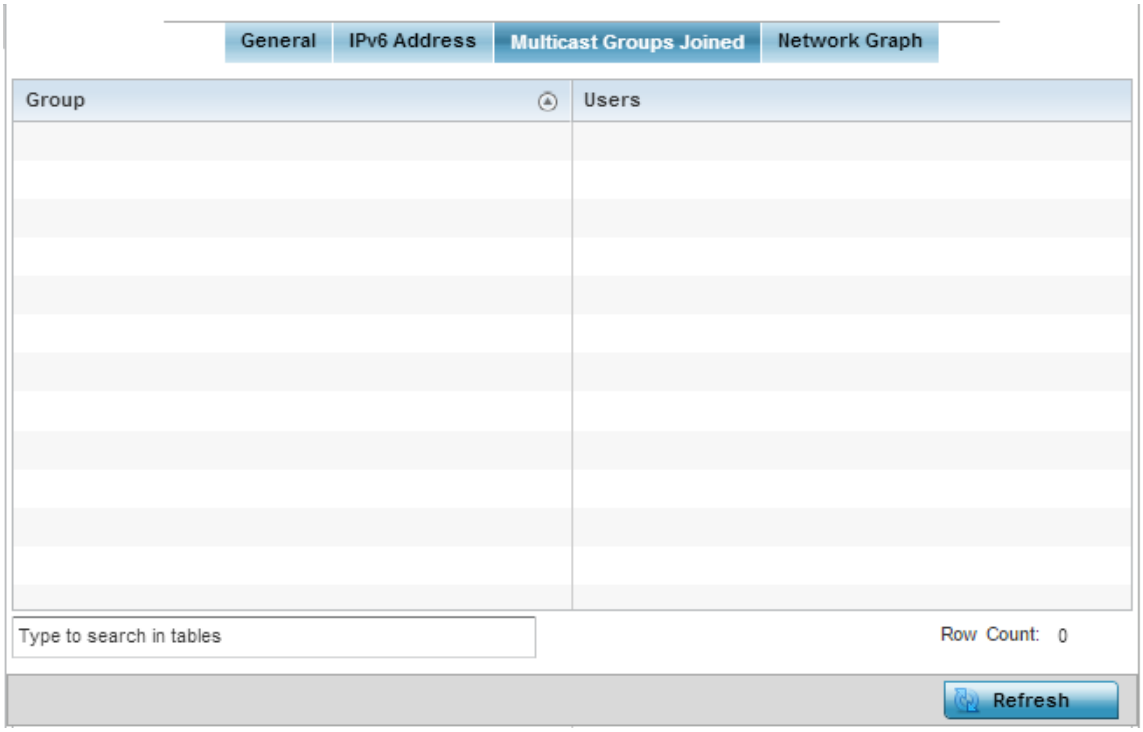


Figure 55: Access Point- Interface Multicast Groups Joined screen

5 The screen 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 select **Refresh** to update the screen's counters to their latest values.

Network Graph

"Interfaces"

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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select Interfaces.

4 Select Network Graph.

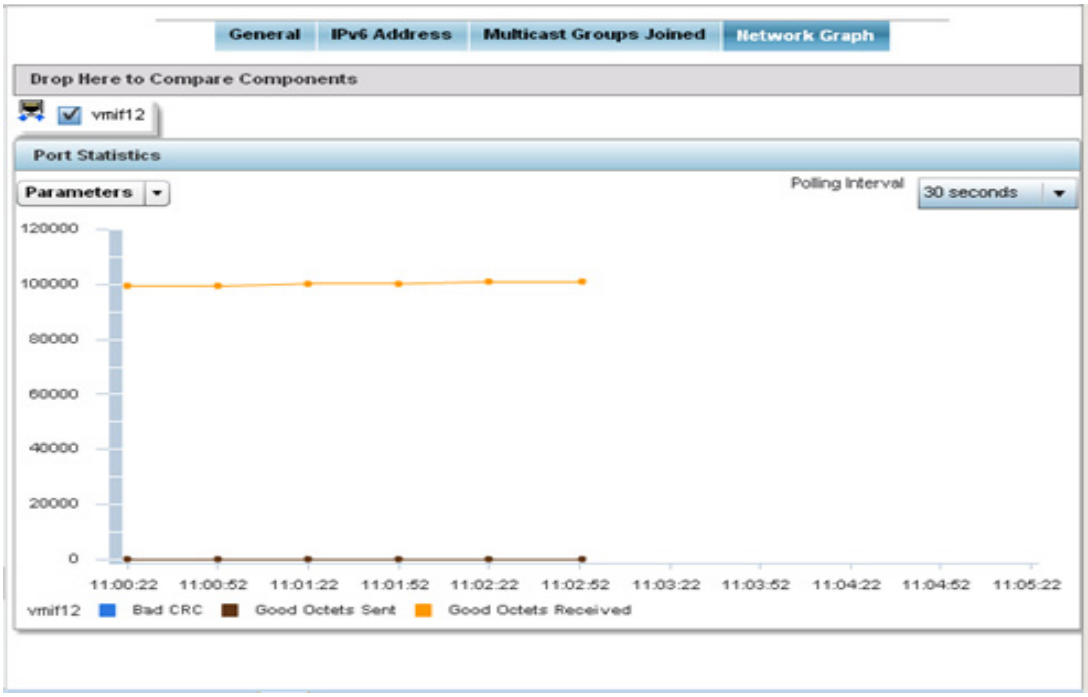


Figure 56: Access Point- Interface Network Graph screen

RTLS

"Access Point Statistics"

The *real time locationing system* (RTLS) 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select RTLS.

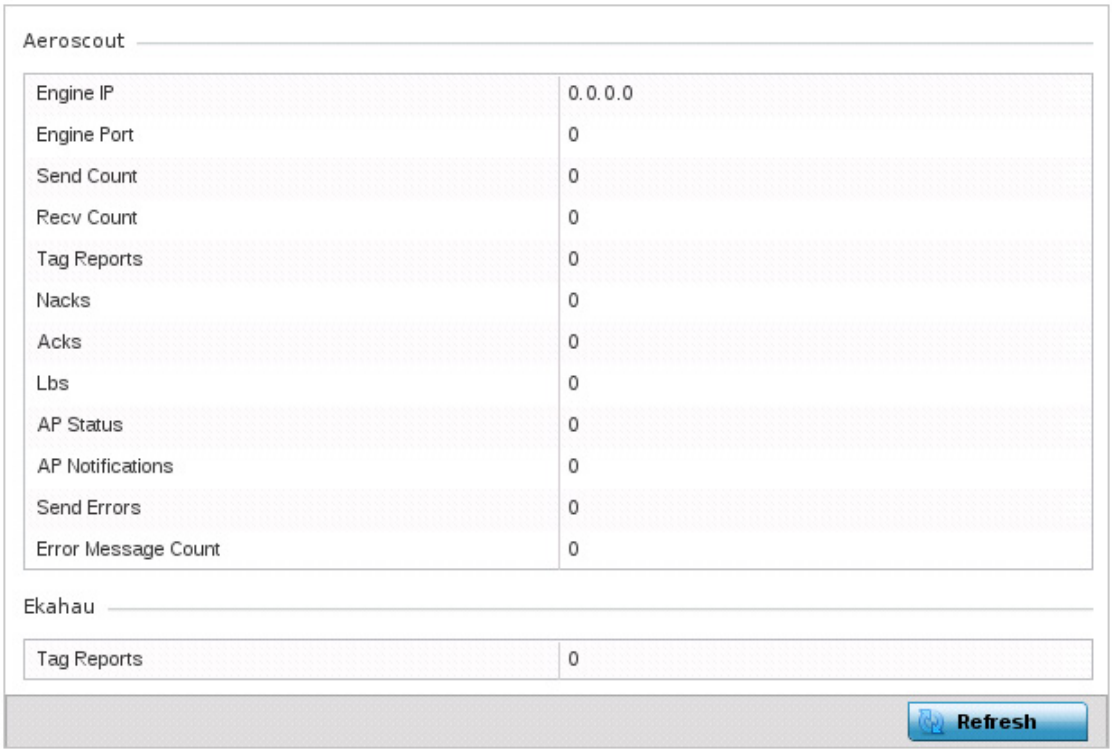


Figure 57: Access Point - RTLS screen

The access point **RTLS** screen displays the following for Aeroscout tags:

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 *location based service* (LBS) frames received from RTLS supported radio devices providing locationing services.
AP Status	Provides the status of peer access points 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.

The access point **RTLS** screen displays the following for Ekahau tags:

Tag Reports	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

PPPoE

"Access Point Statistics"

The *PPPoE* statistics screen displays stats derived from the AP'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 existing Ethernet interface.

To review a selected access point's PPPoE 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 a RF Domain and select one of its connected access points.

3 Select PPPoE.

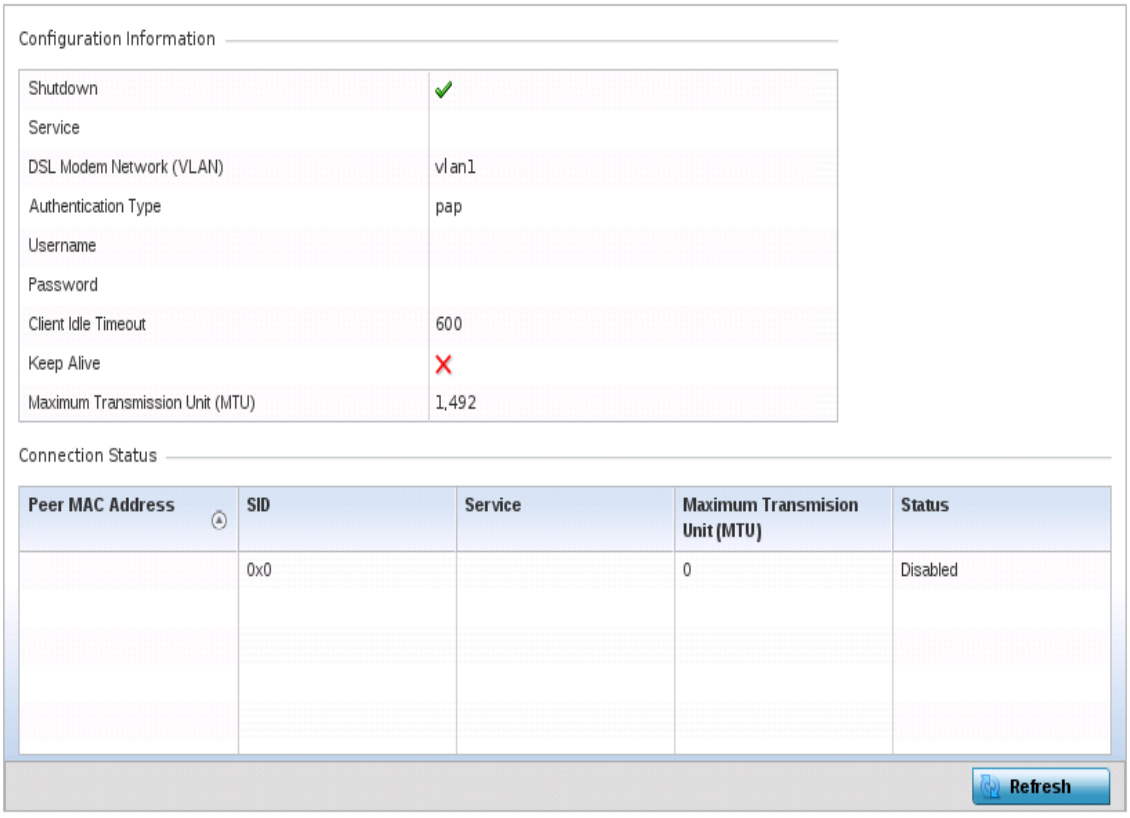


Figure 58: Access Point - PPPoE screen

The **Configuration Information** field screen displays the following:

Shutdown	Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol.
Service	Lists the 128 character maximum PPPoE client service name provided by the service provider.
DSL Modem Network (VLAN)	Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem.
Authentication Type	Lists authentication type used by the PPPoE client whose credentials must be shared by its peer access point. Supported authentication options include *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.
Username	Displays the 64 character maximum username used for authentication support by the PPPoE client.
Password	Displays the 64 character maximum password used for authentication by the PPPoE client.
Client Idle Timeout	The access point uses the listed timeout so it does not sit idle waiting for input from the PPPoE client and the server, that may never come.
Keep Alive	If a keep alive is utilized, the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
Maximum Transmission Unit (MTU)	Displays the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size.

4 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 the **Refresh** button to update the screen's statistics counters to their latest values.

Bluetooth

"Access Point Statistics"

AP8432 and AP8533 model access point radios 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 can raise an alarm.

AP8432 and AP8533 model access points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The access point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and 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 view Bluetooth radio utilization statistics for a selected Access Point and its connected 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 a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Bluetooth**.

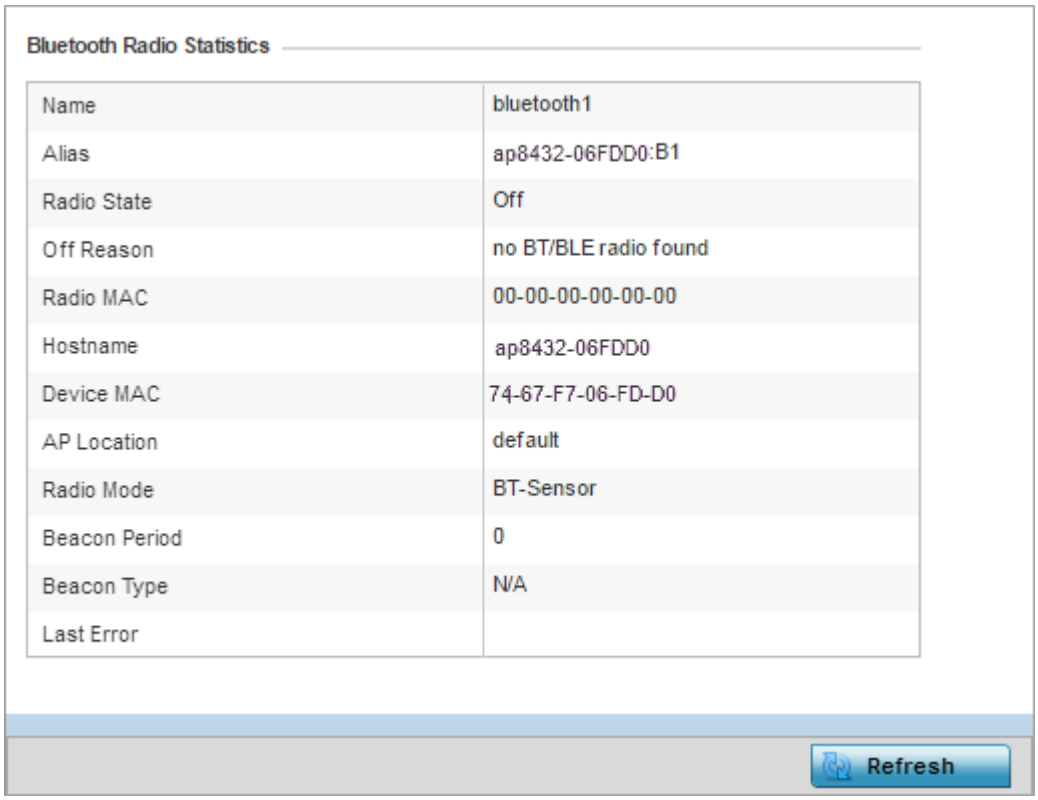


Figure 59: Access Point - Bluetooth screen

The access point's **Bluetooth** screen displays the following:

Name	Lists the administrator assigned name of the access point's Bluetooth radio.
Alias	If an alias has been defined for the access point, 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 access point, it is used in place of the access point's default hostname. 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.
Radio State	Displays the current operational state (On/Off) of the RF Domain member Bluetooth radio.
Off Reason	States an offline access point's reason for bluetooth radio inactivity within the RF Domain.
Radio MAC	Lists the Bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network.

Hostname	Lists the hostname set for the access point as its network identifier. Hostnames cannot include an underscore character.
Device MAC	Lists the access point's factory encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the access point and Bluetooth radio's administrator assigned deployment location.
Radio Mode	Lists an access point's Bluetooth radio functional mode as either *bt-sensor* or *le-beacon*.
Beacon Period	Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds.
Beacon Type	Lists whether this Bluetooth radio is utilizing *eddystone* or *ibeacons* for its RF emissions.
Last Error	Lists descriptive text on any error that is preventing the Bluetooth radio from operating.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

OSPF

"Access Point Statistics"

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.

Refer to the following for detailed descriptions of the tabs available within the OSPF statistics screen:

- "OSPF Summary"
- "OSPF Neighbors"
- "OSPF Area Details"
- "OSPF Route Statistics"
- "OSPF Interface"
- "OSPF State"

OSPF Summary

"OSPF"

To view OSPF summary 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 the default node and select an access point for statistical observation.

3 Select OSPF. The *Summary* tab displays by default.

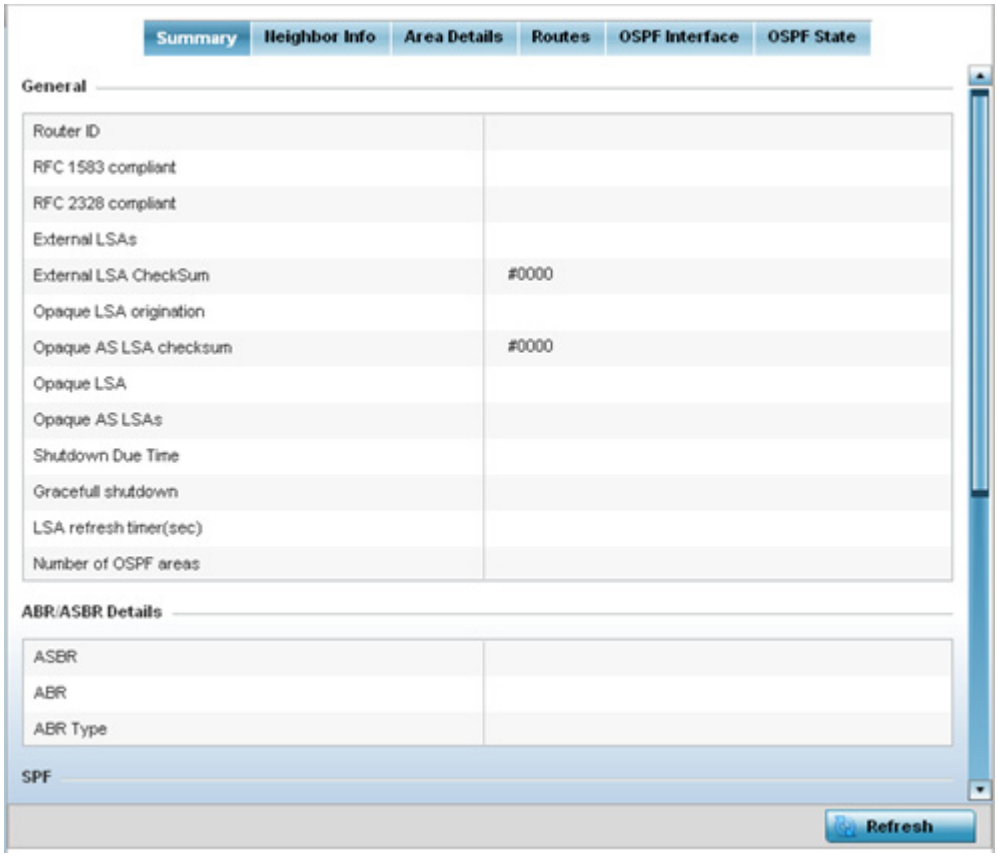


Figure 60: Access Point - OSPF Summary tab

The **Summary** tab 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 *Link-State Advertisement* (LSA) 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 *Autonomous System Boundary Router* (ASBR) data relevant to OSPF routing, including the ASBR, ABR and ABR type. An *Area Border Router* (ABR) 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 *shortest path forwarding* (SPF) *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.

4 Select the **Refresh** button to update the statistics counters to their latest values.

OSPF Neighbors

"OSPF"

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 Select System from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.

3 Select OSPF.

4 Select the **Neighbor Info** tab.

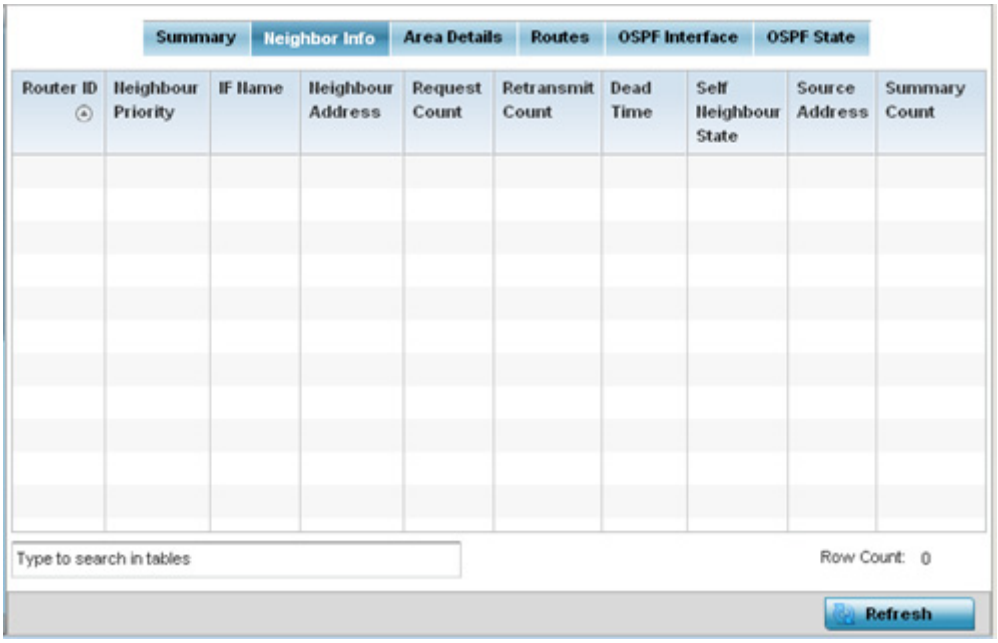


Figure 61: Access Point - OSPF Neighbor Info tab

The **Neighbor Info** tab 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 *designated router* (DR) 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.

5 Select the **Refresh** button to update the statistics counters to their latest values.

OSPF Area Details

"OSPF"

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 *Link State Advertisements* (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 Select System from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.

3 Select OSPF.

4 Select the **Area Details** tab.

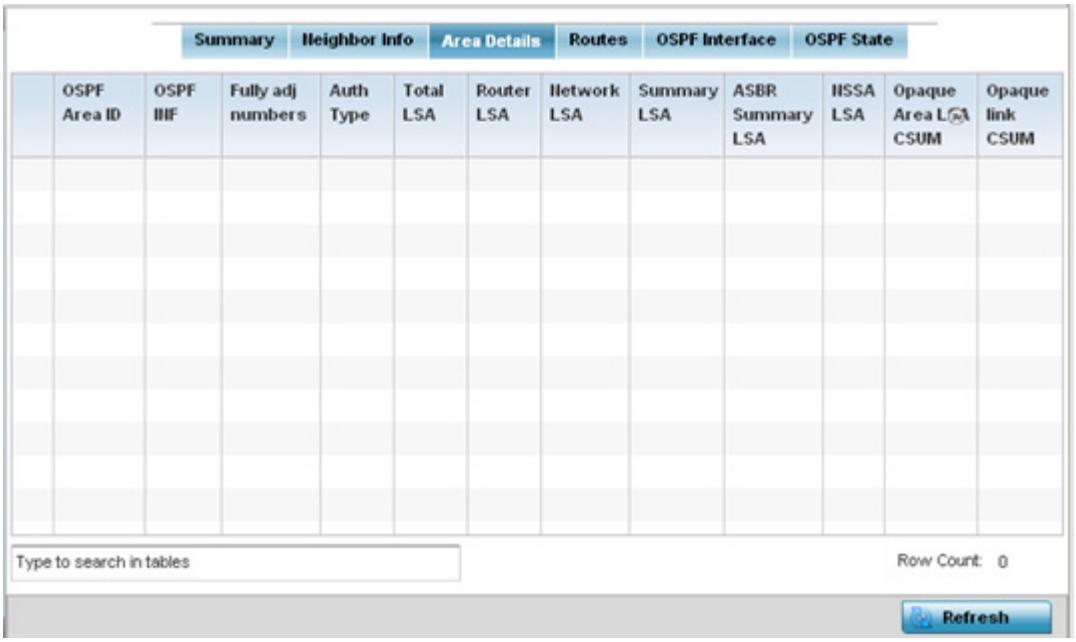


Figure 62: Access Point - OSPF Area Details tab

The **Area Details** tab 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 *Link State Advertisements* (LSAs) 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 LSA 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 the Type-10 opaque link checksum with the complete contents of the LSA.

5 Select the **Refresh** button to update the statistics counters to their latest values.

OSPF Route Statistics

"OSPF"

Refer to the *Routes* tab to assess the status of OSPF *Border Routes, External Routes*, *Network Routes* and *Router Routes*.

To view OSPF route 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 the default node and select an access point for statistical observation.

3 Select OSPF.

4 Select the **Routes** tab. Border Routers tab display by default.

An *area border router* (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 *Autonomous System Boundary Router* (ASBR). Border routers maintain an LSDB for each area supported. They also participate in the backbone.

5 Refer to **External Routes** tab.

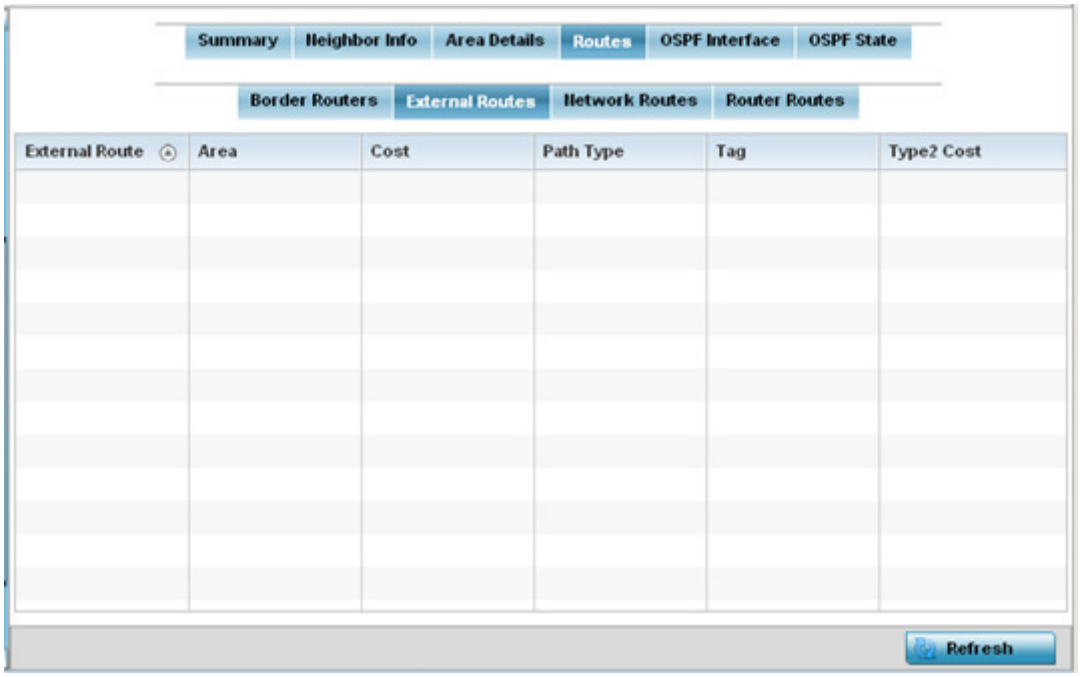


Figure 63: Access Point - OSPF External Routes tab

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 Routes** 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 Refer to the **Network Routes** tab.

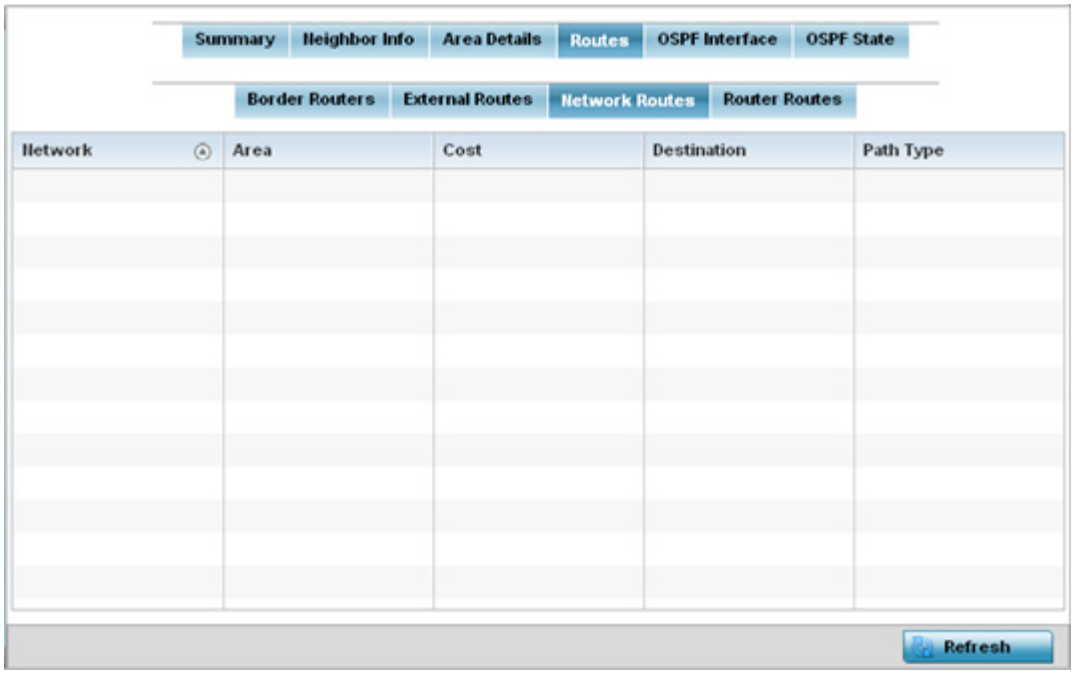


Figure 64: Access Point - OSPF Network Routes tab

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 Routes** tab displays the network name, impacted OSPF area, cost, destination and path type.

7 Select the **Router Routes** tab.

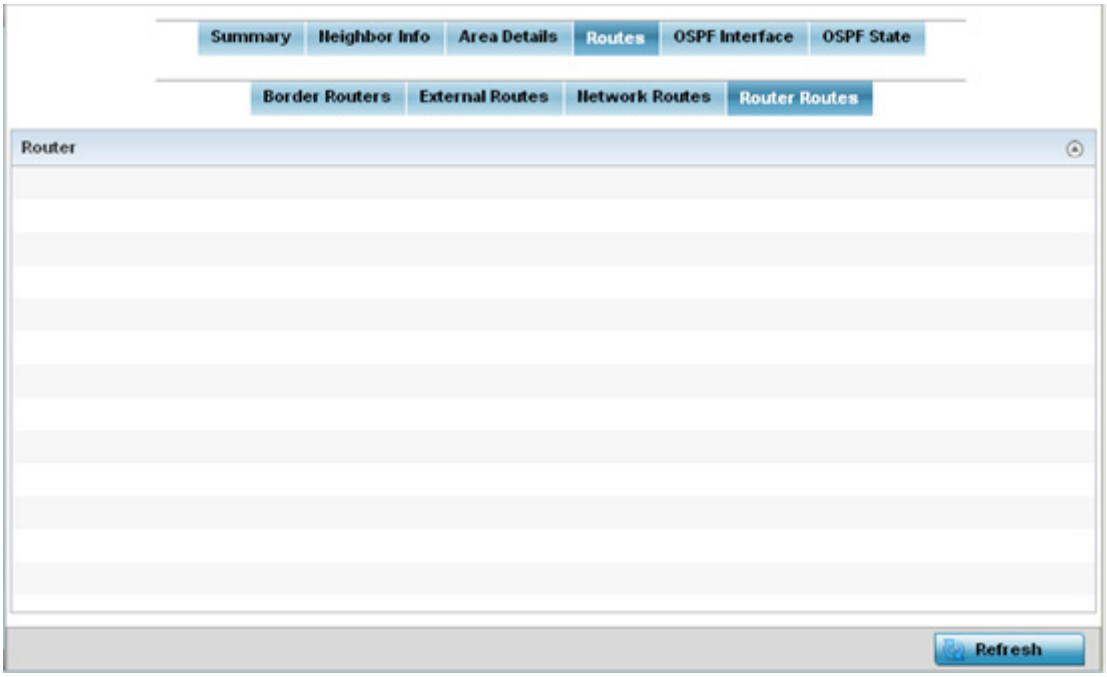


Figure 65: Access Point - OSPF Router Routes tab

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.

8 Select the **Refresh** button (within any of the four OSPF Routes tabs) to update the statistics counters to their latest values.

OSPF Interface

"OSPF"

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 Select System from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.

