

Motorola Solutions AP-6511 Access Point

System Reference Guide

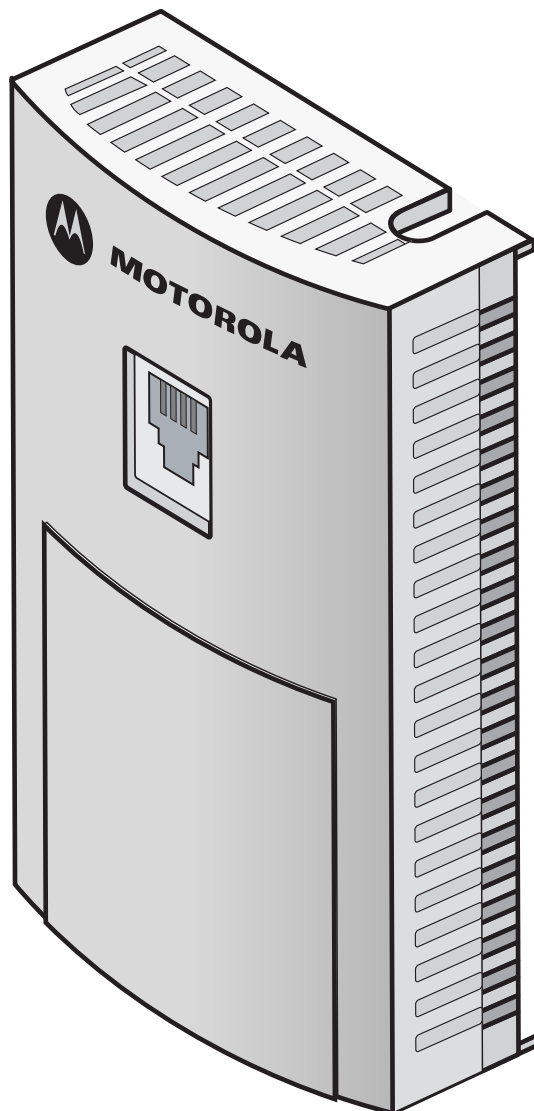




Table of Contents

Chapter About this Guide

Chapter 1 Overview

1.1 About the Motorola Solutions WiNG 5 Software	1-2
--	-----

Chapter 2 Web UI Overview

2.1 Accessing the Web UI	2-2
2.1.1 Browser and System Requirements	2-2
2.1.2 Connecting to the Web UI	2-2
2.2 Glossary of Icons Used	2-4
2.2.1 Global Icons	2-4
2.2.2 Dialog Box Icons	2-5
2.2.3 Table Icons	2-5
2.2.4 Status Icons	2-6
2.2.5 Configurable Objects	2-6
2.2.6 Configuration Objects	2-9
2.2.7 Configuration Operation Icons	2-9
2.2.8 Access Type Icons	2-10
2.2.9 Administrative Role Icons	2-10
2.2.10 Device Icons	2-11

Chapter 3 Getting Started

3.1 Using the Initial Setup Wizard	3-2
--	-----

Chapter 4 Dashboard

4.1 Dashboard	4-2
4.1.1 Dashboard Conventions	4-2
4.1.1.1 Health	4-2
4.1.1.2 Inventory	4-6
4.2 Network View	4-9
4.2.1 Filters Field	4-10
4.2.2 Device Specific Information	4-12

Chapter 5 Device Configuration

5.1 Basic Device Configuration	5-2
5.2 Assigning Certificates	5-5
5.2.1 Certificate Management	5-6

5.2.2 RSA Key Management	5-15
5.2.3 Certificate Creation	5-19
5.2.4 Generating a Certificate Signing Request	5-21
5.3 RF Domain Overrides	5-24
5.4 Profile Overrides	5-27
5.4.1 Profile Interface Override Configuration	5-28
5.4.1.1 Ethernet Port Override Configuration	5-29
5.4.1.2 Virtual Interface Override Configuration	5-35
5.4.1.3 Radio Override Configuration	5-39
5.4.2 Overriding a Profile's Network Configuration	5-47
5.4.2.1 Overriding a Profile's DNS Configuration	5-48
5.4.2.2 Overriding a Profile's ARP Configuration	5-50
5.4.2.3 Overriding a Profile's Quality of Service (QoS) Configuration	5-52
5.4.2.4 Overriding a Profile's Static Route Configuration	5-54
5.4.2.5 Overriding a Profile's Forwarding Database Configuration	5-56
5.4.2.6 Overriding a Profile's Bridge VLAN Configuration	5-58
5.4.2.7 Overriding a Profile's Miscellaneous Network Configuration	5-62
5.4.3 Overriding a Profile's Security Configuration	5-63
5.4.3.1 Overriding a Profile's General Security Settings	5-64
5.4.3.2 Overriding a Profile's Certificate Revocation List (CRL) Configuration	5-66
5.4.3.3 Overriding a Profile's NAT Configuration	5-68
5.4.4 Overriding a Profile's Services Configuration	5-75
5.4.5 Overriding a Profile's Management Configuration	5-77
5.4.6 Overriding a Profile's Miscellaneous Configuration	5-81

Chapter 6 Wireless Configuration

6.1 Wireless LAN Policy	6-3
6.1.1 Basic WLAN Configuration	6-4
6.1.2 Configuring WLAN Security	6-6
6.1.2.1 802.1x EAP, EAP PSK and EAP MAC	6-8
6.1.2.2 MAC Authentication	6-9
6.1.2.3 PSK / None	6-11
6.1.2.4 Captive Portal	6-11
6.1.2.5 WPA/WPA2-TKIP	6-11
6.1.2.6 WPA2-CCMP	6-14
6.1.2.7 WEP 64	6-17
6.1.2.8 WEP 128	6-19
6.1.3 Configuring WLAN Firewall Support	6-21
6.1.4 Configuring Client Settings	6-26
6.1.5 Configuring WLAN Accounting Settings	6-28
6.1.5.1 Accounting Deployment Considerations	6-29
6.1.6 Configuring Advanced WLAN Settings	6-30
6.2 Configuring WLAN QoS Policies	6-34
6.2.1 Configuring a WLAN's QoS WMM Settings	6-36
6.2.2 Configuring a WLAN's QoS Rate Limit Settings	6-41
6.2.3 Configuring a WLAN's QoS Wireless Client Rate Limit Settings	6-44

6.2.3.1 WLAN QoS Deployment Considerations	6-47
6.3 Radio QoS Policy	6-48
6.3.1 Radio QoS Configuration and Deployment Considerations	6-49
6.4 AAA Policy	6-50
6.5 Association ACL	6-52
6.5.1 Association ACL Deployment Considerations	6-53
6.6 Smart RF Policy	6-55
6.6.1 Smart RF Configuration and Deployment Considerations	6-64

Chapter 7 Profile Configuration

7.1 General Profile Configuration	7-4
7.1.1 General Profile Configuration and Deployment Considerations	7-5
7.2 Profile Interface Configuration	7-6
7.2.1 Ethernet Port Configuration	7-6
7.2.2 Virtual Interface Configuration	7-11
7.2.3 Access Point Radio Configuration	7-15
7.2.4 Profile Interface Deployment Considerations	7-24
7.3 Profile Network Configuration	7-25
7.3.1 Setting a Profile's DNS Configuration	7-25
7.3.2 ARP	7-26
7.3.3 Quality of Service (QoS)	7-28
7.3.4 Static Routes	7-29
7.3.5 Forwarding Database	7-30
7.3.6 Bridge VLAN	7-31
7.3.7 Miscellaneous Network Configuration	7-33
7.3.8 Profile Network Configuration and Deployment Considerations	7-34
7.4 Profile Security Configuration	7-36
7.4.1 Defining Profile Security Settings	7-36
7.4.2 Setting the Certificate Revocation List (CRL) Configuration	7-38
7.4.3 Setting the Profile's NAT Configuration	7-39
7.4.4 Profile Security Configuration and Deployment Considerations	7-47
7.5 Profile Services Configuration	7-48
7.5.1 Profile Services Configuration and Deployment Considerations	7-49
7.6 Profile Management Configuration	7-50
7.6.1 Profile Management Configuration and Deployment Considerations	7-53
7.7 Miscellaneous Profile Configuration	7-55

Chapter 8 Security Configuration

8.1 Wireless Firewall	8-2
8.1.1 Configuring a Firewall Policy	8-2
8.1.2 Configuring IP Firewall Rules	8-6
8.1.3 Configuring MAC Firewall Rules	8-9
8.1.4 Firewall Deployment Considerations	8-12
8.2 Intrusion Prevention	8-13
8.2.1 Configuring a WIPS Policy	8-13
8.2.2 Intrusion Detection Deployment Considerations	8-22

Chapter 9 Services Configuration

9.1 Configuring Captive Portal Policies	9-2
9.1.1 Configuring a Captive Portal Policy	9-2
9.1.2 Captive Portal Deployment Considerations	9-13
9.2 Setting the DHCP Server Configuration	9-14
9.2.1 Defining DHCP Pools	9-15
9.2.2 Defining DHCP Server Global Settings	9-23
9.2.3 DHCP Class Policy Configuration	9-25

Chapter 10 Management Access Policy Configuration

10.1 Viewing Management Access Policies	10-2
10.1.1 Adding or Editing a Management Access Policy	10-4
10.1.1.1 Creating an Administrator Configuration	10-5
10.1.1.2 Setting the Access Control Configuration	10-8
10.1.1.3 Setting the Authentication Configuration	10-10
10.1.1.4 Setting the SNMP Configuration	10-11
10.1.1.5 SNMP Trap Configuration	10-14
10.1.2 Management Access Deployment Considerations	10-15

Chapter 11 Diagnostics

11.1 Fault Management	11-2
11.2 Snapshots	11-5
11.2.1 Core Snapshots	11-5
11.2.2 Panic Snapshots	11-6
11.3 Advanced Diagnostics	11-7
11.3.1 UI Debugging	11-7

Chapter 12 Operations

12.1 Device Operations	12-2
12.1.1 Managing Firmware and Config Files	12-2
12.1.1.1 Upgrading Device Firmware	12-5
12.1.2 Managing File Transfers	12-6
12.1.3 Using the File Browser	12-8
12.1.4 AP Upgrade	12-9
12.2 Certificates	12-13
12.2.1 Certificate Management	12-13
12.2.2 RSA Key Management	12-21
12.2.3 Certificate Creation	12-25
12.2.4 Generating a Certificate Signing Request	12-28
12.3 Smart RF	12-31
12.3.1 Managing Smart RF for an RF Domain	12-31

Chapter 13 Statistics

13.1 System Statistics	13-2
13.1.1 Health	13-2

13.1.2 Inventory	13-5
13.2 RF Domain	13-7
13.2.1 Access Points	13-7
13.2.2 AP Detection	13-8
13.2.3 Wireless Clients	13-9
13.2.4 Wireless LANs	13-10
13.2.5 Radio	13-12
13.2.5.1 Radio Status	13-13
13.2.5.2 Radio RF Statistics	13-14
13.2.5.3 Radio Traffic Statistics	13-16
13.2.6 SMART RF	13-17
13.2.7 WIPS	13-18
13.2.7.1 WIPS Events	13-19
13.2.8 Captive Portal	13-19
13.2.9 Historical Data	13-20
13.2.9.1 Viewing Smart RF History	13-21
13.3 Access Point Statistics	13-22
13.3.1 Health	13-22
13.3.2 Inventory	13-24
13.3.3 Device	13-26
13.3.4 AP Upgrade	13-27
13.3.5 AP Detection	13-28
13.3.6 Wireless Client	13-29
13.3.7 Wireless LANs	13-30
13.3.8 Radios	13-32
13.3.8.1 Radio Status	13-33
13.3.8.2 Radio RF Statistics	13-34
13.3.8.3 Radio Traffic Statistics	13-35
13.3.9 Interfaces	13-36
13.3.9.1 General Statistics	13-37
13.3.9.2 Viewing Interface Statistics Graph	13-41
13.3.10 Network	13-41
13.3.10.1 ARP Entries	13-42
13.3.10.2 Route Entries	13-42
13.3.10.3 DHCP Options	13-44
13.3.11 DHCP Server	13-45
13.3.11.1 DHCP Bindings	13-47
13.3.11.2 DHCP Networks	13-48
13.3.12 Firewall	13-48
13.3.12.1 Packet Flows	13-48
13.3.12.2 IP Firewall Rules	13-50
13.3.12.3 MAC Firewall Rules	13-51
13.3.12.4 NAT Translations	13-52
13.3.12.5 DHCP Snooping	13-54
13.3.13 Certificates	13-55
13.3.13.1 Trustpoints	13-55

13.3.13.2 RSA Keys	13-57
13.3.14 WIPS	13-58
13.3.14.1 WIPS Events	13-59
13.3.15 Captive Portal	13-59
13.3.16 Network Time	13-60
13.3.16.1 NTP Status	13-61
13.3.16.2 NTP Association	13-62
13.4 Wireless Client Statistics	13-64
13.4.1 Health	13-64
13.4.2 Details	13-67
13.4.3 Traffic	13-70

About this Guide

This guide provides information about using the following Motorola Solutions AP-6511 Access Point.



NOTE: The screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the Motorola Solutions AP-6511 Access Point is partitioned into the following guides to provide information for specific user needs.

- *Installation Guide* - Describes the basic hardware setup and configuration required to transition to a more advanced configuration of the AP.
- *Motorola Solutions AP-6511 Access Point System Reference Guide* (this guide) - Describes configuration of the Motorola Solutions AP-6511 Access Point using the Access Point's resident Web UI.

Document Conventions

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



NOTE: Indicate 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.

Notational Conventions

The following additional notational conventions are used in this document:

- **GUI** text is used to highlight the following:
 - Screen names
 - Menu items
 - Button names on a screen.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Overview

Motorola Solutions' family of Access Points and wireless controllers enable the centralized distribution of high performance, secure and resilient wireless voice and data services to remote locations with the scalability required to meet the needs of large distributed enterprises.

The AP-6511 Access Point uses a subset of the WING 5 software as an onboard operating system unique to the Access Point. The WING 5 software resident on the AP-6511 Access Point supports a subset of the Enterprise class feature set available on RFS4000, RFS6000 and RFS7000 model controllers. The AP-6511 WING 5 software affords the Access Point those features needed to allow the Access Point to function as an Independent mode "thick" access point suited to hospitality deployments. For more information on the operating modes unique to the WING 5 supported AP-6511 Access Point, see [Web UI Overview on page 2-1](#).

The WiNG 5 architecture is a solution designed for 802.11n 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 between the wireless controllers and APs, the WiNG 5 network can route directly via the best path, as determined by factors including the user, the location, the application and the available wireless and wired resources. WiNG 5 extends the differentiation that adaptive APs offered to the next level by having the services and security now available at every point in the network. The traffic flow is optimized to prevent wired congestion as well as wireless congestion. Traffic flows dynamically, based on user and application, and finds alternate routes to work around any possible network choke points.

1.1 About the Motorola Solutions WiNG 5 Software

A WiNG 5 network uses Access Points to adapt to the dynamic circumstances of their deployment environment. The WiNG 5 architecture provides a customized site-specific deployment, supporting the best path and routes based on the user, location, the application and the best route available (both wireless and wired). A WiNG network assures end-to-end quality, reliability and security without latency and performance degradation. A WiNG 5 network supports rapid application delivery, mixed-media application optimization and quality assurance.

Deploying a new Motorola Solutions WiNG 5 network does not require the replacement of an existing Motorola Solutions wireless infrastructure. WiNG 5 enables the simultaneous use of existing architectures from Motorola Solutions and other vendors, even if those other architectures are centralized models. A wireless network administrator can retain and optimize legacy infrastructure while evolving to WiNG 5 as required.

By distributing intelligence and control between the wireless controllers and Access Points, a WiNG 5 network can route data directly using the best path, as determined by factors including the user, the location, the application and available wireless and wired resources. As a result, the additional load placed on the wired network from 802.11n is significantly reduced, as traffic does not require an unnecessary backhaul to a central controller.

Within a WiNG 5 network, up to 80% of the network traffic can remain on the wireless mesh, and never touch the wired network, so the 802.11n load impact on the wired network is negligible. In addition, latency and associated costs are reduced while reliability and scalability are increased. A WiNG 5 network enables the creation of dynamic wireless traffic flows, so any bottleneck is avoided, and the destination is reached without latency or performance degradation. This behavior delivers a significantly better quality of experience for the end user.

The same distributed intelligence enables more resilience and survivability, since the Access Points keep users connected and traffic flowing with full QoS, security and mobility even if the connection to the wireless controller is interrupted due to a wired network or backhaul problem.

Even when the network is fully operational, outside RF interference sources or unbalanced wireless network loading can be automatically corrected by the WiNG 5 Smart RF system. Smart RF senses interference or potential client connectivity problems and makes the required changes to channel and Access Point radio power while minimizing the impact to latency sensitive applications like VoIP. Using Smart RF, the network can continuously adjust Access Point power and channel assignments for self-recovery if an AP fails or a coverage hole is detected.

Additionally, integrated Access Point sensors in conjunction with AirDefense Network Assurance alerts administrators of interference and network coverage problems, which shortens response times and boosts overall reliability and availability of the WiNG 5 network.

Network traffic optimization protects WiNG 5 networks from broadcast storms and minimizes congestion on the wired network. WiNG 5 networks provide VLAN load balancing, WAN traffic shaping and optimizations in *dynamic host configuration protocol* (DHCP) responses and *Internet group management protocol* (IGMP) snooping for multicast traffic flows in wired and wireless networks. Thus, users benefit from an extremely reliable network that adapts to meet their needs and delivers mixed-media applications.

Firmware and configuration updates are supported within the network, from one Access Point to another, over the air or wire, and can be centrally managed by the controller. Controllers no longer need to push firmware and configurations to each individual Access Point, reducing unnecessary network congestion.

Web UI Overview

The AP-6511 Access Point uses a *Controller AP* version of the WING 5 software. The AP-6511 UI is a subset of the functionality deployed on RFS4000, RFS6000 and RFS7000 model controllers.

The AP-6511's resident user interface contains a set of features specifically designed to enable an AP-6511 to function as either a *Controller AP*, *Standalone AP* or *Dependent mode AP*. In Controller AP mode, an AP-6511 can manage up to 25 other AP-6511s and share data amongst managed Access Points. In Standalone mode, an AP-6511 functions as an autonomous, non-controller adopted, Access Point servicing wireless clients. In Dependent mode, an AP-6511 is reliant on its connected controller for its dependent mode configuration.

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

- [*Accessing the Web UI*](#)
- [*Glossary of Icons Used*](#)

2.1 Accessing the Web UI

An AP6511 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.

2.1.1 Browser and System Requirements

To access the *Graphical User Interface* (GUI), a browser supporting Flash Player 10 is recommended. The system accessing the GUI should have a minimum of 512Mb or RAM for the UI to function properly. The Wi-NG Web UI is based on Flex, and does not use Java as the underlying UI framework.

The following browsers have been validated with the Web UI:

- *Firefox 3.6*
- *Internet Explorer 7.x*
- *Internet Explorer 8.x*



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

2.1.2 Connecting to the Web UI

1. Connect one end of an Ethernet cable to any of the LAN ports on the AP-6511 and connect the other end to a computer with a working Web browser.
2. Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet/network mask of 255.255.255.0.
3. Once the computer has an IP address, point the Web browser to: <http://192.168.0.1/> and the following login screen will display.

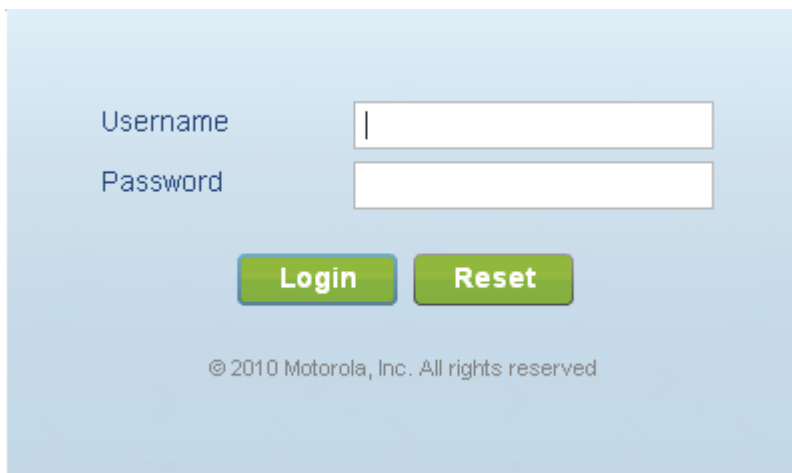


Figure 2-1 Web UI Login Screen

4. Enter the default username **admin** in the **Username** field.
5. Enter the default password **motorola** in the **Password** field.

6. Select the **Login** button to load the management interface.
7. If this is the first time the management interface has been accessed, 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 3-2](#).

2.2 Glossary of Icons Used

The AP-6511's 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*

2.2.1 Global Icons

▶ *Web UI Overview*

This section lists global icons available throughout the interface.



Logoff – 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 policy. To edit a policy, click on the policy and select this button.

2.2.2 Dialog Box Icons

► [Web UI Overview](#)

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 this dialog.



Error in Entry– Indicates there is an error in a value that has been entered in that control. A small red popup provides a likely cause of the error.

2.2.3 Table Icons

► [Web UI Overview](#)

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.

2.2.4 Status Icons

► [Web UI Overview](#)

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 exists 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.

2.2.5 Configurable Objects

► [Web UI Overview](#)

These icons define configurable items within the UI.



Device Configuration – Represents a configuration file applicable to a device category.



Adoption Policy – Represents an adoption policy. Adoption policies are a set of configuration parameters that define how APs and wireless clients are adopted. An AP-6511 Adoption Policy only applies to other AP-6511 models.



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.



Advanced WIPS Policy – States the conditions of an advanced WIPS policy have been invoked. WIPS prevents unauthorized access to the system 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 hotspot services to wireless clients.



DNS Whitelist – A DNS whitelist is used in conjunction with captive portal to provide hotspot 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.



Management Policy – Indicates a management policy is being applied. Management policies are used to configure access control, authentication, traps and administrator permissions.

2.2.6 Configuration Objects

► [Web UI Overview](#)

Configuration icons are used to define the following:



Configuration – Indicates an item capable of being configured by the AP-6511 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.

2.2.7 Configuration Operation Icons

► [Web UI Overview](#)

The following icons are used to define configuration operations:



Revert – When selected, any changes made after the last saved configuration are restored back to the last saved configuration.



Commit – When selected, all changes made to the configuration are written to the system. Once committed, changes cannot be reverted.



Save – When selected, changes are saved to the configuration.

2.2.8 Access Type Icons

► [Web UI Overview](#)

The following icons display a user access type:



Web UI – Defines a Web UI access permission. A user with this permission is permitted to access an associated device's Web UI.



Telnet – Defines a TELNET access permission. A user with this permission is permitted to access an associated device using TELNET.



SSH – Indicates a SSH access permission. A user with this permission is permitted to access an associated device using SSH.



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

2.2.9 Administrative Role Icons

► [Web UI Overview](#)

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 device to which the user is connected.



System – States 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 – Defines 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 the AP-6511.



Web User—Indicates a Web user privilege. A Web user is allowed accessing the device's Web user interface.

2.2.10 Device Icons

► [Web UI Overview](#)

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



System—This icon indicates system-wide impact.



Cluster—This icon indicates a cluster. A cluster is a set of AP-6511s that work collectively to provide redundancy and load sharing.



Access Point—This icon indicates any access point that is a part of the network.



Wireless Client—This icon defines any wireless client connected within the network.

3

Getting Started

AP-6511 model Access Points utilize an initial settings wizard to streamline the process of accessing the wireless network for the first time. The wizard helps configure location, network and WLAN settings and aids in the discovery of access points. For instructions on how to use the initial setup wizard as well as an example walkthrough, see [*Using the Initial Setup Wizard on page 3-2.*](#)

3.1 Using the Initial Setup Wizard

Once the hardware is installed and powered on, complete the following steps to get the AP-6511 up and running and access management functions:

1. Connect one end of an Ethernet cable to the PoE port on the back of the AP-6511. Connect the other end to a computer with a functional Web browser. Use a power injector as needed to consolidate power and Ethernet in one cable.

If your host system is a DHCP server, an IP address is automatically assigned to the AP-6511 and can be used for device connection. However, if a DHCP server is not available, you'll need to derive the IP address from the AP-6511 MAC address. Using this method, the last two bytes of the AP-6511 MAC address become the last two octets of the IP address.

AP-6511 MAC address - 00:C0:23:00:F0:0A

AP-6511 IP address equivalent - 169.254.240.10

To derive the AP-6511's IP address using its factory assigned MAC address:

- a. Open the Windows calculator by selecting *Start > All Programs > Accessories > Calculator*. This menu path may vary slightly depending on your version of Windows.
 - b. With the Calculator displayed, select *View > Scientific*. Select the **Hex** radio button.
 - c. Enter a hex byte of the AP-6511's MAC address. For example, F0.
 - d. Select the **Dec** radio button. The calculator converts F0 into 240. Repeat this process for the last AP-6511 MAC address octet.
2. Point the Web browser to the AP-6511's IP address. The following login screen displays:

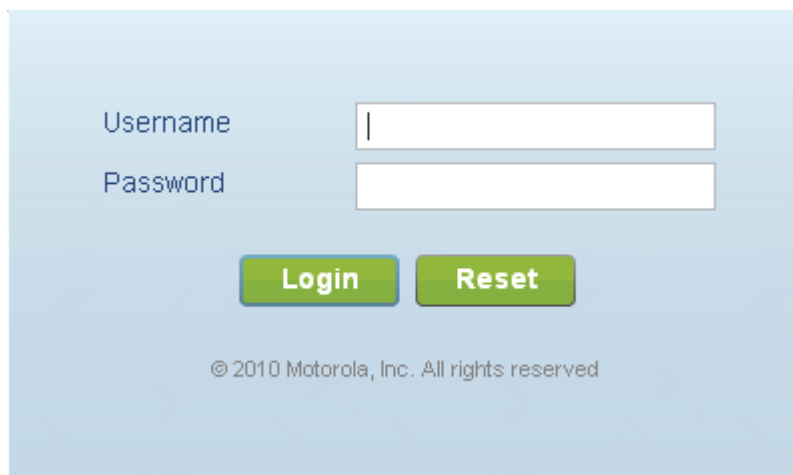
The image shows a web browser login screen with a light blue background. It features two input fields: 'Username' and 'Password'. Below the input fields are two green buttons labeled 'Login' and 'Reset'. At the bottom of the screen, there is a copyright notice: '© 2010 Motorola, Inc. All rights reserved'.

Figure 3-1 Web UI Login Screen

3. Enter the default username **admin** in the **Username** field.
4. Enter the default password **motorola** in the **Password** field.

5. Click the **Login** button to load the management interface.



NOTE: When logging into an AP-6511 for the first time, you will be prompted to change the password to enhance device security in subsequent logins.



NOTE: If you get disconnected when running the setup wizard, you can connect again with actual IP address (once obtained) and resume the wizard.

6. If this is the first time the management interface has been accessed, a dialogue displays to start the initial setup wizard. Click the **Start Wizard** button to run the initial setup wizard.



Figure 3-2 Initial Setup Wizard

7. Select an **Access Point Type** from the available options.
- *Controller AP* - When more than one AP-6511 is deployed, a single AP-6511 can function as a Controller AP to manage Dependent mode AP-6511s. Up to 24 Dependant APs can be connected to a Controller AP.
 - *Standalone AP* - Select this option to deploy this AP-6511 as an autonomous access point.
 - *Dependent AP* - Select this option when deploying the AP-6511 as a Controller AP managed access point. Selecting this option closes the Initial Setup Wizard. A Dependant AP obtains its configuration from a profile stored on the Controller AP. Any manual configuration changes on a Dependant AP are overwritten by the Controller AP upon reboot. A Dependent AP requires a Controller AP in the network.

For this example, choose the Controller AP option. Select Next. The Initial Setup Wizard displays the **System Information** screen for setting administrative credentials and device access protocols.

Access Point Type 1 of 11

The Access Point (AP) should be configured to manage other Access Points (Controller AP), function autonomously (Standalone AP), or be adopted by a Controller (Dependent AP).

Access Point Type

Controller AP

Standalone AP

Dependent AP

Back Next Cancel

Figure 3-3 Initial Setup Wizard - Access Point Type

8. Change the default Password and enter a **Location**, and **Contact** name. Select a **Time Zone** and **Country** for the AP-6511.

Changing the default password is critical before any configuration refinements are made to protect the data exchanged between the AP-6511 and its peers. Ensure the Location represents the AP-6511's deployment area and the Contact accurately reflects the administrator responsible for this AP-6511.

System Information2 of 11

The Controller should be configured with the correct identifying information and a new administrator password to prevent unauthorized access. The country code is especially important in order to ensure regulatory compliance.

Password	<input type="password" value="*****"/>
Location	<input type="text" value="test"/>
Contact	<input type="text" value="Joe Smith"/>
Time Zone	<input style="border-bottom: 1px solid gray;" type="text" value="(GMT-05:00) EST5EDT"/>
Country	<input style="border-bottom: 1px solid gray;" type="text" value="United States-us"/>

Select protocols that will be enabled for device access. HTTP and Telnet should be disabled for more security.

Enable HTTP	<input checked="" type="checkbox"/>
Enable HTTPS	<input type="checkbox"/>
Enable Telnet	<input type="checkbox"/>
Enable SSHv2	<input type="checkbox"/>

Figure 3-4 Initial Setup Wizard - System Information

9. Select any or all of access methods (*HTTP, HTTPS, Telnet* or *SSHv2*) used for connecting to this AP-6511 access point.
10. Select the **Next** button to continue to the **Topology Selection** screen.

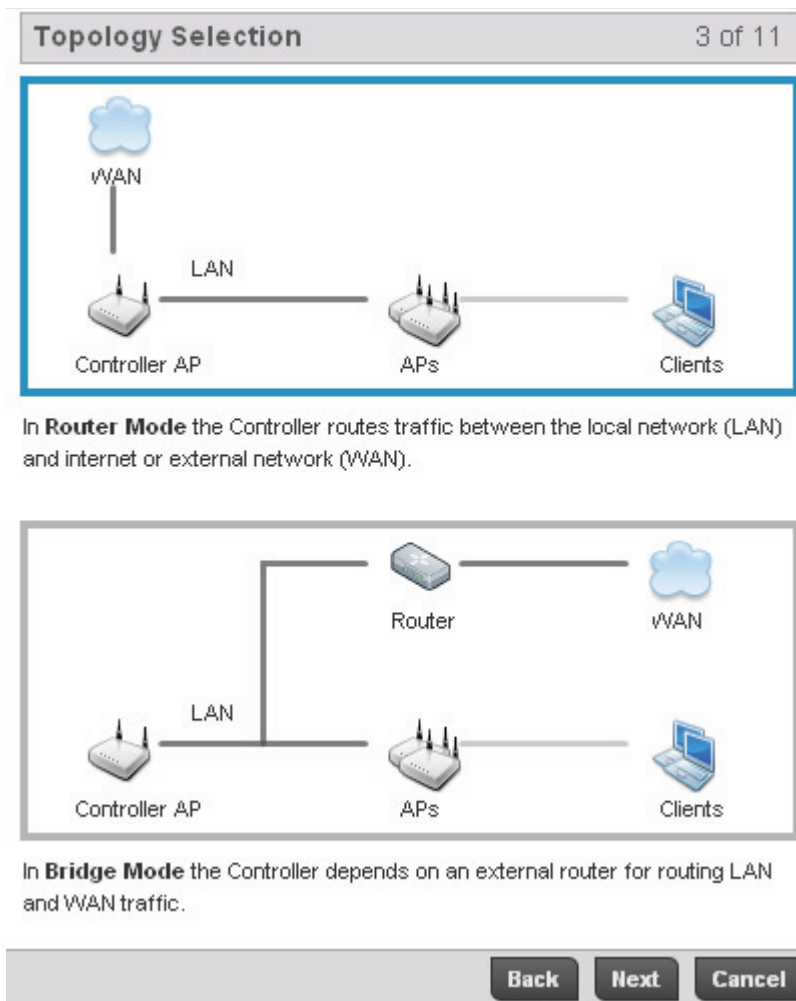


Figure 3-5 Initial Setup Wizard - Topology Selection

11. Select a network topology based on your network's configuration. The network topology mode determines which options are available in subsequent screens.

Router Mode In Router Mode the AP-6511 routes the traffic between the local network (LAN) and internet or external network (WAN).

Bridge Mode Displays the device's factory assigned MAC address used as hardware identifier. The MAC address cannot be revised with the device's configuration.

For the purposes of this example select **Router Mode**.

12. Click the **Next** button to continue to the **LAN Configuration** screen.

LAN Configuration
4 of 11

The LAN interface connects to the access points and LAN ports.

LAN Interface

LAN IP Address/Subnet Use DHCP

What VLAN ID should be used for the LAN interface?

Configure VLANs Manually **Advanced VLAN Configuration**

DHCP Address Assignment

Use the Controller to assign IP addresses to devices

IP Address Range to

Default Gateway

Domain Name Server (DNS)

Primary DNS

Secondary DNS

Figure 3-6 Initial Setup Wizard - LAN Configuration

13. The **LAN Configuration** screen is partitioned into **LAN Interface**, **DHCP Address Assignment** and **Domain Name Server (DNS)**.

The **LAN Interface** section contains configuration for the LAN IP Address and Subnet as well as VLAN configuration.

LAN IP Address / Subnet

Enter an IP Address and a subnet for the LAN interface. If the Use DHCP checkbox is selected this field is not configurable.

Use DHCP

To enable automatic network configuration using a DHCP Server select the Use DHCP checkbox. If this option is enabled the LAN IP Address/Subnet, DHCP Address Assignment and Domain Name fields are populated by the DHCP server.

What VLAN ID should be used for the LAN interface

Select the VLAN ID to associate with the LAN Interface. The default setting is VLAN 1.

Configure VLANs Manually

Select the Configure VLANs Manually checkbox to enable advanced manual VLAN configuration.

For more information on VLAN configuration see [Virtual Interface Configuration on page 7-11](#).

Advanced VLAN Configuration

Select the Advanced VLAN Configuration button to set associations between VLANs and physical interfaces.

For the purposes of this example, select **Use DHCP** and uncheck **Configure VLANs Manually**.

The **DHCP Address Assignment** section contains configuration for the DHCP server on the LAN interface.

Use the Controller to assign IP addresses to devices

Select the **Use the Controller to assign IP addresses to devices** checkbox to enable the DHCP server to provide IP and DNS information to clients on the LAN interface.

IP Address Range

Enter a starting and ending IP Address range to assign to clients on the LAN interface. It's good practice to 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 services on most networks.

The **Domain Name Server (DNS)** section contains configuration for the DNS server on the LAN interface.

Primary DNS

Enter an IP Address for the main Domain Name Server providing DNS services for the AP-6511 LAN interface.

Secondary DNS

Enter an IP Address for the backup Domain Name Server providing DNS services for the AP-6511 LAN interface.

WAN Configuration
5 of 11

The WAN interface connects to the internet or corporate wide area network.

WAN Interface

WAN IP Address/Subnet: Use DHCP

What VLAN ID should be used for the WLAN interface?

What port is connected to the external network?

Enable NAT on the WAN Interface

Gateway

Default Gateway:

Figure 3-7 Initial Setup Wizard - WAN Configuration

14. Select the **Next** button when completed to advance to the WAN Configuration screen.

The WAN Configuration screen is partitioned into **WAN Interface**, and **Gateway** fields.

The **WAN Interface** field contains configuration parameters for the WAN IP Address, Subnet and VLAN.

WAN IP Address/ Subnet	Enter an IP Address and a subnet for the controller's WAN interface. If the Use DHCP checkbox is enabled this field is not configurable.
Use DHCP	To enable automatic network configuration using a DHCP Server, select the Use DHCP checkbox. If this option is enabled the WAN IP Address/Subnet and Gateway fields are populated by the DHCP server.
What VLAN ID should be used for the WLAN interface	Use the spinner to select the VLAN ID to associate with the WLAN Interface. The default setting is VLAN 2100. For more information on VLAN configuration options, see Virtual Interface Configuration on page 7-11 .

What port is connected to the external network?

Use the drop-down menu to select the physical port connected to the WAN interface.

Enable NAT on the WAN Interface

Click the **Enable NAT on WAN Interface** checkbox to enable *Network Address Translation* (NAT) allowing traffic to pass between the WAN and LAN interfaces.

The **Gateway** field contains a configuration field for the **Default Gateway**.

Default Gateway

Enter an IP Address for the Default Gateway on the WAN interface. If the Use DHCP checkbox is enabled, this field is not configurable.

15. Select **Next** when completed to advance to the **WLAN Setup** screen.

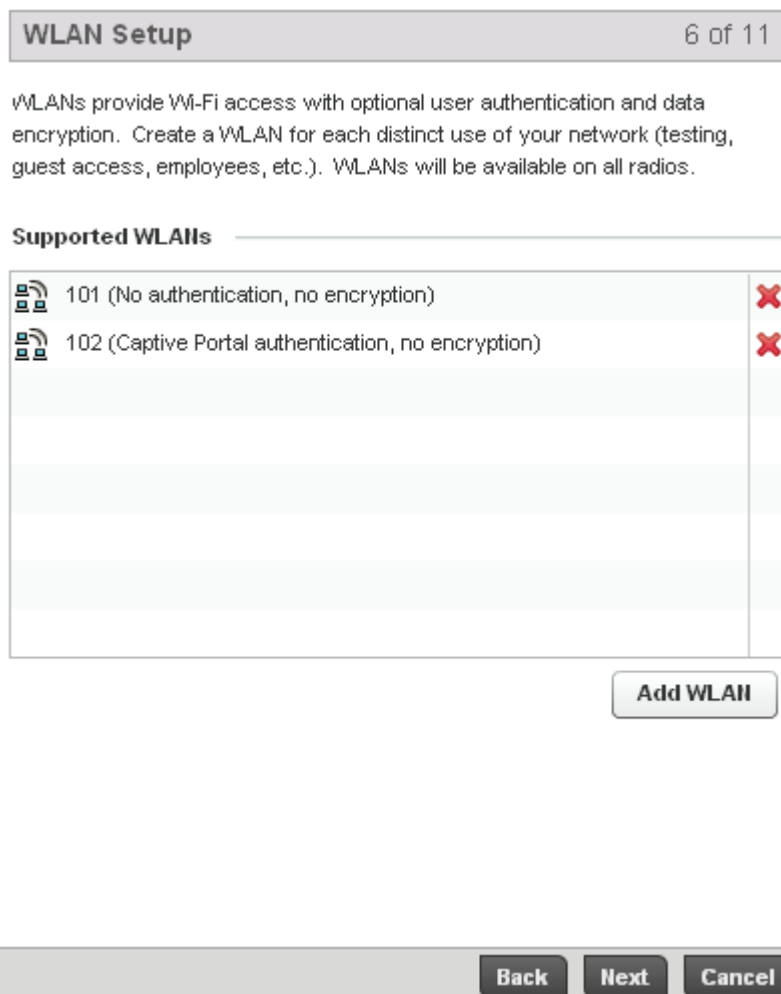


Figure 3-8 Initial Setup Wizard - WLAN Setup

16. The WLAN Setup screen allows you to define which WLANs are initially enabled on the AP-6511.

17. To add a WLAN, select **Add WLAN**.

Figure 3-9 Initial Setup Wizard - Add WLAN

The Add WLAN screen displays the following configuration parameters required to add a WLAN to the AP-6511:

- 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 available for the SSID is 32. Do not use any of the following characters - SSID <> | " & \ ? ,
- WLAN Type** Use the **WLAN Type** to select a basic authentication and encryption scheme for a AP-6511 WLAN. Available options include
- No authentication, no encryption*
 - Captive portal authentication, no encryption*
 - PSK authentication, WPA2 encryption*
 - EAP authentication, WPA2 encryption*
- For more information on WLAN authentication and encryption, see [Configuring WLAN Security on page 6-6](#).