3 Select OSPF.

4 Select the **OSPF Interface** tab.

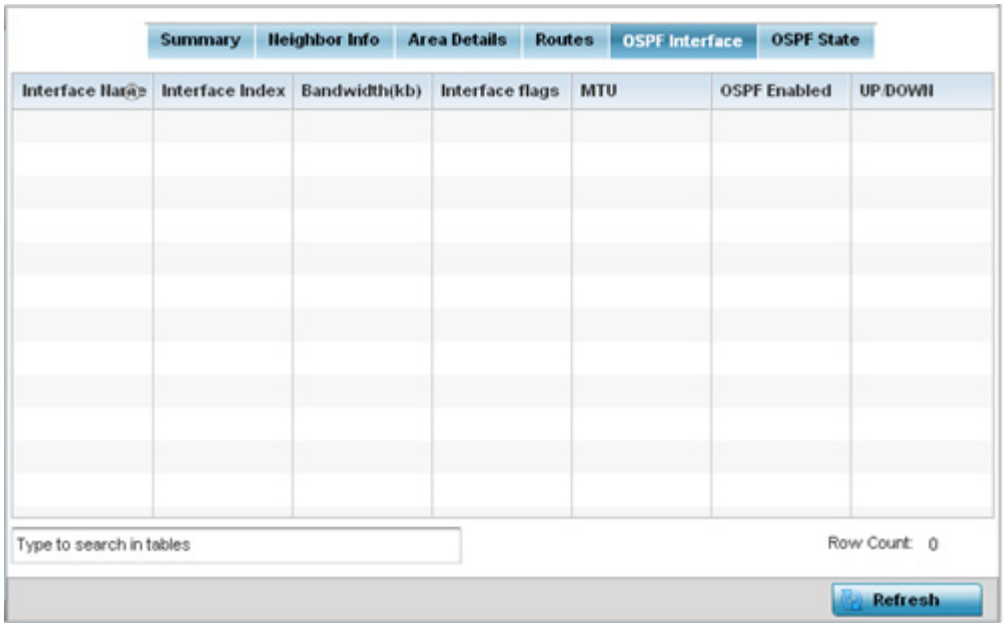


Figure 66: Access Point - OSPF Interface tab

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 (kb)	Lists the OSPF interface bandwidth (in Kbps) in the range of 1 - 10,000,000.
Interface flags	Displays the flag used to determine the interface status.
MTU	Lists the OSPF interface *maximum transmission unit* (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.

5 Select the **Refresh** button to update the statistics counters to their latest values.

OSPF State

"OSPF"

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 is periodically updated on all OSPF members. The access point 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 Select System from the navigation pane (on the left-hand side of the screen), expand the default node and select an access point for statistical observation.

3 Select OSPF.

4 Select the **OSPF State** tab.

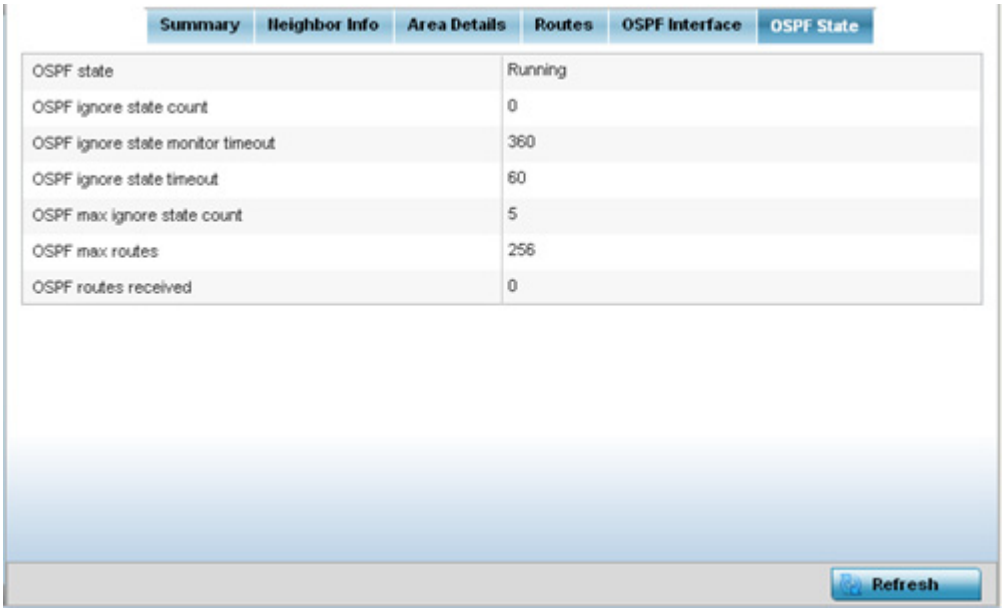


Figure 67: Access Point OSPF - State tab

The **OSPF State** tab describes the following:

OSPF state	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a *link-state database* (LSDB) 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 the access point from detecting changes to the OSPF link state.
OSPF ignore state timeout	Displays the timeout value that the access point remains in the ignore 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.

5 Select the **Refresh** button to update the statistics counters to their latest values.

L2TPv3 Tunnels

"Access Point Statistics"

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 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select L2TPv3.

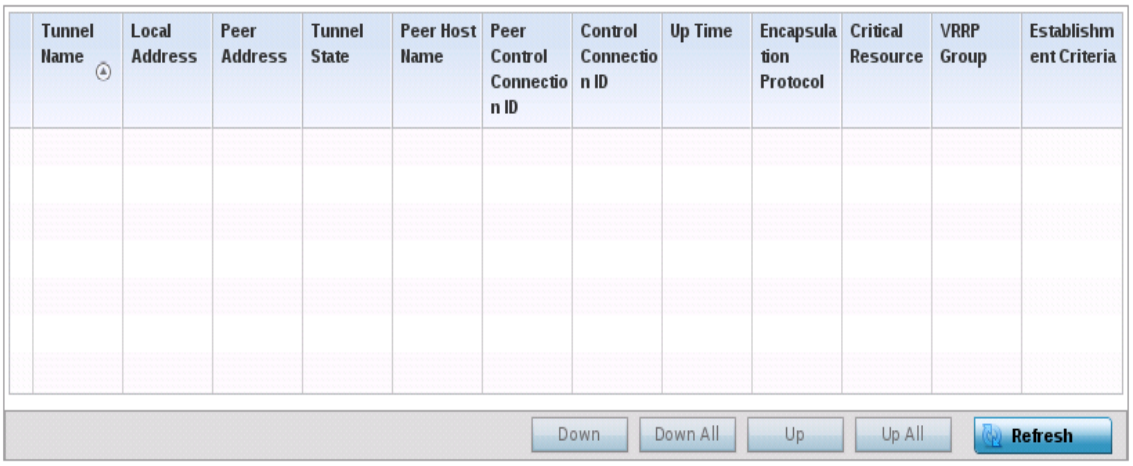


Figure 68: Access Point - L2TPv3 screen

The access point **L2TPv3 Tunnels** 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 pseudowire 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.
Peer	Displays the Peer number. For fast failover, up to two (2) peers can be specified with which the access point can form tunnels. The access point tries to form a tunnel with the peer specified with the peer number 1 first and if this peer is not reachable, tries to form a tunnel with peer 2. This field displays the peer number for the tunnel peer.
Tunnel State	States whether the tunnel is idle (not utilized by peers) or is currently active.
Tunnel Mode	Displays the active/standby state for the tunnel.
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. 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 is a connectivity issue, an event is generated stating a critical resource is unavailable.
VRRP Group	Displays the VRRP group name if configured. VRRP configurations support router redundancy in a wireless network requiring high availability
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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

VRRP

"Access Point Statistics"

The *VRRP* statistics screen displays *Virtual Router Redundancy Protocol* (VRRP) 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select VRRP.

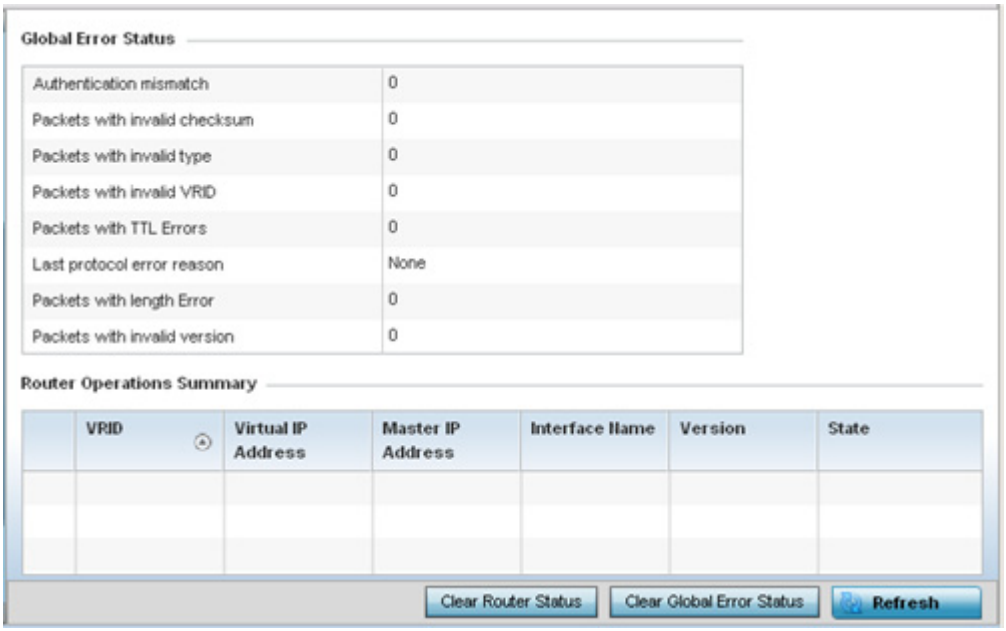


Figure 69: Access Point - VRRP screen

4 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.

5 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 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 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.
Clear Router Status	Select the *Clear Router Status* button to clear the Router Operations Summary table values to zero and begin new data collections.
Clear Global Error Status	Select the *Clear Global Error Status* button to clear the Global Error Status table values to zero and begin new data collections.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Critical Resources

"Access Point Statistics"

The *Critical Resources* statistics screen displays a list of 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 managed access points. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. Thus, 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select Critical Resources.

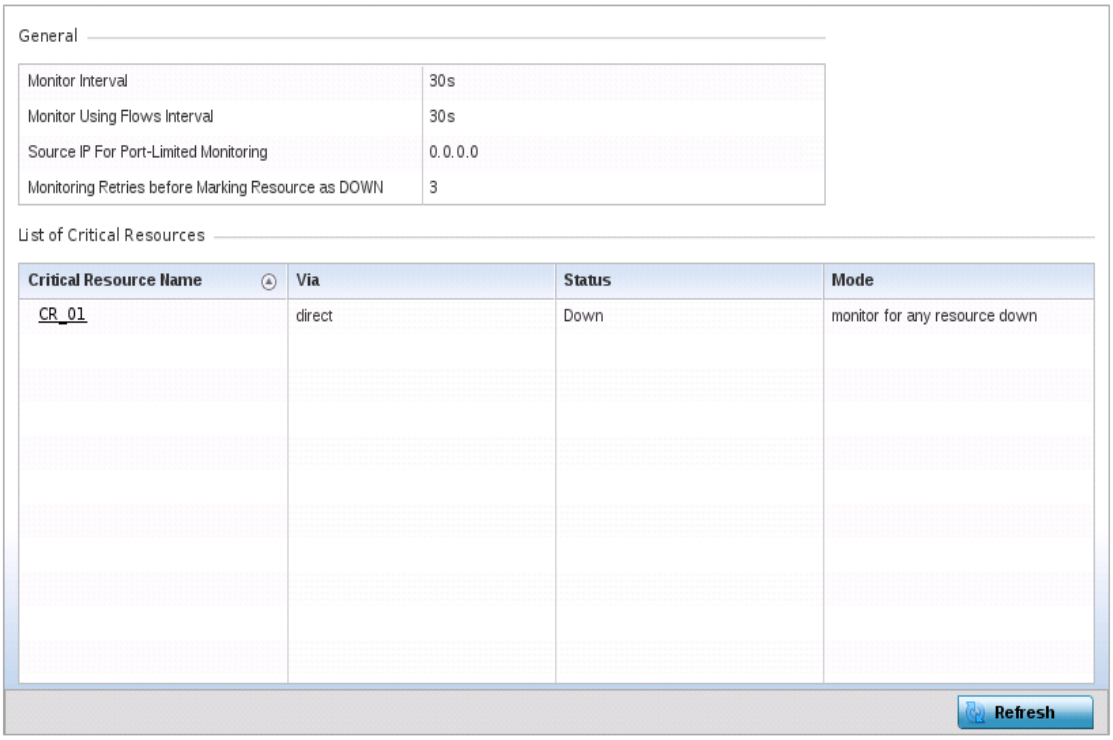


Figure 70: Access Point - Critical Resources screen

4 Refer to the **General** field to assess the **Monitor Interval** and **Monitor Using Flows Interval** used to poll for updates from critical resources and the **Source IP For Port-Limited Monitoring** of critical resources. **Monitoring Retries before Marking Resource as DOWN** are the number of retry connection attempts permitted before this listed resource is defined as down (offline).

The access point **Critical Resource** screen displays the following:

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 is 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 critical resource 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 (either *Up* or *Down*).
Error Reason	Provides an error status as to why the critical resource is not available over its designated VLAN.
Mode	Displays the operational mode of each listed critical resource.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

LDAP Agent Status

"Access Point Statistics"

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.

AP6521 model access point does not support this feature in Standalone AP or Controller AP mode. However, AP6521 model is supported when adopted and managed by a controller or service platform.

For more information on setting LDAP agents as part of the RADIUS server policy, see "Configuring the RADIUS Server" on page 811.

To view access point LDAP agent statistics:

1 Select the Statistics menu from the Web UI."Configuring the RADIUS Server"

2 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select LDAP Agent Status.

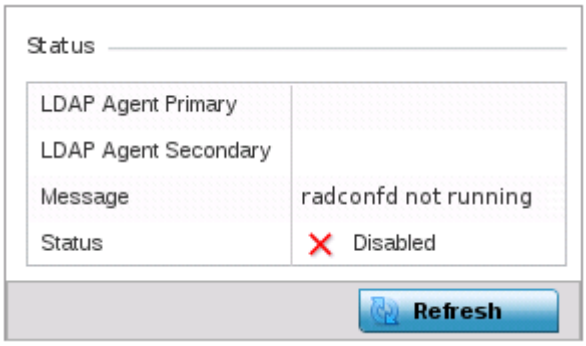


Figure 71: Access Point - LDAP Agent Status screen

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 access point 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 access point 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 access point's connection with the primary or secondary LDAP agent. If there is a problem with the username and password used to connection to the LDAP agent, it would be listed here.
Status	Displays whether the access point has successfully joined the remote LDAP server domain designated to externally validate PEAP-MS-CHAP v2 authentication requests.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Mint Links

"Access Point Statistics"

Wireless controllers and access points use the MiNT protocol as the primary means of device discovery and communication for access point 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 access points during adoption using MLCP (*MiNT Link Creation Protocol*). They can also be manually created between a controller and access point (or) between access points. 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 access points. Level 2 MiNT links also provide partitioning, between access points deployed at various remote sites.

To view an access point's Mint links:

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 a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select Mint Links from the left-hand side of the UI.

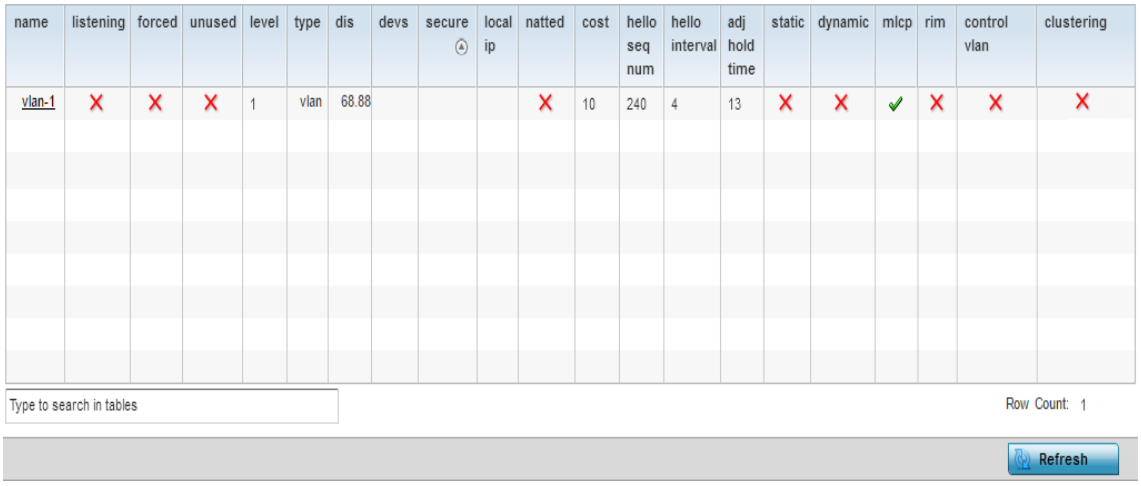


Figure 72: Access Point - MiNT Links screen

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* defines the cost for a packet to travel from its originating port to its end point destination.

The *hello seq number* and *hello interval* 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.

4 Periodically select **Refresh** to update the screen's data counters to their latest values.

5 If needed, select a Mint link from the *name* column to display more granular information for that link.

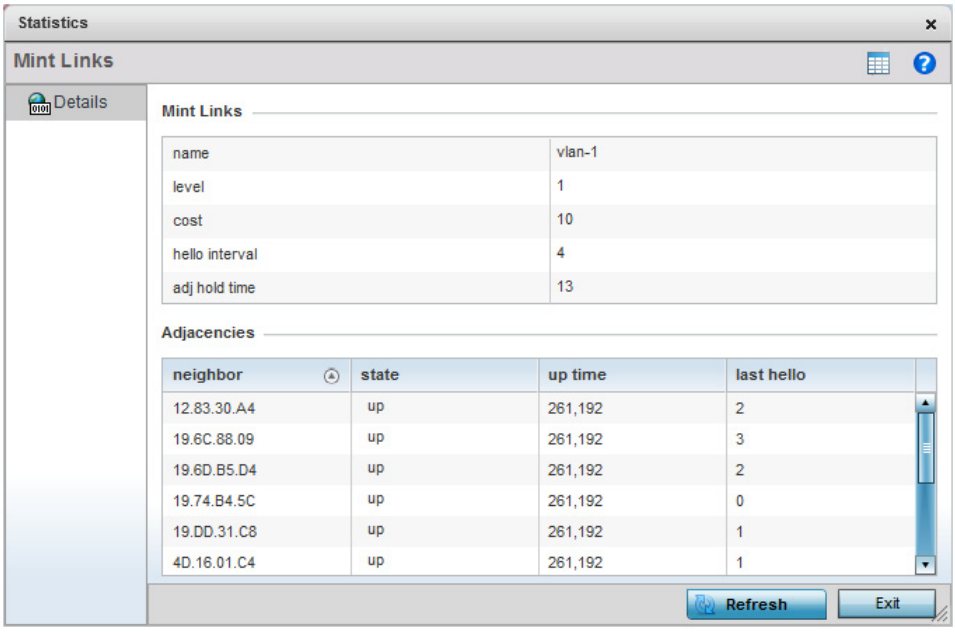


Figure 73: Access Point - Mint Link Details screen

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 statistics counters to their latest values.

Guest Users

"Access Point Statistics"

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.

To view the controller or service platform guest user utilization:

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 a RF Domain and select one of its connected access points.

3 Select Guest Users from the left-hand side of the UI.

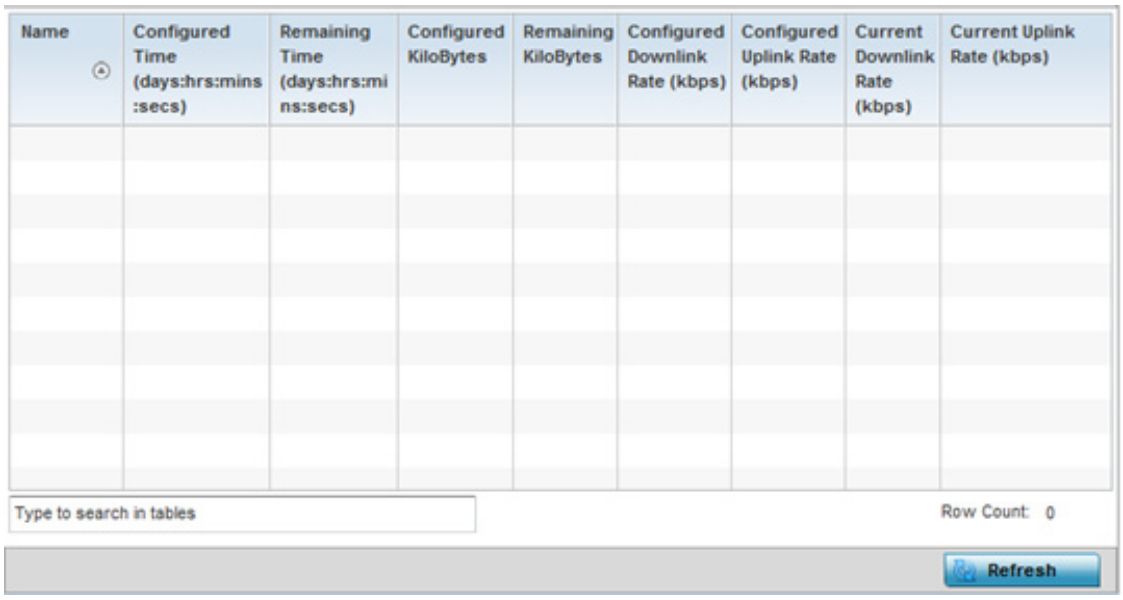


Figure 74: Access Point - Guest Users screen

The **Guest Users** 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 time each listed client was initially configured for (in days:hrs:mins:secs format) in their captive portal session.
Remaining Time (days:hrs:mins:secs)	Displays the time each listed client has remaining (in days:hrs:mins:secs format) in their captive portal session.
Configured KiloBytes	If the user does not have a bandwidth based voucher, the time configured and remaining are labeled as unlimited.
Remaining KiloBytes	If the user does not have a bandwidth based voucher, the time configured and remaining are labeled as unlimited.
Configured Downlink Rate (kbps)	If the user does not have a bandwidth based voucher, the time configured and remaining are labeled as unlimited.
Configured Uplink Rate (kbps)	If the user does not have a bandwidth based voucher, the time configured and remaining are labeled as unlimited.
Current Downlink Rate (kbps)	Displays the current download rate for the guest user in Kilobytes per seconds. This value should not exceed the configured downlink rate.
Current Uplink Rate (kbps)	Displays the current upload rate for the guest user in Kilobytes per seconds. This value should not exceed the configured uplink rate.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

GRE Tunnels

"Access Point Statistics"

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.

To review a selected access point's GRE 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 a RF Domain and select one of its connected access points.

3 Select GRE Tunnels.

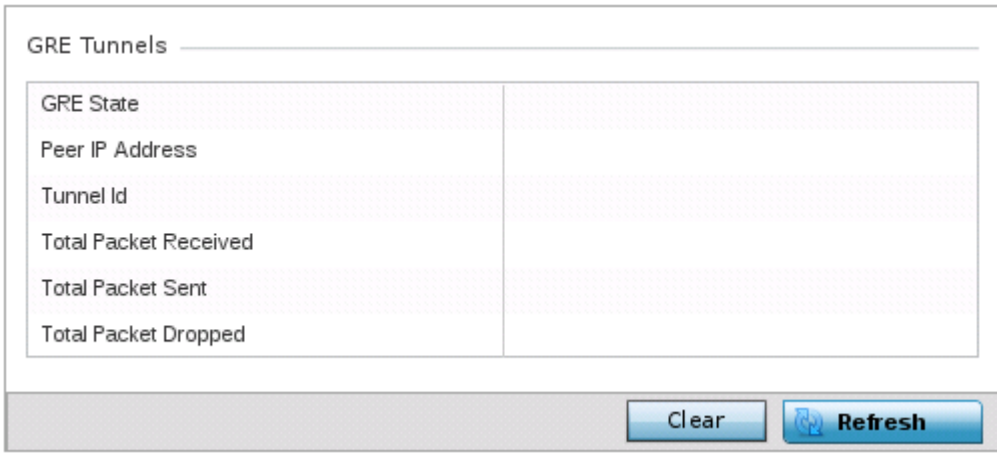


Figure 75: Access Point - GRE Tunnels screen

The access point **GRE Tunnels** screen displays 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.
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 access point 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 access point and a peer at the remote end of the VPN tunnel
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

Dot1x

"Access Point Statistics"

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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select Dot1x from the left-hand side of the UI.

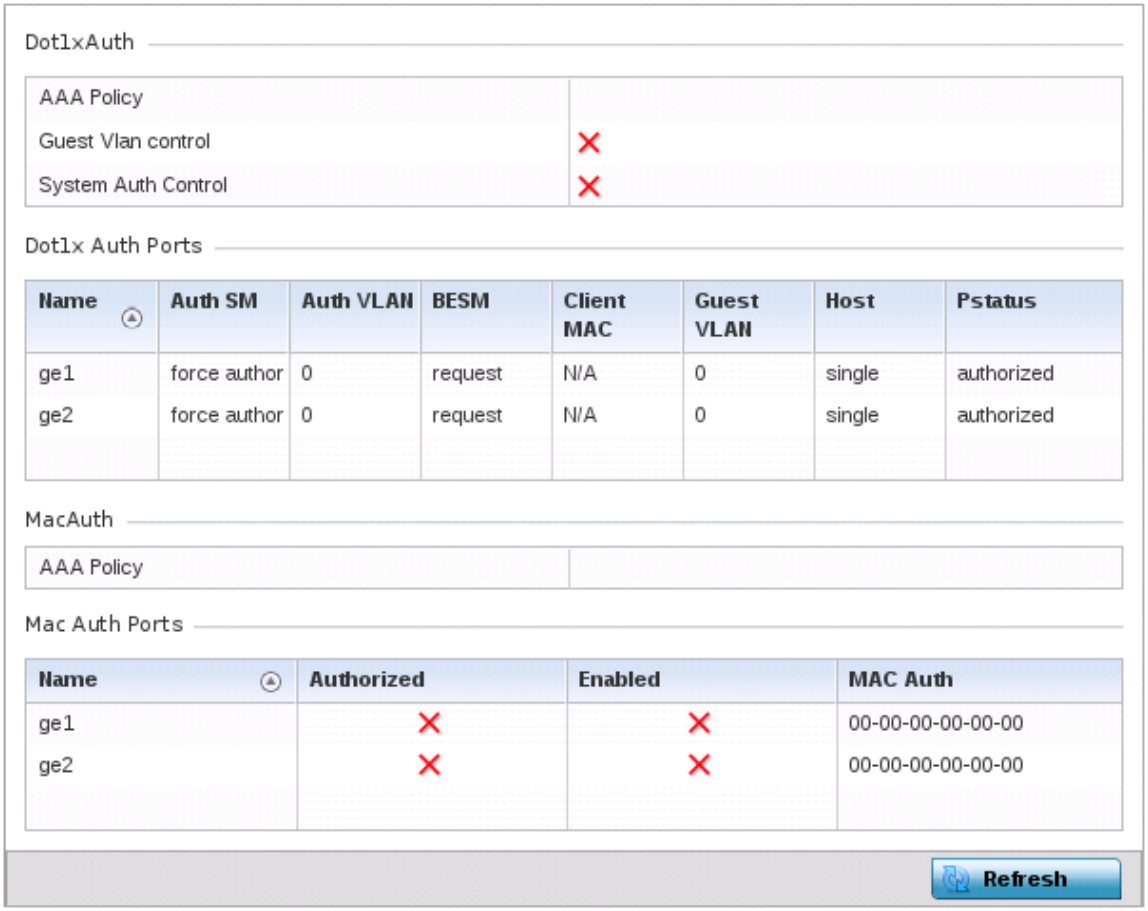


Figure 76: Access Point – Dot1x screen

4 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 access point. A green checkmark designates Dot1x authorization globally enabled. A red X defines Dot1x as globally disabled.

5 Review the following Dot1x Auth Ports utilization information:

Name	Lists the access point ge ports subject to automatic connection and authentication using Dot1x.
Auth SM	Lists the current authentication state of the listed port.
Auth VLAN	Lists the virtual interface utilized post authentication.

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.

6 Refer to the MacAuth table to assess the AAA policy applied to MAC authorization requests.

7 Review the following MAC Auth Ports utilization information:

Name	Lists the access point 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 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 MAC address corresponding to the listed access point port interface on which authentication requests are made.

8 Select the **Refresh** button to update the screen's statistics counters to their latest value.

Network

"Access Point Statistics"

Use the Network screen to view information for performance statistics for ARP, DHCP, Routing and Bridging.For more information, refer to the following:

- "ARP Entries"
- "Route Entries"
- "Default Routes"
- "Bridge"
- "IGMP"
- "MLD"
- "Traffic Shaping"
- "DHCP Options"
- "Cisco Discovery Protocol"
- "Link Layer Discovery Protocol"
- "IPv6 Neighbor"
- "MSTP"

ARP Entries

"Network"

Address Resolution Protocol (ARP) 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 an access point's ARP 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 a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its submenu items.

4 Select **ARP Entries**.

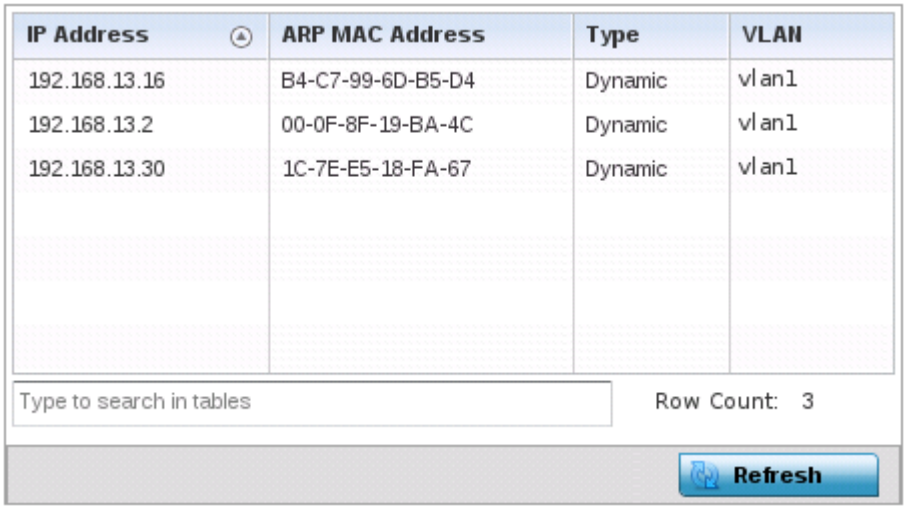


Figure 77: Access Point - Network ARP screen

The **ARP Entries** screen describes the following:

IP Address	Displays the IP address of the client resolved on behalf of the access point.
ARP MAC Address	Displays the MAC address corresponding to the IP address being resolved.
Type	Lists the type of ARP entry.
VLAN	Displays the system assigned VLAN ID where an IP address was found.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Route Entries

"Network"

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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Route Entries**. The **IPv4 Route Entries** table displays by default.

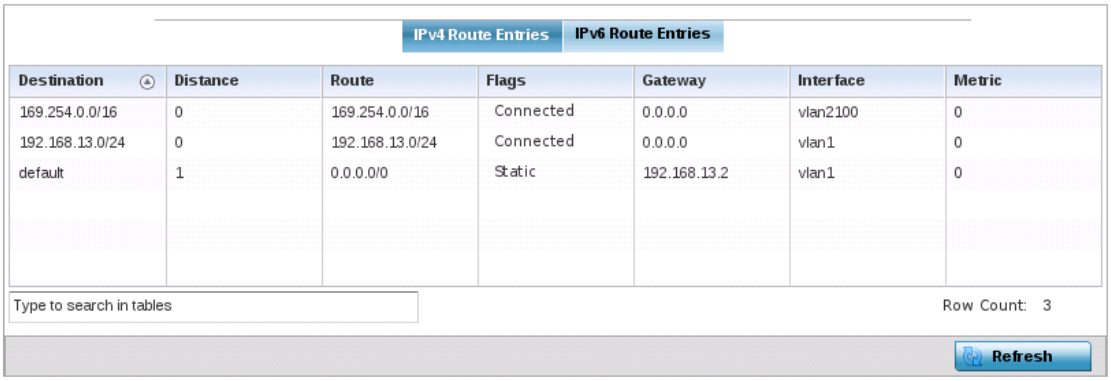


Figure 78: Access Point - Network Route Entries - IPv4 Route Entries screen

The **Route Entries** screen supports the following:

Destination	Displays the IP 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. A direct route is where the destination is directly connected to the forwarding host. With an indirect route, the destination host is not directly connected to the forwarding host. Possible flags include *U* (route is up), *H* (target is a host), *G* (use gateway), *R* (reinstate route for dynamic routing), *D* (dynamically installed by daemon or redirect), *M* (modified from routing daemon or redirect), *A* (installed by addrconf), *C* (cache entry) or*!* (reject route).
Gateway	Displays the IP address of the gateway used to route packets to the specified destination subnet.
Interface	Displays the interface name of the destination subnet.
Metric	Displays the metric (or cost) for this route.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

5 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

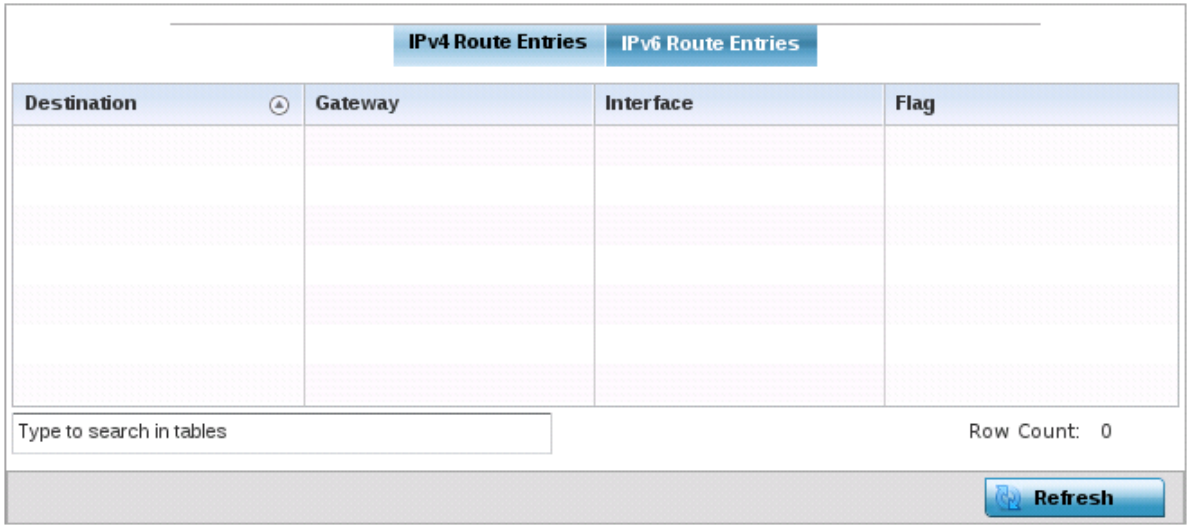


Figure 79: Access Point - Network Route Entries - IPv6 Route Entries screen

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.
Refresh	Select Refresh to update the display to the latest values.

Default Routes

"Network"

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 IPv4 formatted default routes:

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 a RF Domain and select one of its connected access points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Default Routes**. The **IPv4 Default Routes** tab displays by default.

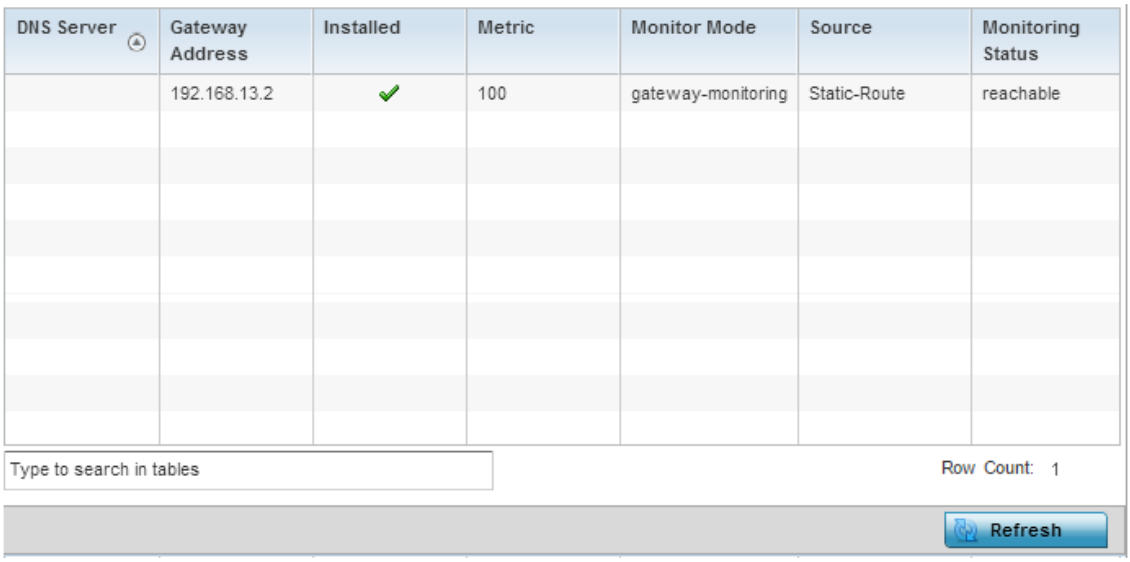


Figure 80: Access Point - Network IPv4 Default Routes screen

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 Address	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.
Refresh	Select *Refresh* to update the display to the latest values.

5 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

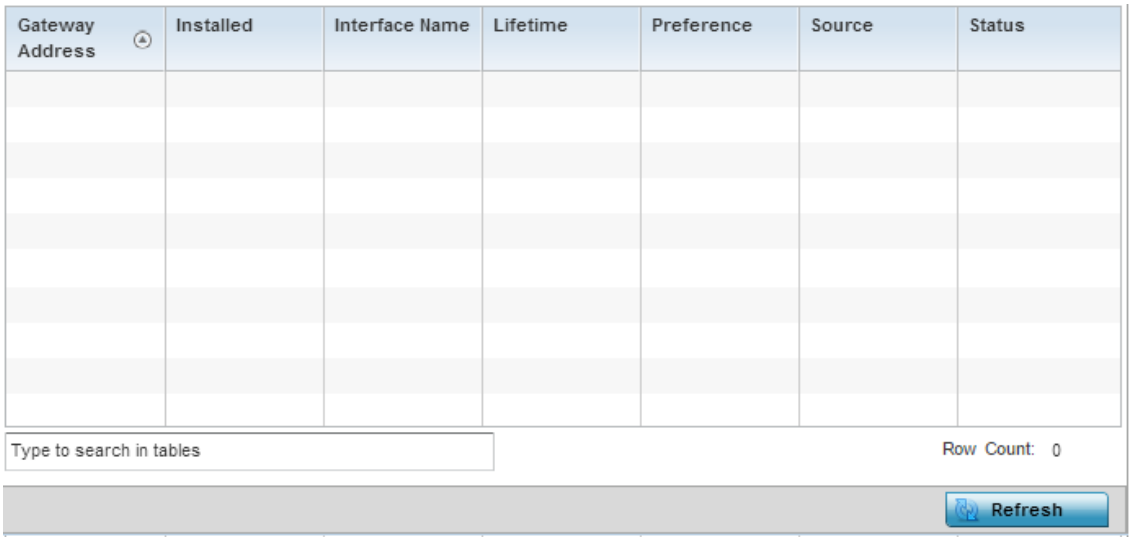


Figure 81: Access Point - Network IPv6 Default Routes screen

The **IPv6 Default Routes** screen provides the following information:

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.
Refresh	Select *Refresh* to update the display to the latest values.

Bridge

"Network"

Bridging is a forwarding technique used in networks. Bridging makes no assumption about where a particular address is located. It relies on the flooding and 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 an access point are very much alike, as an access point can be viewed as a bridge with a number of ports.

The Bridge screen provides details about the Integrate Gateway Server (IGS), 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

The Bridging screen also provides information about the Multicast Router (MRouter), 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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Bridge**.

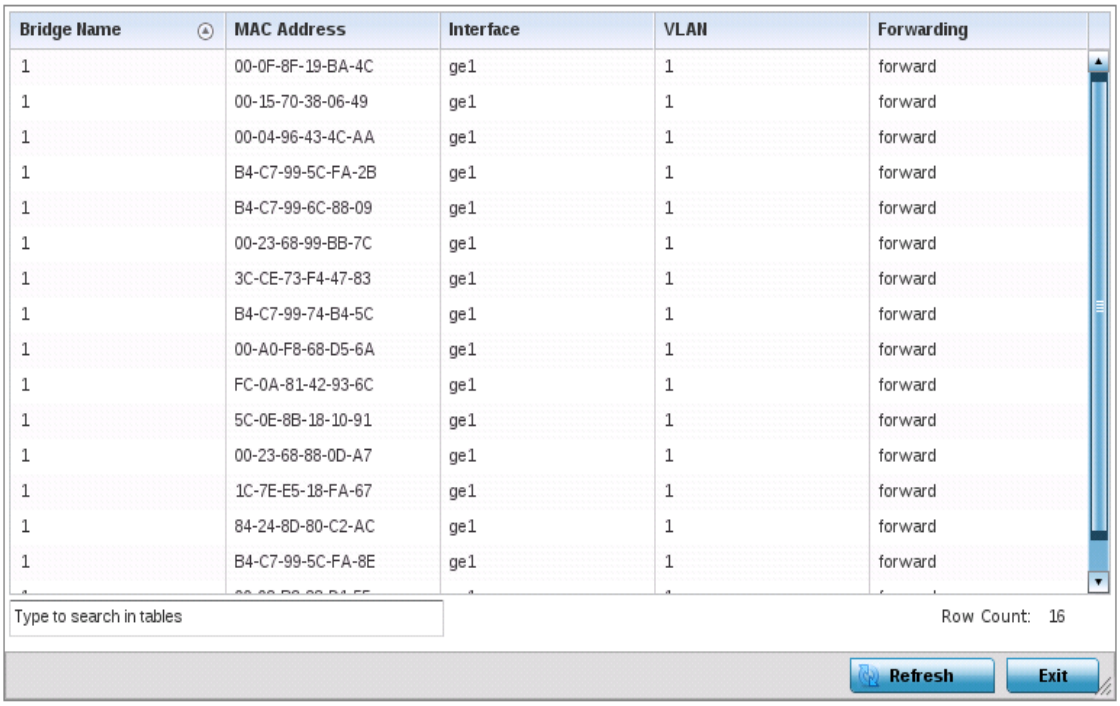


Figure 82: Access Point - Network Bridge screen

5 Review the following bridge configuration attributes:

Bridge Name	Displays the numeric ID of the network bridge.
MAC Address	Displays the MAC address of the bridge selected.
Interface	Displays the interface (access point physical port name) where the bridge transferred packets. Supported access point models have different port configurations.
VLAN	Displays the VLAN the bridge uses a virtual interface.
Forwarding	Displays whether the bridge is forwarding packets.

6 Select **Refresh** to update the counters to their latest values.

IGMP

"Network"

Internet Group Management Protocol (IGMP) 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 a network's IGMP 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 a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **IGMP**.

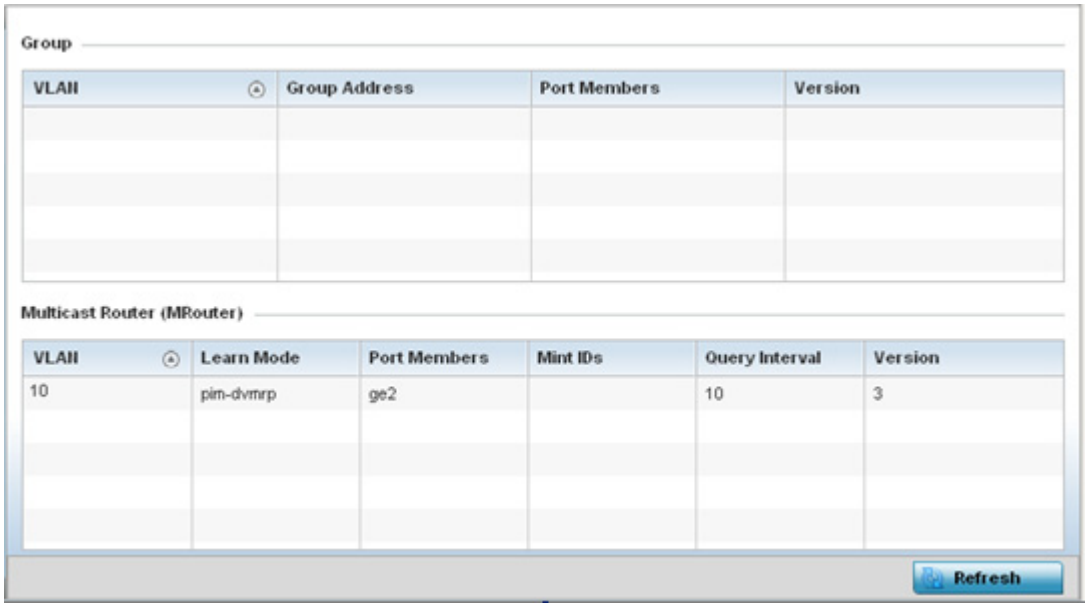


Figure 83: Access Point - Network IGMP screen

The **Group** field displays 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 that hosts are listening to.
Port Members	Displays the ports on which multicast clients have been discovered by the access point. For example, ge1, radio1, etc.
Version	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field displays 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 ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc.
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 point 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

MLD

"Network"

Multicast Listener Discovery (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 configuration options:

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 a RF Domain and select one of its connected access points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **MLD**.

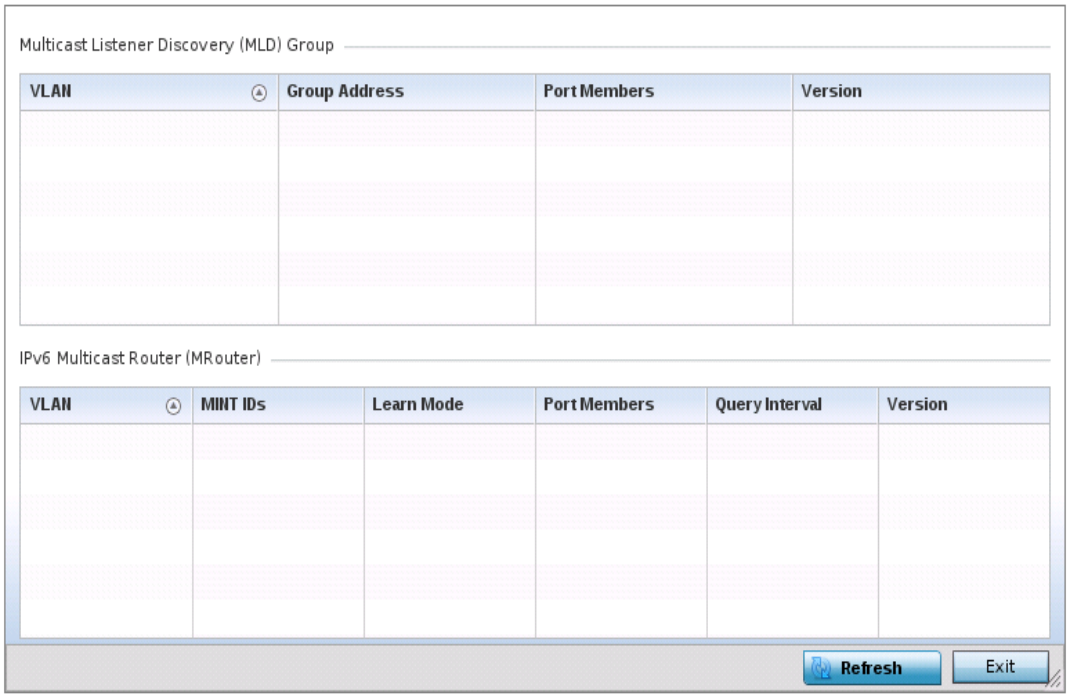


Figure 84: Access Point - Network MLD screen

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, service platform, access point 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Traffic Shaping

"Network"

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, ACL rules take precedence for the traffic shaping class. Using traffic shaping, an application takes precedence over an application category.

To view network the controller or service platform's traffic shaping 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 a RF Domain and select one of its connected access points.

3 Expand the Network menu from the left-hand side of the UI.

4 Select Traffic Shaping. The Status screen displays by default, and lists the access point's traffic shaping status. Status can either be *Running* or *Not Running*.

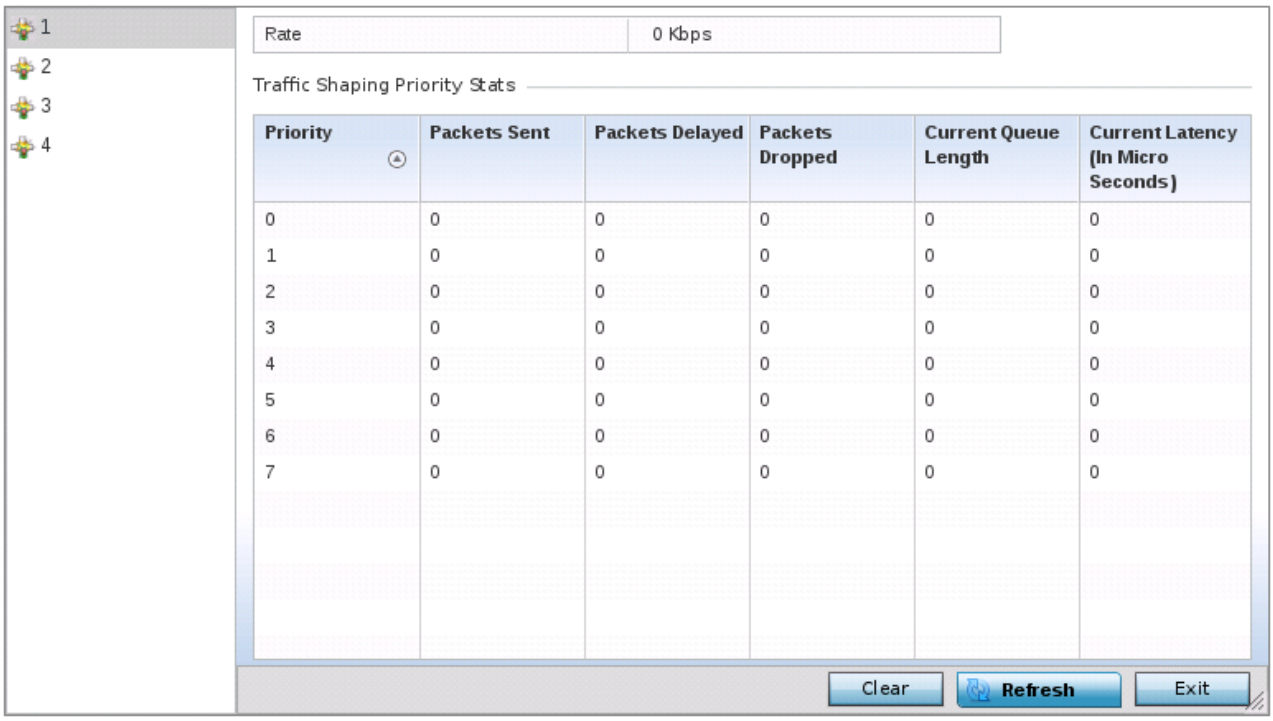


Figure 85: Access Point - Network Traffic Shaping - Statistics screen

5 Select Statistics.

6 Refer to the following Traffic Shaping statistics:

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 Queue Length	Lists the packet length of the data traffic shaped to meet downstream requirements.
Current Latency (In Micro Seconds)	Traffic shaping latency is the time limit after which packets start dropping as a result of the traffic prioritization filter rules applied.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

DHCP Options

"Network"

Supported access points can use a DHCP server resource to provide the dynamic assignment of IP addresses automatically. 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 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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **DHCP Options**.

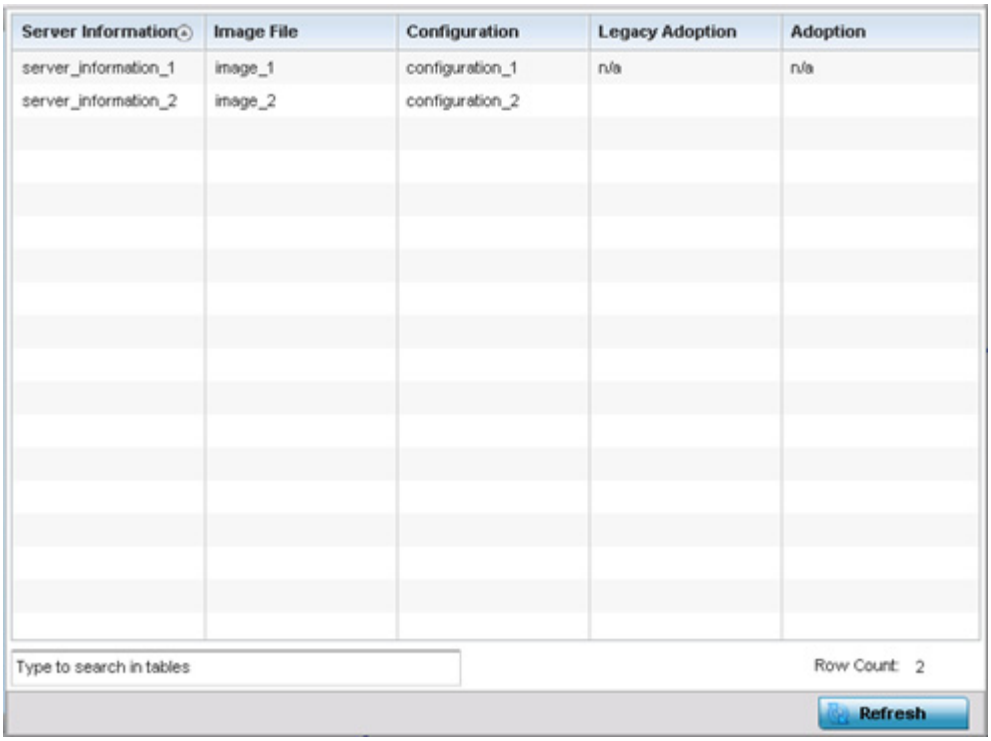


Figure 86: Access Point - Network DHCP Options screen

The **DHCP Options** screen displays 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 image file contains the image of the operating system the client will run. DHCP servers can be configured to support BOOTP.
Configuration	Displays the name of the configuration file on the DHCP server.
Legacy Adoption	Displays historical device adoption information on behalf of the access point.
Adoption	Displays adoption information on behalf of the access point.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Cisco Discovery Protocol

"Network"

The *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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Cisco Discovery Protocol**.

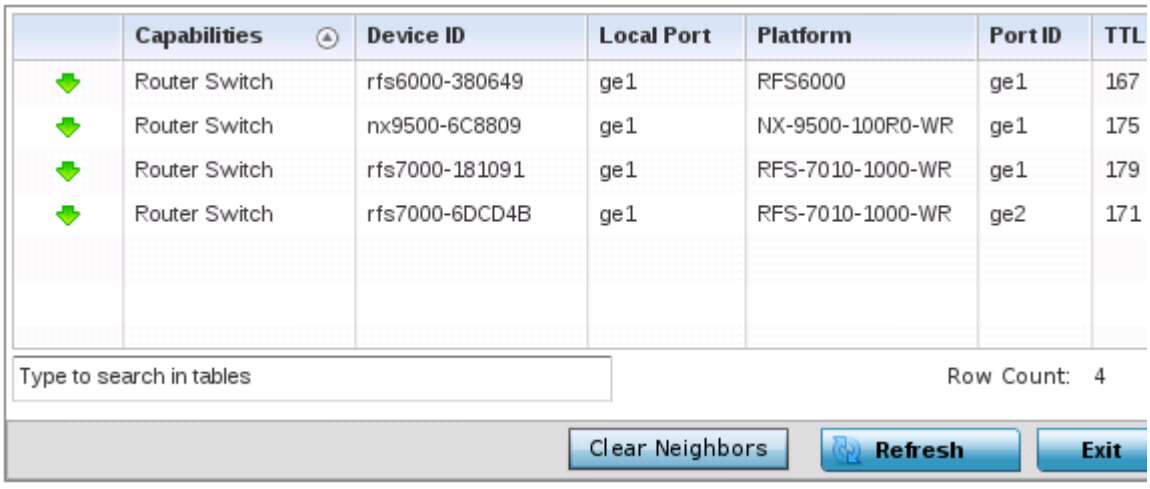


Figure 87: Access Point - Network CDP screen

The **Cisco Discovery Protocol** screen displays the following:

Capabilities	Displays the capabilities code for the device.
Device ID	Displays the configured device ID or name for each listed device.
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 *time to live* (TTL) for each CDP connection.
Clear Neighbors	Select *Clear Neighbors* to remove CDP neighbors from the table and begin a new data collection.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Link Layer Discovery Protocol

"Network"

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) 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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Link Layer Discovery**.

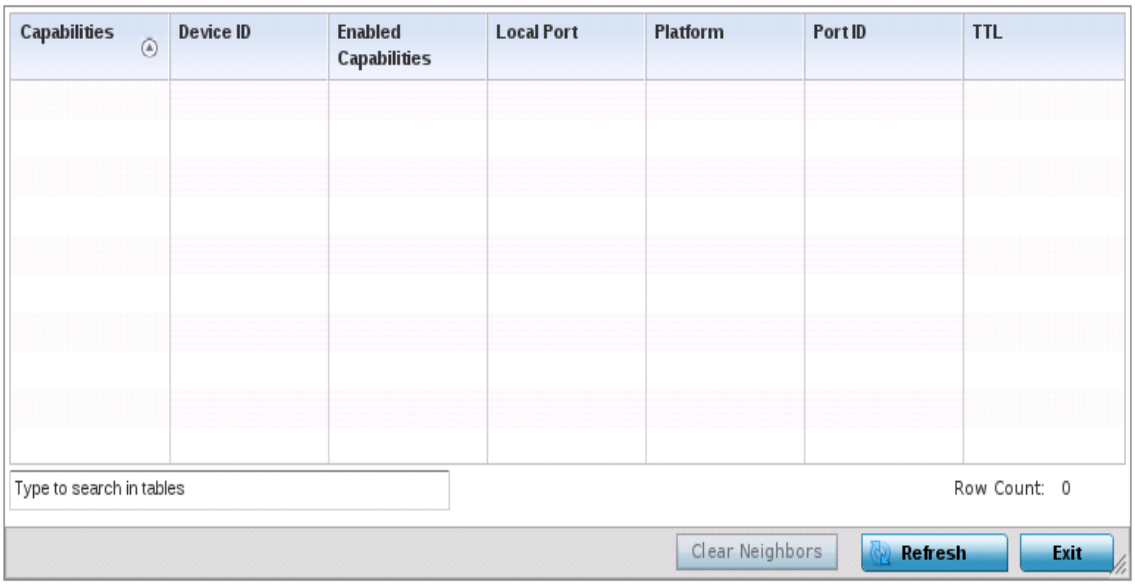


Figure 88: Access Point - Network LLDP screen

The **Link Layer Discovery Protocol** screen displays the following:

Capabilities	Displays the capabilities code for the device as either Router, Trans Bridge, Source Route Bridge, 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 time to live (TTL) for each LLDP connection.
Clear Neighbors	Select *Clear Neighbors* to remove all known LDP neighbors from the table.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

IPv6 Neighbor

"Network"

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 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 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor**.

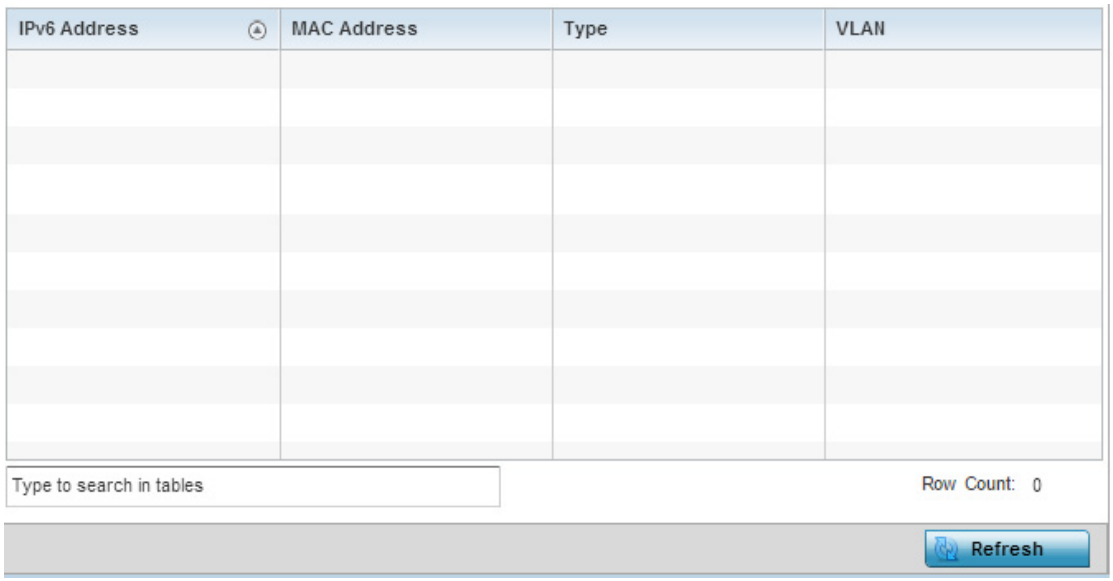


Figure 89: Access Point - Network IPv6 Neighbor screen

The **IPv6 Neighbor** 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

MSTP

- "Network"

The *Multiple Spanning Tree Protocol (*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 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.

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. 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.

Refer to the **MST Config** table to assess the MST configuration invoked and its version information.

The **MST Bridge** table defines whether the bridge is a BDPU filter, guard and Cisco interoperable. A guard determines whether the port enforces MST root bridge placement.

The **MST Port Bridge Detail** table has port specific MST state information.

To view an access point's MSTP 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 a RF Domain and select one of its connected access points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **MSTP**.

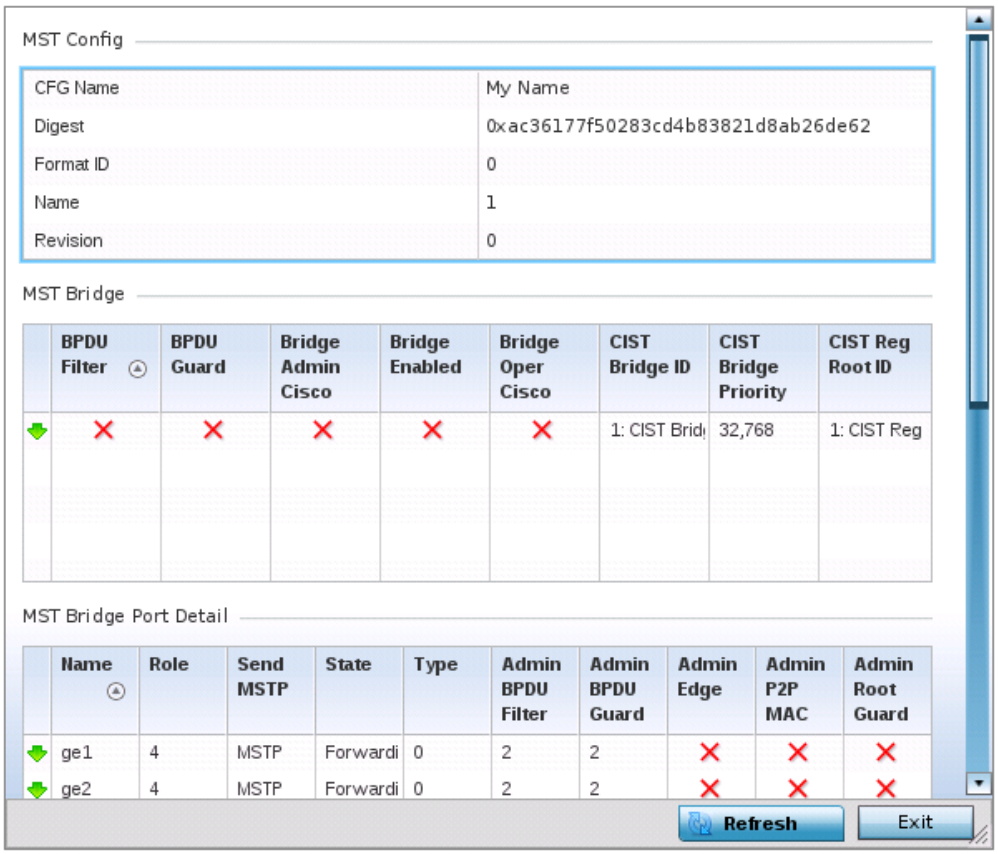


Figure 90: Access Point - Network MSTP screen

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 is enabled.

The **MST Bridge Port Detail** field lists specific access point port status and their current state.

DHCPv6 Relay & Client

"Access Point Statistics"

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 assess the DHCPv6 relay 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 a RF Domain and select one of its connected access points.

3 Select **DHCP Relay & Client** from the left-hand side of the UI.

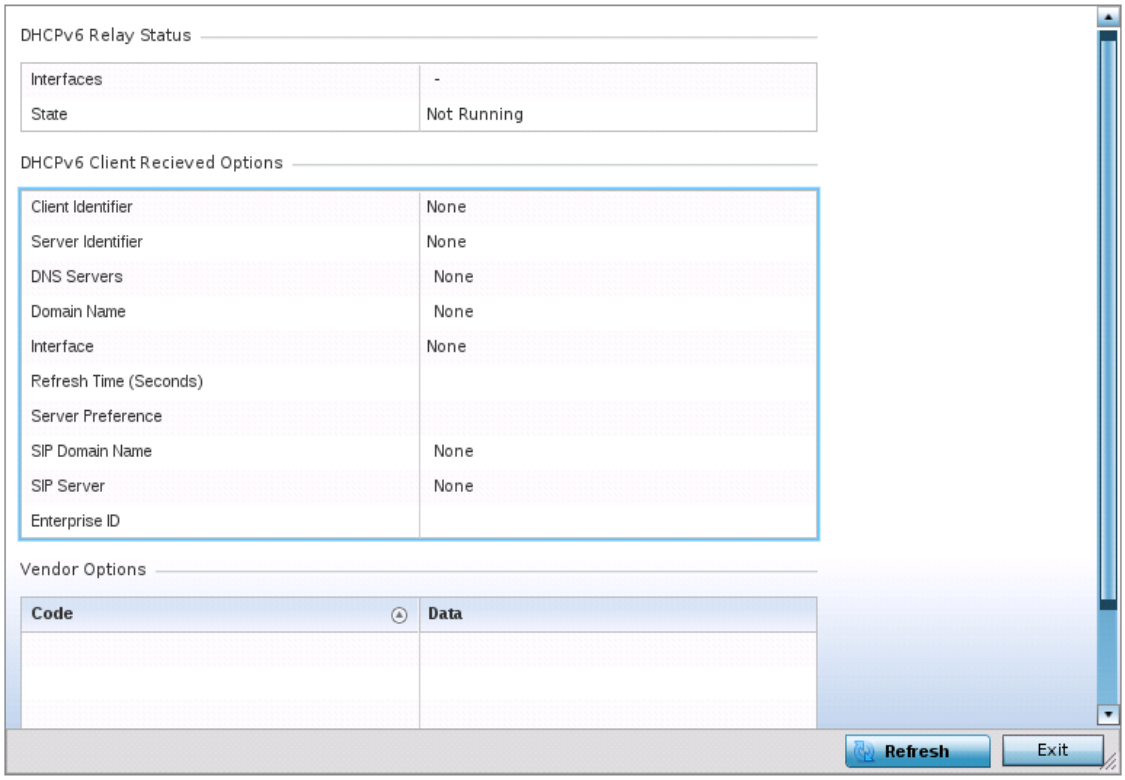


Figure 91: Access Point - DHCP Relay & Client screen

4 The **DHCPv6 Status** tables 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.

5 The **DHCPv6 Client Received Options** tables 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.

6 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.