- VLAN Id** Use the drop-down menu to select a VLAN to segregate traffic for this WLAN. All configured VLANs are available for selection.
- WPA 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 AP-6511 converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

For the purpose of this example, enter a **SSID**, and select **PSK authentication, WPA2 encryption**.

18. Select **OK** to exit the **Add WLAN** screen, then select **Next** to continue to the RADIUS Authentication screen.

RADIUS Authentication 7 of 11

External RADIUS Server

Some WLANs require authentication against an external RADIUS server.

RADIUS Server IP Address ▼

RADIUS Shared Secret



Figure 3-10 Initial Setup Wizard - RADIUS Authentication

19. As you did not select an authentication method that requires RADIUS, no action is required within this screen. Select **Next/Commit** to continue to the AP Discovery screen.

AP Discovery8 of 11

Access Points (APs) can be adopted by this Controller. Please connect the APs to the Controller to start the discovery process. AP name may be edited if desired (just click to edit name).

Hostname	MAC Address	Serial Number
percy	AA-11-00-00-00-00	aa1100000000
mudskipper	AA-22-00-00-00-00	aa2200000000
lancelot	AA-33-00-00-00-00	aa3300000000
	AA-44-00-00-00-00	aa4400000000

Figure 3-11 Initial Setup Wizard - AP Discovery

20. The AP Discovery screen displays a list of Access Points discovered by the AP-6511. The screen lists their **Model**, **Hostname**, **MAC Address** and **Serial Number**. If you have connected any APs recently, select the **Refresh List** button to update the list of known APs.

Optionally, define a **Hostname** for each known AP.

21. Click the **Next** button to continue on the **Wireless Client Association** screen.

Wireless Client Association
9 of 11

Verify WLAN configuration by attempting to associate a wireless client to each supported WLAN. After associating, press the Refresh link to list clients that have successfully associated.

WLAN	MAC Address	IP Address
WLAN1	AA-11-11-00-00-00	10.1.1.0
wlan1	AA-11-11-00-00-00	10.1.1.1
WLAN2	AA-11-22-00-00-00	10.1.2.0
wlan1	AA-11-22-00-00-00	10.1.1.1
WLAN2	AA-11-33-00-00-00	10.1.3.0

↓ Save _____

Clicking Save will persistently store the configuration on the Controller. This means it will remain even if the Controller is restarted.

Figure 3-12 Initial Setup Wizard - Wireless Client Association

22. The **Wireless Client Association** screen displays adopted wireless clients and the WLANs they are associated with.

To verify the WLAN configuration, associate a wireless client with each configured AP-6511 WLAN. After associating, click the **Refresh** button to update the list of associated wireless clients. Select **Save/Next** when completed to continue to the **Date and Time** screen.

Date and Time
10 of 11

The date and time should be configured. An external NTP server provides an accurate and synchronized source if available, otherwise enter the date and time manually.

System Date and Time

Manually enter system date and time

Unavailable **Refresh**

:

AM

PM

! Setting the clock may logout the current session.

Network Time Protocol (NTP)

Use an external NTP server to provide system date and time

NTP Server Address

Figure 3-13 Initial Setup Wizard - Date and Time

23. Either refer to the System Date and Time parameter to manually set the system time, or use the recommended **Network Time Protocol (NTP)** parameter to define an external NTP server resource to periodically synchronize system time with this AP-6511.

If manually providing system time, select the **Update Clock** button to commit the system time to the AP-6511. If using an external NTP resource, provide its numerical IP address and select the **Update NTP** button.

24. Select **Finish** to complete the AP-6511 Initial Setup Wizard. Once complete, a configuration profile is created and assigned to the AP-6511.

In addition to the **Diagram** and **Event Log** tabs available thus far, a **Complete** tab displays confirming the completion of the Initial Setup Wizard. The Complete tab lists the changes made to the user interface to configure the AP-6511.

The Complete tab lists the user interface **Screen** and **Settings** modified by the updates made to the AP-6511 configuration using the Initial Setup Wizard. Scroll to any screen listed within the Complete tab to display that screen within the AP-6511 user interface if additional modifications are required beyond the scope of the Initial Setup Wizard.

4

Dashboard

The dashboard allows network administrators to review and troubleshoot the operation of the devices comprising the AP-6511 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 screen, which is the top level in the device hierarchy.

The dashboard provides the following tools and diagnostics:

- *Dashboard*
- *Network View*

4.1 Dashboard

► Dashboard

The *Dashboard* displays device information organized by device association and inter-connectivity between the connected Access Points and wireless clients.

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

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

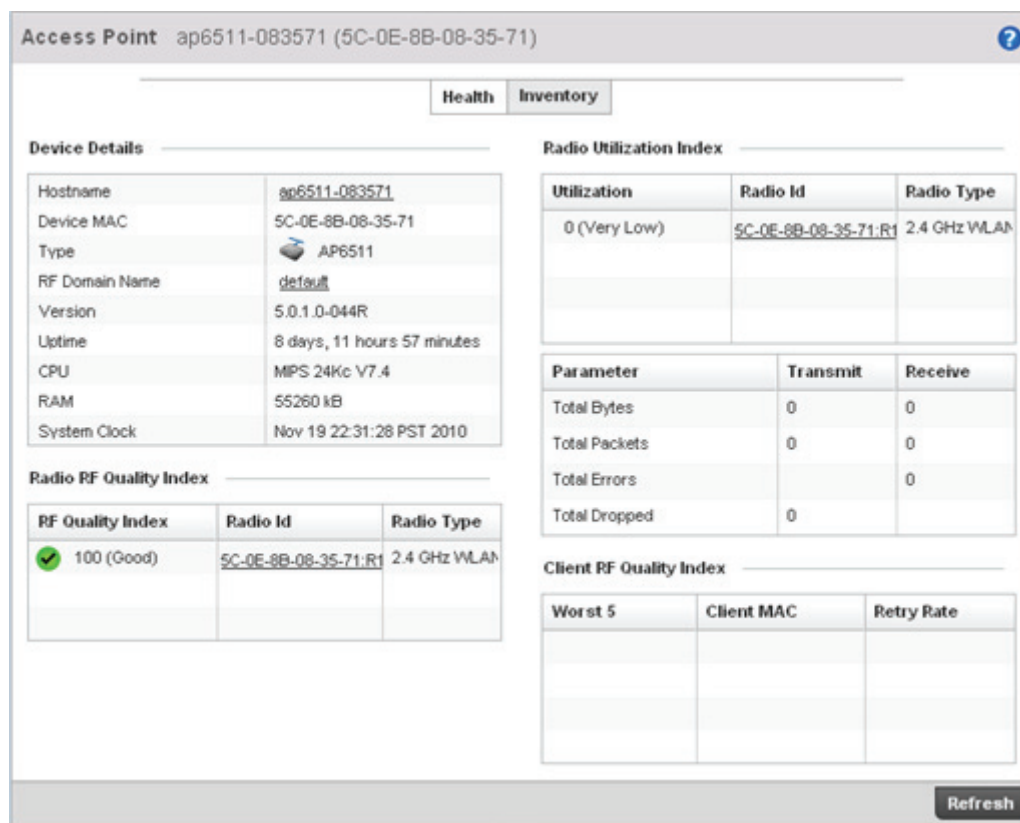


Figure 4-1 Dashboard screen - Health tab

4.1.1 Dashboard Conventions

The Dashboard displays AP-6511 information using the following conventions:

- *Health* – Displays information about the state of the AP-6511 managed network.
- *Inventory* – Displays information on the physical devices being managed by the AP-6511.

4.1.1.1 Health

► Health

The **Health** tab displays information about the state of the AP-6511 managed network.

Access Point ap6511-083571 (5C-0E-8B-08-35-71) ?

Health Inventory

Device Details

Hostname	ap6511-083571
Device MAC	5C-0E-8B-08-35-71
Type	AP6511
RF Domain Name	default
Version	5.0.1.0-044R
Uptime	8 days, 11 hours 57 minutes
CPU	MIPS 24Kc V7.4
RAM	55260 kB
System Clock	Nov 19 22:31:28 PST 2010

Radio Utilization Index

Utilization	Radio Id	Radio Type
0 (Very Low)	5C-0E-8B-08-35-71-R1	2.4 GHz WLAN

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

Radio RF Quality Index

RF Quality Index	Radio Id	Radio Type
✓ 100 (Good)	5C-0E-8B-08-35-71-R1	2.4 GHz WLAN

Client RF Quality Index

Worst 5	Client MAC	Retry Rate

Refresh

Figure 4-2 Dashboard screen - Health tab

Information in this tab is classified as:

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

4.1.1.1.1 Device Details

► Health

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

Device Details


Hostname	ap6511-083571
Device MAC	5C-0E-8B-08-35-71
Type	 AP6511
RF Domain Name	default
Version	5.0.1.0-044R
Uptime	8 days, 11 hours 57 minutes
CPU	MIPS 24Kc V7.4
RAM	55260 kB
System Clock	Nov 19 22:31:28 PST 2010

Figure 4-3 Device Health

This field displays the name assigned to this host, its factory encoded MAC address, model type, RF Domain membership, software version, uptime, CPU and RAM information and system clock. Use this data to determine whether a software upgrade is warranted for the AP-6511 or if perhaps the system clock needs adjustment.

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

4.1.1.1.2 Radio RF Quality Index

▶ *Health*

The Radio RF Quality Index field displays a RF quality table for the AP-6511’s single RF Domain. It’s a percentage of the overall effectiveness of the RF environment. It’s 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
 100 (Good)	5C-0E-8B-08-35-71:R1	2.4 GHz WLAN

Figure 4-4 Radio RF Quality Index

RF Quality displays as the average quality index for the single RF Domain utilized by the AP-6511. The table lists the bottom five (5) RF quality values for the AP-6511’s RF Domain.

The quality is measured as:

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

A 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. A RF Domain contains policies that can determine a Smart RF or WIPS configuration.

Select the RF Domain to view its performance statistics or review the attributes of poorly performing radios.

Use this diagnostic information to define measures to improve radio performance in respect to wireless client load and the radio bands currently supported.

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

4.1.1.1.3 Radio Utilization Index

► *Health*

The Radio Utilization Index field displays how efficiently the RF medium is used by the AP-6511. Traffic utilization is defined as the percentage of throughput relative to the maximum possible throughput for the AP-6511's RF Domain.

Refer to the number of errors and dropped packets to assess AP-6511 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.

Radio Utilization Index

Utilization	Radio Id	Radio Type
0 (Very Low)	<u>5C-0E-8B-08-35-71:R1</u>	2.4 GHz WLAN

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

Figure 4-5 Radio Utilization Index field

4.1.1.1.4 Client RF Quality Index

► *Health*

The Client RF Quality field displays a list of the worst 5 performing clients managed by the AP-6511.

Client RF Quality Index

Worst 5	Client MAC	Retry Rate

Figure 4-6 Client RF Quality Index field

The table displays the following:

- Worst 5** Lists to worst 5 performing client radios connected to this AP-6511.
- Client MAC** Displays the factory encoded MAC address assigned to each of the radios 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.

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

4.1.1.2 Inventory

► *Dashboard Conventions*

The *Inventory* tab displays information relative to the devices managed by this AP-6511. This 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 specific radio.

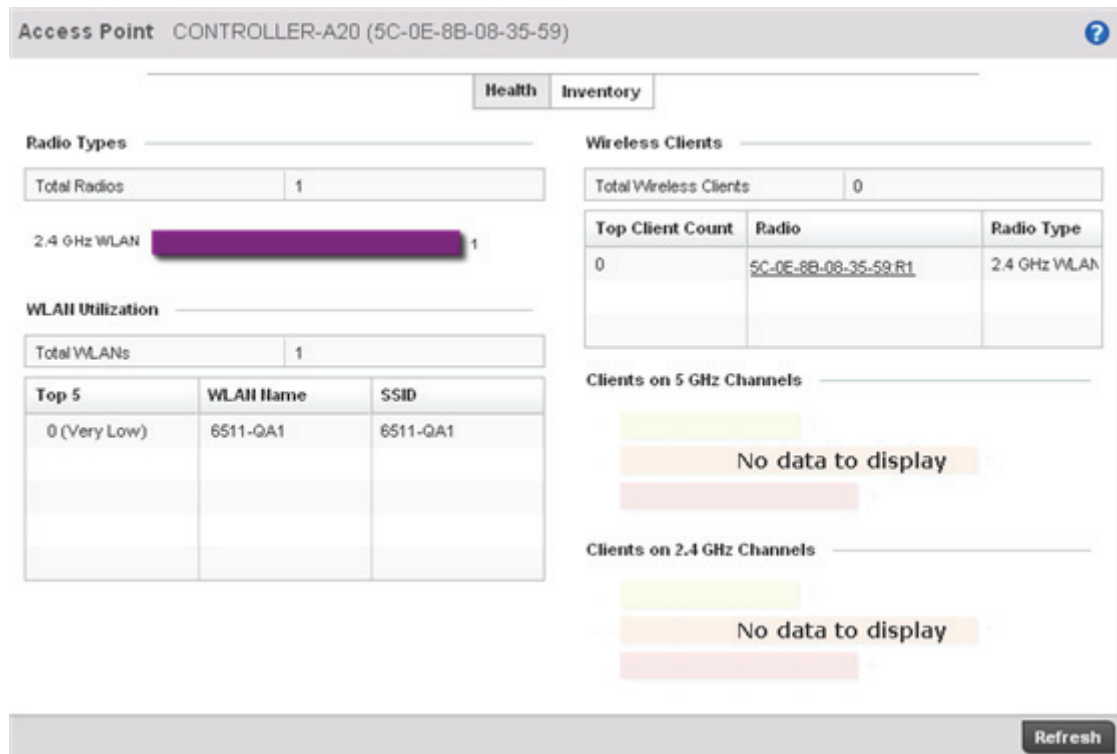


Figure 4-7 System screen - Inventory tab

Information is partitioned into the following fields:

- *Radio Types*
- *WLAN Utilization*
- *Wireless Clients*
- *Client on Channels*

4.1.1.2.5 Radio Types

► [Inventory](#)

The Radio Types field displays the total number and types of radios managed by the AP-6511.

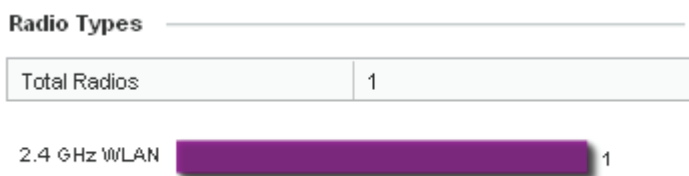


Figure 4-8 Radio Types field

Refer to the **Total Radios** column to review the number of AP-6511 managed radios. Additionally, use the charts on the bottom of the Radio Types field to assess the number WLANs that are utilized in the 2.4 and 5 GHz channels. Do these WLAN deployment support the client needs of this AP-6511?

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

4.1.1.2.6 WLAN Utilization

► [Inventory](#)

The WLAN Utilization field displays the top 5 WLANs utilized by this AP-6511 in respect to deployment on behalf of AP-6511 client support.

The screenshot shows the 'WLAN Utilization' field. At the top, there is a header 'WLAN Utilization' followed by a horizontal line. Below this is a table with two columns: 'Total WLANs' and '1'. Underneath this table is a larger table with three columns: 'Top 5', 'WLAN Name', and 'SSID'. The first row of this table shows '0 (Very Low)' in the 'Top 5' column, '6511-QA1' in the 'WLAN Name' column, and '6511-QA1' in the 'SSID' column. The remaining four rows are empty.

Figure 4-9 Device Types field

The table displays how effectively each WLAN is utilized, its WLAN name and each listed WLANs's SSID.

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

4.1.1.2.7 Wireless Clients

► [Inventory](#)

The Wireless Clients field displays information about the wireless clients managed by this AP-6511.

Wireless Clients

Total Wireless Clients	0	
Top Client Count	Radio	Radio Type
0	<u>5C-0E-8B-08-35-59:R1</u>	2.4 GHz WLAN

Figure 4-10 Wireless Clients field

Information in the Wireless Clients field is presented in two tables. The first table lists the total number of wireless clients managed by this AP-6511. The second table lists an ordered ranking of radios based on their supported client count. Use this information to assess if an AP-6511 managed radio is optimally deployed in respect to its radio type and intended client support requirements.

4.1.1.2.8 Client on Channels

► [Inventory](#)

The **Client of Channels** field displays a bar-graph for wireless clients segregated by their operating frequency. Information for each channel is further classified based on 802.11x band.

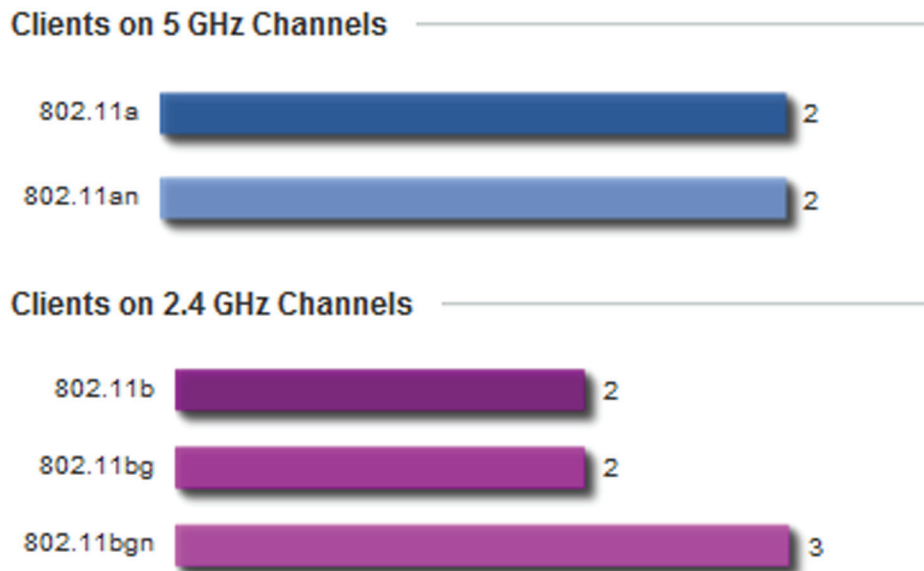


Figure 4-11 Client On Channel field

For 5 GHz, information is displayed in the *802.11a* and *802.11an* radio bands. For 2.4 GHz, information is displayed in the *802.11b*, *802.11bg*, and *802.11bgn* radio bands.