DHCP Server

"Access Point Statistics"

Controllers and service platforms contain an internal *Dynamic Host Configuration Protocol* (DHCP) server. DHCP can provide IP addresses automatically. 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:

- "DHCP Server General Information"
- "DHCP Server Bindings"
- "DHCP Server Networks"

DHCP Server General Information

"DHCP Server"

To view *General* DHCP status and binding information for both DHCPv4 and DHCPv6:

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 a RF Domain and select one of its connected access points.

3 Expand the DHCP Server menu from the left-hand side of the UI.

4 Select **General.**

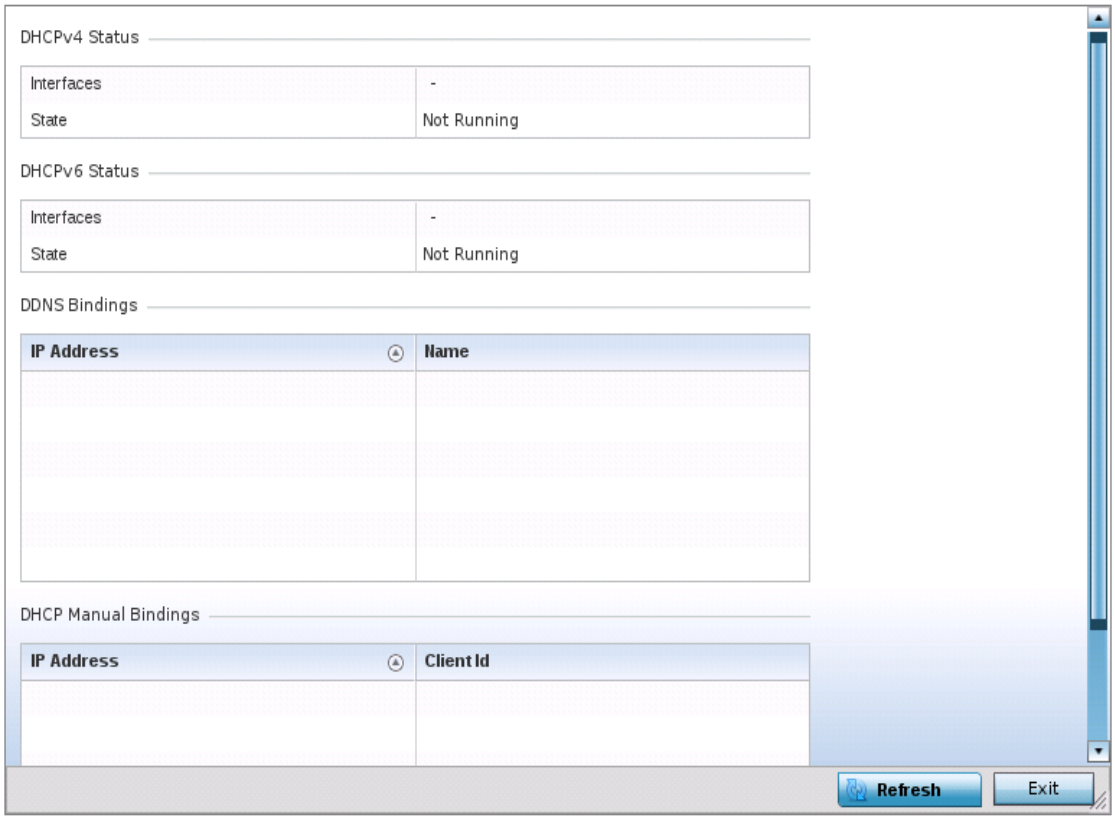


Figure 92: Access Point - DHCP Server General screen

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.

5 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.

6 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

DHCP Server Bindings

"DHCP Server"

The *DHCP Binding* screen displays DHCP binding expiry time, client IP addresses and their MAC address.

To view a network's DHCP Bindings:

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 a RF Domain and select one of its connected access points.

3 Select DHCP Server and expand the menu to reveal its sub menu items.

4 Select **Bindings**.

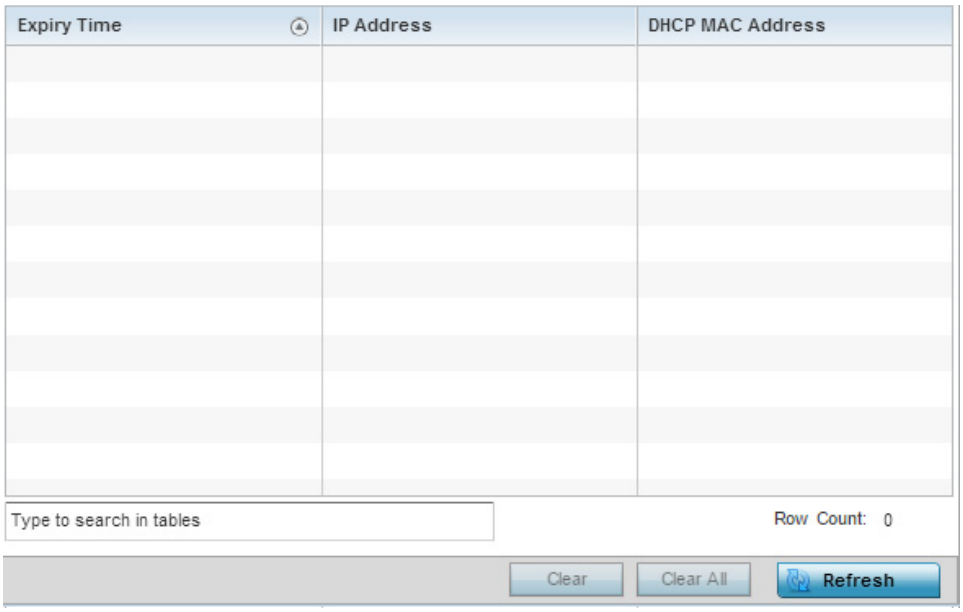


Figure 93: Access Point - DHCP Server Bindings screen

The **DHCP Bindings** screen displays the following:

Expiry Time	Displays the expiration of the lease used by a requesting client for DHCP resources.
IP Address	Displays the IP address for each DHCP resource requesting client.
DHCP MAC Address	Displays the hardware encoded MAC address (client Id) of each DHCP resource requesting client.
Clear	Select a table entry and select *Clear* to remove the client from the list of devices requesting DHCP services.
Clear All	Select *Clear All* to remove all listed clients from this list of DHCP resource requesting clients.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

DHCP Server Networks

"DHCP Server"

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 use from the pool, the pool name, the used addresses and the total number of addresses.

To view a network's DHCP Networks:

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 the a RF Domain and select one of its connected access points.

3 Select DHCP Server and expand the menu to reveal its sub menu items.

4 Select **Networks**.

The **Network Pool** screen displays the following:

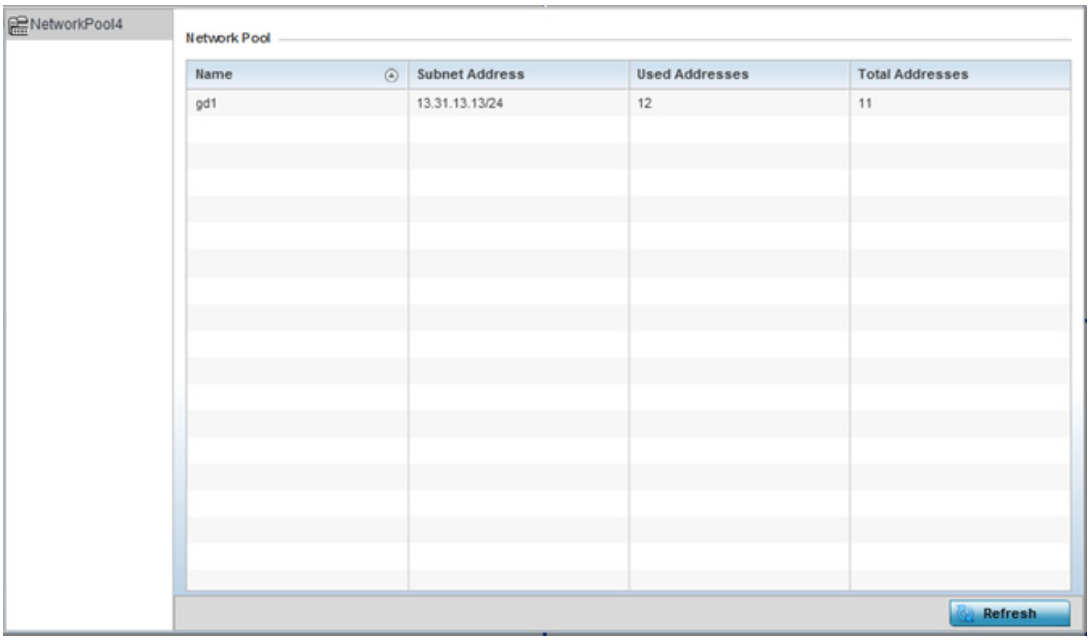


Figure 94: Access Point - DHCP Server Networks screen

Name	Displays the name of the DHCP pool.
Subnet Address	Displays the subnet addresses of the DHCP Pool.
Used Addresses	Number of addresses that have already been leased to requesting clients.
Total Addresses	Total available addresses that can be leased to requesting clients.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

Firewall

"Access Point Statistics"

A firewall is a part of a computer system or network designed to block unauthorized access while permitting authorized communications. It is 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:

- "Packet Flows"
- "Denial of Service"
- "IP Firewall Rules"
- "IPv6 Firewall Rules"
- "MAC Firewall Rules"
- "NAT Translations"
- "DHCP Snooping"
- "IPv6 Neighbor Snooping"

Packet Flows

"Firewall"

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.

1 To view access point packet flows statistics:

2 Select the Statistics menu from the Web UI.

3 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

4 Select **Firewall** and expand the menu to reveal its sub menu items.

5 Select **Packet Flows**.

6 Periodically select **Refresh** to update the statistics counters to their latest values. **Clear All** clears all the statistics counters and begins a new data collection.

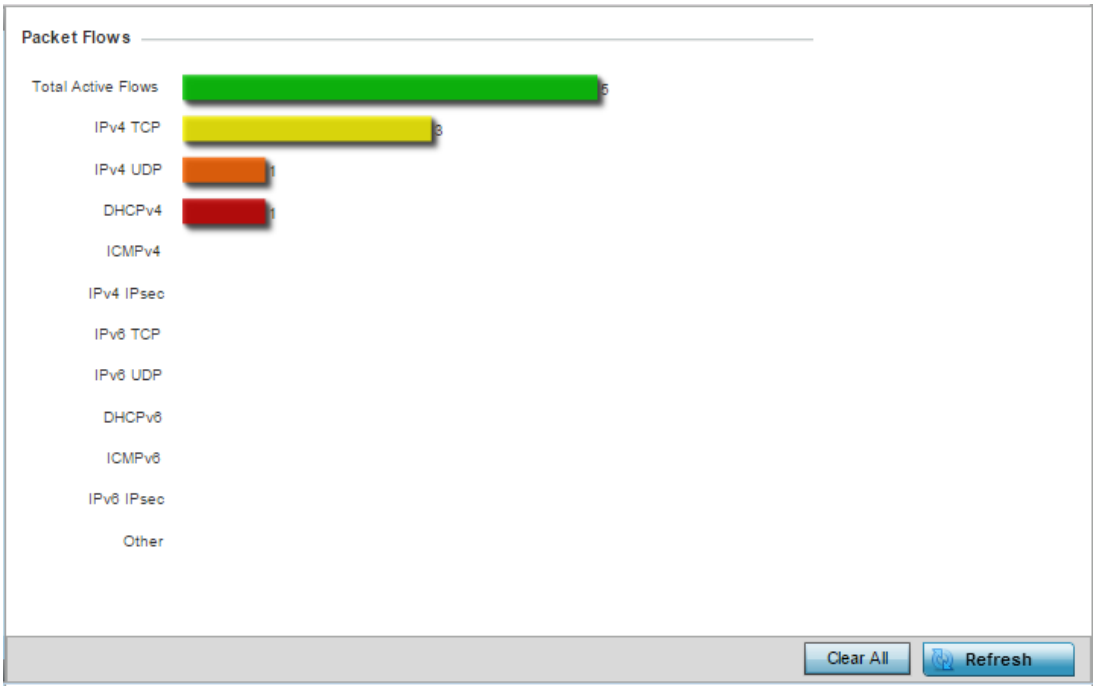


Figure 95: Access Point - Firewall Packet Flows screen

Denial of Service

"Firewall"

A *denial-of-service attack* (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 access point DoS attack information:

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 a RF Domain and select one of its connected access points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **Denial of Service**.

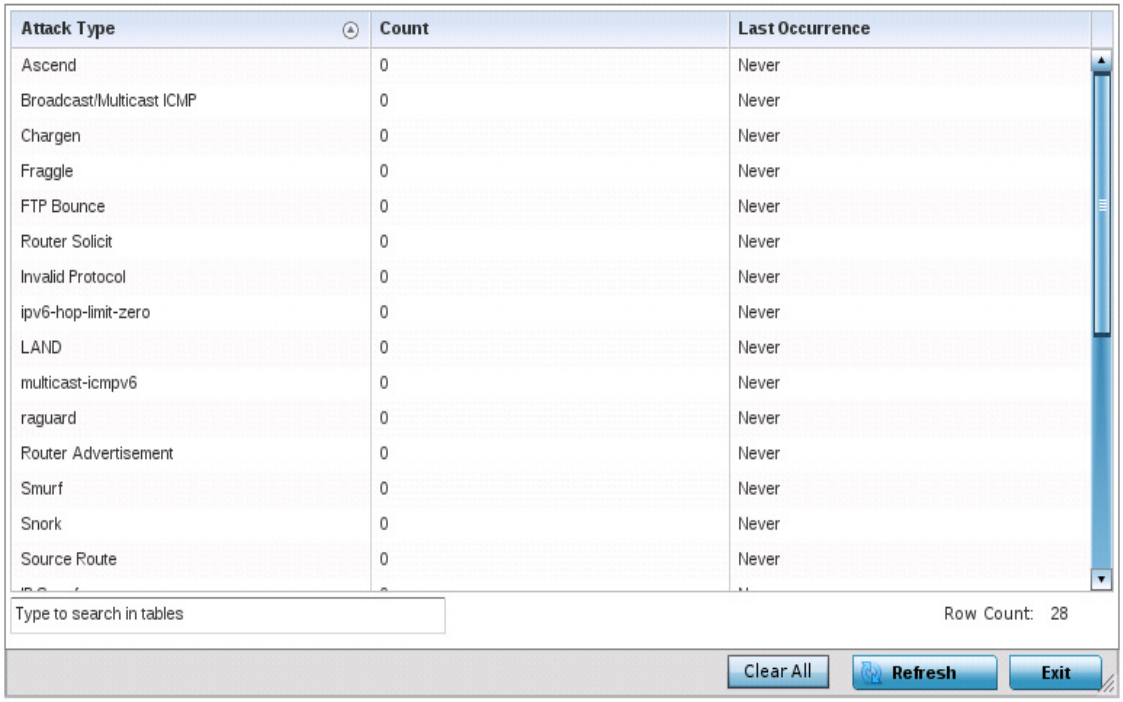


Figure 96: Access Point - Firewall Denial of Service screen

The **Denial of Service** screen displays the following:

Attack Type	Displays the *Denial of Service* (DoS) attack type.
Count	Displays the number of times the access point's firewall has detected each listed DoS attack.
Last Occurrence	Displays the when the attack event was last detected by the access point firewall.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

IP Firewall Rules

"Firewall"

Create firewall rules to let any computer to send traffic to, or receive traffic from, programs, system services, computers or users. Firewall rules can be created to take 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 the IP firewall rules:

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 a RF Domain and select one of its connected access points.

3 Select Firewall and expand the menu to reveal its sub menu items.

4 Select **IP Firewall Rules**.

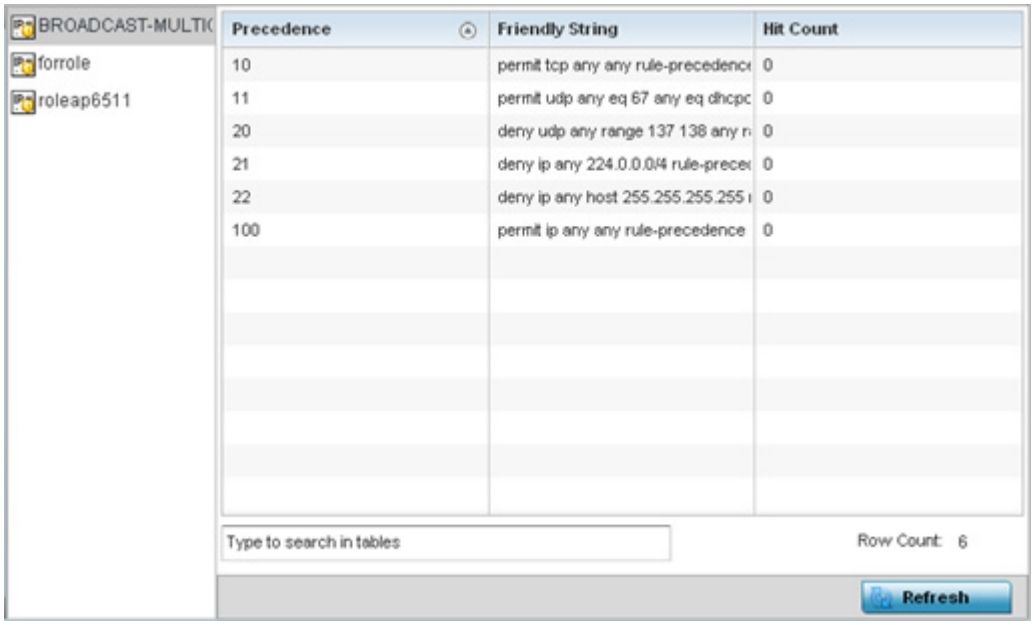


Figure 97: Access Point - Firewall IP Firewall Rules screen

The **IP Firewall Rules** screen displays the following:

Precedence	Displays the precedence value applied to packets. The rules within an *Access Control Entries* (ACL) list are based on precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence.
Friendly String	The friendly string provides information as to which firewall the rules apply.
Hit Count	Displays the number of times each firewall rule has been triggered.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

IPv6 Firewall Rules

"Firewall"

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 *neighbor discovery* (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.

- *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 existing IPv6 firewall rules:

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 a RF Domain and select one of its connected access points.

3 Expand the Firewall menu from the left-hand side of the UI.

4 Select **IPv6 Firewall Rules.**

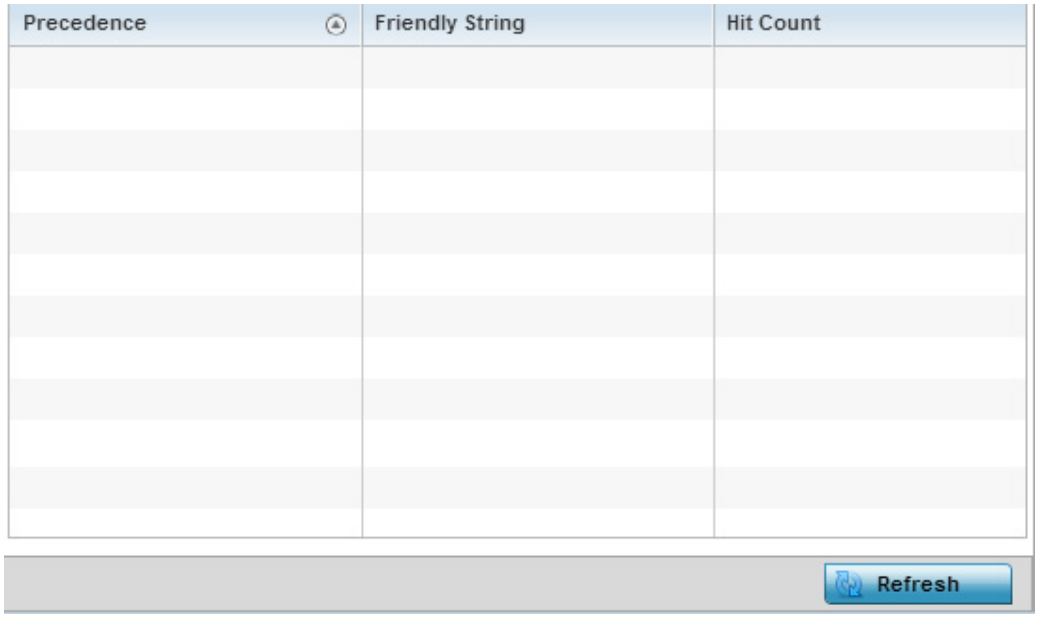


Figure 98: Access Point - Firewall IPv6 Firewall Rules screen

The **IPv6 Firewall Rules** screen displays the following:

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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

MAC Firewall Rules

"Firewall"

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 is 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **MAC Firewall Rules**.

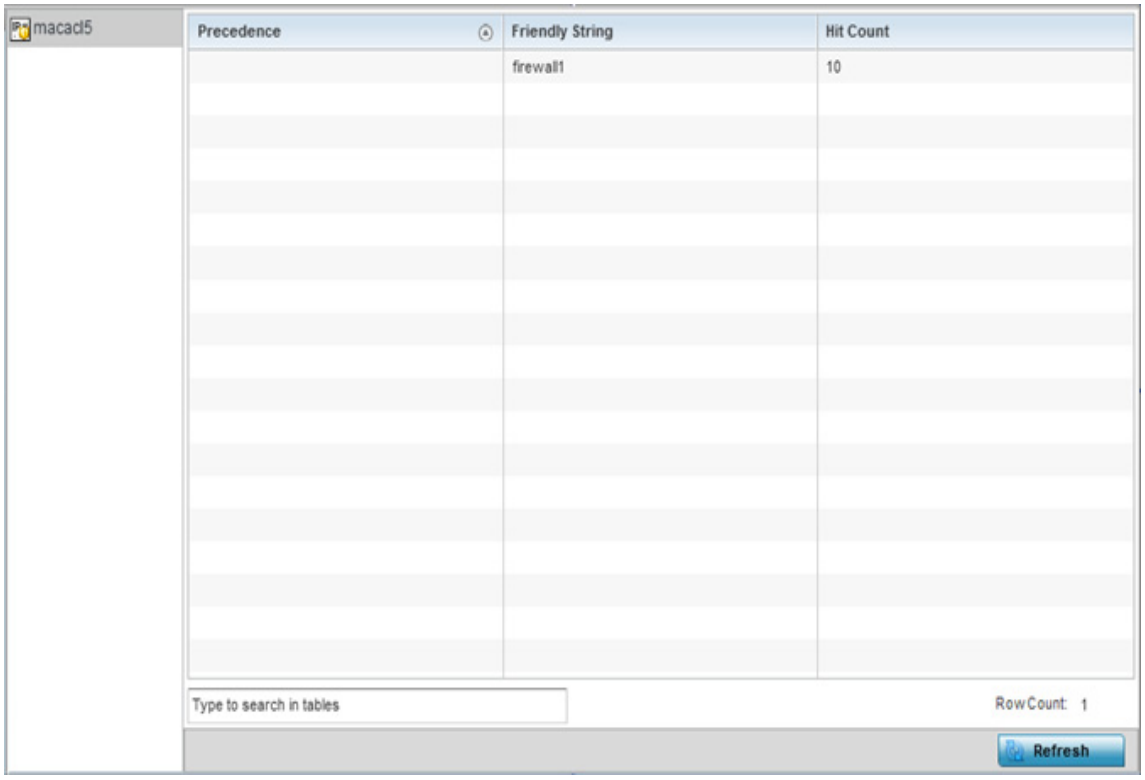


Figure 99: Access Point - Firewall MAC Firewall Rules screen

The **MAC Firewall Rules** screen displays the following information:

Precedence	Displays a precedence value, which are applied to packets. The rules within an *Access Control Entries* (ACL) list are based on their precedence. Every rule has a unique precedence between 1 and 5000. You cannot add two rules with the same precedence value.
Friendly String	This is a string that provides information as to which firewall the rules apply.
Hit Count	Displays the number of times each WLAN ACL has been triggered.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

NAT Translations

"Firewall"

Network Address Translation (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 an access point. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an 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 view the Firewall's NAT translations:

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 a RF Domain and select one of its connected access points.

3 Select **F**irewall and expand the menu to reveal its sub menu items.

4 Select **NAT Translations**.

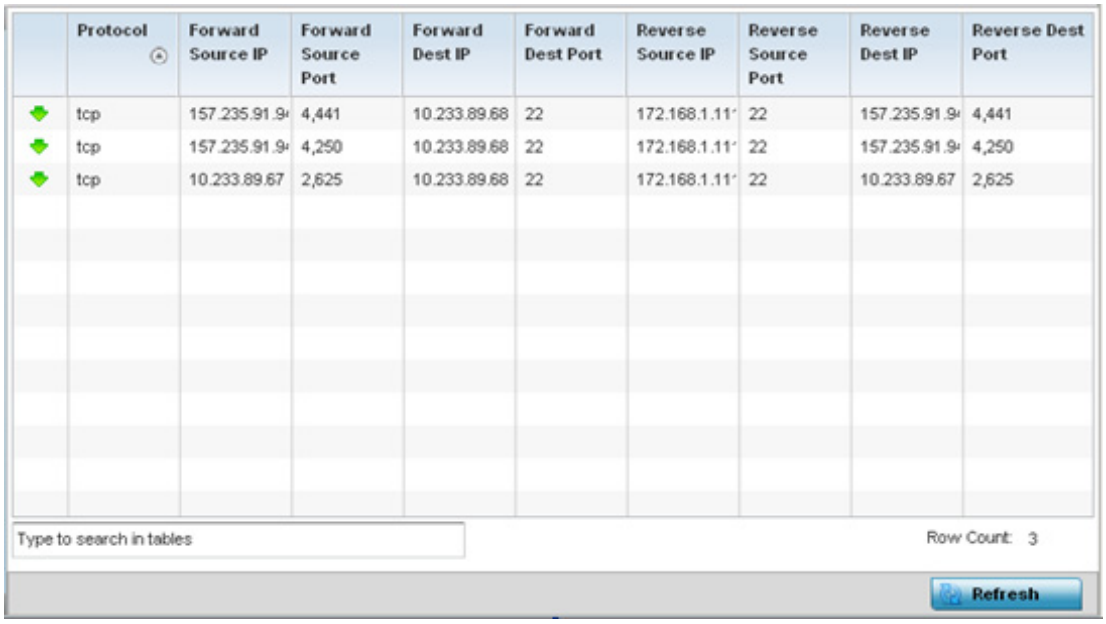


Figure 100: Access Point - Firewall NAT Translation screen

The **NAT Translations** screen displays the following:

Protocol	Lists the NAT translation IP protocol as either *TCP*, *UDP* or *ICMP*.
Forward Source IP	Displays the source IP address for the forward NAT flow.
Forward Source Port	Displays the source port for the forward NAT flow (contains ICMP ID if it is an ICMP flow).
Forward Dest IP	Displays the destination IP address for the forward NAT flow.
Forward Dest Port	Destination port for the forward NAT flow (contains ICMP ID if it is an ICMP flow).
Reverse Source IP	Displays the source IP address for the reverse NAT flow.
Reverse Source Port	Displays the source port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
Reverse Dest IP	Displays the destination IP address for the reverse NAT flow.
Reverse Dest Port	Displays the destination port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

DHCP Snooping

"Firewall"

When DHCP servers are allocating IP addresses to clients on the LAN, DHCP snooping can be configured to better enforce the security on the LAN to allow only clients with specific IP/MAC addresses.

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 a RF Domain and select one of its connected access points.

3 Select Firewall and expand the menu to reveal its sub menu items.

4 Select **DHCP Snooping**.

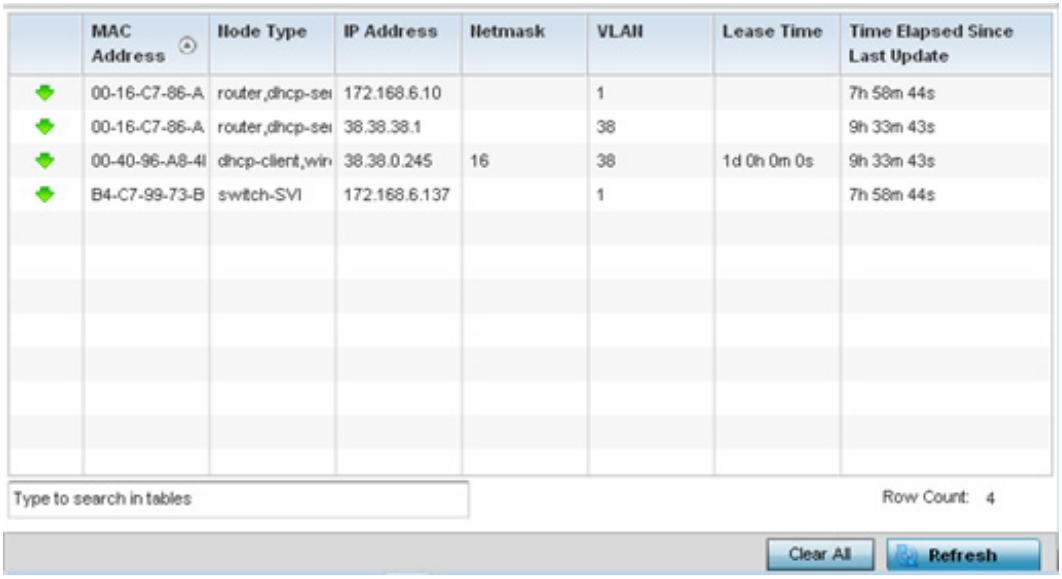


Figure 101: Access Point - Firewall DHCP Snooping screen

The **DHCP Snooping** screen displays the following:

MAC Address	Displays the MAC address of the client requesting DHCP resources from the controller or service platform.
Node Type	Displays the NetBios node 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 VLAN used as a virtual interface for the newly created DHCP configuration.
Lease Time	When a DHCP server allocates an address for a DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease time is the time an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are 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 Updated	Displays the time the server was last updated.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

IPv6 Neighbor Snooping

"Firewall"

IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 *neighbor discovery* (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.

To review IPv6 neighbor snooping statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the Firewall menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor Snooping.**

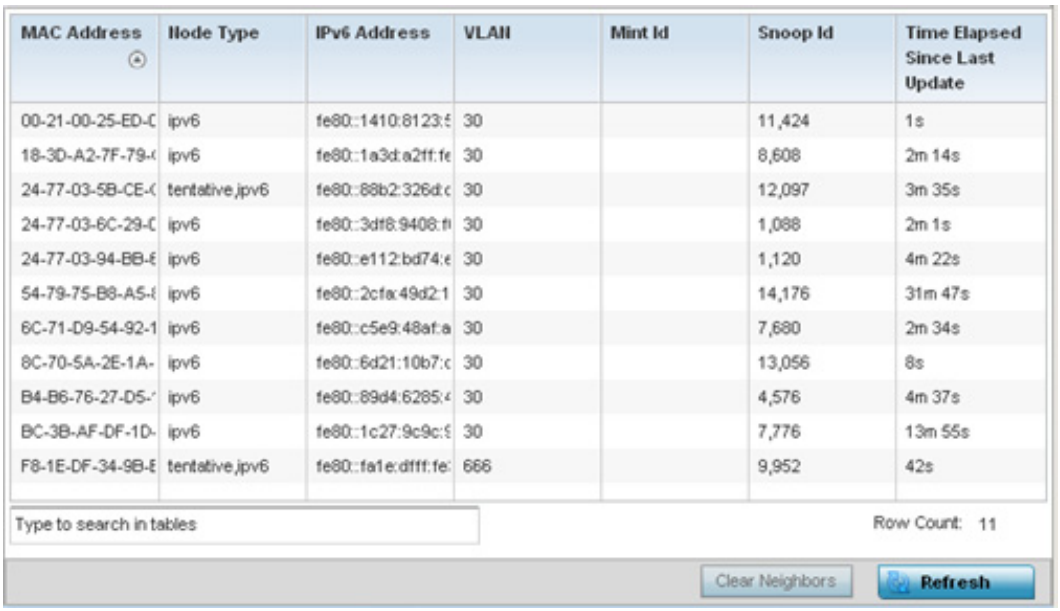


Figure 102: Access Point - Firewall IPv6 Neighbor Snooping screen

The **IPv6 Neighbor Snooping** screen displays the following:

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.
Clear Neighbors	Select *Clear Neighbors* to revert the counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's counters to their latest values.

VPN

"Access Point Statistics"

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 tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

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.

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.

VPN statistics are partitioned into the following:

- "IKESA"

- "IPSec"

IKESA

- "VPN"

The *IKESA* screen allows for the review of individual peer security association 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 a RF Domain and select one of its connected access points.

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IKESA**.

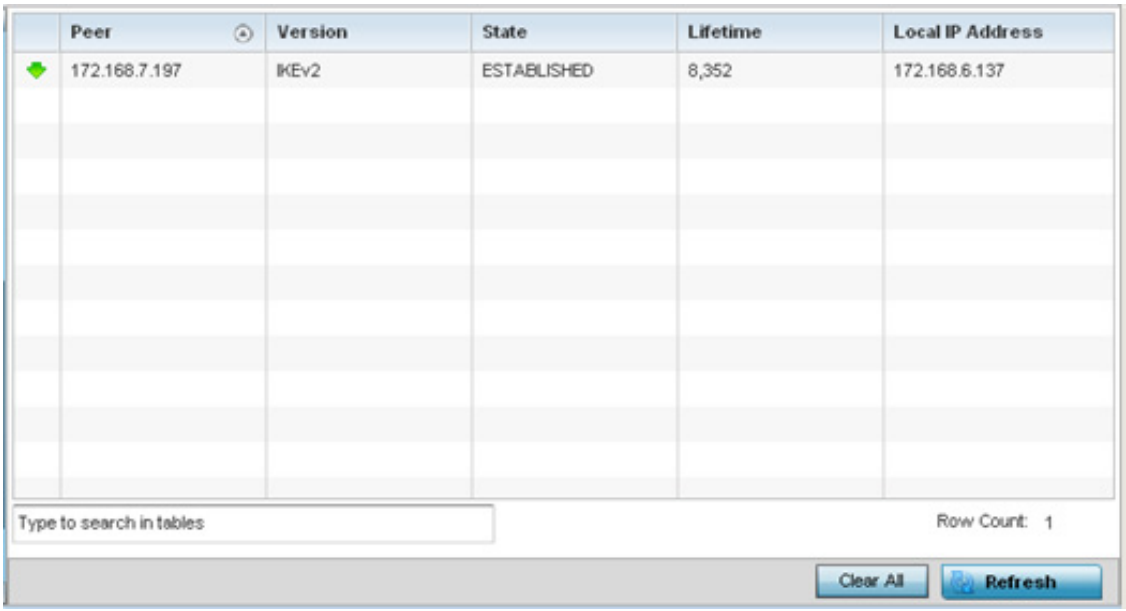


Figure 103: Access Point - VPN IKESA screen

5 Review the following VPN peer security association statistics:

Peer	Lists peer IDs for peers sharing security associations (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 security association (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.
Clear All	Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

IPSec

"VPN"

Use the *IPSec* VPN screen to assess tunnel status between networked peers.

To view IPSec VPN status for tunnelled peers:

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 a RF Domain and select one of its connected access points

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IPSec**.

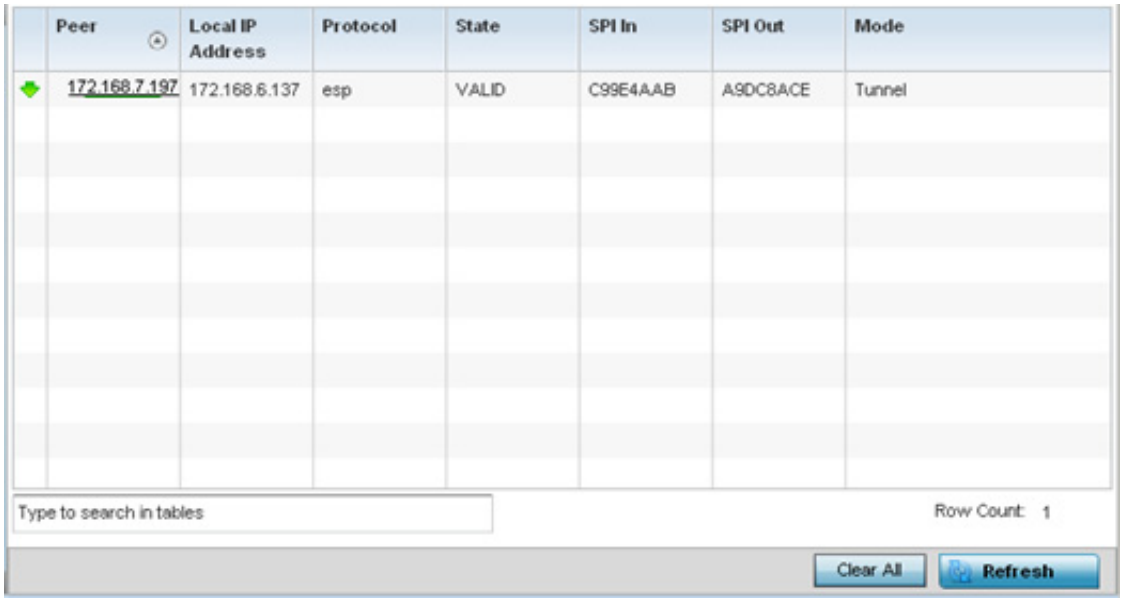


Figure 104: Access Point - VPN IPSec screen

5 Review the following VPN peer security association statistics:

Peer	Lists IP addresses for peers sharing *security associations* (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 *stateful packet inspection* (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.
Clear All	Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Certificates

"Access Point Statistics"

The *Secure Socket Layer* (SSL) protocol ensures secure transactions between Web servers and browsers. SSL uses a third-party certificate authority 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:

- "Trustpoints"
- "RSA Keys"

Trustpoints

"Certificates"

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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points

3 Select **Certificates** and expand the menu to reveal its sub menu items.

4 Select **Trustpoints**.

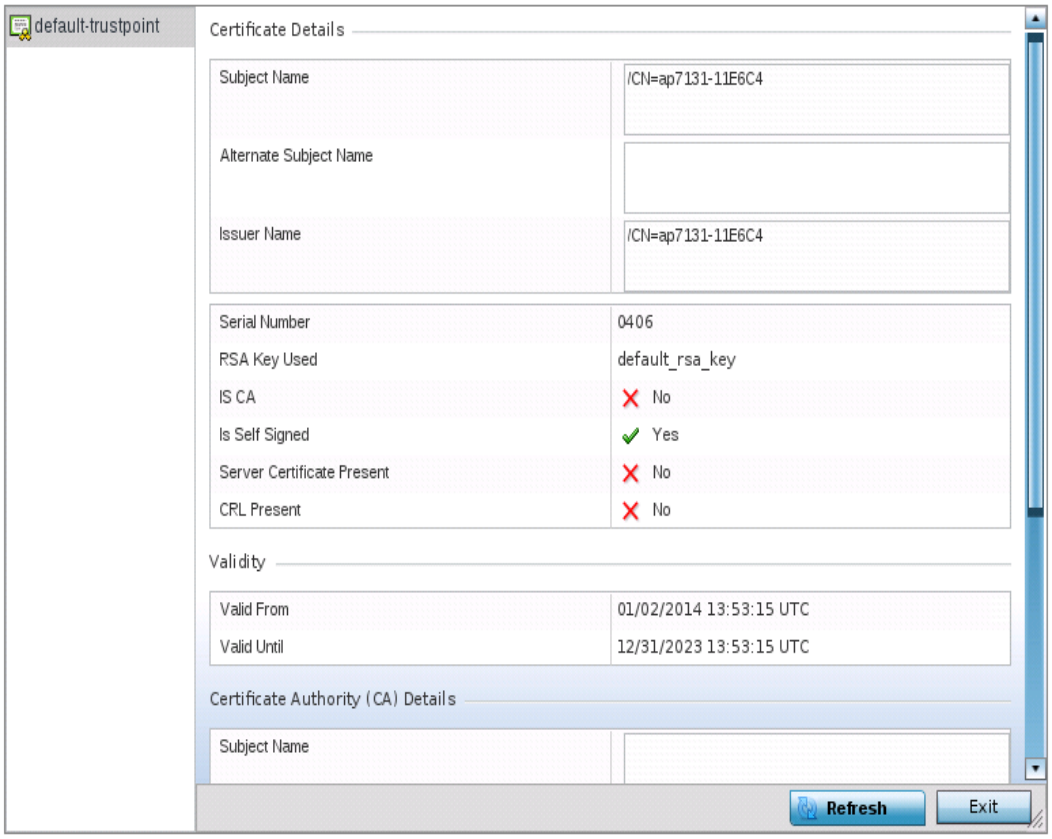


Figure 105: Access Point - Certificate Trustpoint screen

The Certificate Details field displays the following:

Subject Name	Lists details about the entity to which the certificate is issued.
Alternate Subject Name	Displays alternative details to the information specified under the *Subject Name* field.
Issuer Name	Displays the name of the organization issuing the certificate.
Serial Number	The unique serial number of the certificate issued.
RSA Key Used	Displays the name of the key pair generated separately, 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 Certificate Present	Displays whether a server certification is present or not (Yes/No).
CRL Present	Displays whether a *Certificate Revocation List* (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 stating the beginning of the certificate's validity.
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 begins.
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.

RSA Keys

"Certificates"

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 *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 RSA Key details:

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 a RF Domain and select one of its connected access points

3 Select **Certificates** and expand the menu to reveal its sub menu items.

4 Select **RSA Keys**.

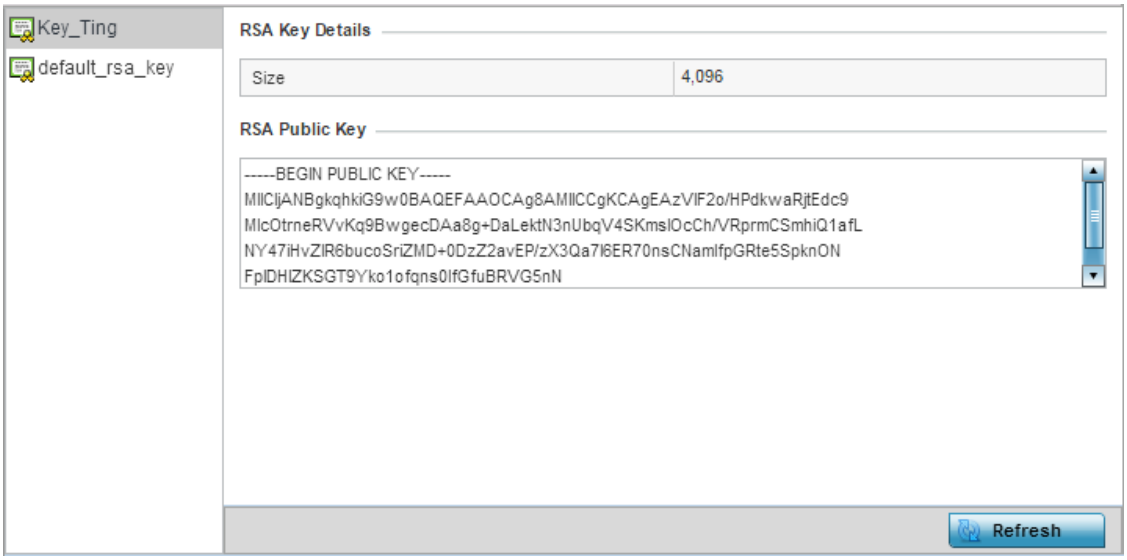


Figure 106: Access Point - Certificate RSA Keys screen

The RSA Key Details field displays the size (in bits) of the desired key. If not specified, a default key size of 1024 is used.

The RSA Public Key field lists the public key used for encrypting messages.

5 Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.

WIPS

"Access Point Statistics"

A *Wireless Intrusion Prevention System* (WIPS) monitors the radio spectrum for the presence of unauthorized access points and take measures to prevent an intrusion. Unauthorized attempts to access a controller or service platform 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 the blacklisted clients (unauthorized access points) intruded into 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:

- "WIPS Client Blacklist"
- "WIPS Events"

WIPS Client Blacklist

"WIPS"

This *Client Blacklist* displays blacklisted clients detected by this access point using WIPS. Blacklisted clients are not allowed to associate to this access points.

To view the WIPS client blacklist for this access point:

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 a RF Domain and select one of its connected access points.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **Client Blacklist**.

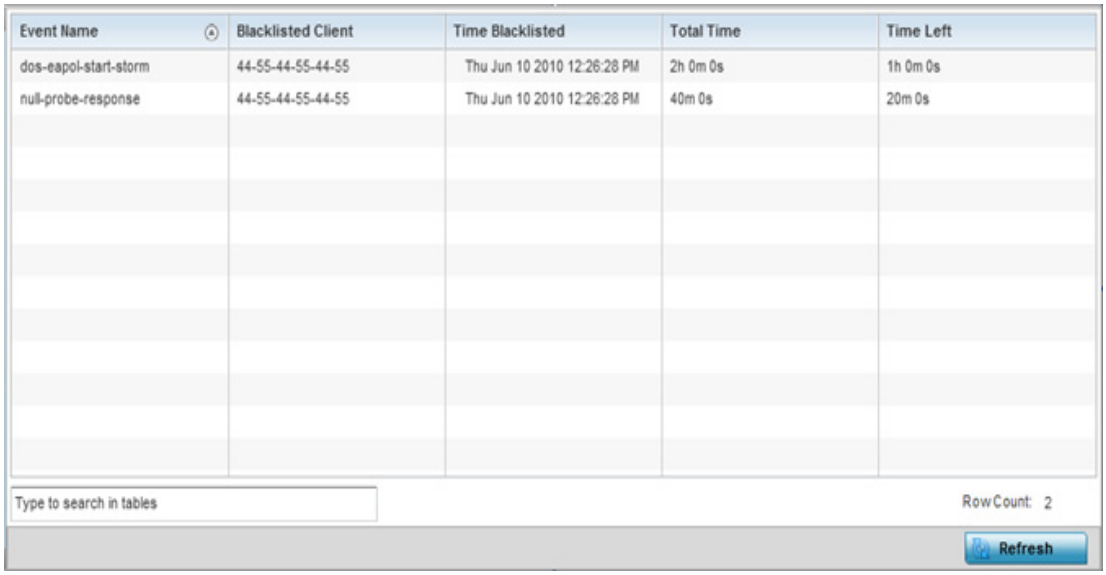


Figure 107: Access Point - WIPS Client Blacklist screen

The WIPS **Client Blacklist** screen displays the following:

Event Name	Displays the name of the event that resulted in the blacklisting.
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.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

WIPS Events

"WIPS"

To view the WIPS events 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 a RF Domain and select one of its connected access points.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **WIPS Events**.

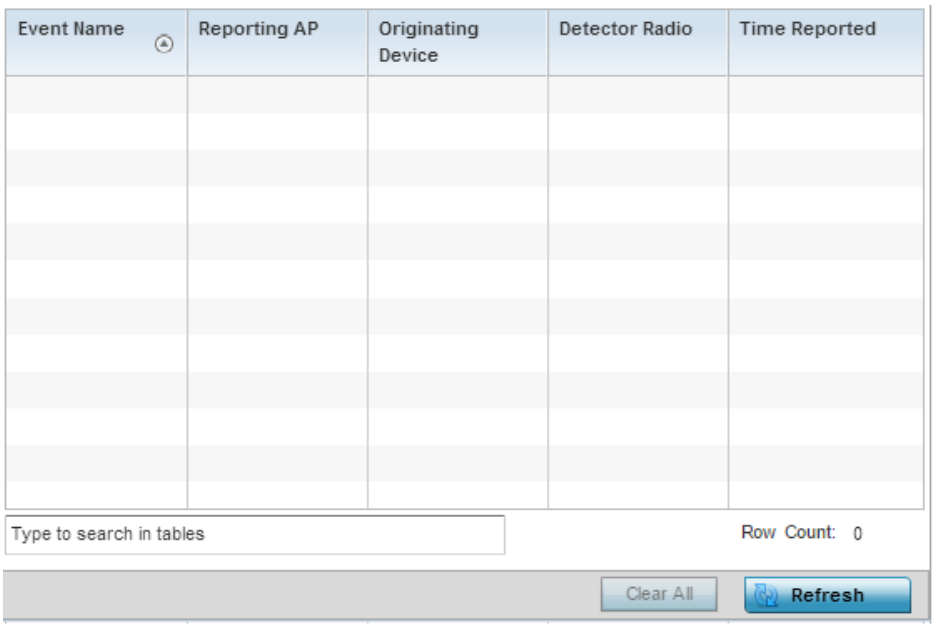


Figure 108: Access Point - WIPS Events screen

The **WIPS Events** screen provides the following:

Event Name	Displays the name of the detected wireless intrusion event.
Reporting AP	Displays the MAC address of the access point reporting the listed intrusion.
Originating Device	Displays the MAC address of the intruding device.
Detector Radio	Displays the number of the detecting access point radio.
Time Reported	Displays the time when the intrusion event was detected.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Sensor Servers

"Access Point Statistics"

Sensor servers allow the monitor and download of data from multiple sensors 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Sensor Servers**.

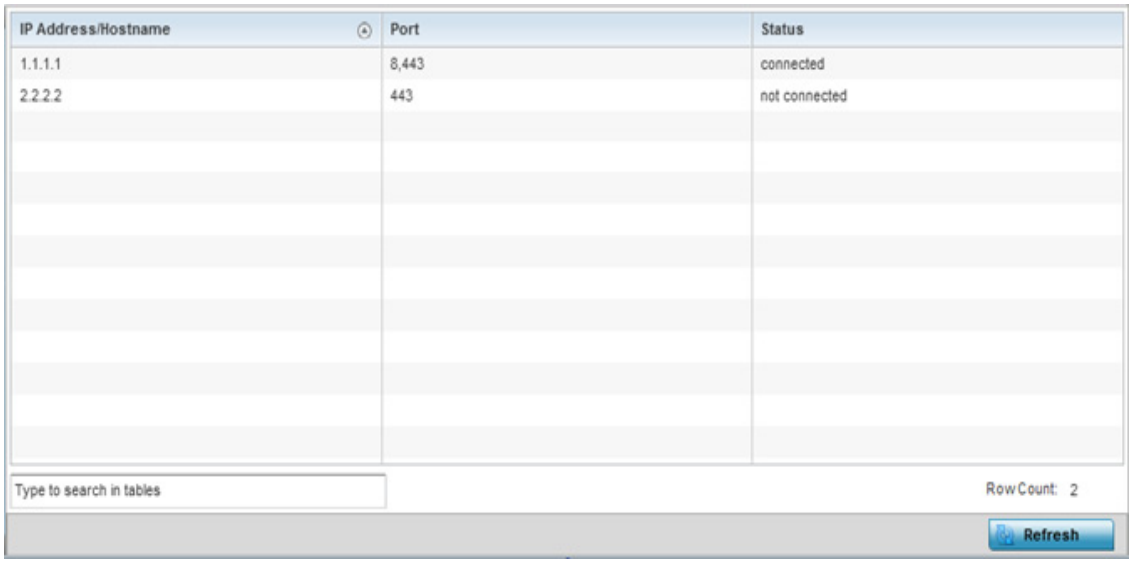


Figure 109: Access Point - Sensor Servers screen

The **Sensor Servers** screen displays the following:

IP Address/ Hostname	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 resource is connected or not.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Bonjour Services

"Access Point Statistics"

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.

To view the available Bonjour Services:

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 a RF Domain and select one of its connected access points.

3 Select **Bonjour Services**.

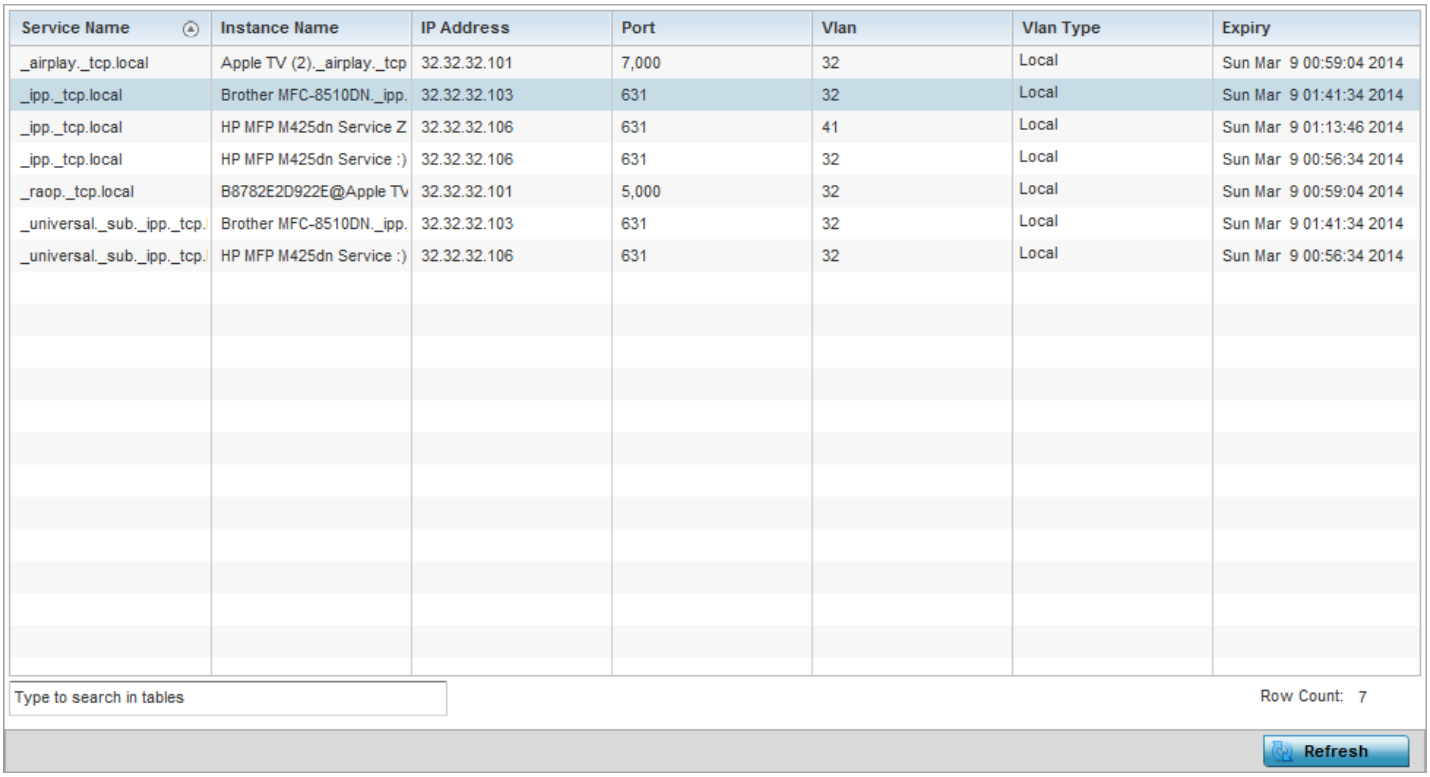


Figure 110: Access Point - Bonjour Services

The **Bonjour Services** screen displays the following:

Service Name	Displays the name of the Bonjour service that is available.
Instance Name	Displays the name of the device providing the service advertised in the *Service Name* field.
IP Address	Displays the IP address of the device providing the Bonjour Service.
Port	Displays the port on which the device provides the Bonjour Service
VLAN	Displays the VLAN on which the advertised Bonjour Service is available.
VLAN Type	Displays *local* if the VLAN on which a service is advertised is local to this network. Displays *tunneled* otherwise.
Expiry	Displays the time at which the advertised service expires.

4 Select **Refresh** to refresh the displayed statistics.

Captive Portal

"Access Point Statistics"

A captive portal forces a HTTP client to use a special Web page for authentication before using the 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 the captive portal statistics of an access point:

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 a RF Domain and select one of its connected access points.

3 Select **Captive Portal**.

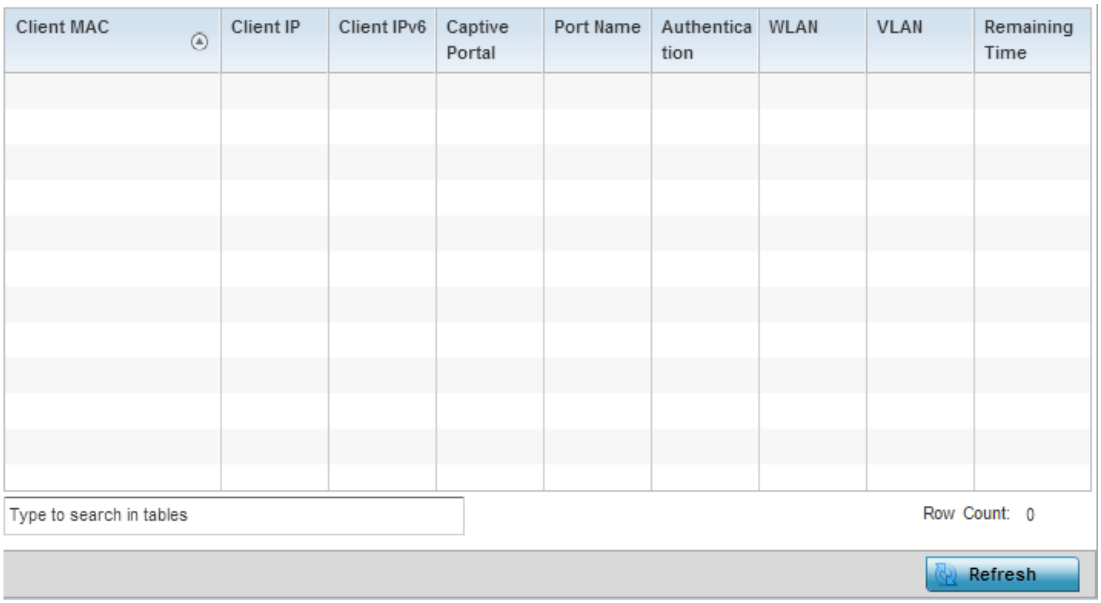


Figure 111: Access Point - Captive Portal screen

The **Captive Portal** screen displays the following:

Client MAC	Displays the MAC address of requesting wireless clients. The client address displays as a link that can be selected to display configuration and network address information in greater detail.
Client IP	Displays the IP addresses of captive portal resource requesting wireless clients.
Client IPv6	Displays the IPv6 addresses of captive portal resource requesting wireless clients.
Captive Portal	Displays type of the captive portal page.
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 requesting clients.
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 hosted Internet, and access point connectivity.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Network Time

"Access Point Statistics"

Network Time Protocol (NTP) is central to networks that rely on their access point(s) to supply system time. Without NTP, access point supplied network 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 access point managed enterprise network. The access point can use a dedicated server to supply system time. The access point 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"
- "NTP Association"

NTP Status

"Network Time"

To view the Network Time statistics of an access point:

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 a RF Domain and select one of its connected access points.

3 Select **Network Time.**

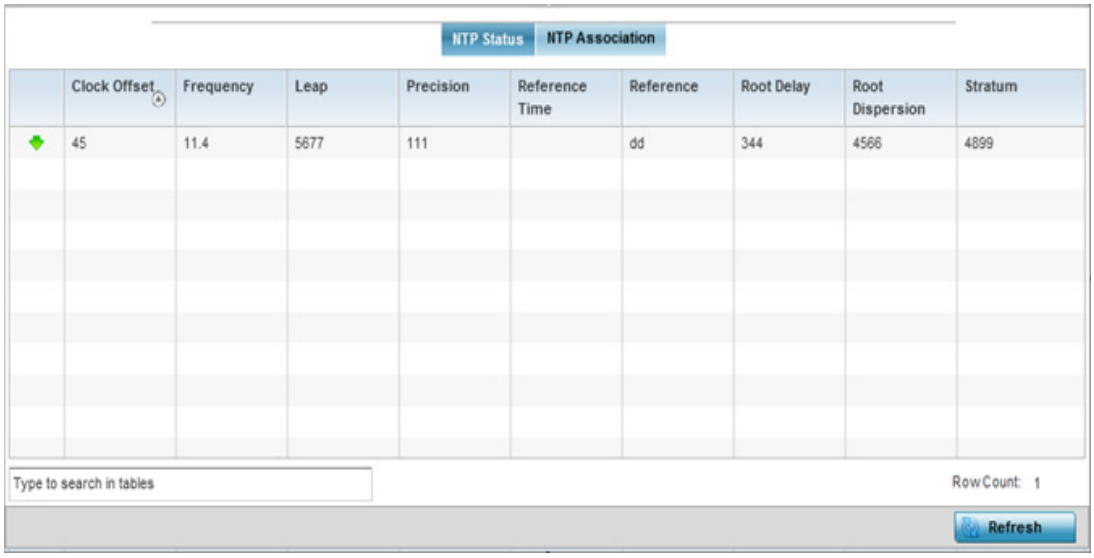


Figure 112: Access Point - NTP Status screen

The **NTP Status** tab displays by default with the following information:

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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

NTP Association

"Network Time"

The interaction between the access point and an NTP server constitutes an association. NTP associations can be either peer associations (the access point synchronizes to another system or allows another system to synchronize to it), or a 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Network Time** and expand the menu to reveal its sub menu items. The **NTP Status** tab displays by default.

4 Select the **NTP Association** tab.

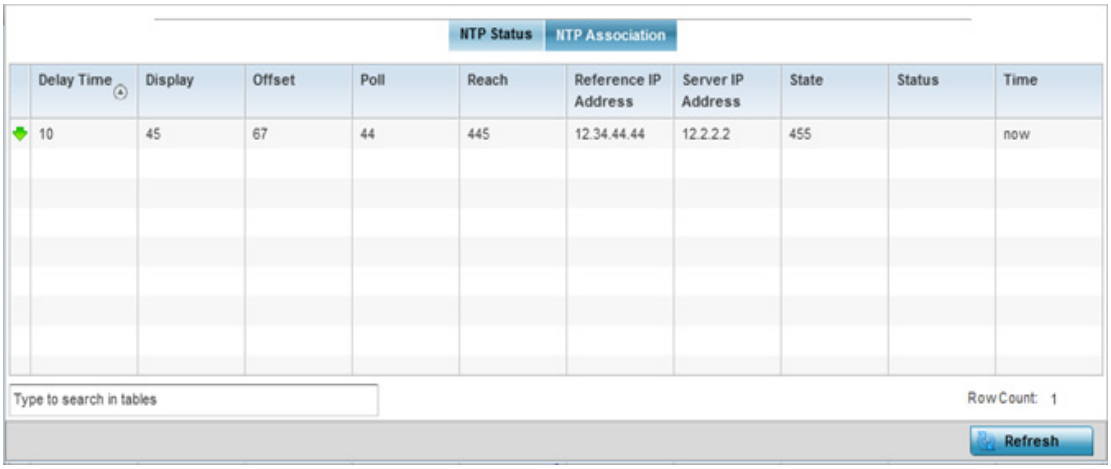


Figure 113: Access Point - NTP Association screen

The **NTP Association** 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 access point is synchronized to this NTP server. • *Unsynced* - Indicates the access point 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 access point chooses a master to synchronize with. • *Candidate* - Indicates this NTP master server may be considered for selection the next time the access point 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Load Balancing

"Access Point Statistics"

An access point load can be viewed in a graph 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. The channels can also be filtered for display. 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 Select System from the navigation pane (on the left-hand side of the screen). Expand a RF Domain and select one of its connected access points.

3 Select **Load Balancing**.

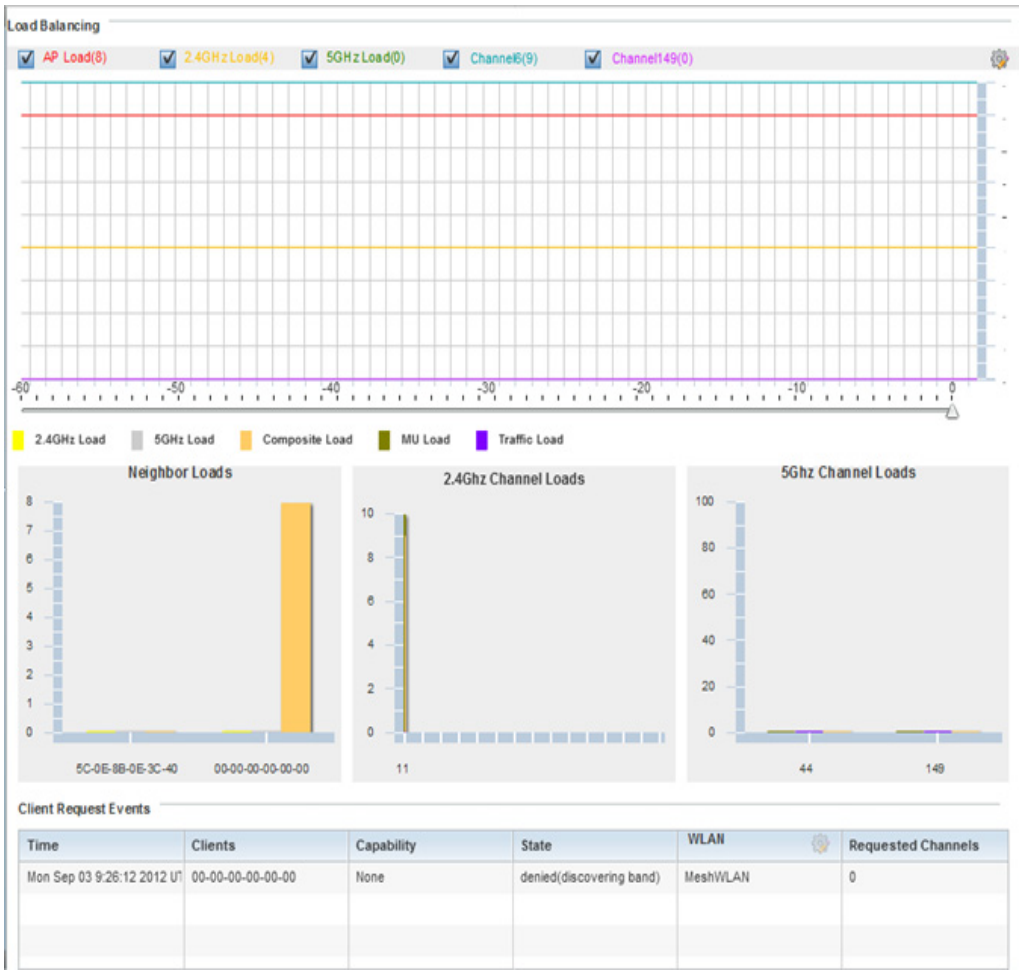


Figure 114: Access Point - Load Balancing screen

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. Remember, AP6532 and AP7161 models can support up to 256 clients per access point and AP6521 model supports up to 128 clients per access point.

Environmental Sensors (AP8132 Models Only)

"Access Point Statistics"

An AP8132 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 AP8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To view an AP8132 model access point's environmental 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 a RF Domain and select one of its connected AP8132 access points.