4.2 Network View

► [Dashboard](#)

The Network View displays device topology association between an AP-6511 its RF Domain and its managed wireless clients. This association is displayed using a number of different graph and filter options.

To review the Network Topology, select **Dashboard > Overview > Network**.

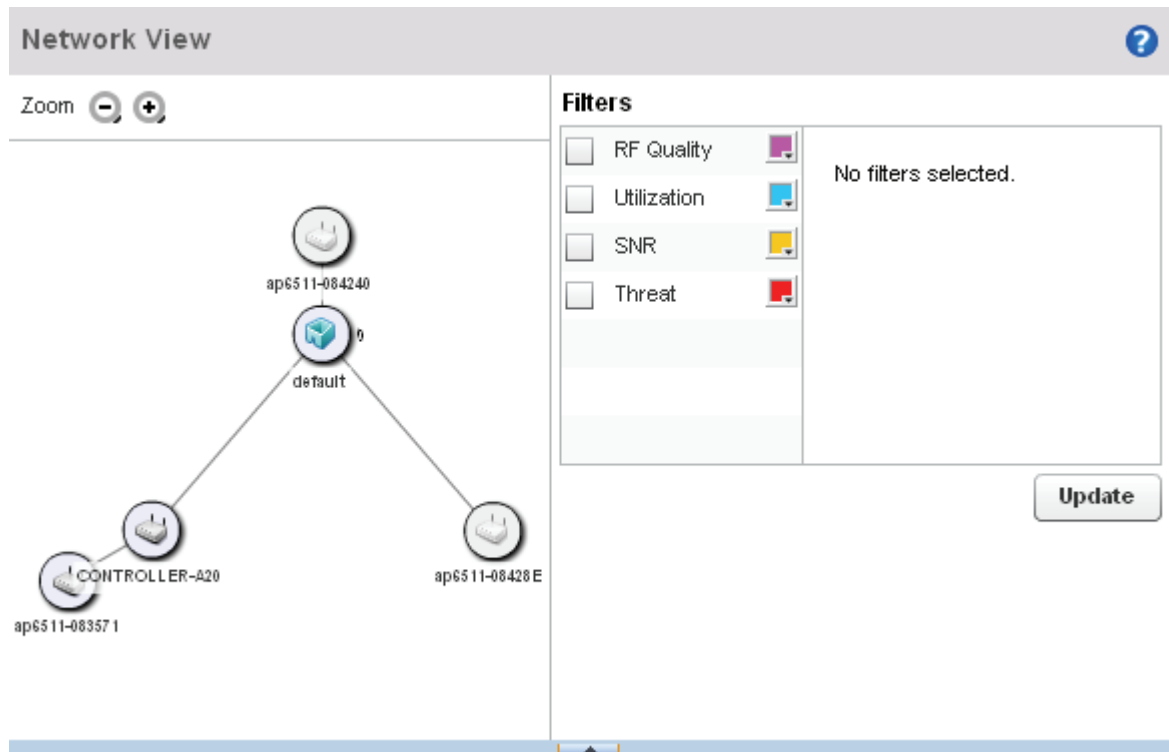


Figure 4-12 Network View Topology

The screen displays icons for the different views that can be created. Apart from device specific icons, the following three icons are available:

- *default* – Displays information about the AP-6511's default RF Domain.
- *system* – Displays information about the current system.

Use these icons to navigate within the Network view and manipulate the display.

Select the **Settings** link to define how devices are displayed within the Network View.

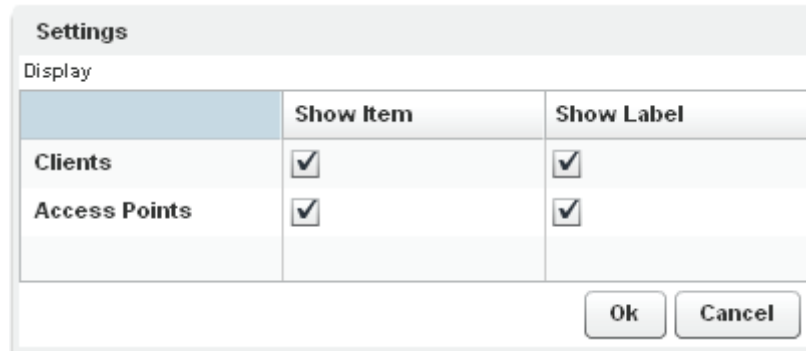


Figure 4-13 Network View - Settings field

Select either **Access Points** or **Clients** (or both) to display them within the Network View topology. Similarly, select the **Show Label** option to display hardware MAC address.

The left-hand side of the Network View display contains an expandable System column where peer AP-6511 Access Points can be selected and expanded to displays connected peers. Use the System area as required to review device connections within an AP-6511 managed network. Many of these peer devices are available for device connection to Controller AP mode AP-6511s.

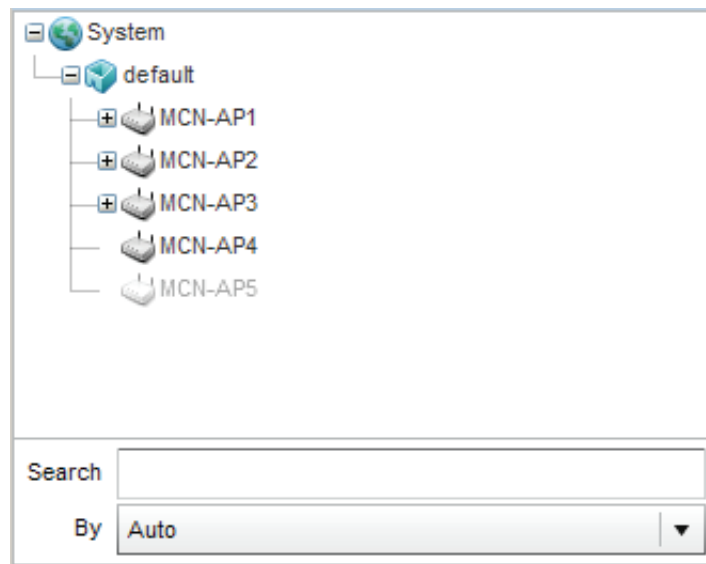



Figure 4-14 Network View - System field


4.2.1 Filters Field


► Network View


The *Filters* field is located on the top right-hand side of the Network View screen. It provides different options to fetch information.

Filters

RF Quality 

Utilization 

SNR 

Threat 

Poor (0-14)

Average (15-24)

Good (25-100)

SNR (Signal to Noise Ratio) determines signal strength relative to noise in dB.

Update

Figure 4-15 Filters field

The following filter options are available:

- **RF 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. The available ranges are:
 - *Poor (0-29)* – Filters clients based on RF health in the range of 0-29.
 - *Good (30-59)* – Filters clients based on RF health in the range of 30-59.
 - *Excellent (60-100)* – Filters clients based on RF health in the range of 60-100.
- **Utilization** – Select this option to filter based on the percentage of current throughput relative to maximum throughput. The available filter ranges are:
 - *Low (0-29)* – Filters in the range of 0-29 percent.
 - *Medium (30-59)* – Filters in the range of 30-59 percent.
 - *High (60-100)* – Filters in the range of 60-100 percent.
- **SNR** – Select this option to filter based on a signal to noise ratio in decibels. The available filter ranges are:
 - *Poor (0-14)* – Filters clients based on the SNR value in the range of 0-14.
 - *Average (15-24)* – Filters clients based on the SNR value in the range of 15-24.
 - *Good (25-100)* – Filters clients based on the SNR value in the range of 25-100.
- **Threat** – Select this option to filter based on a threat perception for a RF Domain. Threat perception is based on the number of Rogue APs and WIDS events generated by a RF Domain. The available filter ranges are:
 - *Low (0-1)* – Filters based on low threat perception in the range 0-1.
 - *Medium (2-3)* – Filters based on medium threat perception in the range 2-3.
 - *High (4-5)* – Filters based on high threat perception in the range 4-5.

Multiple options can be selected to refine the filtering outcome.

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

4.2.2 Device Specific Information

► [Network View](#)

The device specific information field displays information for a selected device. The screen displays the Access Points factory encoded MAC address and serial number. While this information cannot be modified by the administrator, it does enable the administrator to review the device’s system uptime within the AP-6511 managed network.


ap6511-083571		
Access Point (AP6511)		
Configuration		
MAC Address	5C-0E-8B-08-35-71	
Serial Number	10161521100004	
Status		
Uptime	8 days, 14 hours 43 minutes	
Statistics		

Figure 4-16 AP-6511 Device Specific Information

Optionally select the Statistics link at the bottom of the display a screen where Access Point device data can be reviewed on a much more granular level. For more information, see [Health on page 4-2](#).

Device Configuration

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

When a device is initially managed, it requires several basic configuration parameters be set and its deployment location defined. Additionally, the number of permitted device licenses (purchased directly from Motorola) needs to be accessed to determine whether new devices can be adopted.

Refer to the following to set a AP-6511 basic configuration, license configuration and certificate usage:

- [*Basic Device Configuration*](#)
- [*Assigning Certificates*](#)

An AP-6511 RF Domain allows an administrator to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share, as their general client support roles are quite similar. However, device configurations may need periodic refinement and overrides from their original RF Domain administered design. For more information, see [*RF Domain Overrides on page 5-24*](#).

Profiles enable administrators to assign a common set of configuration parameters and policies to Access Points. 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. Both default and user defined profiles are supported implementing new features or updating existing parameters to groups of Access Points.

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 [*Profile Overrides on page 5-27*](#).

Adoption is the process an Access Point uses to discover controllers available in the network, pick the most desirable controller, establish an association with the controller and optionally obtain an image upgrade.

At adoption, an AP solicits and receives multiple adoption responses from controllers available on the network. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

5.1 Basic Device Configuration

Setting a device's Basic Configuration is required to assign an individual device name, deployment location, and system time. Similarly, the Basic Configuration screen is where Profile and RF Domain assignments are made.

Profiles enable administrators to assign a common set of configuration parameters and policies to Access Points. Profiles can be used to assign common 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.



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

To assign a device an AP-6511 a Basic Configuration:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the Configuration tab.
3. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

The **Basic Configuration** screen displays by default.

The screenshot shows a web-based configuration interface for a device. It is divided into four main sections:

- Configuration:** Contains three text input fields: "System Name" (with the value "ap6511-083571"), "Building", and "Floor".
- Profile:** Features a "Profile Name" dropdown menu currently set to "DAP-20". To the right of the dropdown are two icons: a plus sign in a square and a gear.
- Device Overrides:** Contains a single button labeled "Clear Overrides" with a circular arrow icon.
- Set Clock:** Shows the current "Device Time" as "Nov 20 01:28:58 PST 2010" with a "Refresh" link. Below this is a "New Time" section with a date picker, a time input showing "1 : 0", and radio buttons for "AM" and "PM". An "Update Clock" button is positioned below the time input. A yellow warning icon and text state: "Setting the clock may logout the current session."

Figure 5-1 Device Basic Configuration screen

4. 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 device supports.
- Building** Assign the target a device a Building name representative of the location the device is physically deployed. The name cannot exceed 64 characters. Assigning a building name is helpful when grouping devices in Profiles, as devices in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location
- Floor** Assign the target a device a building Floor name representative of the location the Access Point was physically deployed. The name cannot exceed 64 characters. Assigning a building Floor name is helpful when grouping devices in Profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.

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

If a profile configuration does not exist suiting the deployment requirements of the target device, select the **Create** icon to create a new profile configuration, or select the **Edit** icon to modify the configuration of a selected profile. For more information on profile configuration, see [Profile Configuration on page 7-1](#).

6. Refer to the **Set Clock** parameter to update the AP-6511 system time.

Refer to the **Device Time** parameter to assess the device's current time, or whether the device time is unavailable. Select **Refresh** as required to update the device's 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.

When completed, select **Update Clock** to commit the updated time to the AP-6511.

7. Select **OK** to save the changes to the basic configuration. Selecting **Reset** reverts the screen to its last saved configuration.

5.2 Assigning Certificates

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

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

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

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a client to access 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.

To configure AP-6511 certificate usage:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the Configuration tab.
3. Select **Certificates** from the Device menu.

Management Security

HTTPS Trustpoint	Pending	<input type="radio"/>		
	Stored	<input checked="" type="radio"/>	default-trustpoint	Launch Manager
SSH RSA Key	Pending	<input type="radio"/>		
	Stored	<input checked="" type="radio"/>	default_rsa_key	Launch Manager

Information

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

OK x Reset x Exit

Figure 5-2 Device Certificates screen

4. 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 [Certificate Management on page 5-6](#).

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 5-15](#).



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

5. 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:

- [Certificate Management](#)
- [RSA Key Management](#)
- [Certificate Creation](#)
- [Generating a Certificate Signing Request](#)

5.2.1 Certificate Management

▶ [Assigning 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 a AP-6511. 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.

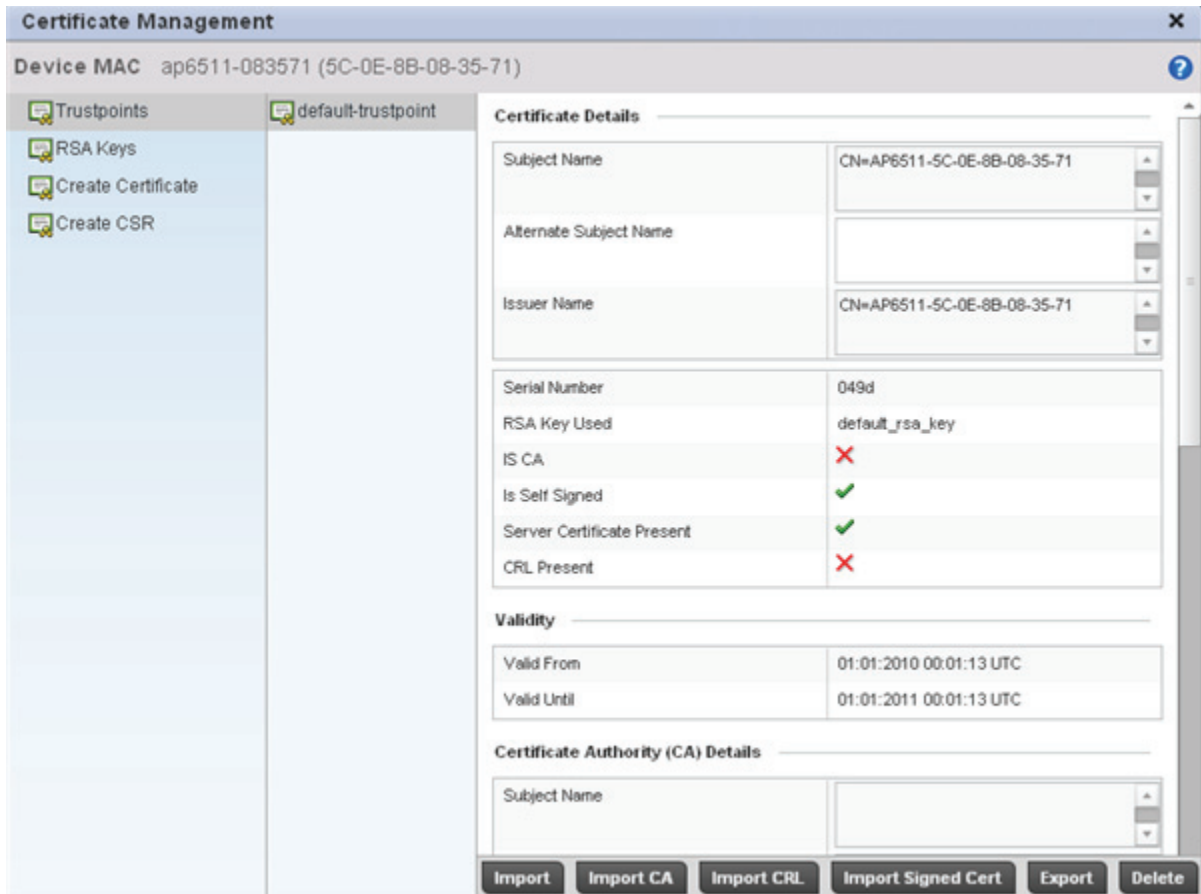


Figure 5-3 Certificate Management - Trustpoints screen

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 the **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. The **Import New Trustpoint** screen displays.

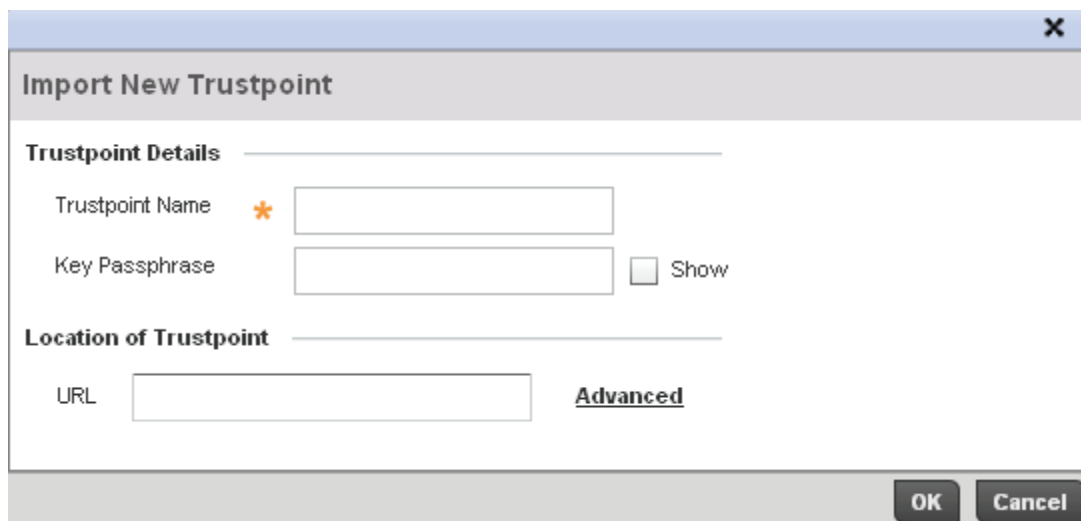


Figure 5-4 Certificate Management - Import New Trustpoint screen

4. Define the following configuration parameters required for the **Import** 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.
- Key Passphrase** Define the key used by both the device and the server (or repository) of the target trustpoint. Select the **Show** textbox to expose the actual characters used in the key. Leaving the Show checkbox unselected displays the passphrase as a series of asterisks “*”.
- 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 also dependent on the selected protocol.
- Protocol** Select the protocol used for importing the target trustpoint. Available options include:
tftp
ftp
sftp
http
cf
usb1
usb2
- Port** Use the spinner control to set the port. This option is not valid for *cf*, *usb1*, and *usb2*.
- IP Address** Enter IP address of the server used to import the trustpoint. This option is not valid for *cf*, *usb1*, and *usb2*.

Hostname	Provide the hostname of the server used to import the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the trustpoint. Enter the complete relative path to the file on the server.

5. Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
6. To optionally import a CA certificate, select the **Import CA** button from the Certificate Management screen.

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.

Figure 5-5 Certificate Management - Import CA Certificate screen

7. Define the following configuration parameters required for the **Import** of the CA certificate:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
From Network	Select the From Network radio button to provide network address information to the location of the target CA certificate. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
Cut and Paste	Select the Cut and Paste radio button to copy an existing CA certificate into the cut and past field. When pasting a valid CA certificate, no additional network address information is required.

Protocol	Select the protocol used for importing the target CA certificate. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1</i> <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter the IP address of the server used to import the CA certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the CA certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the CA certificate. Enter the complete relative path to the file on the server.

8. Select **OK** to import the defined CA certificate. Select **Cancel** to revert the screen to its last saved configuration.
9. To optionally import a CRL, select the **Import CRL** button from the Certificate Management screen.

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 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.

For information on creating the CRL used with a trustpoint, refer to [Setting the Certificate Revocation List \(CRL\) Configuration on page 7-38](#).

Figure 5-6 Certificate Management - Import CRL screen

10. Define the following configuration parameters required for the **Import** of the CRL:

- | | |
|------------------------|--|
| Trustpoint Name | Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate. |
| From Network | Select the From Network radio button to provide network address information to the location of the target CRL. The number of additional fields that populate the screen is dependent on the selected protocol. |
| Cut and Paste | Select the Cut and Paste radio button to copy an existing CRL into the cut and past field. When pasting a CRL no additional network address information is required. |
| URL | Provide the complete URL to the location of the CRL. If needed, select Advanced to expand the dialog to display network address information for the location of the target CRL. The number of additional fields that populate the screen is dependent on the selected protocol. |
| Protocol | Select the protocol used for importing the CRL. Available options include:
<i>tftp</i>
<i>ftp</i>
<i>sftp</i>
<i>http</i>
<i>cf</i>
<i>usb1</i>
<i>usb2</i> |
| Port | Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> . |

IP Address	Enter IP address of the server used to import the CRL. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the CRL. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the CRL. Enter the complete relative path to the file on the server.

11. Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.
12. To import a signed certificate, select the **Import Signed Cert** button from the Certificate Management screen.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

Self-signed certificates cannot be revoked which may allow an attacker who has already gained access to monitor and inject data into a connection to spoof an identity if a private key has been compromised. However, CAs have the ability to revoke a compromised certificate, which prevents its further use.

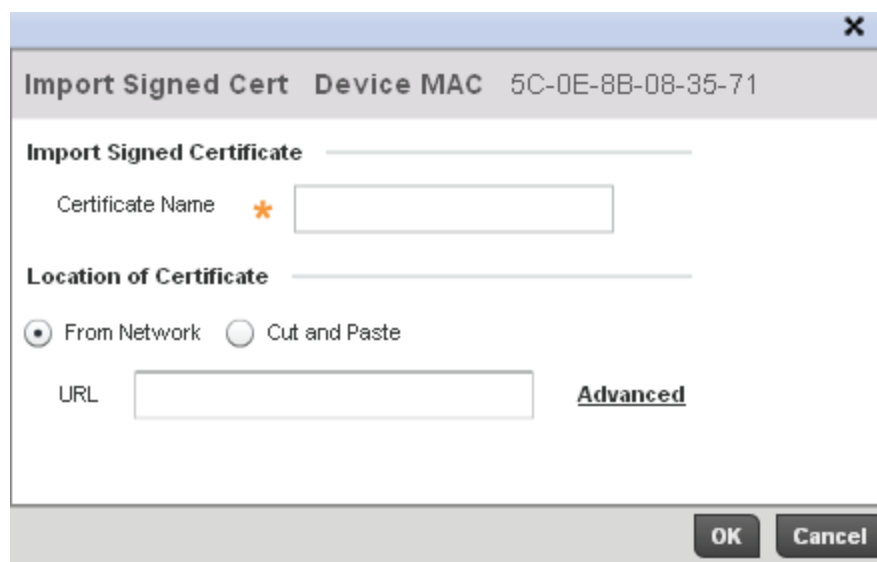


Figure 5-7 Certificate Management - Import Signed Cert screen

13. Define the following configuration parameters required for the **Import** of the CA certificate:

Certificate Name	Enter the 32 character maximum name of the trustpoint with which the certificate should be associated.
From Network	Select the From Network radio button to provide network address information to the location of the target signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol.
Cut and Paste	Select the Cut and Paste radio button to copy an existing signed certificate into the cut and past field. When pasting a signed certificate, no additional network address information is required.

URL	Provide the complete URL to the location of the signed certificate. If needed, select Advanced to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol.
Protocol	Select the protocol used for importing the target signed certificate. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1</i> <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to import the signed certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the signed certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the signed certificate. Enter the complete relative path to the file on the server.

14. Select **OK** to import the signed certificate. Select **Cancel** to revert the screen to its last saved configuration.

15. 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's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

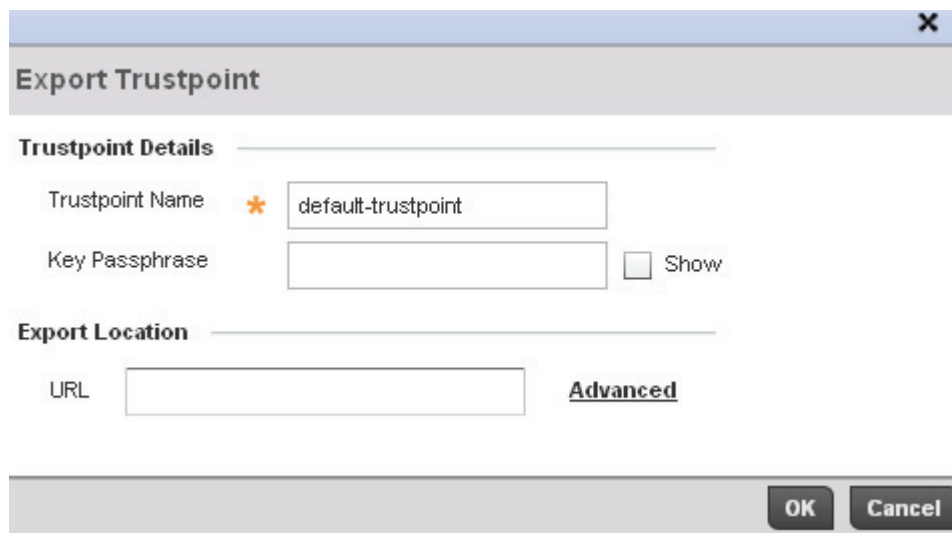


Figure 5-8 Certificate Management - Export Trustpoint screen

16. 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.
- Key Passphrase** Define the key used by both the device and the server (or repository) of the target trustpoint. Select the **Show** textbox to expose the actual characters used in the key. Leaving the Show checkbox unselected displays the passphrase as a series of asterisks “*”.
- 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 also 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*
- Port** Use the spinner control to set the port. This option is not valid for *cf*, *usb1*, and *usb2*.
- IP Address** Enter IP address of the server used to export the trustpoint This option is not valid for *cf*, *usb1*, and *usb2*.

Hostname	Provide the hostname of the server used to export the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the trustpoint. Enter the complete relative path to the file on the server.

17. Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
18. 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** checkbox 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

5.2.2 RSA Key Management

▶ Assigning Certificates

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's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1. Select the **Launch Manager** button from either the SSH RSA Key or RADIUS Server Certificate parameters (within the Certificate Management screen).
2. Select **RSA Keys** from the upper, left-hand, side of the Certificate Management screen.

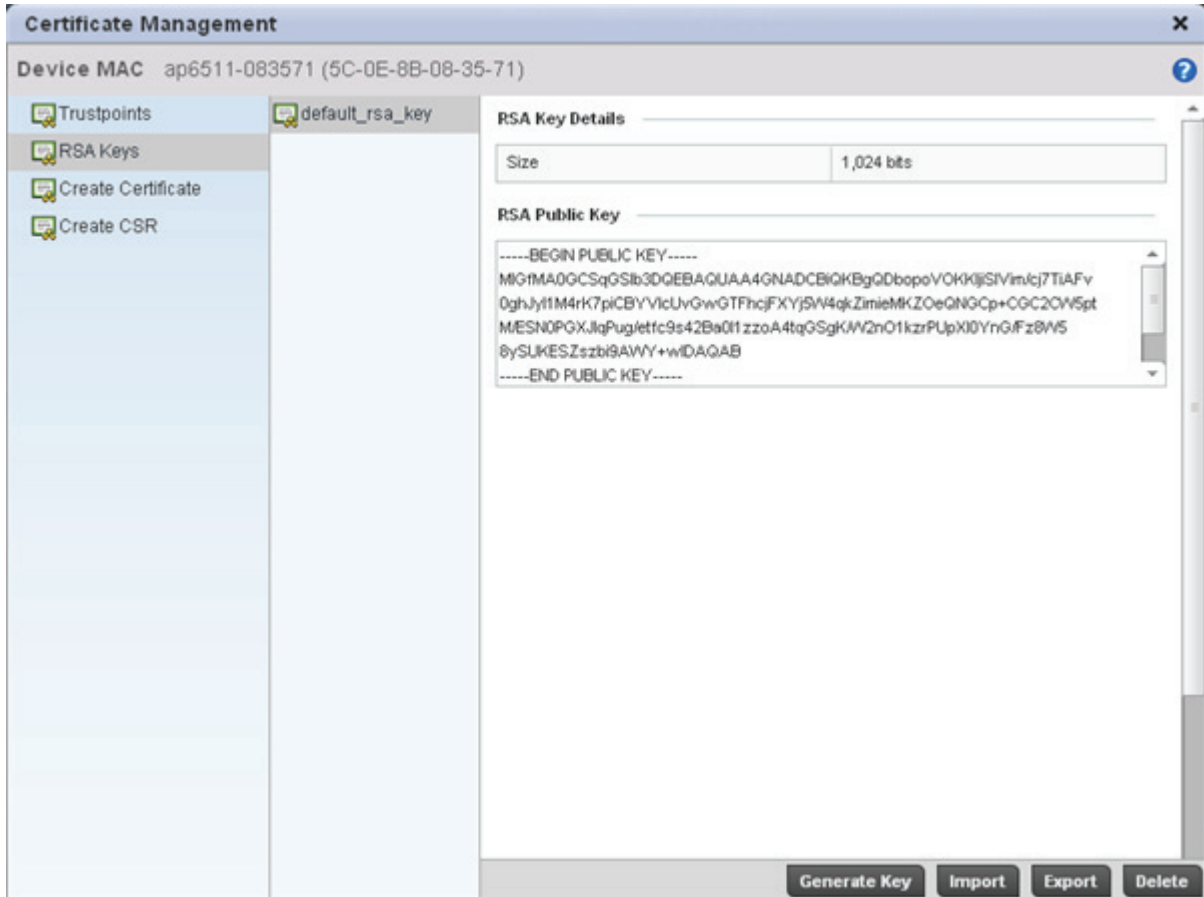


Figure 5-9 Certificate Management - RSA Keys screen

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 **Generate Key** to create a new key with a defined size.

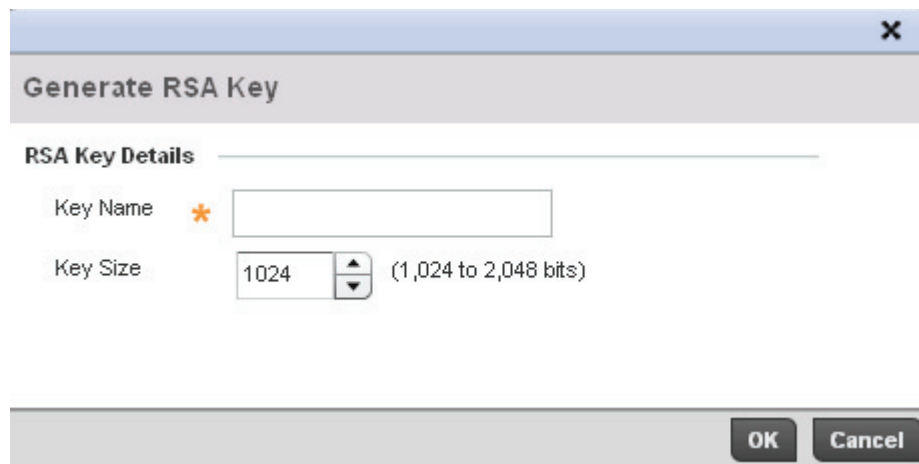


Figure 5-10 Certificate Management - Generate RSA Key screen

5. Define the following configuration parameters required for the **Import** of the key:

- Key Name** Enter the 32 character maximum name assigned to the RSA key.
- Key Size** Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 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 5-11 Certificate Management - Import New RSA Key screen

8. Define the following configuration parameters required for the **Import** of the RSA key:

- Key Name** Enter the 32 character maximum name assigned to the RSA key.
- Key Passphrase** Define the key used by both the AP-6511 and the server (or repository) of the target RSA key. Select the **Show** textbox to expose the actual characters used in the passphrase. Leaving the Show checkbox 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 also dependent on the selected protocol.

Protocol	Select the protocol used for importing the target key. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1</i> <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to import the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

9. Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.
10. To optionally export a RSA key to a remote location, select the **Export** button from the RSA Keys screen.
Export the key to a RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

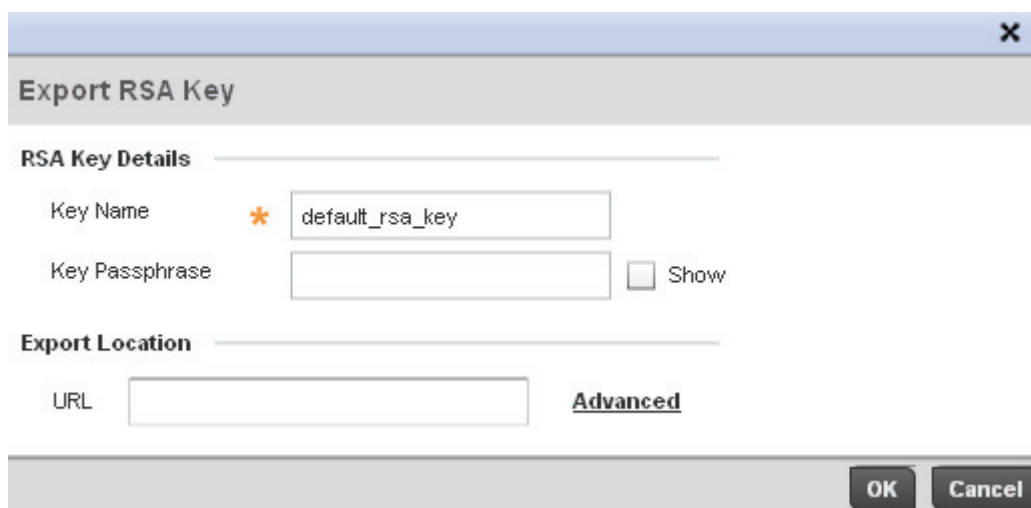


Figure 5-12 Certificate Management - Export RSA Key screen

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 both the AP-6511 and the server. Select the Show textbox to expose the actual characters used in the passphrase. Leaving the Show checkbox 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: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1</i> <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	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 its 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** checkbox to remove the certificate the key supported. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

5.2.3 Certificate Creation

► Assigning 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:

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** from the upper, left-hand, side of the Certificate Management screen.

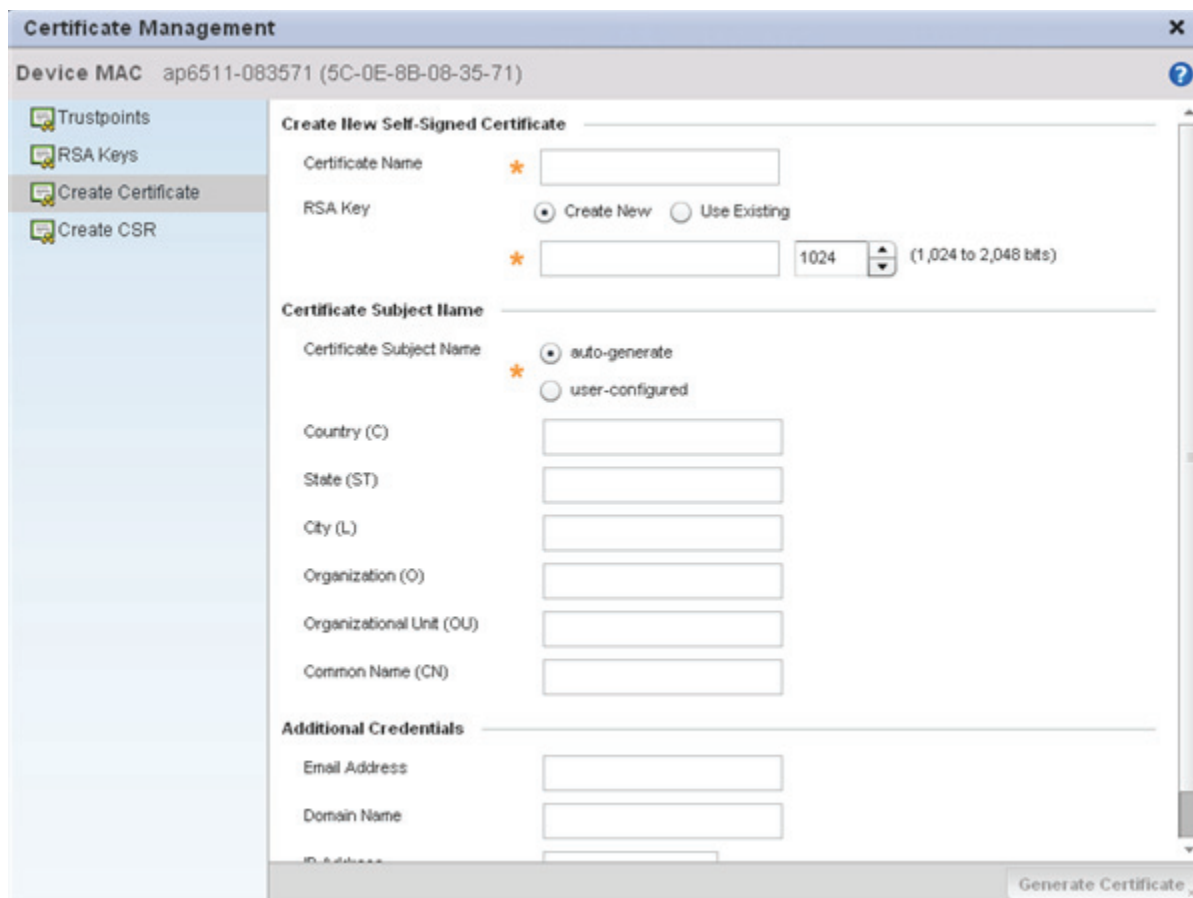


Figure 5-13 Certificate Management - Create Certificate screen

3. Define the following configuration parameters required to **Create New Self-Signed Certificate**:

- Certificate Name** Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
- Use an Existing RSA Key** Select the radio button and 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 a New RSA Key** 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 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting (1024) to ensure optimum functionality. For more information on creating a new RSA key, see [RSA Key Management on page 5-15](#).

4. Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-defined</i> 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 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 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 Org. Unit for the name of the organization unit used in the certificate. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Select the following **Additional Credentials** required for the generation of the self signed certificate:

Email Address	Provide an email address used as the contact address for issues relating to this certificate request.
Domain Name	Enter a <i>fully qualified domain name</i> (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 Create Certificate screen to produce the certificate.

5.2.4 Generating a Certificate Signing Request

► Assigning 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 the **Launch Manager** button from either the SSH RSA Key or RADIUS Server Certificate parameters (within the Certificate Management screen).
2. Select **Create CSR** from the upper, left-hand, side of the Certificate Management screen.