3 Select **Environment**.

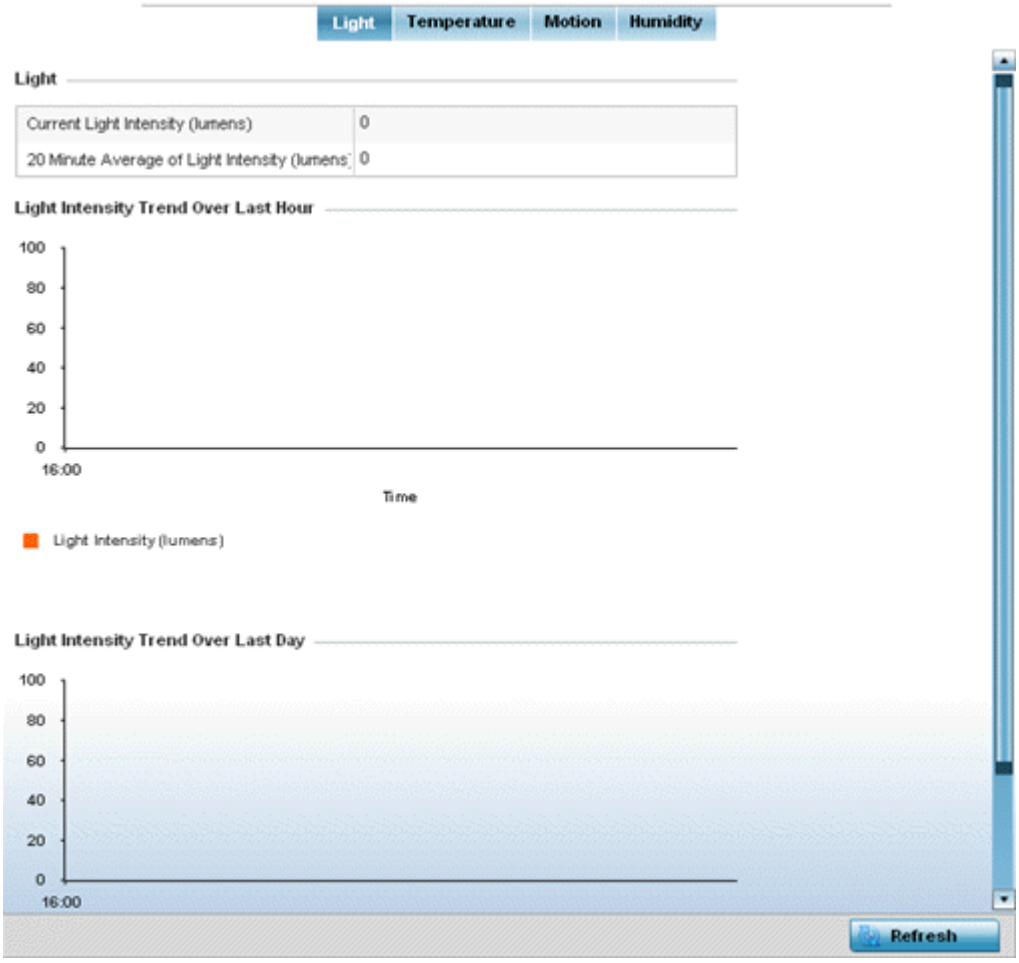


Figure 115: Access Point - Environmental Sensor screen (Light tab)

The **Light** tab displays by default, with additional *Temperature, Motion* and *Humidity* tabs available for unique sensor reporting. Each of these sensor measurements helps the administrator determine whether the immediate deployment area is occupied by changes in the access point's environment.

4 Refer to the **Light** table to assess the sensor's detected light intensity within the AP8132 immediate deployment area.

Light intensity is measured by the sensor in lumens. The table displays the **Current Light Intensity (lumens)** and a **20 Minute Average of Light Intensity (lumens)**. Compare these two items to determine whether the 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. For more information, see "Environmental Sensor Configuration" on page 293.

5 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.

6 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 AP8132 can be upgraded or powered off during specific hours of the day.

7 Select the **Temperature** tab.

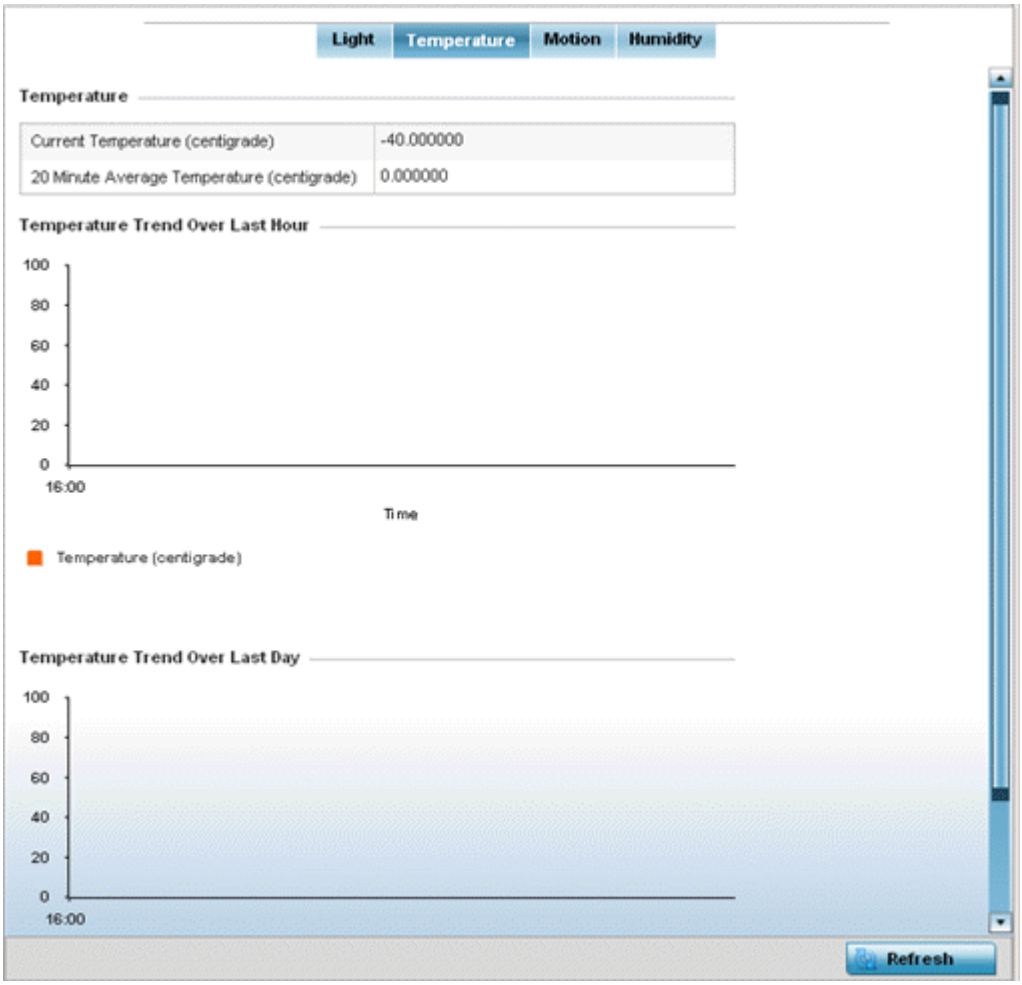


Figure 116: Access Point - Environmental Sensor screen (Temperature tab)

8 Refer to the **Temperature** table to assess the sensor's detected temperature within the AP8132's immediate deployment area.

Temperature is measured in centigrade. The table displays the **Current Temperature (centigrade)** and a **20 Minute Average Temperature (centigrade)**. Compare these two items to determine whether the AP8132's deployment location remains consistently

heated. For more information on enabling the sensor, see "Environmental Sensor Configuration" on page 293.

9 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.

10 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 AP8132 can be upgraded or powered off during specific hours of the day.

11 Select the **Motion** tab.

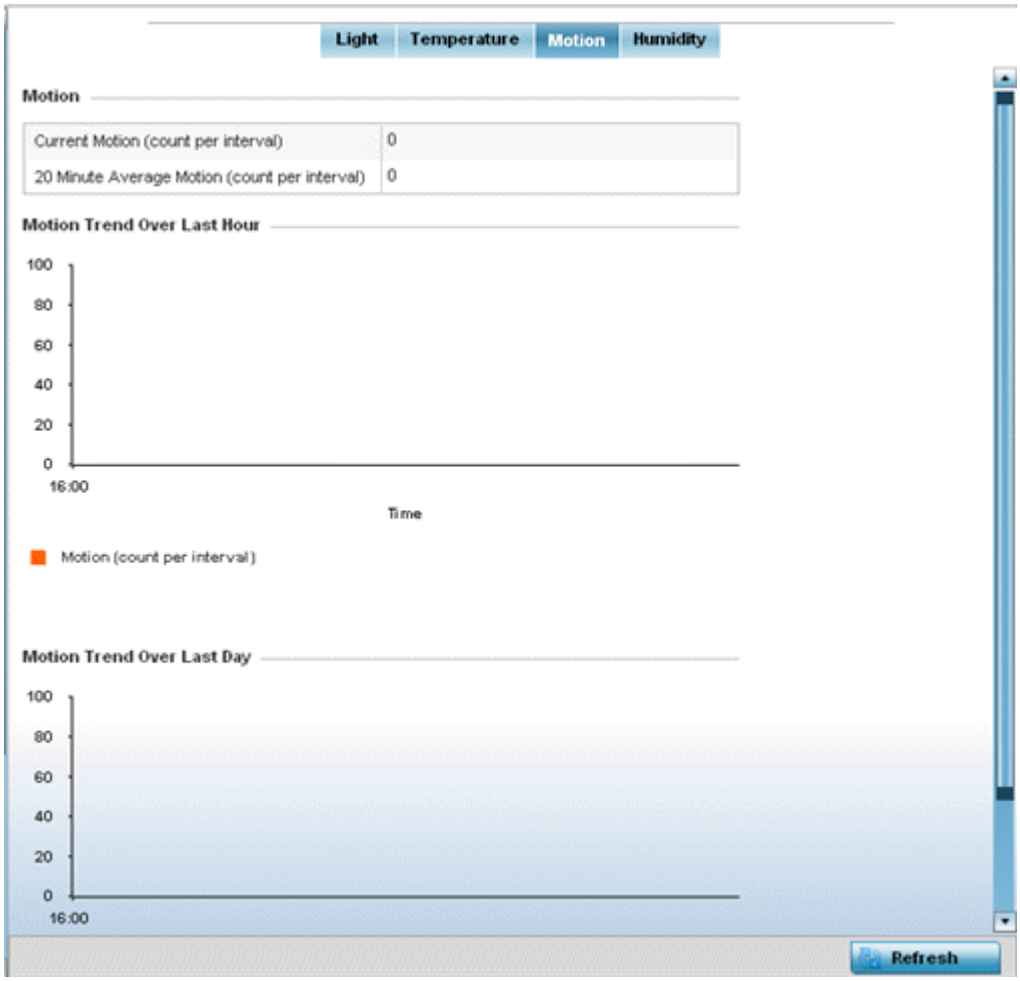


Figure 117: Access Point - Environmental Sensor screen (Motion tab)

12 Refer to the **Motion** table to assess the sensor's detected movement within the AP8132's immediate deployment area.

Motion is measured in intervals. The table displays the **Current Motion (count per interval)** and a **20 Minute Average Motion (count per interval)**. Compare these two items to determine whether the AP8132's deployment location remains consistently occupied by client users. For more information on enabling the sensor, see "Environmental Sensor Configuration" on page 293.

13 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.

14 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 AP8132 can be upgraded or powered off during specific hours of the day.

15 Select the **Humidity** tab.

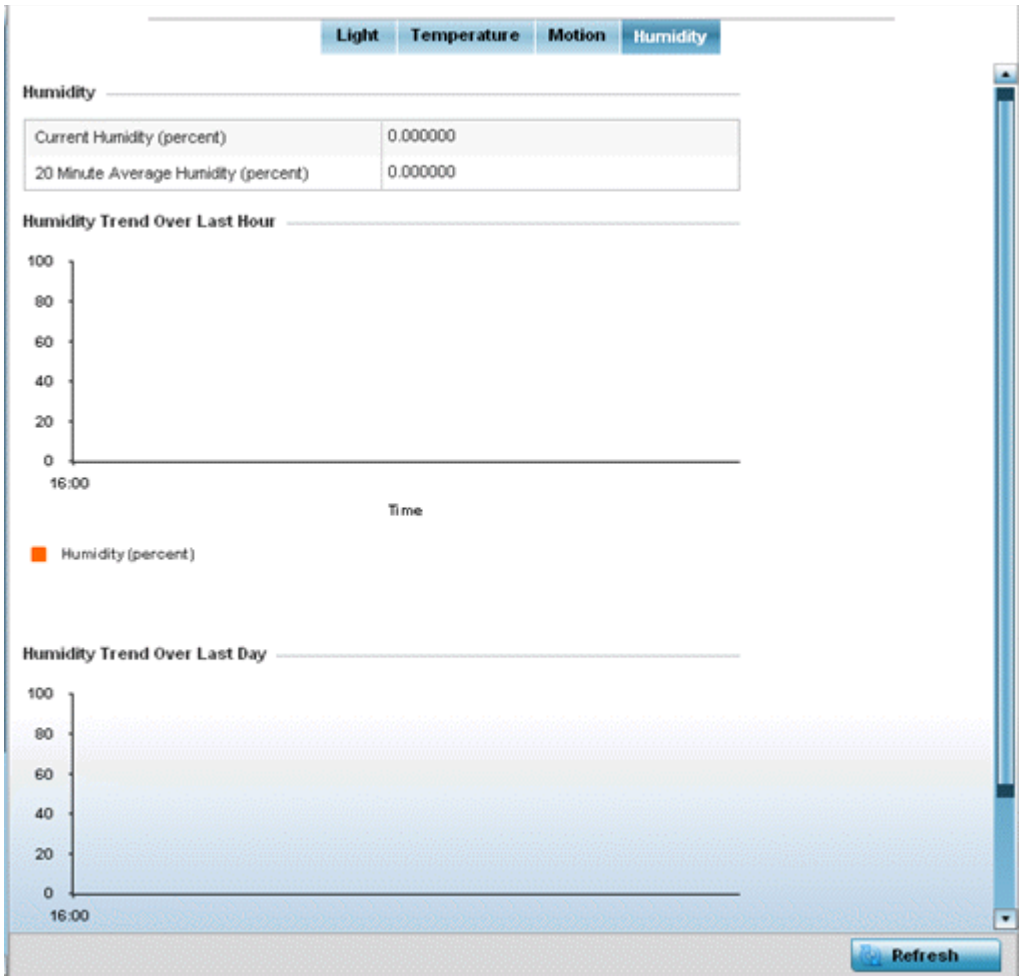


Figure 118: Access Point - Environmental Sensor screen (Humidity tab)

16 Refer to the **Humidity** table to assess the sensor's detected humidity fluctuations within the AP8132's immediate deployment area.

Humidity is measured in percentage. The table displays the **Current Humidity (percent)** and a **20 Minute Average Humidity (percent)**. Compare these two items to determine whether the AP8132's deployment location remains consistently humid (often a by-product of temperature). For more information on enabling the sensor, see "Environmental Sensor Configuration" on page 293.

17 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.

18 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 AP8132 can be upgraded or powered off during specific hours of the day.

Wireless Client Statistics

"Statistics"

The wireless client statistics display read-only statistics for a client selected from within its connected access point directory. It provides an overview of the health of wireless clients in the network. Use this information to assess if configuration changes are required to improve client performance.

Wireless clients statistics can be assessed using the following criteria:

- "Health"
- "Details"
- "Traffic"
- "WMM TSPEC"
- "Association History"
- "Graph"

Health

"Wireless Client Statistics"

The *Health* screen displays information on the overall performance of a selected wireless client.

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 a RF Domain, select an access point, then a connected client.

3 Select **Health**.

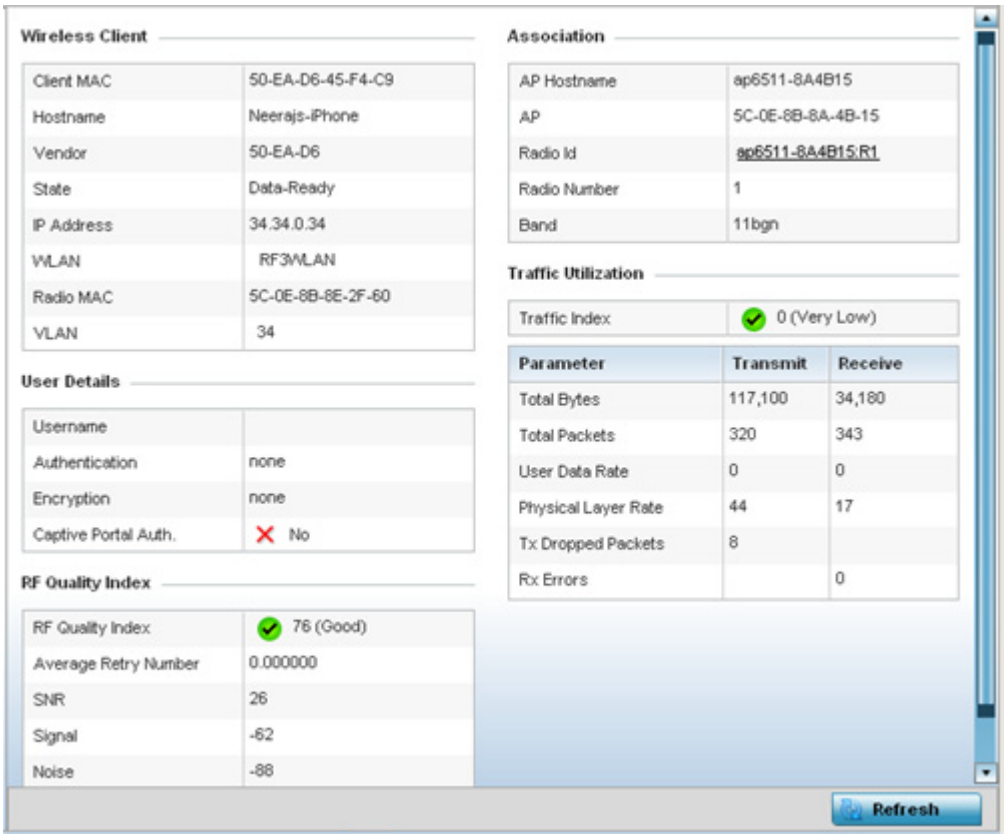


Figure 119: Wireless Client - Health screen

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 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 clients'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 managing the client's connected access point, controller or service platform.
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 *signal to noise* (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.

4 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 is 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)

The **Traffic Utilization** 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Details

"Wireless Client Statistics"

The *Details* screen provides granular performance 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 a RF Domain, select an access point, then a connected client.

3 Select **Details**.

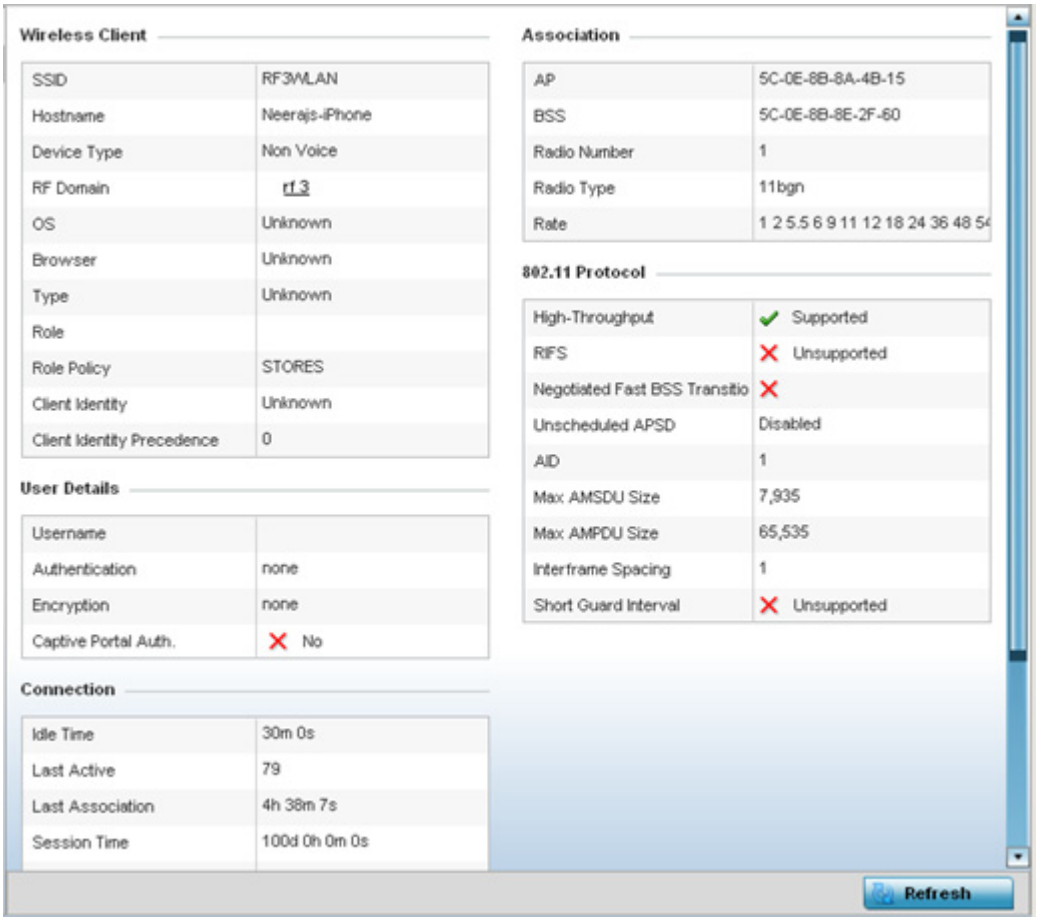


Figure 120: Wireless Client - Details screen

The Wireless Client field displays the following:

SSID	Displays the client's *Service Set ID* (SSID).
Hostname	Lists the hostname assigned to the client when initially managed by the 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 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 network.
Role Policy	Lists the user role set for the client as it became a access point managed device.
Client Identity	Displays the unique vendor identity of the listed device as it appears to its adopting device.
Client Identity Precedence	Lists the numeric precedence this client uses in establishing its identity amongst its peers.

The User Details field displays the following:

Username	Displays the unique name of the administrator or operator managing the client's connected access point.
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 the access point.
SM Power Save Mode	Displays whether this feature is enabled on the wireless client. The *spatial multiplexing* (SM) 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 802.11 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 maximum data rate at the physical layer.
Max User Rate	Displays the maximum 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 client's connected access point.
BSS	Displays the *Basic Service Set* (BSS) 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 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 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 the successful packet delivery over a communication channel.
RIFS	Displays whether this feature is supported. RIFS is a required 802.11n feature that improves performance by reducing the amount of dead time between OFDM transmissions.
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.
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.
AID	Displays the *Association ID* (AID) 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 that are wrapped in an 802.11n MAC header. AMPDUs are used in a very noisy environment to provide reliable packet transmission. This value is the maximum AMPDU size in bytes.
Interframe Spacing	Displays the 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 *inter-symbol interference* (ISI). 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%.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

Traffic

"Wireless Client Statistics"

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 a RF Domain, an access point, then a connected client.

3 Select **Traffic**.



Figure 121: Wireless Client - Traffic screen

Traffic Utilization statistics employ an index, which measures how efficiently the traffic medium is used. It is defined as the percentage of current throughput relative to the maximum possible throughput. 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/multicast 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 *Power Save Poll* (PSP) 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	Displays the connected client's *signal to noise ratio* (SNR). A high SNR could warrant a different access point connection to improve performance.
Signal	Displays the power of the radio signals in - dBm.
Noise	Displays the disturbing influences on the signal 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.
MOS Score	Displays average voice call quality using the *Mean Opinion Score* (MOS) 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 is 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 *Voice over IP* (VoIP) 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.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values

WMM TSPEC

"Wireless Client Statistics"

The 802.11e *Traffic Specification* (TSPEC) provides a set of parameters that define the characteristics of the traffic stream, (operating requirement and scheduling etc.). The sender TSPEC specifies parameters available for packet flows. Both sender and the receiver use TSPEC.

The TSPEC screen provides 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 a RF Domain, an access point, then a connected client.

3 Select **WMM TPSEC**.

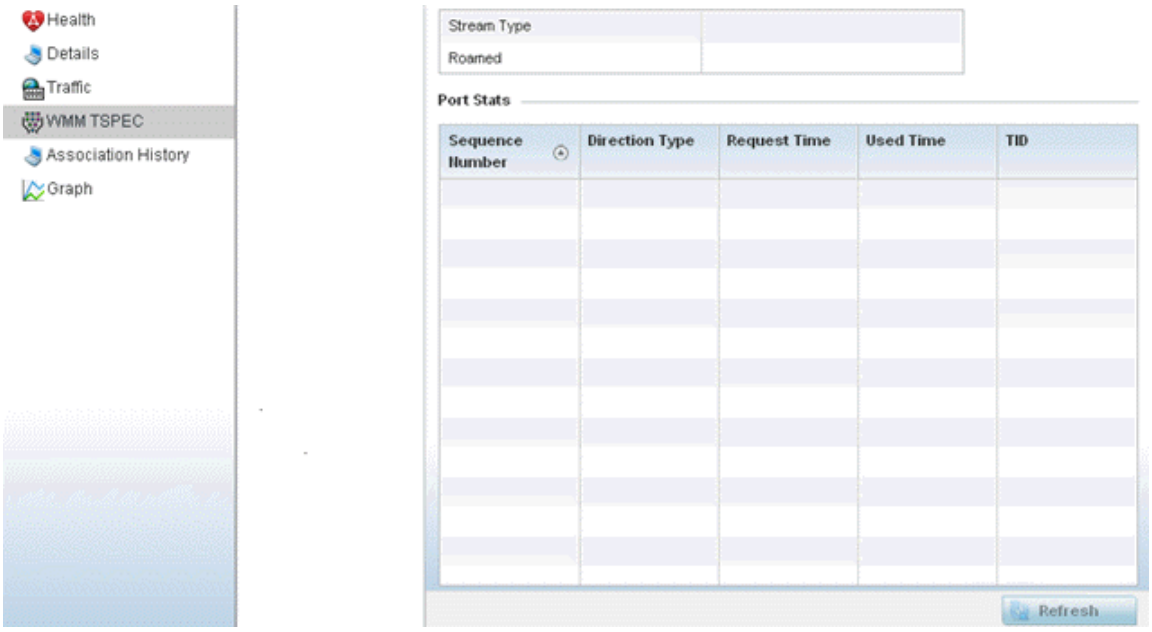


Figure 122: Wireless Client - WMM TPSEC screen

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 a 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 *delete traffic stream* (DELTS) 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.

Association History

"Wireless Client Statistics"

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. 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 or service platform 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 a RF Domain, an access point, then a connected client.

3 Select **Association History**.

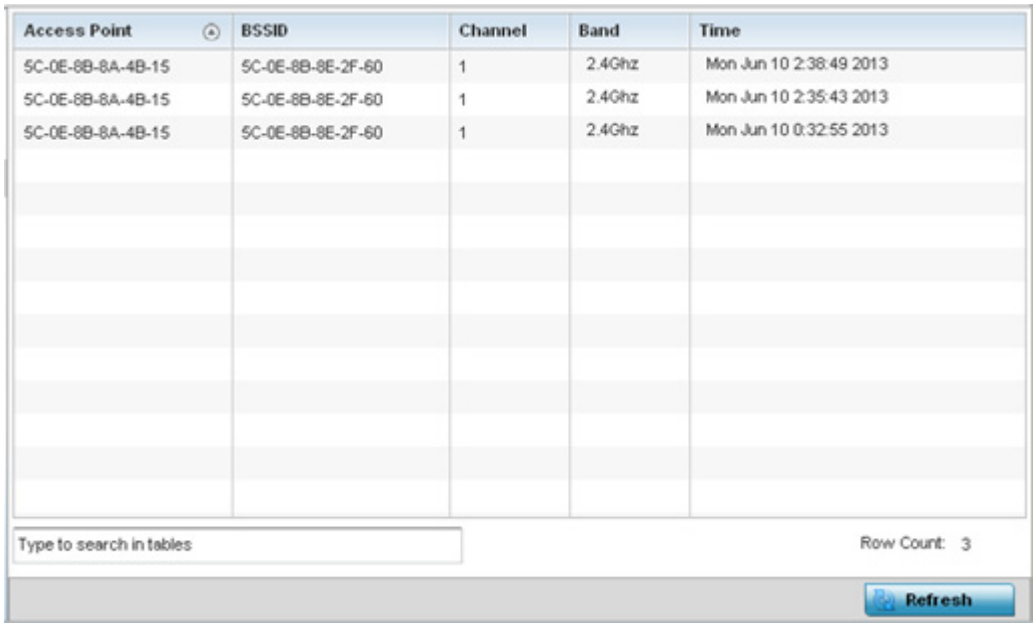


Figure 123: Wireless Client - Association History screen

Refer to the following to discern 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.

4 Select **Refresh** to update the screen to its latest values.

Graph

"Wireless Client Statistics"

Use the client **Graph** to assess a connected client's radio performance and diagnose performance issues that might negatively impact 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 a RF Domain, an access point then a connected client.

3 Select **Graph**.

4 Use the **Parameters** drop down menu to define from 1- 3 variables assessing client 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*. 30 seconds is the default value.

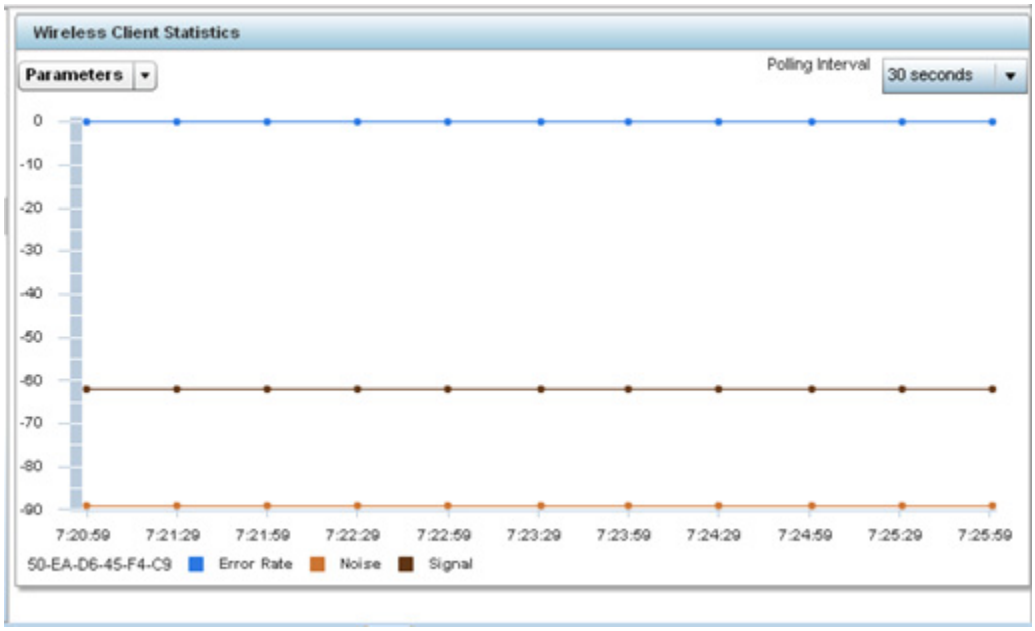


Figure 124: Wireless Client - Graph

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.

14 WiNG Events

WiNG outputs an event message for configuration changes and status updates to enable an administrator to assess the success or failure of specific configuration activities. Use the information in this chapter to review system generated event messages and their descriptions.

Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/encryption and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices. By default, there's 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 839.

Event History Messages

To review event history messages:

1 Select **Configuration** > **Diagnostics** > **Fault Management** > **Event History** to display the Event History screen.