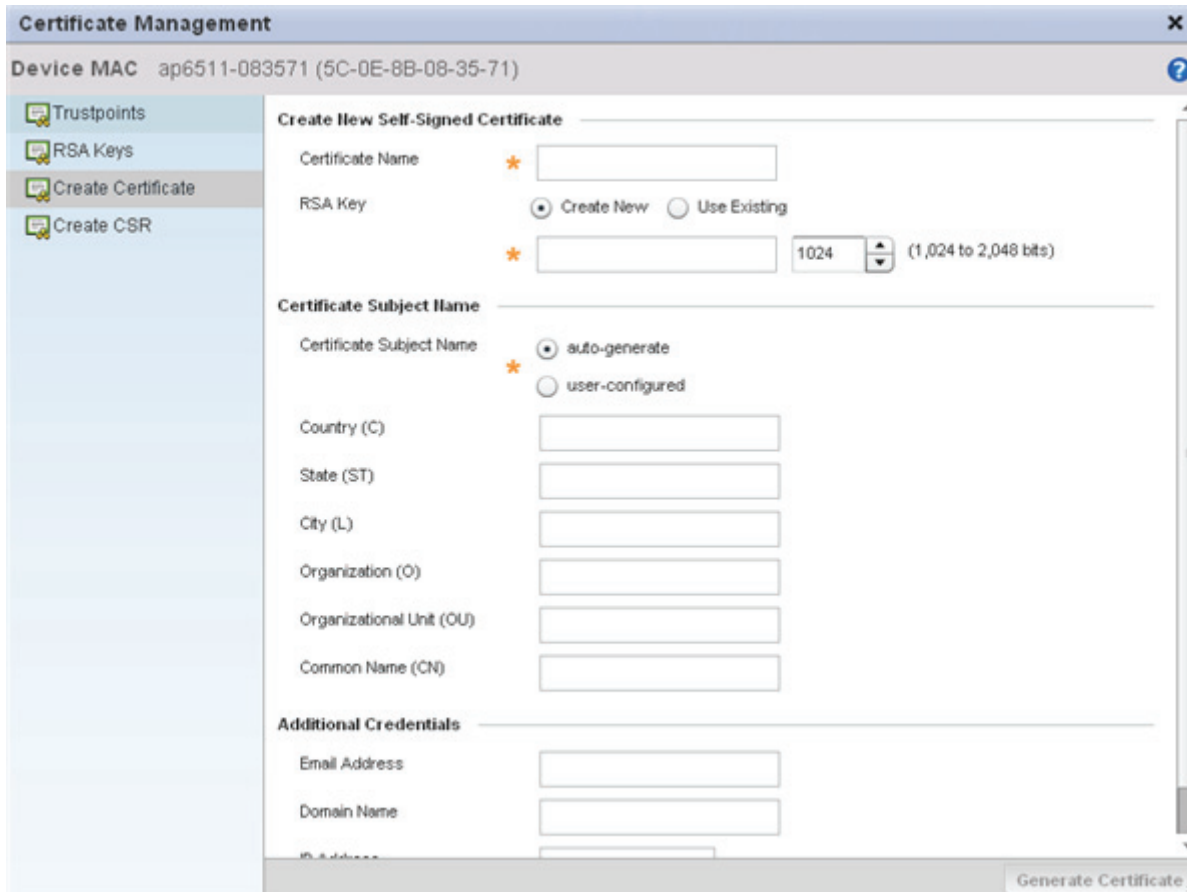


Figure 5-14 Certificate Management - Create CSR screen

3. Define the following configuration parameters required to **Create New Certificate Signing Request (CSR)**:

Use an Existing RSA Key

Select the radio button and 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 a New RSA Key

To create a new RSA key, select the radio button to define a 32 character name used to identify the RSA key. Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting (1024) to ensure optimum functionality. For more information on creating a new RSA key, see [RSA Key Management on page 5-15](#).

4. Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-defined</i> 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 Org. Unit for the name of the organization unit used in the CSR. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an email address used as the contact address for issues relating to this CSR.
Domain Name)	Enter a <i>fully qualified domain name</i> (FQDN) is 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 produce the CSR.

5.3 RF Domain Overrides

Use **RF Domain Overrides** to define configurations overriding the configuration set by the target device's original RF Domain assignment.

An AP-6511 RF Domain allows an administrator to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement from their original RF Domain administered design. Unlike a RFS series controller, an AP-6511 Access Point supports a single RF domain.

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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

4. Select **RF Domain Overrides** from the Device menu to expand it into sub menu options.
5. Select **RF Domain**.

Basic Configuration



Location

Contact



Time Zone

Country Code


SMART RF


SMART RF Policy  

Wireless IPS

WIPS Policy  

Statistics

Window Index	Sample Interval	Window Size	





OK  Reset 

Figure 5-15 RF Domain Overrides screen



NOTE: A blue override icon (to the left of any parameter) defines the parameter as having an override applied. To revert the override back to its original setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting.

- 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	Displays the location set for the device as part of its RF Domain configuration.
Contact	Displays the contact set for the device as part of its RF Domain configuration.
Time Zone	Displays the time zone set for the device as part of its RF Domain configuration.
Country Code	Displays the country code set for the device as part of its RF Domain configuration.

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

When a radio fails or is faulty, a Smart RF policy can be used to provide automatic recovery by instructing neighboring Access Points to increase their transmit power to compensate for the coverage loss.

8. Select the **Create** icon to define a new Smart RF policy that can be applied to the RF Domain or select the **Edit** icon to modify or override an existing Smart RF policy.

For an overview of Smart RF and instructions on how to create a Smart RF policy that can be used with a RF Domain, see [Smart RF Policy on page 6-55](#).

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

The AP-6511 supports *Wireless Intrusion Protection System (WIPS)* to provide continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. The AP-6511 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.

10. Select the **Create** icon to define a new WIPS policy that can be applied to the RF Domain or select the **Edit** icon to modify or override an existing WIPS policy.

For an overview of WIPS and instructions on how to create a WIPS policy that can be used with a RF Domain, see [Intrusion Prevention on page 8-13](#).

11. Refer to the **Statistics** field to set the following data:

Window Index	Use the spinner control to set a numerical index used as an identifier for each RF Domain statistics configuration defined.
Sample Interval	Use the spinner control to define the interval (in seconds) used to capture statistics supporting the listed RF Domain configuration. The default is 5 seconds.
Window Size	Use the spinner control to set the number of samples used to define RF Domain statistics. The default value is 3 samples.

12. Select **OK** to save the changes and overrides made to the RF Domain configuration. Selecting **Reset** reverts the screen to its last saved configuration.

5.4 Profile Overrides

Profiles enable administrators to assign a common set of configuration parameters and policies. 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.

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

To review a profile's original configuration requirements and the options available for a target device, refer to [Profile Configuration on page 7-1](#).



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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.


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

4. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
5. Select **General** if it doesn't display by default.

Controller AP Set as Controller AP

Adoption Policy Adoption Policy  

Network Time Protocol (NTP)

Autokey	Key	Prefer	Server IP	Version	




Figure 5-16 Profile Overrides - General screen



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

19. Set the AP as a **Controller AP**. A Controller AP mediates the configuration and monitoring of a multiple AP-6511 deployment. A Controller AP can adopt other APs and provide a single management and control node for a deployment.
20. Use the **Adoption Policy** drop-down menu to select an AP-6511 specific AP adoption policy. An Adoption Policy screen displays requiring a name be defined before the policy's configuration can be set.
6. 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:

AutoKey	Select the radio button to enable an autokey configuration for the NTP resource. The default setting is disabled.
Key	If an autokey is not being used, manually enter a 64 character maximum key shared for interoperation.
Prefer	Select the radio button to designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources will be given first opportunity to connect to and provide NTP calibration.
Server IP	Set the IP address of each server added as a potential NTP resource.
Version	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.

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

5.4.1 Profile Interface Override Configuration

An AP-6511 requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A virtual interface defines which IP address is associated with each connected VLAN ID.

If the profile is configured to support an Access Point radio, an additional Radios option is available, unique to the Access Point's radio configuration.

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

- [Ethernet Port Override Configuration](#)
- [Virtual Interface Override Configuration](#)
- [Radio Override Configuration](#)

5.4.1.1 Ethernet Port Override Configuration

► Profile Interface Override Configuration

Use an Ethernet Port override to change (modify) parameters of an AP-6511 Ethernet Port configuration.

Displays the physical port name reporting runtime data and statistics. The following ports are available on an AP-6511:

- AP6511 - fe1, fe2, fe3, fe4, up1

To define an AP-6511 profile Ethernet port configuration override:

1. Select the **Configuration** tab from the Web UI.
2. Select **Devices** from the Configuration tab.
3. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

4. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 a parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
fe1	Ethernet		✓ Enabled	Access	1	✗	
fe2	Ethernet		✓ Enabled	Access	1	✗	
fe3	Ethernet		✓ Enabled	Access	1	✗	
fe4	Ethernet		✓ Enabled	Access	1	✗	
up1	Ethernet		✓ Enabled	Access	1	✗	

Row Count: 5

Edit
Exit

Figure 5-17 Profile Overrides - 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 model.
Type	Displays the physical port type. Cooper is used on RJ45 Ethernet ports and Optical materials are used on fiber optic gigabit Ethernet ports.
Description	Displays an administrator defined description for each listed port.
Admin Status	A green checkmark defines the port as active and currently enabled with the profile. A red "X" defines the port as currently disabled and not available for use. The interface status can be modified with the port configuration as required
Mode	Displays the profile's current switching mode as either <i>Access</i> or <i>Trunk</i> (as defined within the Ethernet Port Basic Configuration screen). If <i>Access</i> 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 <i>Trunk</i> , the port allows packets from a list of VLANs added to the trunk. A port configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
Tag Native VLAN	A green checkmark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to <i>Trunk</i> .

8. To edit (or override) the configuration of an existing AP-6511 port, select it from amongst those displayed and select the **Edit** button. The Ethernet port **Basic Configuration** screen displays by default.

Figure 5-18 Ethernet Ports - Basic Configuration screen

9. Set (or override) the following Ethernet port **Properties**:

- | | |
|--|---|
| Description | Provide a brief description for the AP-6511 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 the radio button to allow the Cisco discovery protocol for receiving data on this port. |

- Cisco Discover Protocol Transmit** Select the radio button to allow the Cisco discovery protocol for transmitting data on this port.
- Link Layer Discovery Protocol Receive** Select this option to snoop LLDP on this port. The default setting is enabled.
- Link Layer Discovery Protocol Transmit** Select this option to transmit LLDP PDUs on this port. The default setting is disabled.

10. Define (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 from the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to *Trunk*, the port allows packets from a list of VLANs you add to the trunk. A port configured as *Trunk* supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. *Access* is the default mode.

Native VLAN Use the spinner control to define a numerical **Native VLAN ID** between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.

Tag Native VLAN Select the radio button 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 to. 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. Optionally select the **Port Channel** checkbox and define (or override) a setting between 1 - 8 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.

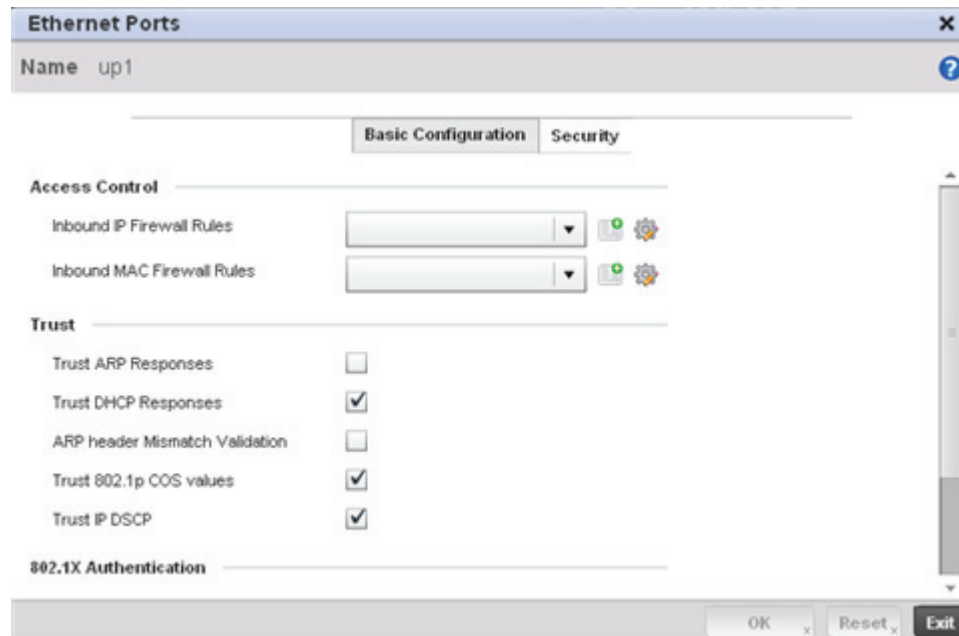


Figure 5-19 Ethernet Ports - Security screen

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

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

15. 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 8-2](#).

16. Refer to the **Trust** field to define the following:

- | | |
|---------------------------------------|--|
| Trust ARP Responses | Select the radio button to enable ARP trust on this port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled. |
| Trust DHCP Responses | Select the radio button 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 the radio button to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled. |
| Trust 802.1p COS values | Select the radio button to enable 802.1p COS values on this port. The default value is enabled. |
| Trust IP DSCP | Select the radio button 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.

17. Select the **Enable** checkbox within the **802.1x Authentication** field to enable a username and password pair to be used when authenticating users on this port.
18. 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.

5.4.1.2 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

- 4. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
- 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 a parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		Enabled	1	zeroconf

Type to search in tables Row Count: 1

Add **Edit** **Delete** **Exit**

Figure 5-20 Profile Overrides - Virtual Interfaces screen

- 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 between 1 - 4094, and cannot be modified as part of a Virtual Interface edit.
Type	Displays the type of Virtual Interface for each listed interface.
Description	Displays the description defined for the Virtual Interface when it was either initially created or edited.
Admin Status	A green checkmark defines the listed Virtual Interface configuration as active and enabled with its supported profile. A red "X" defines the Virtual Interface as currently disabled. The interface status can be modified when a new Virtual Interface is created or an existing one modified.
VLAN	Displays the numerical VLAN ID associated with each listed interface.
IP Address	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.

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.

- 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.

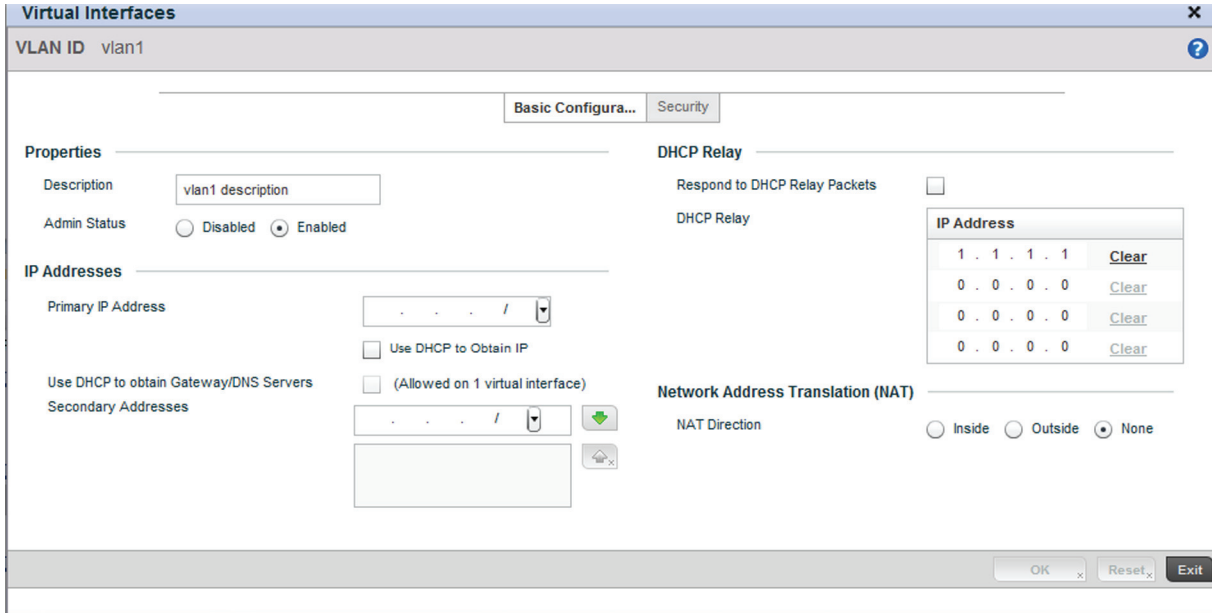


Figure 5-21 Profile Overrides - Virtual Interfaces Basic Configuration screen

The **Basic Configuration** screen displays by default regardless of a whether a new Virtual Interface is being created or an existing one modified.

- If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID between 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 <i>Disabled</i> or <i>Enabled</i> 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. Set or override the following network information from within the **IP Addresses** field:

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.

12. Refer to the **DHCP Relay** field to set or override the DHCP relay server configuration used with the Virtual Interface.

13. Select the **Respond to DHCP Relay Packets** option to allow the DHCP server to respond to relayed DHCP packets on this interface.

14. Provide IP addresses for DHCP server relay resources.

The interface VLAN and gateway should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to an DHCP Server. The interface VLAN and gateway interface cannot be the same.

15. 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 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 to 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 7-39](#) for instructions on creating a profile's NAT configuration.

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

17. Select the **Security** tab.

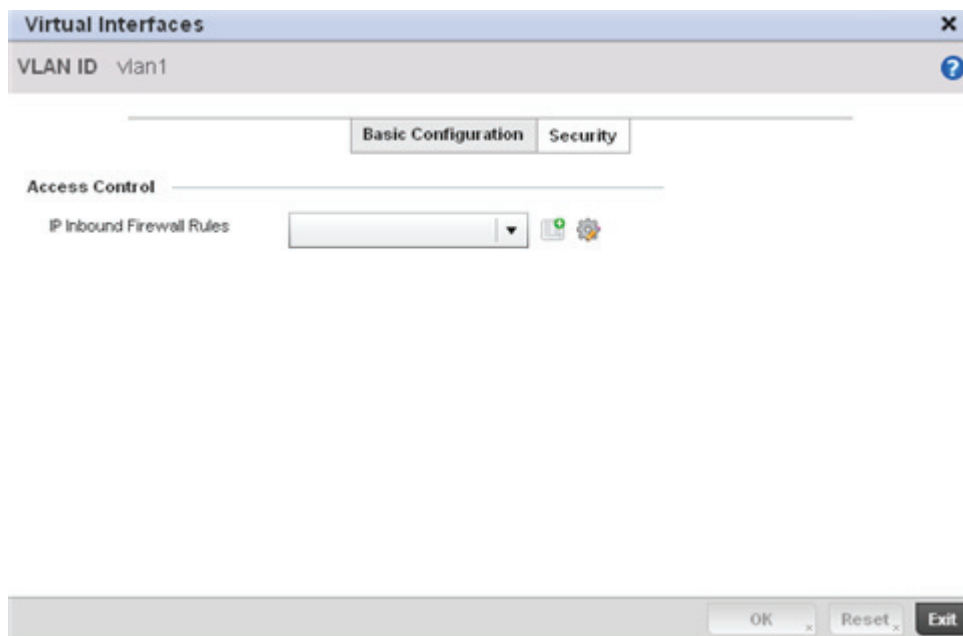


Figure 5-22 Profile Overrides - Virtual Interfaces Security screen

18. Use the **Inbound IP Firewall Rules** drop-down menu to select the firewall rule configuration to apply to this Virtual Interface.