2 Select **Fetch Historical Events** to display the diagnostic events in the Event History table.

3 Refer to the following (read only) information to assess logged diagnostic events.

ADOPT-SERVICE SNMP_SUCCESS 6	SNMP framework success
ADOPT-SERVICE SNMP_FAILURE 6	SNMP framework failure
ADOPT-SERVICE TUT_TEMPERATURE_ALARM_RAISED ([str])	Temperature alarm raised on sensor
ADOPT-SERVICE TUT_TEMPERATURE_ALARM_CLEARED ([str])	Temperature alarm cleared on sensor
ADOPT-SERVICE TUT_TEMPERATURE_ALARM_CLEARED ([str])	Temperature alarm cleared on sensor
ADOPT-SERVICE TUT_FAN_ALARM_CLEARED 5 IPX ([str])	Fan alarm cleared on ID
ADOPT-SERVICE TUT_PWRCTRL_ALARM_RAISED 5 IPX ([str])	Power controller alarm raised
ADOPT-SERVICE TUT_PWRCTRL_ALARM_CLEARED 5 IPX ([str])	Power controller alarm cleared
ADOPT-SERVICE TUT_LINE_POWER_ALARM_RAISED 5 IPX ([str]) Line power alarm raised on id [str]	Line power alarm raised
ADOPT-SERVICE TUT_LINE_POWER_ALARM_CLEARED 5 IPX ([str]) Line power alarm cleared on id [str]	Line power alarm cleared

ADOPT-SERVICE TUT_WLAN_CLIENT_ASSOC 6 IPX ([str]) Client [str] on interface index [str] associated	Client associated
ADOPT-SERVICE TUT_WLAN_CLIENT_DISASSOC 6 IPX ([str]) Client [str] on interface index [str] disassociated with status code [str], [str]	Client disassociated
ADOPT-SERVICE TUT_WLAN_CLIENT_ASSOC_FAILURE 3 IPX ([str]) Association failed for Client [str] on interface index [str] with status code [str], [str]	Association failed for client on specified interface index
ADOPT-SERVICE TUT_WLAN_CLIENT_AUTH 6 IPX ([str])	Client on interface index authenticated
ADOPT-SERVICE TUT_WLAN_CLIENT_DEAUTH 6 IPX ([str])	Client on interface index deauthenticated with status code
ADOPT-SERVICE TUT_WLAN_CLIENT_AUTH_FAILURE 3 IPX ([str])	Authentication failed for client on interface index with status code
ADOPT-SERVICE TUT_RADIO_ADAPTIVE_POWER_CHANGE 5 IPX ([str])	Interface with operational status and power levels
ADOPT-SERVICE TUT_RF_MONITOR_MODE_CHANGE 5 IPX ([str])	RF monitor status changed to on interface
ADOPT-SERVICE IPX_EVENT_FAILURE 3 IPX ([str])	Failed to raise WiNG event
AP NO_IMAGE_FILE [str] firmware image is not present on controller	Access point firmware not on controller
AP IMAGE_PARSE_FAILURE Format of [str] firmware image on controller is invalid	Invalid access point firmware file
AP LEGACY_AUTO_UPDATE Legacy Access Point [str] [mac] being updated	Legacy access point updated
AP AP_ADOPTED [str] [mac] adopted	Access point adopted
AP AP_UNADOPTED [str] [mac] un-adopted	Access point unadopted
AP AP_RESET_DETECTED 6 [str] [mac] reset itself	Access point reset detected
AP AP_RESET_REQUEST 6 [str] [mac] reset request	Access point user requested reset
AP AP_TIMEOUT 6 str] [mac] timed out, reset sent to AP	Access point timed out
AP ADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] adopted and configured. Radios: Count=[str], Bss: [str]	Access point adopted and configured
AP UNADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] unadopted. Radios: Count=[str], Bss: [str]	Access point unadopted
AP ADOPTED_TO_CONTROLLER Joined successfully with controller [qstr]([str])	Access point adopted to controller

AP ONLINE Access Point [dev] is now online. Offline Reason is [str]. Offline count is [int]	Access point online
AP OFFLINE Access Point [dev] is now offline. Offline Reason is [str]. Offline count is [int]	Access point offline
AP OFFLINE Device [dev]([str]) is offline, last seen:[int] minutes ago on switchport [str]	Adopted device offline
AP RESET Reset Access Point mac [dev], [str]	Access point reset
AP ADOPTION_REDIRECTED Access Point([qstr]/[qstr]/[dev]) cdp:[qstr] lldp:[qstr] redirected to the controller host/pair [qstr] - [qstr]	Access point redirected
AP AP_AUTOUP_TIMEOUT 4 AUTOUPGRADE: [str] mac [str] Autoupgrade timed out	Time out while auto upgrading an access point
AP AP_AUTOUP_REBOOT 5 AUTOUPGRADE: [str] mac [str] Autoupgrade rebooting	Rebooting access point 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
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
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 success
ADV-WIPS ADV-WIPS-EVENT-26 4 Detected DoS RTS flood attack against [mac] [str]	DoS RTS flood attack
ADV-WIPS ADV-WIPS-EVENT-222 4 Detected Invalid Channel Advertisement for [mac] [str]	Invalid channel advertisement
ADV-WIPS ADV-WIPS-EVENT-63 4 Detected Windows ZERO Configuration Memory Leak on [mac] [str]	Windows ZERO configuration memory leak
ADV-WIPS ADV-WIPS-EVENT-220 4 Detected Unauthorized Bridge [mac] [str]	Unauthorized bridge
AP SW_CONN_LOST 0 Lost connectivity with controller after config update. Rebooting and reverting to older working configuration	Controller connectivity lost
AAA RADIUS_DISCON_MSG5 Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr]	Received RADIUS resource disconnect request
AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr]	Client VLAN updated by RADIUS
AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr]	Start time from RADIUS resource not yet valid

AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr]	Session time from RADIUS resource already expired
CAPTIVE-PORTAL AUTH_SUCCESS6 Captive-portal authentication success for client [mu] ([qstr-ip]) user [qstr]	Authentication success
CAPTIVE-PORTAL AUTH_FAILED6 Captive-portal authentication failed for client [mu] ([qstr-ip])	Authentication failed
CAPTIVE-PORTAL SESSION_TIMEOUT6 Captive-portal session timed out for client [mu] ([qstr-ip])	Session timed out
CAPTIVE-PORTAL CLIENT_DISCONNECT 6 Captive-portal session disconnected for client [mu] ([qstr-ip])	Client disconnected
CAPTIVE-PORTAL PURGE_CLIENT6 Captive-portal: Purge client [mu] by new client [mu] for user [qstr]	Client purged
CAPTIVE-PORTAL FLEX_LOG_ACCESS 6 [qstr]: [qstr] allowed access for client [mu] ([qstr-ip])	Flex log access granted for client
CAPTIVE-PORTAL INACTIVITY_TIMEOUT 6 Captive-portal session cleared for client [mu] ([qstr-ip]) after inactivity timeout	Client timed out due to inactivity
CAPTIVE-PORTAL ALLOW_ACCESS6 Captive-portal allow access for client [mu] ([qstr-ip])	Client allowed access
CAPTIVE-PORTAL CLIENT_REMOVED6 Captive-portal session removed for client [mu] ([qstr-ip]) on policy change/admin action	Client removed due to admin changes
CAPTIVE-PORTAL PAGE_CRE_FAILED3 Page creation failed for policy [qstr], file [qstr], Error [qstr]	Page creation failure
CAPTIVE-PORTAL DATA_LIMIT_EXCEED6 Data limit exceed, Usage:[int] KBytes, Action:[str], client [mu] ([ip])	Client data limit exceeded
CAPTIVE-PORTAL VLAN_SWITCH6 Client [mu] ([ip]) switching from vlan [int] to vlan [int]	Client VLAN switch
CAPTIVE-PORTAL SERVER_MONITOR_STATE_CHANGE6 Captive-portal policy [qstr]: service monitor [str] server status changing from [qstr] to [qstr]	Captive portal server monitor state changed
CAPTIVE-PORTAL NO_SERVICE_PAGE_SENT6 Captive-portal sent no service page to client [mu] ([ip]) as [str] server is down	No service page sent to client
CERTMGR RSA_KEY_ACTIONS_SUCCESS 6 [str] of RSA key [str] successful	Successful completion of RSA key related actions (import, export etc.)
CERTMGR RSA_KEY_ACTIONS_FAILURE 3 [str] of RSA key [str] failed: [str]	Failure of RSA key related actions (import, export etc.)
CERTMGR CA_CERT_ACTIONS_SUCCESS 6 [str] of CA certificate for trustpoint [str] successful	Successful completion of CA certificate related actions (import, export etc.)

CERTMGR CA_CERT_ACTIONS_FAILURE 3 [str] of CA certificate for trustpoint [str] failed: [str]	Failure of CA certificate actions (import, export etc.)
CERTMGR SRV_CERT_ACTIONS_SUCCESS 6 [str] of Server Certificate of trustpoint [str] successful	Successful completion of server certificate actions (import, export etc.)
CERTMGR SVR_CERT_ACTIONS_FAILURE 3 [str] of Server Certificate of trustpoint [str] failed: [str]	Failure of server certificate actions (import, export etc.)
CERTMGR CSR_EXPORT_SUCCESS 6 Export of Certificate Signing Request for [str] successful	Successful export of certificate signing request
CERTMGR CSR_EXPORT_FAILURE 3 Export of Certificate Signing Request for [str] failed: [str]	Failed to export certificate signing request
CERTMGR CRL_ACTIONS_SUCCESS 6 [str] of CRL for trustpoint [str] successful	Successful completion of certificate revocation list action
CERTMGR CRL_ACTIONS_FAILURE 3 [str] of CRL for trustpoint [str] failed: [str]	Certificate revocation list action failure
CERTMGR DELETE_TRUSTPOINT_ACTION 6 Deletion of trustpoint [str] successful	Deletion of trustpoint
CERTMGR IMPORT_TRUSTPOINT 6 Import of Trustpoint [str] [str]	Import of trustpoint
CERTMGR EXPORT_TRUSTPOINT 6 Export of Trustpoint [str] [str]//	Export of trustpoint
CERTMGR CERT_EXPIRY 4 [str] certificate for trustpoint [str] [str]	Certificate expiration
CERTMGR CA_KEY_ACTIONS_SUCCESS 6 [str] of CA private key for trustpoint [str] successful	Successful completion of CA private key actions
CERTMGR CA_KEY_ACTIONS_FAILURE 3 [str] of CA private key for trustpoint [str] failed: [str]	Failure of CA private key actions
CLUSTER CMASTER_CFG_UPDATE_FAIL 3 Cluster master config update to [str] failed, Err: [str]	Cluster master config update failed
CLUSTER MAX_EXCEEDED 4 Max cluster members ([uint]) exceeded, clustering will not function properly until corrected	Max cluster count exceeded
CLUSTER STATE_CHANGE 4 Active cluster member changed. Present active [str]. Previous active [str].	Active cluster membership change
CLUSTER STATE_CHANGE_INACTIVE 4 Member [str] (load[int]) changing state from Active to Standby. New member [str] standby load [int].	Cluster member change from active to standby
CLUSTER STATE_CHANGE_ACTIVE 4 Member [str] (load[int]) changing state from Standby to Active. New member [str] standby load [int]	Cluster member change from standby to active
CLUSTER STATE_RETAIN_ACTIVE 4 Member [str] (load[int]) retaining Active state. New member [str] standby load [int]	Cluster member retaining active state
CRM CRITICAL_RESOURCE_UP5 Critical Resource [str] is UP	Critical resource is up

CRM CRITICAL_RESOURCE_DOWN 5 Critical Resource [str] is DOWN	Critical resource is down
CERTMGR-LITE INVALIDCACERT 5 CA Certificate imported for the trustpoint [str] is invalid	CA certificate is invalid
CERTMGR-LITE INVALIDSERVCERT 5 Server Certificate imported for the trustpoint [str] is invalid	Server certificate is invalid
CERTMGR-LITE INVALIDCERTCRL 5 Certificate Crl Imported for trustpoint [str] is invalid	CRL is invalid
CERTMGR-LITE CERTEXPIRED 5 [str] Certificate of trustpoint [str] is expired//	Certificate is expired
CERTMGR-LITE INVALIDCERTKEY 5 Private key imported for trustpoint [str] is not valid	Private key is invalid
CERTMGR-LITE INVALIDRSAKEY 5 Rsakey imported is not valid [str] is invalid//	RSA key import operation
CERTMGR-LITE KEYDECRYPTFAILE 4 Rsakey cannot be decrypted with the password provided	RSA key cannot be decrypted with provided password
CERTMGR-LITE CERTIMPORTED 6 [str] Certificate imported for the trustpoint [str]	Certificate imported for trustpoint
CERTMGR-LITE CERTKEYIMPORTED 6 Private key imported for the trustpoint [str]	Private key imported for trustpoint
CERTMGR-LITE RSAKEYIMPORTED 6 Rsakey imported with the name [str]	RSA key imported
CERTMGR-LITE DELETETRUSTPOINT 6 Trustpoint [str] is deleted	Trustpoint deleted
CERTMGR-LITE DELETERSAKEY 6 Rsakey [str] is deleted	RSA Key deleted
CERTMGR-LITE CERTREQUESTGEN 6 Certificate request generated for the trustpoint [str]	Certificate requested generated
CERTMGR-LITE CERTSELFSIGNEDGEN 6 Selfsigned certificate generated for the trustpoint [str]	Self signed certificate generated
CERTMGR-LITE RSAKEYGEN 6 Rsa key [str] generated	RSA key generated
CERTMGR-LITE ERROR 5 [str]	Certificate manager general error
CERTMGR-LITE CERT_EXPIRY4 [str] certificate for trustpoint [str] [str]	Certificate about to expire
CERTMGR CERT_RENEW_FAILED1 Certificate renew in field failed reason [str]	Certificate renew failure reason
DHCPSVR DHCPSVR_STOP 6 DHCP server is stopped	DHCP server stopped
DIAG WD_RESET_SYS 2 The system has been RESET by the Watchdog	Log watchdog reset
DIAG CPU_USAGE_TOO_HIGH 4 CPU Usage too high. Limit of [int]*(0.1%) exceeded. Current CPU usage is [int]*(0.1%)	Log CPU load detected as too high

DIAG CPU_USAGE_TOO_HIGH_RECOVER 4 CPU Usage too high recover. Limit is [int]*(0.1%)	Current CPU usage is too high
DIAG CPU_LOAD 4 [str] minute average load limit exceeded, value is [str]% limit is [str]% (top processes: [str])	CPU average load limit exceeded
DIAG RAM_USAGE 6 [str], pid [uint], has exceeded ram usage limit [uint].[uint]%, now using [uint].[uint]%	Log processor RAM usage has exceeded RAM limit
DIAG MEM_USAGE_TOO_HIGH 6 Memory Usage too high. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%)	Memory usage too high
DIAG MEM_USAGE_TOO_HIGH_RECOVER 6 Memory Usage too high recover. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%)	Memory usage detected as too high
DIAG BUF_USAGE 6 [uint] byte buffer usage greater than expected, [uint] used, warning level [uint]	Log buffer usage greater than anticipated
DIAG HEAD_CACHE_USAGE 6 socket buffer head cache usage is greater than expected, usage [uint], warning level [uint]	Log head cache usage greater than anticipated
DIAG IP_DEST_USAGE 6 IP destination cache usage is greater than expected, usage [uint], warning level [uint]	Log destination cache usage greater than anticipated
DIAG FREE_RAM 6 Free RAM, [str]% is less than limit [str]%. Top Memory process: [str]/[uint] using [uint].[uint]% , [str]/[uint] using [uint].[uint]% , [str]/[uint] using [uint].[uint]%	Log RAM space less than limit
DIAG FREE_FLASH_DISK 4 Free [str] file system space, [str]% is less than limit [str]%	Log free disk space less than limit
DIAG DISK_USAGE 4 Disk usage too high	Log disk usage too high
DIAG NEW_LED_STATE 6 LED state message [str] from module [str]	Log LED message from module
DIAG FREE_FLASH_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint]	Log INodes less than system limit
DIAG FREE_NVRAM_DISK 4 Free [str] file system space, [str]% is less than limit [str]%	Log file system space less than limit
DIAG FREE_NVRAM_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint]	Log free INodes on file system less than limit
DIAG FREE_RAM_DISK 4 Free [str] file system space, [str]% is less than limit [str]%	Log free file system space less than limit
DIAG FREE_RAM_INODES 4 [uint] Free INodes on [str] file system is less than limit [uint]	LOG_FREE_VARFS_INODES
DIAG FD_COUNT 4 FD Usage [uint] is over limit [uint]	HUMM
DIAG DISK_USAGE 4 Disk usage too high	Log disk utilization usage too high
DIAG NEW_LED_STATE 6 LED state message [str] from module [str]	Log LED state message from module

DIAG LED_IDENTIFY 6 LED identify sequence [str]	Log identification sequence
DHCPSVR RELAY_NO_IFACE 4 Dhcp relay cannot be allowed on interface [str] as it does not exist	No interface for DHCP relay
DHCPSVR RELAY_IFACE_NO_IP 4 Dhcp relay cannot be allowed on interface [str] as it does not have an IP address	No IP address on DHCP relay interface
DHCPSVR RELAY_START 6 DHCP relay agent started on [str]	DHCP relay agent started
DHCPSVR RELAY_STOP 6 DHCP relay agent stopped	DHCP relay agent stopped
DHCPSVR DHCPSVR_START 6 DHCP server is started	DHCP server started
DIAG FAN_UNDERSPEED 4 Fan [str] under speed: [uint] RPM is under limit [uint] RPM	Fan speed under set RPM limit
DIAG ELAPSED_TIME 7 Elapsed time since last diag run appears to be zero	Log elapsed time since last diagnostic run
DIAG AUTOGEN_TECH_SPRT 6 Auto generated tech-support dump file [str] [str]	Log generation of tech support dump file
DIAG POE_INIT_FAIL 3 Could not initialize the PoE manager	Log PoE manager intialization failure
DIAG POE_POWER_LEVEL 4 POE power consumption is [uint]W which exceeds [uint]% of [uint]W power budget	Log power consumption exceeds power budget limit
DIAG POE_READ_FAIL 3 Could not read from the PoE	Log PoE read failure
DIAG POE_STATE_CHANGE 4 port [uint] POE state changed to [str]	Log PoE state change
DIAG RAID_DEGRADED 4 RAID array is degraded	Log RAID array degraded
DIAG RAID_ERROR 4 RAID array management error [uint]	Log RAID array management error
DIAG PWRSPLY_FAIL 4 Power supply failure, no longer redundant	Log power supply failure
DIAG HDD_FAILING 4 HDD is failing	Log HDD failure
DIAG UNDER_VOLTAGE 4 Voltage [str]V under low limit [str]V	Log voltage sensor under low limit
DIAG OVER_VOLTAGE 4 Voltage [str]V over high limit [str]V	Log voltage sensor over high limit
DIAG LOW_TEMP 6 Temp sensor [str] [str]C under low limit [str]C	Log temperature sensor under low limit
DIAG HIGH_TEMP 4 Temp sensor [str] [str]C over high limit [str]C	Log temperature sensor over high limit
DIAG OVER_TEMP 0 Temp sensor [str] [str]C over maximum limit [str]C Shutdown switch	Log temperature sensor over max limit
DIAG WD_STATE_CHANGE 6 Watchdog is now [str]	Log watchdog state

DOT1X DOT1X_SUCCESS 6 Client [qstr] 802.1x/ EAP authentication success on interface [qstr]// 802.1x authentication successful	802.1X authentication successful
DOT1X DOT1X_FAILED 5 Client [qstr] failed 802.1x/EAP authentication on interface [qstr]// 802.1x authentication failure	802.1X authentication failed
DOT11 COUNTRY_CODE 5 Country of operation configured to [str]	Country of operation configured
DOT11 COUNTRY_CODE_ERROR 1 Error setting country of operation. [str]	Error setting country of operation
DOT11 CLIENT_ASSOCIATED 6 Client [qstr] associated to wlan [qstr] ssid [qstr] on radio [qstr]	Client associated event
DOT11 CLIENT_DISASSOCIATED 6 Client [qstr] disassociated from wlan [qstr] radio [qstr]: [str] (reason code:[uint])	Client disassociated
DOT11 CLIENT_DENIED_ASSOC 5 Client [qstr] denied association on radio [qstr] [str]: [str]	Client denied association
DOT11 CLIENT_ASSOC_IGNORED 6 Client [qstr] ignored association on radio [qstr] [str]: [str]	Client ignored association
DOT11 WPA_WPA2_SUCCESS 6 Client [qstr] completed [str] handshake on wlan [qstr] radio [qstr]	Client completed WPA/WPA2 handshake
DOT11 WPA_WPA2_FAILED 5 Client [qstr] failed [str] handshake on wlan [qstr] radio [qstr]	Client failed WPA/WPA2 handshake
DOT11 WPA_WPA2_KEY_ROTN 6 Rotating wpa/wpa2 group keys on wlan [qstr] /	Rotating WPA/WPA2 group keys on WLAN
DOT11 TKIP_MIC_FAIL_REPORT 5 TKIP message integrity check failure reported by [mac] on wlan [qstr]	TKIP MIC failure report
DOT11 TKIP_MIC_FAILURE 5 TKIP message integrity check failed in packet from [mac] on wlan [qstr]	TKIP MIC check failed
DOT11 TKIP_CNTRMEAS_START 4 Initiating TKIP countermeasures on wlan [qstr] ssid [qstr]	TKIP countermeasures initiated
DOT11 TKIP_CNTRMEAS_END 4 TKIP countermeasures ended on wlan [qstr] ssid [qstr] //	TKIP countermeasures ended
DOT11 EAP_SUCCESS 6 Client [qstr] 802.1x/EAP (type:[str]) authentication success on wlan [qstr] radio [qstr] username [str]	EAP authentication success
DOT11 EAP_FAILED 5 Client [qstr] failed 802.1x/ EAP authentication on wlan [qstr] radio [qstr]	EAP authentication failure
DOT11 EAP_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP authentication on wlan [qstr] radio [qstr]	EAP authentication timed out
DOT11 EAP_SERVER_TIMEOUT 5 Radius server [str] timeout authenticating client [qstr] on wlan [qstr] radio [qstr]	RADIUS server timed out

DOT11 EAP_CACHED_KEYS 6 Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x	Key cache used for authentication
DOT11 EAP_OPP_CACHED_KEYS 6 Opportunistic Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x.	Opportunistic key caching used for authentication
DOT11 EAP_PREAUTH_SUCCESS 6 Client [qstr] 802.1x/EAP (type:[str]) pre-authentication success on wlan [qstr] bss [mac]	EAP pre authentication success
DOT11 EAP_PREAUTH_FAILED 5 Client [qstr] failed 802.1x/EAP pre-authentication on wlan [qstr] bss [mac]	EAP pre-authentication failed
DOT11 EAP_PREAUTH_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP pre-authentication on wlan [qstr]	EAP pre-authentication client timeout detected
DOT11 EAP_PREAUTH_SERVER_TIMEOUT 5 Radius server [qstr] timeout pre-authenticating client [qstr] on wlan [qstr]	EAP pre-authentication server timeout detected
DOT11 FT_ROAM_SUCCESS 6 Client [qstr] fast bss transition roam to wlan [qstr] ssid [qstr] on radio [qstr]	Client fast BSS transition roam to WLAN SSD ID on radio
DOT11 GAL_RX_REQUEST 6 Received request to validate [qstr] on global assoc-list [qstr] from [qstr] on rf-domain [qstr]	Received request to validate global association request for RF Domain
DOT11 GAL_TX_RESPONSE 6 Sending global assoc-list [qstr] response for [qstr] to [qstr] on rf-domain [qstr], result: [str]	Sending global association response for RF Domain
DOT11 GAL_VALIDATE_REQ 6 Sending global assoc-list validation request to controller for [qstr]	Sending global association list validation to controller
DOT11 GAL_VALIDATE_FAILED 6 Received global assoc-list validation failure for [qstr]	Received global association list validation failures
DOT11 GAL_VALIDATE_SUCCESS 6 Received global assoc-list validation success for [qstr]	Received global association list validation successes
FWU FWUDONE 6 Firmware update successful, new version is [str]	Update successfully completed
FWU FWUABORTED 6 Firmware update aborted	Update aborted
FWU FWUNONEED 6 Firmware update not required, running and update versions same [str]	Update not required, running and update version are the same
FWU FWUSYSERR 3 Firmware update unsuccessful, system cmd [str] failed	Update unsuccessful, system cmd failed
FWU FWUBADCONFIG 3 Firmware update unsuccessful, unable to read configuration file	Update unsuccessful, unable to read config file
FWU FWUSERVERUNDEF 3 Firmware update unsuccessful, update server undefined	Update unsuccessful, server undefined
FWU FWUFILEUNDEF 3 Firmware update unsuccessful, update file undefined	Update unsuccessful, update file undefined

FWU FWUSERVERUNREACHABLE 3 Firmware update unsuccessful, server [str] unreachable	Update unsuccessful, server unreachable
FWU FWUCOULDNTGETFILE 3 Firmware update unsuccessful, couldn't get file, [str] //	Update unsuccessful, could not get file
FWU FWUVERMISMATCH 3 Firmware update unsuccessful, version mismatch, expected [str], actual [str] //	Update unsuccessful, version mismatch
FWU FWUPRODMISMATCH 3 Firmware update unsuccessful, product mismatch, expected [str], actual [str]	Update unsuccessful, product mismatch
FWU FWUCORRUPTEDFILE 3 Firmware update unsuccessful, corrupted firmware file	Update unsuccessful, corrupted file
FWU FWUSIGNMISMATCH 3 Firmware update unsuccessful, signature mismatch, [str]	Update unsuccessful, signature mismatch
FWU FWUUNSUPPORTEDHW 3 Firmware update unsuccessful, unsupported hardware	Update unsuccessful, unsupported hardware version
FWU FWUUNSUPPORTEDMODELNUM 3 Firmware update unsuccessful, unsupported FIPS model number	Update unsuccessful, unsupported FIPS model number
ISDN_EMERG 0 Emergency: [str]	ISDN emergency
ISDN_ALERT 1 Alert: [str]	ISDN alert
ISDN_CRIT 2 Critical: [str]	ISDN critical
ISDN_ERR 3 Error: [str]	ISDN error
ISDN_WARNING 4 Warning: [str]	ISDN warning
ISDN_NOTICE 5 Notice: [str]	ISDN notice
ISDN_INFO 6 Info: [str]	ISDN information
ISDN_DEBUG 7 Debug: [str]	ISDN debug
L2TPV3 L2TPV3_TUNNEL_UP 5 L2TPV3 tunnel [str] is UP	L2TPV3 tunnel is up
L2TPV3 L2TPV3_TUNNEL_DOWN 5 L2TPV3 tunnel [str] is DOWN	L2TPV3 tunnel is down
LICMGR LIC_INSTALLED 6 [str] license installed	License installation
LICMGR LIC_INSTALL_DEFAULT 6 [str] default license installed, count: [int]	Default license installation
LICMGR LIC_INSTALL_COUNT 6 [str] license installed, count: [int]	License count
LICMGR LIC_REMOVED 6 [str] license removed	License removed
LICMGR LIC_INVALID 3 [str] license invalid Error: [str]	License installation failed
MESH MESH_LINK_UP 5 Mesh link up between radio [qstr] and radio [qstr]	Mesh link up
MESH MESH_LINK_DOWN 5 Mesh link down between radio [qstr] and radio [qstr]	Mesh link down
MGMT LOG_KEY_DELETED 4 Rsakey [str] associated with ssh is deleted so ssh is restarted with default rsa key	RSA key associated with SSH is deleted

MGMT LOG_KEY_RESTORED 6Rsakey [str] associated with ssh is added so ssh is restarted with new key	RSA key associated with SSH is added
MGMT LOG_TRUSTPOINT_DELETED 4 Trustpoint [str] associated with https is deleted or expired so https is restarted with default trustpoint	Trustpoint associated with HTTPS is deleted
MGMT LOG_HTTP_START 5 [str] started in external mode	Web server started in external mode
MGMT LOG_HTTP_LOCAL_START 5 thttpd started in localhost mode	Web server started in local mode
MGMT LOG_HTTPS_START 5 stunnel started	Secure Web server started
MGMT LOG_HTTPS_WAIT 5 waiting for thttpd to start	Waiting for Web server to start
MGMT LOG_HTTP_INIT 5 [str] status started is [uint] and external mode is [uint]	Web server started
MESH MESHPOINT_LOOP_PREVENT_ON 4 Meshpoint [qstr] loop prevention on (port [str]), wired traffic is blocked	Wired traffic is blocked
MESH MESHPOINT_LOOP_PREVENT_OFF 4 Meshpoint loop prevention off (port [str]), all wired traffic is allowed	Wired traffic is allowed
MESH MESHPOINT_ROOT_CHANGE 6 Meshpoint [qstr] root changed from [mac] to [mac] via next hop [mac]	Meshpoint root changed
MESH MESHPOINT_PATH_CHANGE 6 Meshpoint [qstr] next hop changed from [mac] to [mac] for [mac]	Meshpoint next hop changed
NSM IFUP 4 Interface [str] is up	Interface up
NSM IFDOWN 4 Interface [str] is down	Interface down
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	Interface DHCP lease expired

NSM DHCPNAK 5 Interface [str] lost its DHCP IP address [ip], DHCP NAK response from server	DHCP Server returned DHCP NAK response
NSM NSM_NTP 6 Look up host [str] [str]//	Translate host name
NSM IF_FAILOVER 5 Interface [str] failover to Interface [str]	Interface failover
NSM IF_FAILBACK 5 Interface [str] failback to Interface [str]	Interface failback
PM PROCSTART 6 Starting process [str]	Process started
PM PROCRSTRT 3 Process str]"is not responding. Restarting process	Process restarted
PM PROCMAXRSTRT 1 Process [str] reached its maximum number of allowed restarts	Process reached max number of restarts
PM PROCSYSRSTRT 0 Process [str] reached its maximum number of allowed restarts. Rebooting the system.	Process reached max restarts. Rebooting system.
PM PROCSTOP 5 Process [str] has been stopped	Process has been stopped
PM PROCID 5 Process [str] changed its PID from [int] to [int]	Process changed PID
PM STARTUPCOMPLETE 5 System startup complete	System startup completed
PM PROCNORESP 4 Process [str] is not responding ([uint]/[uint])	Process is not responding
RADCONF RADIUSDSTART 6 Radius Server Started	RADIUS server started
RADCONF RADIUSDSTOP 6 Radius Server Stopped	RADIUS server stopped
RADCONF COULD_NOT_STOP_RADIUSD 3 radiusd could not be stopped	RADIUS server failed to stop
RADIO RADIO_STATE_CHANGE 5 Radio [qstr] changing state from [qstr] to [qstr]	Radio state changed
RADIO RADAR_SCAN_STARTED 6 Radar scan on primary channel [uint] freq [uint] MHz for a duration [uint] secs on radio [qstr]	Radar scan started
RADIO RADAR_SCAN_COMPLETED 6 Radar scan done on primary channel [uint] freq [uint] MHz on radio [qstr]	Radar scan completed
RADIO RADAR_DETECTED 4 Radar found on channel [uint] freq [uint] MHz	Radar detected
RADIO RADAR_DET_INFO 4 Radar info: Radio: [qstr]. New channel: [uint] freq [uint] MHz. Scan time: [uint] secs	Radar info
RADIO RESUME_HOME_CHANNEL 6 Operation on home channel [uint] freq [uint] MHz resumes on radio [qstr] after earlier radar detect	Radio resuming on home channel
RADIO ACS_SCAN_STARTED 6 ACS scan started on radio [qstr]	ACS scan started

RADIO ACS_SCAN_COMPLETE 6 ACS scan done, channel [uint] selected on radio [qstr]	ACS scan complete
RADIO_ANTENNA_ERROR 3 antenna type [str] in is not supported on radio [uint] of device [str]	Invalid (unsupported) antenna detected on this radio
RADIO CHANNEL_COUNTRY_MISMATCH 3 Channel [str] not valid in country of operation [str] for [str] [str]	Channel and country of operation mismatch
SYSTEM HTTP_ERR 3 [str] did not start	Web server did not start
SYSTEM LOGIN_FAIL_BAD_ROLE 3 Log-in failed - [qstr] is an undefined user role - user [qstr] from [qstr]	Failed login attempt - no such user role
SYSTEM LOGOUT 6 Logged out user [qstr] with privilege [qstr] from [qstr]	Logout event
SYSTEM WARM_START 6 System Warm Start Reason : [str] Timestamp: [str]	System warm start
SYSTEM WARM_START_RECOVER 6 Warm Start Recover. Reason: [str] Timestamp: [str]	System warm 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
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

A Publicly Available Software

General Information

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in the following products:

Access Points

- AP650, AP6521, AP6522, AP6522M, AP6532, AP6562, AP7161, AP7181, AP7502, AP7522, AP7532, AP7562, AP8122, AP8132, AP8163, AP8232, AP8432 and AP8533.

Wireless Controllers and Service Platforms

- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX5500, NX5500E, NX7500, NX75XX, NX7510E, NX9500, NX9510, NX9600, NX9610, VX9000, VX9000E

Open Source Software Used

The Support site, located at *www.extremenetworks.com/support* provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Name	Version	URL	License
Apache Web Server	1.3.41	http://www.apache.org/	*Apache License, Version 2.0*
Asterisk	1.2.24	http://www.asterisk.org/	*GNU General Public License, version 2*
accepts	1.2.10	http://registry.npmjs.org/accepts/-/accepts-1.2.10.tgz	*MIT License*
advas	0.2.3	http://advas.sourceforge.net/	*GNU General Public License, version 2*
alivepdf	0.1.4.9	https://code.google.com/p/alivepdf/	*MIT License*
apscheduler	3.0.1	https://pypi.python.org/pypi/APScheduler/	*MIT License*
async	1.3.0	http://registry.npmjs.org/async/-/async-1.3.0.tgz	*MIT License*
autoconf	2.69	http://www.gnu.org/software/autoconf/	*GNU General Public License, version 2*
automake	1.11.6	http://www.gnu.org/software/automake/	*GNU General Public License, version 2*
bash	4.2	http://www.gnu.org/software/bash/	*GNU General Public License, version 2*
binutils	2.23	http://www.gnu.org/software/binutils/	*GNU General Public License, version 2*
bison	2.3	http://www.gnu.org/software/bison/	*GNU General Public License, version 2*
bluez	5.7	http://www.bluez.org/	*GNU General Public License, version 2*

Name	Version	URL	License
body-parser	1.13.2	http://registry.npmjs.org/body-parser/-/body-parser-1.13.2.tgz	*MIT License*
bridge	1.0.4	http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/	*GNU General Public License, version 2*
bridge-utils	1.0.4	http://sourceforge.net/projects/bridge/	*GNU General Public License, version 2*
buffer-crc32	0.2.5	http://registry.npmjs.org/buffer-crc32/-/buffer-crc32-0.2.5.tgz	*MIT License*
busybox	1.14.4	http://www.busybox.net/	*GNU General Public License, version 2*
bytes	2.1.0	http://registry.npmjs.org/bytes/-/bytes-2.1.0.tgz	*MIT License*
colors	1.1.2	http://registry.npmjs.org/colors/-/colors-1.1.2.tgz	*MIT License*
compression	1.5.1	http://registry.npmjs.org/compression/-/compression-1.5.1.tgz	*MIT License*
conect-mongo	0.8.2	http://registry.npmjs.org/connect-mongo/-/connect-mongo-0.8.2.tgz	*MIT License*
cookie	0.1.3	http://registry.npmjs.org/cookie/-/cookie-0.1.3.tgz	*MIT License*
cookie-parser	1.3.5	http://registry.npmjs.org/cookie-parser/-/cookie-parser-1.3.5.tgz	*MIT License*
cookie-signature	1.0.6	http://registry.npmjs.org/cookie-signature/-/cookie-signature-1.0.6.tgz	*MIT License*
cuint	0.2.0	http://registry.npmjs.org/cuint/-/cuint-0.2.0.tgz	*MIT License*
cycle	1.0.3	https://registry.npmjs.org/cycle/-/cycle-1.0.3.tgz	*MIT License*
czjson	1.0.8	https://pypi.python.org/pypi/czjson/1.0.8	*GNU Lesser General Public License 2.1*
dash	0.5.7	http://gondor.apana.org.au/~herbert/dash/	*The BSD License*
debug	2.2.0	https://registry.npmjs.org/debug/-/debug-2.2.0.tgz	*MIT License*
depd	1.0.1	http://registry.npmjs.org/depd/-/depd-1.0.1.tgz	*MIT License*
dfu-util	0.8	http://dfu-util.gnumonks.org/	*GNU General Public License, version 2*
dhcp	3.0.3	http://www.isc.org/software/dhcp	*ISC License*
diffutils	2.8.1	http://www.gnu.org/software/diffutils/	*GNU General Public License, version 2*
dmalloc	5.5.2	http://dmalloc.com/	None
dmidecode	2.11	http://savannah.nongnu.org/projects/dmidecode/	*GNU General Public License, version 2*
dnsmasq	2.47	http://www.thekelleys.org.uk/dnsmasq/doc.html	*GNU General Public License, version 2*

Name	Version	URL	License
dosfstools	2.11	http://www.daniel-baumann.ch/software/dosfstools/	*GNU General Public License, version 2*
dropbear	0.55	http://matt.ucc.asn.au/dropbear/dropbear.html	*DropBear License*
e2fsprogs	1.41.13	http://e2fsprogs.sourceforge.net/	*GNU General Public License, version 2*
ejs	2.3.3	http://registry.npmjs.org/ejs/-/ejs-2.3.3.tgz	*Apache License, Version 2.0*
engine.io	1.5.2	http://registry.npmjs.org/engine.io/-/engine.io-1.5.2.tgz	*MIT License*
escape-html	1.0.2	http://registry.npmjs.org/escape-html/-/escape-html-1.0.2.tgz	*MIT License*
ethtool	2.6.35	http://www.kernel.org/pub/software/network/ethtool/	*GNU General Public License, version 2*
event-loop-lag	1.1.0	http://registry.npmjs.org/event-loop-lag/-/event-loop-lag-1.1.0.tgz	*MIT License*
express	4.13.1	http://registry.npmjs.org/express/-/express-4.13.1.tgz	*MIT License*
express-session	1.11.3	http://registry.npmjs.org/express-session/-/express-session-1.11.3.tgz	*MIT License*
eyes	0.1.8	http://github.com/cloudhead/eyes.js	*MIT License*
finalhandler	0.4.0	http://registry.npmjs.org/finalhandler/-/finalhandler-0.4.0.tgz	*MIT License*
flashrom	0.9.4	http://flashrom.org/Flashrom	*GNU General Public License, version 2*
flex	4.5.1.21328	http://flex.sourceforge.net/	*The BSD License*
fluks	0.2	https://github.com/markuspeloquin/fluks	*MIT License*
freedos	4.5.1.21328	http://www.freedos.org/download/	*GNU General Public License, version 2*
freeipmi	1.1	http://www.gnu.org/software/freeipmi/	*GNU General Public License, version 3*
fresh	0.3.0	http://registry.npmjs.org/fresh/-/fresh-0.3.0.tgz	*MIT License*
futures	2.2.0	https://github.com/agronholm/pythonfutures	*The BSD License*
gcc	4.1.2	http://gcc.gnu.org/	*GNU General Public License, version 2*
gdb	7.2	http://www.gnu.org/software/gdb/	*GNU General Public License, version 3*
gdbm	1.8.3	http://www.gnu.org/s/gdbm/	*GNU General Public License, version 2*
genext2fs	1.4.1	http://genext2fs.sourceforge.net/	*GNU General Public License, version 2*
glib2	2.30.2	http://www.gtk.org/	*GNU Lesser General Public License 2.1*
glibc	2.7	http://www.gnu.org/software/libc/	*GNU General Public License, version 2*

Name	Version	URL	License
has-binary-data	0.1.5	http://registry.npmjs.org/has-binary-data/-/has-binary-data-0.1.5.tgz	*MIT License*
hdparm	9.38	http://sourceforge.net/projects/hdparm/	*GNU General Public License, version 2*
hooks	0.3.2	http://registry.npmjs.org/hooks/-/hooks-0.3.2.tgz	*MIT License*
hostapd	0.6.9	http://hostap.epitest.fi/hostapd/	*GNU General Public License, version 2*
hotplug	1.3	http://sourceforge.net/projects/linux-hotplug/	*GNU General Public License, version 2*
hotplug2	0.9	http://isteve.bofh.cz/~isteve/hotplug2/	*GNU General Public License, version 2*
i2ctools	3.0.3	http://www.lm-sensors.org/wiki/I2CTools	*GNU General Public License, version 2*
iconv-lite	0.4.11	http://registry.npmjs.org/iconv-lite/-/iconv-lite-0.4.11.tgz	*MIT License*
igb	5.2.9.4	http://sourceforge.net/projects/e1000/	*GNU General Public License, version 2*
ipaddr	2.1.0	http://code.google.com/p/ipaddr-py/	*Apache License, Version 2.0*
ipkg-utils	1.7	http://www.handhelds.org/sources.html	*GNU General Public License, version 2*
ipmitool	1.8.11	http://ipmitool.sourceforge.net/	*The BSD License*
iproute2	050816	http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2	*GNU General Public License, version 2*
iptables	1.4.3	http://www.netfilter.org/projects/iptables/index.html	*GNU General Public License, version 2*
ipxe	1.0.0	http://ipxe.org/	*GNU General Public License, version 2*
isstream	0.1.2	https://registry.npmjs.org/isstream/-/isstream-0.1.2.tgz	*MIT License*
js-yaml	3.3.1	http://registry.npmjs.org/js-yaml/-/js-yaml-3.3.1.tgz	*MIT License*
kerberos	None	http://web.mit.edu/Kerberos/	*GNU General Public License, version 2*
kexec-tools	2.0.3	http://kernel.org/pub/linux/utils/kernel/kexec/	*GNU General Public License, version 2*
libbson	1.1.0	http://github.com/mongodb/libbson	*Apache License, Version 2.0*
libcares	1.7.1	http://c-ares.haxx.se/	*The BSD License*
libcurl	7.30.0	http://curl.haxx.se/libcurl/	*The BSD License*
libdevmapper	2.02.66	ftp://sources.redhat.com/pub/lvm2/old	*GNU Lesser General Public License 2.1*
libexpat	2.0.0	http://expat.sourceforge.net/	*MIT License*
libffi	3.0.7	http://sourceware.org/libffi/	*MIT License*
libgcrypt	1.4.5	ftp://ftp.gnupg.org/GnuPG/libgcrypt/	*GNU Lesser General Public License 2.1*

Name	Version	URL	License
libgmp	4.2.2	http://gmplib.org/	*GNU Lesser General Public License, version 3.0*
libgnutls	3.2.12	ftp://ftp.gnupg.org/GnuPG/gnutls/v3.0/	*GNU Lesser General Public License, version 3.0*
libgpg-error	1.6	ftp://ftp.gnupg.org/GnuPG/libgpg-error/	*GNU Lesser General Public License 2.1*
libharu	2.1.0	http://libharu.org/	*MIT License*
libhttp-parser	None	None	*MIT License*
libiconv	1.14	http://savannah.gnu.org/projects/libiconv/	*GNU General Public License 2.0*
libjson	0.10	http://sourceforge.net/projects/libjson/	*The BSD License*
libkerberos	0.1	http://web.mit.edu/kerberos/dist/	*The BSD License*
libncurses	5.4	http://www.gnu.org/software/ncurses/	*MIT License*
libnettle	2.7	http://www.lysator.liu.se/~nisse/nettle/	*GNU Lesser General Public License 2.1*
libnuma	2.0.10	https://github.com/numactl/numactl/	*GNU Lesser General Public License, version 2.0*
libpam	1.1.1	http://www.kernel.org/pub/linux/libs/pam/	*The BSD License*
libpcap	1.0.0	http://www.tcpdump.org/	*The BSD License*
libpcre	8.21	ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/	*The BSD License*
libpopt	1.14	http://freecode.com/projects/popt	*MIT License*
libraryopt	1.01	http://sourceforge.net/projects/libraryopt/	*GNU General Public License, version 2*
libreadline	4.3	http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html	*GNU General Public License, version 2*
libtool	2.4.2	http://www.gnu.org/software/libtool/	*GNU General Public License, version 2*
libusb	0.1.12	http://www.libusb.org/	*GNU Lesser General Public License, version 2.0*
libusb	1.0.18	http://www.libusb.org/	*GNU Lesser General Public License, version 2.0*
libvirt	0.9.11	http://libvirt.org/sources/	*GNU Lesser General Public License 2.1*
libxml2	2.8.0	http://xmlsoft.org/	*MIT License*
libxslt	1.1.26	http://xmlsoft.org/xslt/	*MIT License*
lighttpd	1.4.37	http://www.lighttpd.net/	*MIT License*
lilo	22.6	http://lilo.alioth.debian.org/	*The BSD License*
linux	2.6.28.9	http://www.kernel.org/	*GNU General Public License, version 2*
linux	2.6.35.9	http://www.kernel.org/	*GNU General Public License, version 2*
lodash	3.10.0	http://registry.npmjs.org/lodash/-/lodash-3.10.0.tgz	*MIT License*

Name	Version	URL	License
log-timestamp	0.1.2	http://registry.npmjs.org/log-timestamp/-/log-timestamp-0.1.2.tgz	*MIT License*
ltp	20130904	https://github.com/linux-test-project/ltp	*GNU General Public License, version 2*
lxml	2.3beta1	http://lxml.de/	*The BSD License*
lzma	4.32	http://www.7-zip.org/sdk.html	*GNU Lesser General Public License, version 2.0*
lzma	4.57	http://www.7-zip.org/sdk.html	*GNU Lesser General Public License, version 2.0*
lzo	2.03	http://www.oberhumer.com/opensource/lzo/	*GNU General Public License, version 2*
M2Crypto	0.21.1	http://chandlerproject.org/bin/view/Projects/MeTooCrypto	*The BSD License*
m4	1.4.16	http://www.gnu.org/software/m4/	*GNU General Public License, version 2*
madwifi	trunk-r3314	http://madwifi-project.org/	*The BSD License*
mdadm	3.2.2	http://neil.brown.name/blog/mdadm	*GNU General Public License, version 2*
media-typer	0.3.0	http://registry.npmjs.org/media-typer/-/media-typer-0.3.0.tgz	*MIT License*
memtester	4.0.8	http://pyropus.ca/software/memtester/	*GNU General Public License, version 2*
merge-descriptors	1.0.0	http://registry.npmjs.org/merge-descriptors/-/merge-descriptors-1.0.0.tgz	*MIT License*
method-override	2.3.4	http://registry.npmjs.org/method-override/-/method-override-2.3.4.tgz	*MIT License*
methods	1.1.1	http://registry.npmjs.org/methods/-/methods-1.1.1.tgz	*MIT License*
mii-diag	2.09	http://freecode.com/projects/mii-diag	*GNU General Public License, version 2*
mkyaffs	None	http://www.yaffs.net/	*GNU General Public License, version 2*
mod_ssl	2.8.3.1-1.3.41	http://www.modssl.org/	*The BSD License*
mongo-c-driver	1.1.0	http://github.com/mongodb/mongo-c-driver	*Apache License, Version 2.0*
mongo-python-driver	2.7.1	http://github.com/mongodb/mongo-python-driver	*Apache License, Version 2.0*
mongodb	3.0.5	http://www.mongodb.org/	*GNU Lesser General Public License, version 3.0*
mongoose	4.0.7	http://registry.npmjs.org/mongoose/-/mongoose-4.0.7.tgz	*MIT License*
mpath	0.2.1	http://registry.npmjs.org/mpath/-/mpath-0.2.1.tgz	*MIT License*
mpromise	0.5.5	http://registry.npmjs.org/mpromise/-/mpromise-0.5.5.tgz	*MIT License*
mquery	1.6.2	http://registry.npmjs.org/mquery/-/mquery-1.6.2.tgz	*MIT License*

Name	Version	URL	License
ms	0.7.1	http://registry.npmjs.org/ms/-/ms-0.7.1.tgz	*MIT License*
mtd	2009-05-05	http://www.linux-mtd.infradead.org/	*GNU General Public License, version 2*
mtd-utils	1.4.4	http://www.linux-mtd.infradead.org/	*GNU General Public License, version 2*
mtd-utils	2009-05-05	http://www.linux-mtd.infradead.org/	*GNU General Public License, version 2*
muri	1.1.0	http://registry.npmjs.org/muri/-/muri-1.1.0.tgz	*MIT License*
nano	1.2.4	http://www.nano-editor.org/	*GNU General Public License, version 2*
net-snmp	5.3.0.1	http://net-snmp.sourceforge.net/	*The BSD License*
no-vnc	None	http://kanaka.github.io/noVNC/	*Mozilla Public License, version 2*
node-mongodb-native	1.4.35	http://github.com/mongodb/node-mongodb-native	*Apache License, Version 2.0*
node.js	0.12.7	http://nodejs.org/	*MIT License*
ntp	4.2.6p4	http://www.ntp.org/index.html	*The BSD License*
numactl	2.0.10	https://github.com/numactl/numactl/	*GNU General Public License, version 2*
Open Scales	2.2	http://openscales.org/	*GNU Lesser General Public License, version 3.0*
OpenStreetMap		http://www.openstreetmap.org/	*Creative Commons Attribution-ShareAlike License, version 3.0*
on-headers	1.0.0	http://registry.npmjs.org/on-headers/-/on-headers-1.0.0.tgz	*MIT License*
openldap	2.4.40	http://www.openldap.org/foundation/	*The Open LDAP Public License*
openllpd	0.0.3alpha	http://openlldp.sourceforge.net/	*GNU General Public License, version 2*
openssh	6.6p1	http://www.openssh.com/	*The BSD License*
openssl	0.9.8zg	http://www.openssl.org/	*OpenSSL License*
openssl	1.0.0i	http://www.openssl.org/	*OpenSSL License*
openssl	1.0.1g	http://www.openssl.org/	*OpenSSL License*
openssl-fips	1.2.3	http://www.openssl.org/	*OpenSSL License*
openwrt	trunk-r15025	http://www.openwrt.org/	*GNU General Public License, version 2*
opkg	trunk-r4564	http://code.google.com/p/opkg/	*GNU General Public License, version 2*
oprofile	0.9.2	http://oprofile.sourceforge.net/news/	*GNU Lesser General Public License 2.1*
ProGuard	4.8	http://proguard.sourceforge.net/	*GNU General Public License, version 2*
PyPDF2	1.23	http://mstamy2.github.com/PyPDF2	*The BSD License*

Name	Version	URL	License
parseurl	1.3.0	http://registry.npmjs.org/parseurl/-/parseurl-1.3.0.tgz	*MIT License*
path-to-regexp	1.2.0	http://registry.npmjs.org/path-to-regexp/-/path-to-regexp-1.2.0.tgz	*MIT License*
pciutils	3.1.8	http://mj.ucw.cz/sw/pciutils/	*GNU General Public License, version 2*
pdnsd	1.2.5	http://members.home.nl/p.a.rombouts/pdnsd/	*GNU General Public License, version 2*
picocom	1.6	http://code.google.com/p/picocom/	*GNU General Public License, version 2*
pillow	2.8.1	http://python-pillow.github.io/	*MIT License*
ping	1.0	None	*The BSD License*
pkg-config	0.22	http://pkg-config.freedesktop.org/wiki/	*GNU General Public License, version 2*
portmap	6.0	http://neil.brown.name/portmap/	*The BSD License*
posix	2.0.1	http://registry.npmjs.org/posix/-/posix-2.0.1.tgz	*MIT License*
ppp	2.4.5	http://ppp.samba.org/ppp/	*The BSD License*
ppp	2.4.3	http://ppp.samba.org/ppp/	*The BSD License*
preppy	2.3.1	https://bitbucket.org/rptlab/preppy	*The BSD License*
procname	0.2	http://code.google.com/p/procname/	*GNU Lesser General Public License, version 2.0*
procps	3.2.8	http://procps.sourceforge.net/	*GNU General Public License, version 2*
proxy-addr	1.0.8	http://registry.npmjs.org/proxy-addr/-/proxy-addr-1.0.8.tgz	*MIT License*
psmisc	22.8	http://sourceforge.net/projects/psmisc/	*GNU General Public License, version 2*
pure-ftpd	1.0.22	http://www.pureftpd.org/project/pure-ftpd	*The BSD License*
pychecker	0.8.18	http://pychecker.sourceforge.net/	*The BSD License*
pyparsing	1.5.1	http://sourceforge.net/projects/pyparsing/	*The BSD License*
pytz	2014.10	http://pythonhosted.org/pytz	*MIT License*
pyxapi	0.1	http://www.pps.jussieu.fr/%7Eylg/PyXAPI/	*GNU General Public License, version 2*
pyyaml	3.11	http://pyyaml.org/	*MIT License*
qdbm	1.8.77	http://qdbm.sourceforge.net/	*GNU General Public License, version 2*
qs	4.0.0	http://registry.npmjs.org/qs/-/qs-4.0.0.tgz	*The BSD License*
quagga	0.99.16	http://www.quagga.net	*GNU General Public License, version 2*
quilt	0.47	http://savannah.nongnu.org/projects/quilt/	*GNU General Public License, version 2*
radius	2.2.3	http://freeradius.org/	*GNU General Public License, version 2*

Name	Version	URL	License
range-parser	1.0.2	http://registry.npmjs.org/range-parser/-/range-parser-1.0.2.tgz	*MIT License*
raw-body	2.1.2	http://registry.npmjs.org/raw-body/-/raw-body-2.1.2.tgz	*MIT License*
redis	3.0.3	http://redis.io/	*The BSD License*
redis	0.12.1	http://registry.npmjs.org/redis/-/redis-0.12.1.tgz	*MIT License*
regexp-clone	0.0.1	http://registry.npmjs.org/regexp-clone/-/regexp-clone-0.0.1.tgz	*MIT License*
report-lab	3.1.44	http://www.reportlab.com	*The BSD License*
rp-pppoe	3.1.0	http://www.roaringpenguin.com/products/pppoe	*GNU General Public License, version 2*
rsync	3.0.6	http://rsync.samba.org/	*GNU General Public License, version 3*
safestr	1.0.3	http://www.zork.org/	*The BSD License*
samba	3.5.1	http://www.samba.org	*GNU General Public License, version 3*
sed	4.1.2	http://www.gnu.org/software/sed/	*GNU General Public License, version 2*
semaphore	1.0.3	http://registry.npmjs.org/semaphore/-/semaphore-1.0.3.tgz	*MIT License*
send	0.13.0	http://registry.npmjs.org/send/-/send-0.13.0.tgz	*MIT License*
serve-static	1.10.0	http://registry.npmjs.org/serve-static/-/serve-static-1.10.0.tgz	*MIT License*
setproctitle	1.1.8	http://code.google.com/p/py-setproctitle	*The BSD License*
setuptools	11.3.1	https://bitbucket.org/pypa/setuptools	*Python License, Version 2 (Python-2.0)*
sliced	1.0.1	http://registry.npmjs.org/sliced/-/sliced-1.0.1.tgz	*MIT License*
smarttools	6.2	http://smartmontools.sourceforge.net	*GNU General Public License, version 2*
snmpagent	5.0.9	http://sourceforge.net/	*The BSD License*
socket.io	1.3.6	http://registry.npmjs.org/socket.io/-/socket.io-1.3.6.tgz	*MIT License*
socket.io-adapter	0.3.1	http://registry.npmjs.org/socket.io-adapter/-/socket.io-adapter-0.3.1.tgz	*MIT License*
socket.io-adapter-mongo	0.1.4	http://registry.npmjs.org/socket.io-adapter-mongo/-/socket.io-adapter-mongo-0.1.4.tgz	*MIT License*
socket.io-client	1.3.6	http://registry.npmjs.org/socket.io-client/-/socket.io-client-1.3.6.tgz	*MIT License*
socket.io-parser	2.2.4	http://registry.npmjs.org/socket.io-parser/-/socket.io-parser-2.2.4.tgz	*MIT License*
sqlite3	3070900	http://www.sqlite.org/	None

Name	Version	URL	License
squashfs	3.0	http://squashfs.sourceforge.net/	*GNU General Public License, version 2*
squid	2.7.STABLE9	http://www.squid-cache.org/	*GNU General Public License, version 2*
stack-trace	0.0.9	https://registry.npmjs.org/stack-trace/-/stack-trace-0.0.9.tgz	*MIT License*
stackless python	2.7.5	http://www.stackless.com/	*GNU General Public License, version 2*
sticky-session	0.1.0	http://registry.npmjs.org/sticky-session/-/sticky-session-0.1.0.tgz	*MIT License*
strace	4.5.20	http://sourceforge.net/projects/strace/	*The BSD License*
stress	1.0.4	http://people.seas.harvard.edu/~apw/stress/	*GNU General Public License, version 2*
strongswan	4.4.0	http://www.strongswan.org	*GNU General Public License, version 2*
stunnel	4.31	http://www.stunnel.org/	*GNU General Public License, version 2*
svg2rlg	0.3	http://code.google.com/p/svg2rlg/	*The BSD License*
sysstat	9.0.5	http://sebastien.godard.pagesperso-orange.fr/	*GNU General Public License, version 2*
tar	1.17	http://www.gnu.org/software/tar/	*GNU General Public License, version 2*
tcpdump	4.0.0	http://www.tcpdump.org/	*The BSD License*
tinyproxy	1.8.3	https://banu.com/tinyproxy/	*GNU General Public License, version 2*
type-is	1.6.4	http://registry.npmjs.org/type-is/-/type-is-1.6.4.tgz	*MIT License*
tz	2014b	http://www.iana.org/time-zones/repository/releases/	*GNU General Public License, version 2*
tzlocal	1.1.2	https://github.com/regebro/tzlocal	"CCO 1.0 Universal"
u-boot	trunk-2010-03-30	http://www.denx.de/wiki/U-Boot/	*GNU General Public License, version 2*
u-boot	trunk-2010-05-10	http://www.denx.de/wiki/U-Boot/	*GNU General Public License, version 2*
uClibc	0.9.29	http://www.uclibc.org/	*GNU General Public License, version 2*
uClibc	0.9.30.2	http://www.uclibc.org/	*GNU General Public License, version 2*
uci	0.7.5	http://www.openwrt.org/	*GNU General Public License, version 2*
udev	147	https://launchpad.net/udev	*GNU General Public License, version 2*
udev	r147	http://www.kernel.org/pub/linux/utils/kernel/hotplug/	*GNU General Public License, version 2*
usbutils	0.73	http://www.linux-usb.org/	*GNU General Public License, version 2*

Name	Version	URL	License
util-linux	2.20	http://www.kernel.org/pub/linux/utils/util-linux/	*GNU General Public License, version 2*
utils-merge	1.0.0	http://registry.npmjs.org/utils-merge/-/utils-merge-1.0.0.tgz	*MIT License*
valgrind	3.5.0	http://valgrind.org/	*GNU General Public License, version 2*
validator	3.41.2	http://registry.npmjs.org/validator/-/validator-3.41.2.tgz	*MIT License*
vary	1.0.1	http://registry.npmjs.org/vary/-/vary-1.0.1.tgz	*MIT License*
wanpipe	3.5.18	http://wiki.sangoma.com/wanpipe-linux-drivers	*GNU General Public License, version 2*
websocket	2.4	https://github.com/nori0428/mod_websocket	*MIT License*
wget	1.14	http://www.gnu.org/software/wget/	*GNU General Public License, version 3*
winston	1.0.1	http://registry.npmjs.org/winston/-/winston-1.0.1.tgz	*MIT License*
wireless_tools	r29	http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html	*GNU General Public License, version 2*
wpa_supplicant	2.0	http://hostap.epitest.fi/wpa_supplicant/	*The BSD License*
ws	0.7.2	http://registry.npmjs.org/ws/-/ws-0.7.2.tgz	*MIT License*
wuftpd	1.0.21	http://wu-ftpd.therockgarden.ca/	*WU-FTPD Software License*
XenAPI	None	http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html	*GNU General Public License, version 2*
xen	4.1.5	http://www.xen.org/	*GNU General Public License, version 2*
xen-crashdump-analyser	20130505	http://xenbits.xen.org/people/andrewcoop/	*GNU General Public License, version 2*
xen-tools	4.2.1	http://xen-tools.org/software/xen-tools/	*GNU General Public License, version 2*
xxhashjs	0.1.1	http://registry.npmjs.org/xxhashjs/-/xxhashjs-0.1.1.tgz	*MIT License*
z3c-rml	2.7.2	http://pypi.python.org/pypi/z3c.rml	*Zope Public License (ZPL) Version 2.0*
zlib	1.2.8	http://www.zlib.net/	*zlib License*
zope-event	4.0.3	http://pypi.python.org/pypi/zope.event	*Zope Public License (ZPL) Version 2.0*
zope-interface	4.1.1	http://pypi.python.org/pypi/zope.interface	*Zope Public License (ZPL) Version 2.1*
zope-schema	4.4.2	http://pypi.python.org/pypi/zope.schema	*Zope Public License (ZPL) Version 2.0*
zwave	0.1	http://code.google.com/p/open-zwave/	*GNU Lesser General Public License, version 2.1*

OSS Licenses

Apache License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication

that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

The BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ”AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Creative Commons Attribution-ShareAlike License, version 3.0

Creative Commons

Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. REATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

"Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other

alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

"Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.

"Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

4. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

5. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

6. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

7. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

8. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which

are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

9. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

10. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

11. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

12. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

13. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;

b to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";

c to Distribute and Publicly Perform the Work including as incorporated in Collections; and,

d to Distribute and Publicly Perform Adaptations

For the avoidance of doubt:

1. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

2. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,

3. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the *Uniform Resource Identifier* (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

b You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US)); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the "Applicable License"), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with

every copy of the ork as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

3. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

4. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS

FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the emainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of he Licensor and You.

The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at http://creativecommons.org/.

DropBear License

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2004 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are .

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen , Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GNU General Public License, version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by

someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

IIf a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an

application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do

not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

Creative Commons Legal Code CC0 1.0 Universal CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

2 You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a The modified work must itself be a software library.

b You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

5 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code,

which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

6 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

7 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

8 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

9 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

11 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

12 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

    This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

13 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

14 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

15 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will

be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

16 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCO 1.0 Universal

Creative Commons Legal Code

CC0 1.0 Universal

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDELEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an "owner") of an original work of authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the

further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;

moral rights retained by the original author(s) and/or performer(s);

publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;

rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;

rights protecting the extraction, dissemination, use and reuse of data in a Work;

database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and

other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and

unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the “License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

Limitations and Disclaimers.

No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.

Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.

Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work.

Affirmer understands and acknowledges that Creative Commons is not a party to this document and has no duty or obligation with respect to this CC0 or use of the Work.

GNU General Public License, version 3

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution andmodification follow.

TERMS AND CONDITIONS

Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case o interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files forthe work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing i not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of echnological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section

7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules andprotocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise ofights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing

software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OFSUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

ISC License

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OFTHIS SOFTWARE.

GNU Lesser General Public License, version 3.0

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General PublicLicense, supplemented by the additional permissions listed below.

Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each ofthe following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by

this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU General Public License 2.0

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA
02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, thus in effect making the program proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library,and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public Licensefor libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in

header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

IIf a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place

satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they

do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU Lesser General Public License, version 2.0

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which wa designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.

* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other han as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest you rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, s the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy

simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose thatchoice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU Lesser General Public License, version 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too,

receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a The modified work must itself be a software library.
   b You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the

Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to

satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

MIT License

Permission is hereby granted, without written agreement and without icense or royalty fees, to use, copy, modify, and distribute this software and its documentation for any purpose, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

Mozilla Public License, version 2

Version 2.0

1. Definitions

1.1. Contributor means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. Contributor Versionâ means the combination of the Contributions of others (if any) used by a Contributor and that particular Contribution.

1.3. Contribution means Covered Software of a particular Contributor.

1.4. Covered Software means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. Incompatible With Secondary Licenses means

1. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

2. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. Executable Form means any form of the work other than Source Code Form.

1.7. Larger Work means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. License means this document.

1.9. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. Modifications means any of the following:

1. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

2. any new file in Source Code Form that contains any Covered Software.

1.11. Patent Claims of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. Secondary License means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. Source Code Form means the form of the work preferred for making modifications.

1.14. You (orYour) means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

1. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

2. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

1. for any code that a Contributor has removed from Covered Software; or

2. for infringements caused by: (i) Your and any other third partyâ€™s modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

3. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipientsâ€™ rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

1. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

2. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipientsâ€™ rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an â€œas isâ€?basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such partyâ€™s negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/. You may add additional accurate notices of copyright ownership.

Exhibit B - Incompatible With Secondary Licenses Notice

This Source Code Form is Incompatible With Secondary Licenses, as defined by the Mozilla Public License, v. 2.0.

The Open LDAP Public License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenSSL License

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contac openssl-core@openssl.org

5. Products derived from this software may not be called "OpenSSL" nor may OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes oftware written by Tim Hudson (tjh@cryptsoft.com).

WU-FTPD Software License

WU-FTPD SOFTWARE LICENSE

Use, modification, or redistribution (including distribution of any modified or derived work) in any form, or on any medium, is permitted only if all the following conditions are met:

1. Redistributions qualify as "freeware" or "Open Source Software" under the following terms:

a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery. Where redistribution of this software is as part of a larger package or combined work, this restriction applies only to the costs of materials and delivery of this software, not to any other costs associated with the larger package or combined work.

b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means all files included in the original distribution, including all modifications or additions, on a medium and in a form allowing fully working executable programs to be produced.

2. Redistributions of Source Code must retain the copyright notices as they appear in each Source Code file and the COPYRIGHT file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the"Copyright Notice" refers to the following language:

Copyright (c) 1999,2000,2001 WU-FTPD Development Group.

All rights reserved.

Portions Copyright (c) 1980, 1985, 1988, 1989, 1990, 1991, 1993, 1994

The Regents of the University of California.

Portions Copyright (c) 1993, 1994 Washington University in Saint Louis.

Portions Copyright (c) 1996, 1998 Berkeley Software Design, Inc.

Portions Copyright (c) 1998 Sendmail, Inc.

Portions Copyright (c) 1983, 1995, 1996, 1997 Eric P. Allman.

Portions Copyright (c) 1989 Massachusetts Institute of Technology.

Portions Copyright (c) 1997 Stan Barber.

Portions Copyright (c) 1991, 1992, 1993, 1994, 1995, 1996, 1997 Free Software Foundation, Inc.

Portions Copyright (c) 1997 Kent Landfield.

Use and distribution of this software and its source code are governed by the terms and conditions of the WU-FTPD Software License ("LICENSE").

If you did not receive a copy of the license, it may be obtained online at http://www.wu-ftpd.org/license.html

4. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by the WU-FTPD Development Group, the Washington University at Saint Louis, Berkeley Software Design, Inc., and their contributors."

5. Neither the name of the WU-FTPD Development Group, nor the names of any copyright holders, nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission. The names "wuftpd" and "wu-ftpd" are trademarks of the WU-FTPD Development Group and the Washington University at Saint Louis.

6. Disclaimer/Limitation of Liability:

THIS SOFTWARE IS PROVIDED BY THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, AND CONTRIBUTORS, "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WU-FTPD DEVELOPMENT GROUP, THE COPYRIGHT HOLDERS, OR CONTRIBUTORS, BE LIABLE FOR ANY DIRECT, NDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. USE, MODIFICATION, OR REDISTRIBUTION, OF THIS SOFTWARE IMPLIES ACCEPTANCE OF ALL TERMS AND CONDITIONS OF THIS LICENSE.

zlib License

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org, madler@alumni.caltech.edu

Python License, Version 2 (Python-2.0)

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

------ --

This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided

herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSFtrademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive,royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI OPEN SOURCE LICENSE AGREEMENT (for Python 1.6b1)

IMPORTANT: PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY.

BY CLICKING ON "ACCEPT" WHERE INDICATED BELOW, OR BY COPYING, INSTALLING OR OTHERWISE USING PYTHON 1.6, beta 1 SOFTWARE, YOU ARE DEEMED TO HAVE AGREED TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6, beta 1 software in source or binary form and its associated documentation,as released at the www.python.org Internet site on August 4, 2000 ("Python 1.6b1").

Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6b1 alone or in any derivative version, provided, however, that CNRIs License Agreement is retained in Python 1.6b1, alone or in any derivative version prepared by Licensee.

Alternately, in lieu of CNRIs License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6, beta 1, is made available subject to the terms and conditions in CNR Is License Agreement. This Agreement may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1011. This Agreement may also be obtained from a proxy server on the Internet using the URL:http://hdl.handle.net/1895.22/1011".

In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6b1 or any part thereof, and wants to make the derivative work available to the public as provided herein, then Licensee hereby agrees to indicate in any such work the nature of the modifications made to Python 1.6b1.

CNRI is making Python 1.6b1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR

WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6b1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING PYTHON 1.6b1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of Virginia, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6b1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Zope Public License (ZPL) Version 2.0

Zope Public License (ZPL) Version 2.0

This software is Copyright (c) Zope Corporation (tm) and Contributors. All rights reserved.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of contributions made by Zope Corporation and many individuals on behalf of Zope Corporation. Specific attributions are listed in the accompanying credits file.

Zope Public License (ZPL) Version 2.1

Zope Public License (ZPL) Version 2.1

A copyright notice accompanies this license document that identifies the copyright holders.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.