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 8-2](#).

19. 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.

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 or radio2.
Type	Displays the type of radio housed by each listed Access Point.
Description	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
Admin Status	A green checkmark defines the listed 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.
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. 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.

7. If required, select a radio configuration and select the **Edit** button to modify or override portions of its configuration.

Figure 5-24 Profile Overrides - Access Point Radio Settings tab

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

8. Define or override the following radio configuration parameters from within the **Properties** field:

- | | |
|-------------------------|---|
| Description | Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations. |
| Admin Status | Either select the Active or Shutdown radio button to define this radio's current status. When defined as Active, 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 there's no existing suiting the radio's intended operation, select the Create icon to define a new QoS policy that can be applied to this profile. For more information, see Radio QoS Policy on page 6-48 . |
| 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 <i>Access Control List</i> (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 fields in the packet are compared against 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. For more information, see Association ACL on page 6-52 . |

9. Set or override the following profile **Radio Settings** for the selected Access Point radio.

RF Mode	Set the mode to either 2.4 GHz WLAN or 5 GHz WLAN 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 a radio as a detector, disable Sensor support on the other Access Point radio.
Lock Radio Band	Select the radio button to lock Smart RF 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 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.
Transmit Power	Set the transmit power of the selected Access Point radio. If using a dual or three radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value.
Antenna Gain	Set the antenna between 0.00 - 30.00 dBm. The access point's <i>Power Management Antenna Configuration File (PMACF)</i> 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. Motorola Solutions recommends 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, 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.
Dynamic Chain Selection	Select the radio button for the radio to dynamically change the number of transmit chains. This option is enabled by default.

Rate	Once the radio band is provided, the Rate drop-down menu populates with rate options depending on the 2.4 or 5 GHz band selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).
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 between 1- 128.

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 <i>Delivery Traffic Indication Messages</i> (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 Port) 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 (between 1 - 2,347 bytes) for use by the WLAN's adopted Access Point radios. RTS is a transmitting station's signal that requests a *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.
- Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.
- Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.
- A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.
- Short Preamble** If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectralLink 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 the radio button to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

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

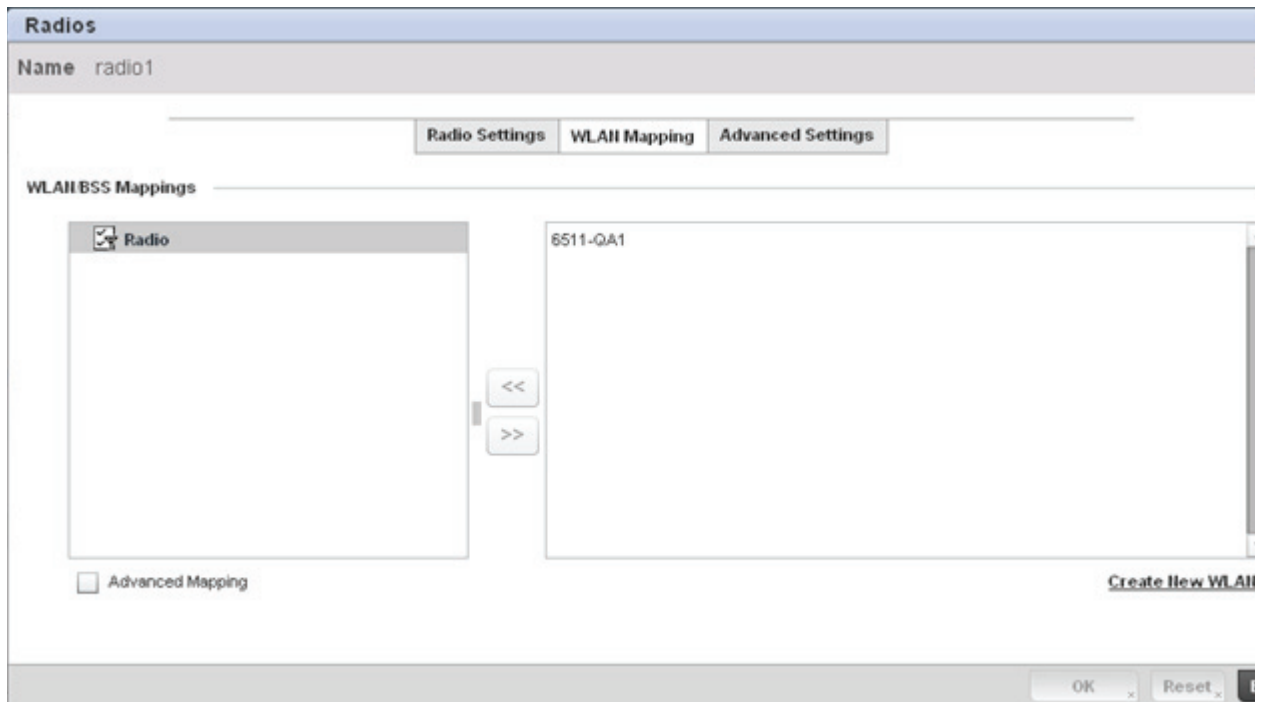


Figure 5-25 Profile Overrides - WLAN Mapping tab

12. Refer to the **WLAN/BSS Mappings** field to set or override 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.

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 **Advanced Settings** tab.

The screenshot shows the 'Advanced Settings' tab for a radio profile named 'radio1'. The configuration is organized into several sections:

- Aggregate MAC Protocol Data Unit (A-MPDU):**
 - A-MPDU Modes: Transmit and Receive (dropdown)
 - Minimum Gap Between Frames: 4 (microseconds) (dropdown)
 - Received Frame Size Limit: 65535 (bytes) (dropdown)
 - Transmit Frame Size Limit: 65535 (0 to 65,535 bytes) (spinner)
- Aggregate MAC Service Data Unit (A-MSDU):**
 - A-MSDU Modes: Receive Only (dropdown)
- Reduced Interframe Spacing (RIFS):**
 - RIFS Mode: Receive Only (dropdown)
- Non-Unicast Traffic:**
 - Non-Unicast Transmit Rate: highest-basic, highest-b (dropdown)
 - Non-Unicast Forwarding: Follow DTIM (dropdown)
- Client Load Balancing:**
 - Client Count Weight: 10 (0 to 10) (spinner)
 - Client Count Trigger Number: 10 (1 to 255) (spinner)
 - Throughput Weight: 0 (0 to 10) (spinner)
 - Throughput Trigger Number: 10 (1 to 1,000) (spinner)
- Sniffer Redirect (Packet Capture):**
 - Host for Redirected Packets: . . . (text box)
 - Channel to Capture Packets: 1 (dropdown)

At the bottom right, there are 'OK' and 'Reset' buttons.

Figure 5-26 Profile Overrides - Access Point Radio Advanced Settings tab

15. 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 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 4 microseconds.

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 between 0 - 65,535 bytes). The default value is 65535 bytes.

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

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.

17. Define a **Reduced Interframe Spacing (RIFS)** mode using the drop-down menu. This value determines whether interframe spacing is applied to Access Point 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.

18. 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.

19. Refer to the **Client Load Balancing** field to define or override how the Access Point radio supports clients based on a maximum count for the radio, a count trigger and throughput.

Client Count Weight	Sets the client load per Access Point radio between 0 - 10. Motorola Solutions recommends considering the client load on an Access Point before defining its radio configuration. The higher the number of clients, the greater the strain on a radio's resources. The default weight is 10 clients. Setting the weight to 0 defines the weight as not considered.
Client Count Trigger Number	The trigger value is the number of client association on the Access Point radio before load balancing is triggered. The configurable range is between 1 - 255. The default trigger client count is 10 clients.
Throughput Weight	Set a throughput weight ratio on the Access Point radio between 0 - 10. The higher the value, the greater the anticipated load on the Access Point radio. The default throughput weight is 0.
Throughput Trigger Number	When the average Access Point radio throughput exceeds the trigger number (as defined between 1 - 1,100), load balancing is initiated for the radio. The default throughput trigger number is 10.

20. 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.

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

5.4.2 Overriding a Profile's Network Configuration

Setting a profile's 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 profile configuration. Applying an override removes the device from the profile configuration that may be shared by

other devices and requires careful administration to ensure this one device still supports the deployment requirements within the network.

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

- [Overriding a Profile's DNS Configuration](#)
- [Overriding a Profile's ARP Configuration](#)
- [Overriding a Profile's Quality of Service \(QoS\) Configuration](#)
- [Overriding a Profile's Static Route Configuration](#)
- [Overriding a Profile's Forwarding Database Configuration](#)
- [Overriding a Profile's Bridge VLAN Configuration](#)
- [Overriding a Profile's Miscellaneous Network Configuration](#)

5.4.2.1 Overriding a Profile's DNS Configuration

► [Overriding a Profile's 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's 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
4. Select **Network** to expand its sub menu options.
5. Select **DNS**.

Domain Name System (DNS)

Domain Name

Enable Domain Lookup

DNS Servers

Name Servers

IP/Hostname		
<input type="text" value="0 . 0 . 0 . 0"/>	IP Address ▼	Clear
<input type="text" value="0 . 0 . 0 . 0"/>	IP Address ▼	Clear
<input type="text" value="0 . 0 . 0 . 0"/>	IP Address ▼	Clear

Figure 5-27 Profile Overrides - Network DNS screen



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

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 DNS configuration data:

Enable Domain Lookup

Select the radio button to enable DNS. When enabled, human friendly domain names can be converted into numerical IP destination addresses. The radio button is selected by default.

Name Servers

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.

8. Select **OK** to save the changes and overrides made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

5.4.2.2 Overriding a Profile's ARP Configuration

► *Overriding a Profile's 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 AP-6511, the AP-6511 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

5.4.2.3 Overriding a Profile's Quality of Service (QoS) Configuration

► *Overriding a Profile's Network Configuration*

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 that is applied to a packet. This QoS 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 an QoS configuration for DSCP mappings:

1. Select **Devices** from the Configuration tab.
2. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Quality of Service (QoS)

DSCP Mapping

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

OK Reset Exit

Figure 5-29 Profile Overrides - Network QoS screen

6. 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*

7. Use the spinner controls within the **802.1p Priority** field for each **DSCP** row to change or override the priority value.
8. Select the **OK** button located to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.4.2.4 Overriding a Profile's Static Route Configuration

► *Overriding a Profile's Network Configuration*

Use the **Static Routes** screen to set or override 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 create or override a profile's static routes:

1. Select **Devices** from the Configuration tab.
2. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
4. Select **Network** to expand its sub menu options.
5. Select **Static Routes**.



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Static Routes

Network Address	Gateway	Default Gateway	

+ Add Row

Use Network Address of 0.0.0.0/0 to set Default Gateway

OK

Figure 5-30 Static Routes screen

6. Select **Add Row +** as needed to include single rows in the static routes table.
7. Add IP addresses and network masks in the **Network** column.
8. Set or override the **Gateway** used to route traffic.

A green checkmark in the Default Gateway column defines a default gateway being applied. A red "X" means a gateway assignment has been made.

A default gateway is desirable when an IP address does not match any other routes in the routing table. A gateway routes traffic from a managed device to another network segment. The default gateway connects the network to the outside network (Internet). The gateway is associated with a router, which uses headers and forwarding tables to determine where packets are sent, providing the path for the packet in and out of the gateway. Setting a default gateway for a device profile can help segregate network traffic, on behalf of a profile, to a single default gateway.

9. Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.4.2.5 Overriding a Profile's Forwarding Database Configuration

► *Overriding a Profile's 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's determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

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 profile's forwarding database configuration:

1. Select **Devices** from the Configuration tab.
2. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

5.4.2.6 Overriding a Profile's Bridge VLAN Configuration

► *Overriding a Profile's 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

- Trust ARP Response** When ARP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks.
- Trust DHCP Responses** When DHCP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.
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.

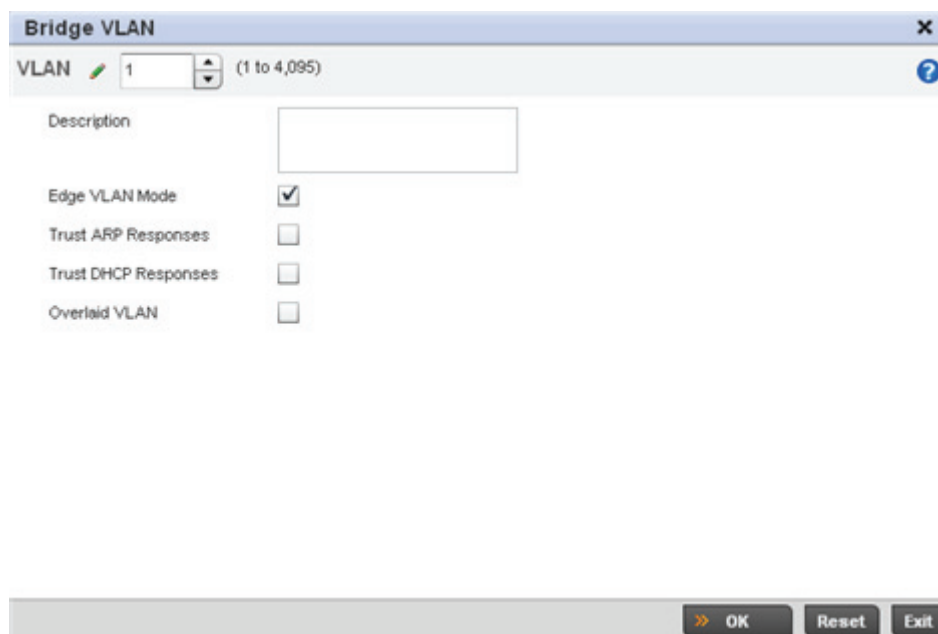


Figure 5-33 Profile Overrides - Network Bridge VLAN screen, General tab

8. The **General** tab displays by default.
9. If adding a new Bridge VLAN configuration, use the spinner control to define or override a **VLAN ID** between 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined. VLAN IDs 0 and 4095 are reserved and unavailable.
10. Set or override the following General Bridge VLAN parameters:

- Description** If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
- Edge VLAN Mode** Select the radio button to enable edge VLAN mode. When selected, the IP address in the VLAN is not used for normal operations, as its now designated to isolate devices and prevent connectivity. This feature is enabled by default.
- Trust ARP Response** Select the radio button 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 the radio button 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.

Overlaid VLAN Select this checkbox to separate this VLAN from the wired VLAN used by the AP-6511. This feature is disabled by default.

11. Select the **OK** button to save the changes and overrides to the General tab. Select **Reset** to revert to the last saved configuration.

5.4.2.7 Overriding a Profile's Miscellaneous Network Configuration

► *Overriding a Profile's 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 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

DHCP Settings

Include Hostname in DHCP Request

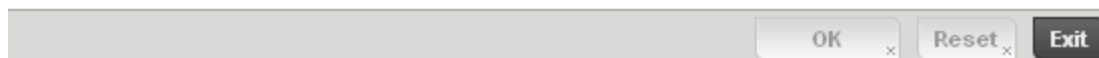


Figure 5-34 Profile Overrides - Network Miscellaneous screen

6. Select the **Include Hostname in DHCP Request** checkbox to include a hostname in a DHCP lease for a requesting device. This feature is disabled by default.

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

5.4.3 Overriding a Profile's Security Configuration

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can be navigated from the **Configuration > Profiles** section of the UI to the **Configuration > Security** portion of the UI to create the required security policy configuration. Once created, a policy's 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 device models within the network.

For more information on applying an override to an existing device profile, refer to the following sections:

- [Overriding a Profile's General Security Settings](#)
- [Overriding a Profile's Certificate Revocation List \(CRL\) Configuration](#)
- [Overriding a Profile's NAT Configuration](#)

5.4.3.1 Overriding a Profile's General Security Settings

► *Overriding a Profile's 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 that profile. However, as deployment requirements arise, an individual device 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
4. Select **Security** to expand its sub menu options.
5. Select **General**.



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

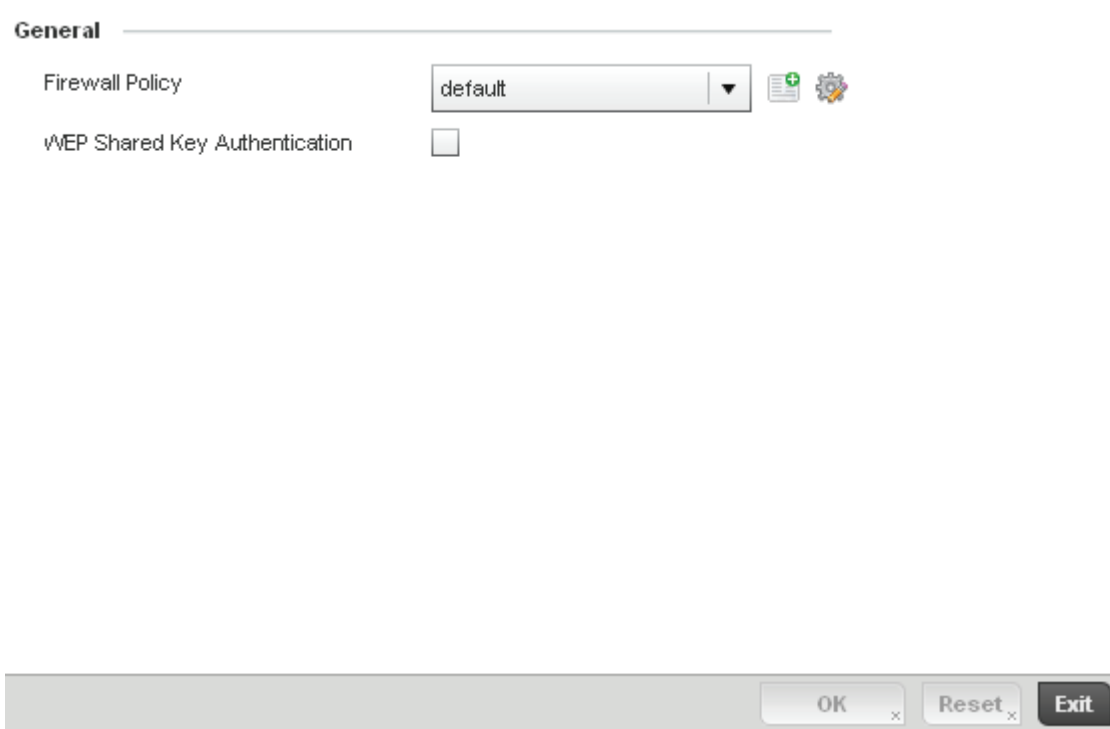


Figure 5-35 Profile Overrides - General Security screen

6. Refer to the **General** field to assign or override the following:

Firewall Policy

Use the drop-down menu to select an existing Firewall Policy to use as an additional security mechanism with this profile. All devices using this profile and Access Point 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 overridden as needed using the **Edit** icon. For more information, see *Wireless Firewall on page 8-2* and *Configuring a Firewall Policy on page 8-2*.

WEP Shared Key Authentication

Select the radio button to require devices using this profile to use a WEP key to access the network using this profile. Clients without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

7. Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

5.4.3.2 Overriding a Profile's Certificate Revocation List (CRL) Configuration

► *Overriding a Profile's 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 Certificate Revocation configuration or override:

1. Select **Devices** from the Configuration tab.
2. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.


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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Certificate Revocation List (CRL) Update Interval

Trustpoint Name	URL	Hours	

 + Add Row

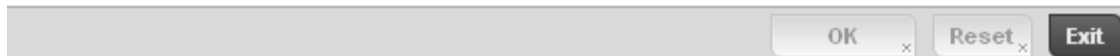


Figure 5-36 Profile Overrides - Certificate Revocation screen

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.

- a. Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.
 - b. Enter the resource ensuring the trustpoint's legitimacy within the URL field.
 - c. Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.
7. Select **OK** to save the changes and overrides made within the Certificate Revocation screen. Select **Reset** to revert to the last saved configuration.

5.4.3.3 Overriding a Profile's NAT Configuration

► *Overriding a Profile's 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 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 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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
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 revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

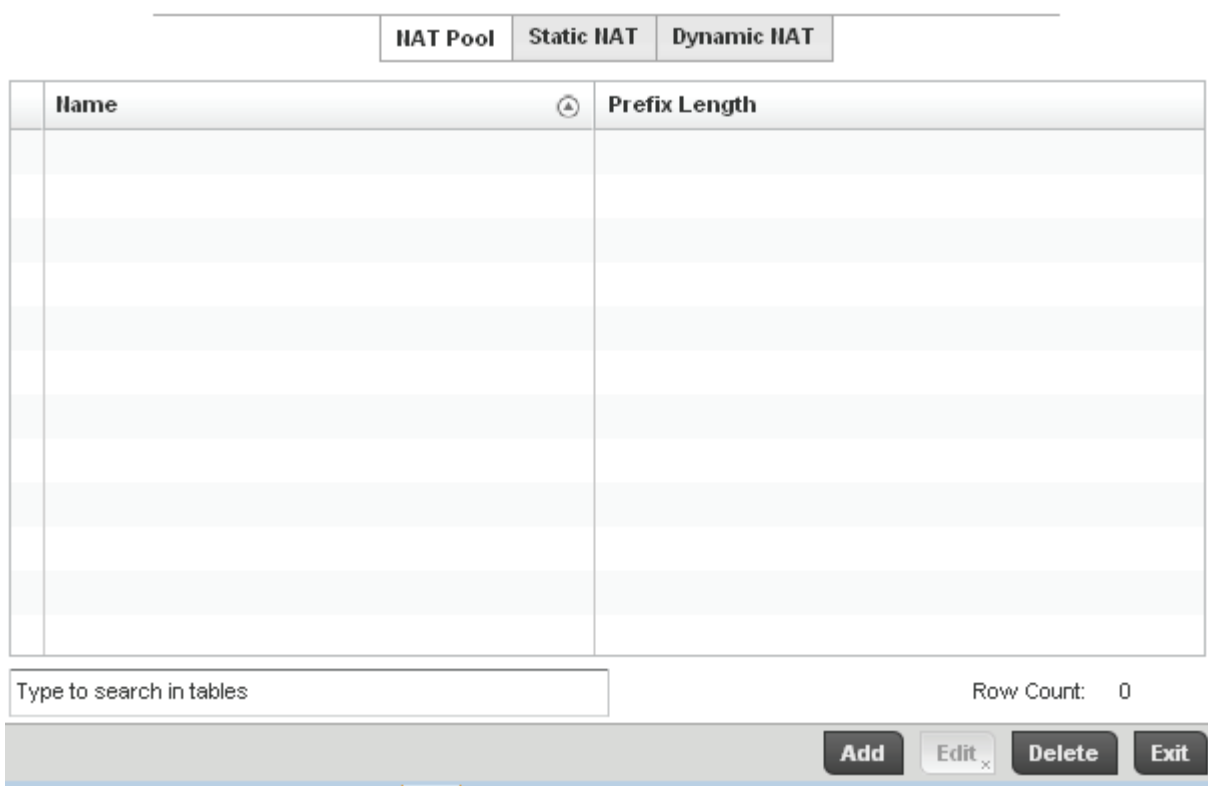


Figure 5-37 Profile Overrides - NAT Pool screen

The **NAT Pool** displays by default. The NAT Pool screen lists those NAT policies created thus far. Any of these policies can be selected and applied to a profile.

6. 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.

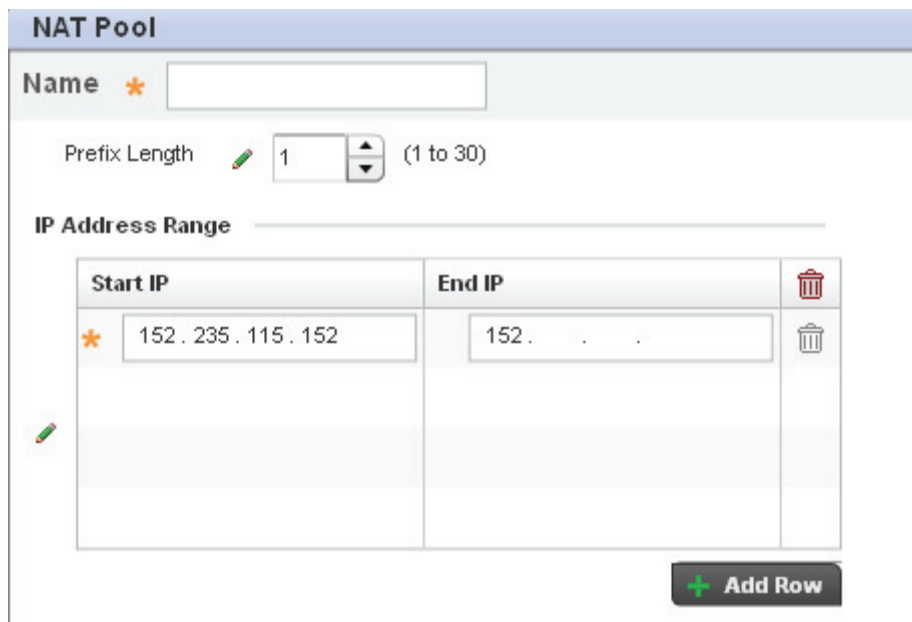


Figure 5-38 NAT Pool screen

- 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.
- Prefix Length** Use the spinner control to set the netmask (between 1 - 30) of the network the pool address belongs to.
- 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.

Select the **+ Add Row** button as needed to append additional rows to the IP Address Range table.

- 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.
- Select the **Static NAT** tab.
The Source tab displays by default.

NAT Pool
Static NAT
Dynamic NAT

Source
Destination

Source

Source IP	NAT IP	Network	
			🗑

+ Add Row

OK x
Reset x
E

Figure 5-39 Profile Overrides - Static NAT screen

To map a source IP address from an internal network to a NAT IP address click the **+ Add Row** button. Enter the internal network IP address in **Source IP** field. Enter the NAT IP address in the **NAT IP** field.

Use the **Network** drop-down menu to set the NAT type either *Inside* or *Outside*. 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.

10. 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.

NAT Pool Static NAT Dynamic NAT					
Source Destination					
Protocol	Destination IP	Destination Port	NAT IP	NAT Port	Network

Type to search in tables Row Count: 0

Add **Edit** x **Delete** **Exit**

Figure 5-40 NAT Destination screen

21. Select **Add** to create a new NAT destination configuration, **Edit** to modify or override the attributes of an existing configuration or **Delete** to permanently remove a NAT destination.

The screenshot shows a configuration window titled "Destination" with a sub-header "Add Destination NAT". Under the "Settings" section, the following parameters are visible:

- Protocol:** A dropdown menu set to "UDP".
- Destination IP:** A text input field containing "152.235.115.252".
- Destination Port:** A spinner control set to "179" and a dropdown menu set to "bgp". A range "(1 to 65,535)" is shown to the right.
- NAT IP:** A text input field containing "152.125.252.52".
- NAT Port:** A checked checkbox, a spinner control set to "1", and a dropdown menu set to "other". A range "(1 to 65,535)" is shown to the right.
- Network:** A dropdown menu with a star icon next to it.

At the bottom of the window are three buttons: "OK", "Reset", and "Exit".

Figure 5-41 NAT Destination Add screen

11. Set or override the following **Destination** configuration parameters:

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

Protocol

Select the protocol for use with static translation. TCP, UDP and Any are available options. TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The *User Datagram Protocol* (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is Any.

Destination IP

Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) 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. Inside is the default setting.

- 12. Select **OK** to save the changes or overrides made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.
- 13. 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.

NAT Pool
Static NAT
Dynamic NAT

Source List ACL	Network	Interface	Overload Type	NAT Pool	Overload IP ▲

Type to search in tables

Row Count: 0

Add
Edit ✕
Delete
Exit

Figure 5-42 Profile Overrides - Dynamic NAT screen

14. Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

- | | |
|------------------------|---|
| Source List ACL | Lists an ACL name to define the packet selection criteria for the NAT configuration. NAT is applied only on packets which match a rule defined in the access-list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination. |
| Network | Displays <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration. |
| Interface | Lists the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. |
| Overload Type | Select the radio button to define the Overload Type used with the listed IP ACL rule. Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . 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 <i>One Global IP Address</i> is selected as the Overload Type, define an IP address used as a filter address for the IP ACL rule. |

Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify or override an existing configuration or **Delete** to permanently remove a configuration.

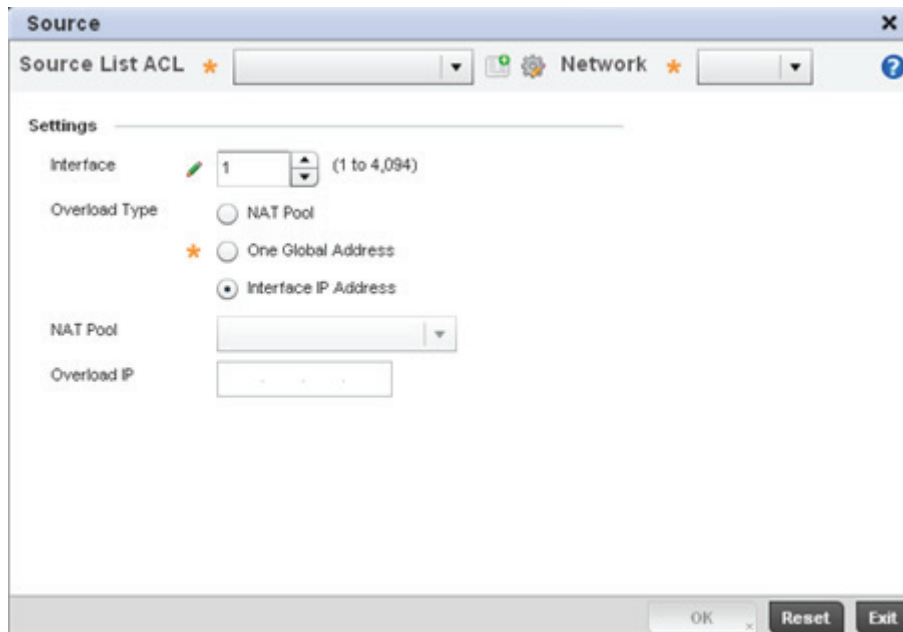


Figure 5-43 Dynamic NAT Add screen

15. 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 <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.
Interface	Use the drop-down menu to select the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected adequately supports the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
Overload Type	Select the radio button of Overload Type used with the listed IP ACL rule. Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . 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 <i>One Global IP Address</i> is selected as the Overload Type, define an IP address used as a filter address for the IP ACL rule.

16. Select **OK** to save the changes or overrides made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

5.4.4 Overriding a Profile's Services Configuration

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 a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
4. Select **Services**.



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

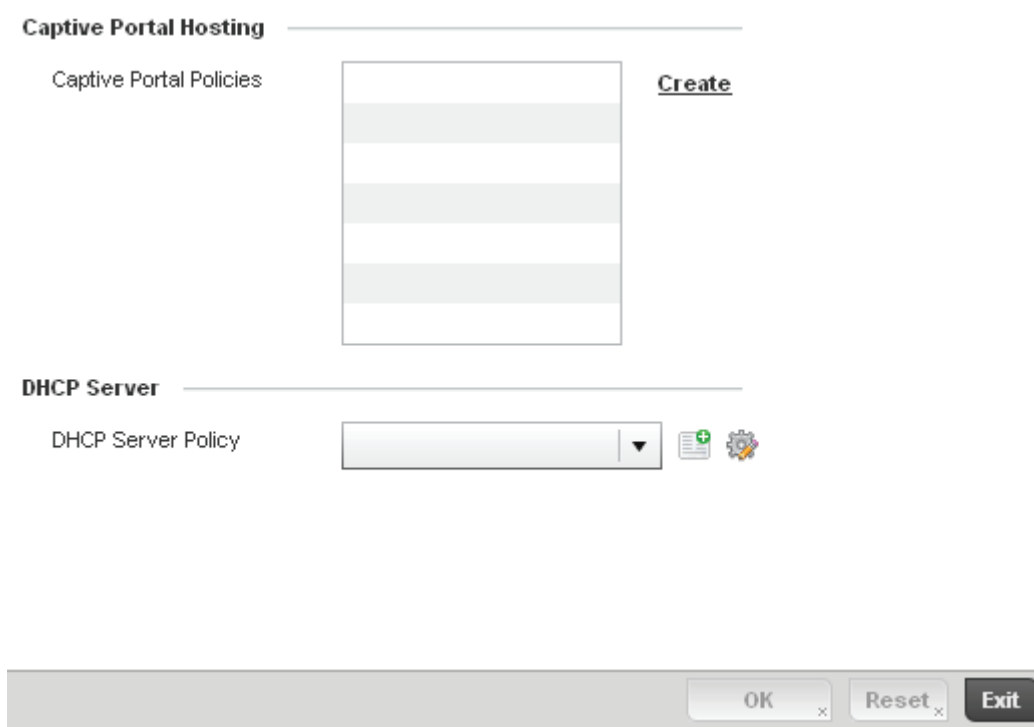


Figure 5-44 Profile Overrides - Services screen

5. Refer to the **Captive Portal** 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 guests temporary and restrictive access to the network. The primary means of securing such guest access is a hotspot.

A captive portal policy's hotspot configuration provides secure authenticated access using a standard Web browser. Hotspots 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 hotspot, additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on the hotspot'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 a Captive Portal Policy on page 9-2](#).

6. Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP server policy. If an existing DHCP policy does not meet the profile's requirements, select the **Create** icon to create a new policy configuration that can be applied to this profile or the **Edit** icon to modify the parameters of an existing DHCP Server policy.

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

Either select an existing captive portal policy or select the **Create** button to create a new captive portal configuration that can be applied to this profile. For more information, see *Configuring a Captive Portal Policy on page 9-2*

7. Select **OK** to save the changes or overrides made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

5.4.5 Overriding a Profile's Management Configuration

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 device's configuration must be modified from its original device profile configuration.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support.

To define or override a profile's management configuration:

1. Select **Devices** from the Configuration tab.
2. Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

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

3. Select **Profile Overrides** from the Device menu to expand it into sub menu options.
4. Select **Management**.



NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To revert the override back to its original profile setting, select the override icon to display an **Action** pop-up. Select the **Remove Override** checkbox to revert the override to its original setting for this profile.

Management Policy

Management Policy: default [Create] [Edit]

Message Logging

Enable Message Logging:

Remote Logging Host:

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Facility to Send Log Messages: local7

Syslog Logging Level: Warning

Console Logging Level: Warning

Buffered Logging Level: Warning

Time to Aggregate Repeated Messages: 0 Seconds (0 to 60)

Forward Logs to Controller: Error

System Event Messages

Enable System Events:

Enable System Event Forwarding:

OK [x] Reset [x] Exit

Figure 5-45 Profile Overrides - Management Settings screen

5. Refer to the **Management Policy** field to set or override a management configuration for use with this profile. A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If no management policies exist meeting the data access requirements of this profile, select the **Create** icon to access a series of screens used to define administration, access control and SNMP configurations. Select an existing policy and select the **Edit** icon to modify the configuration of an existing management policy. For more information, see [Management Access Policy Configuration on page 10-1](#).

6. Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to discern an overall pattern that may be negatively impacting performance using the profile.

Enable Message Logging

Select the radio button 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** as needed to remove an IP address.

Facility to Send Log Messages

Use the drop-down menu to specify the local server facility (if used) for the profile event log transfer.

Syslog Logging Level

Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - *Emergency*, 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.

Console Logging Level

Event severity coincides with the 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 the checkbox to define a log level for forwarding event logs to the control. Log levels include *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Info* and *Debug*. The default logging level is *Error*.

7. Refer to the **System Event Messages** field to define or override how AP-6511 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's important to log individual events to discern an overall pattern that may be negatively impacting performance. This settings 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.

8. Select **OK** to save the changes and overrides made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.
9. Select **Firmware** from the Management menu.

Figure 5-46 Profile Overrides - Management Firmware screen

10. Select the **Enable Configuration Update** radio button (from within the **Automatic Configuration Update** field) to enable automatic configuration file updates for the profile from a location external to the device.

If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update.

11. Refer to the **Automatic Firmware Upgrade** field to define or override the configuration used by the profile to update device firmware.

Enable Firmware Upgrade Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. This value is disabled by default.

12. Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware upgrade from a local file.

Enable Controller Upgrade of AP Firmware Select this radio button to enable adopted Access Point radios to upgrade to a newer firmware version using a resident firmware file for that AP model. This parameter is disabled by default.

Number of Concurrent Upgrades. Use the spinner control to define the maximum number (1 - 20) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind that during a firmware upgrade, the AP is offline and unable to perform its normal wireless client support function until the upgrade process is complete.

13. 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.

14. Select **Heartbeat** from the Management menu.

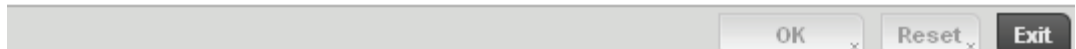


Figure 5-47 Profile Overrides - Management Heartbeat screen

15. 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.
16. Select **OK** to save the changes and overrides made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

5.4.6 Overriding a Profile's Miscellaneous Configuration

Refer to the advanced profile's **Miscellaneous** menu item to set or override a profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection. Access Point LED behavior and RF Domain management can also be defined from within the Miscellaneous screen.

1. Select the **Miscellaneous** menu item.

Device RADIUS Authentication Parameters _____

NAS-Identifier Attribute

NAS-Port-Id Attribute

LEDs (Light Emitting Diodes) _____

Turn on LEDs



Figure 5-48 Profile Overrides - Miscellaneous screen

2. 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.
3. Set a **NAS-Port-Id Attribute** up to 253 characters in length.
This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates.
4. Refer to the **Turn off LEDs** option to disable an adopted Access Point's LEDs. This feature is enabled by default.
5. Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

Wireless Configuration

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one 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 be used to provide an abundance of services, including data communications (allowing mobile devices to access applications), email, 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 only provide service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

The wireless configuration is comprised the following policies:

- *Wireless LAN Policy*
- *Configuring WLAN QoS Policies*
- *Radio QoS Policy*
- *AAA Policy*
- *Association ACL*
- *Smart RF Policy*

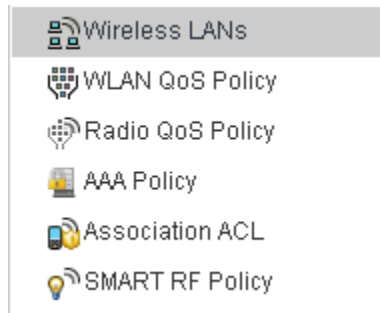


Figure 6-1 Configuration > Wireless field

6.1 Wireless LAN Policy

To review the attributes of existing WLANs and, if necessary, modify their configurations:

1. Select **Configuration > Wireless > Wireless LANs** to display a high-level display of existing WLANs.

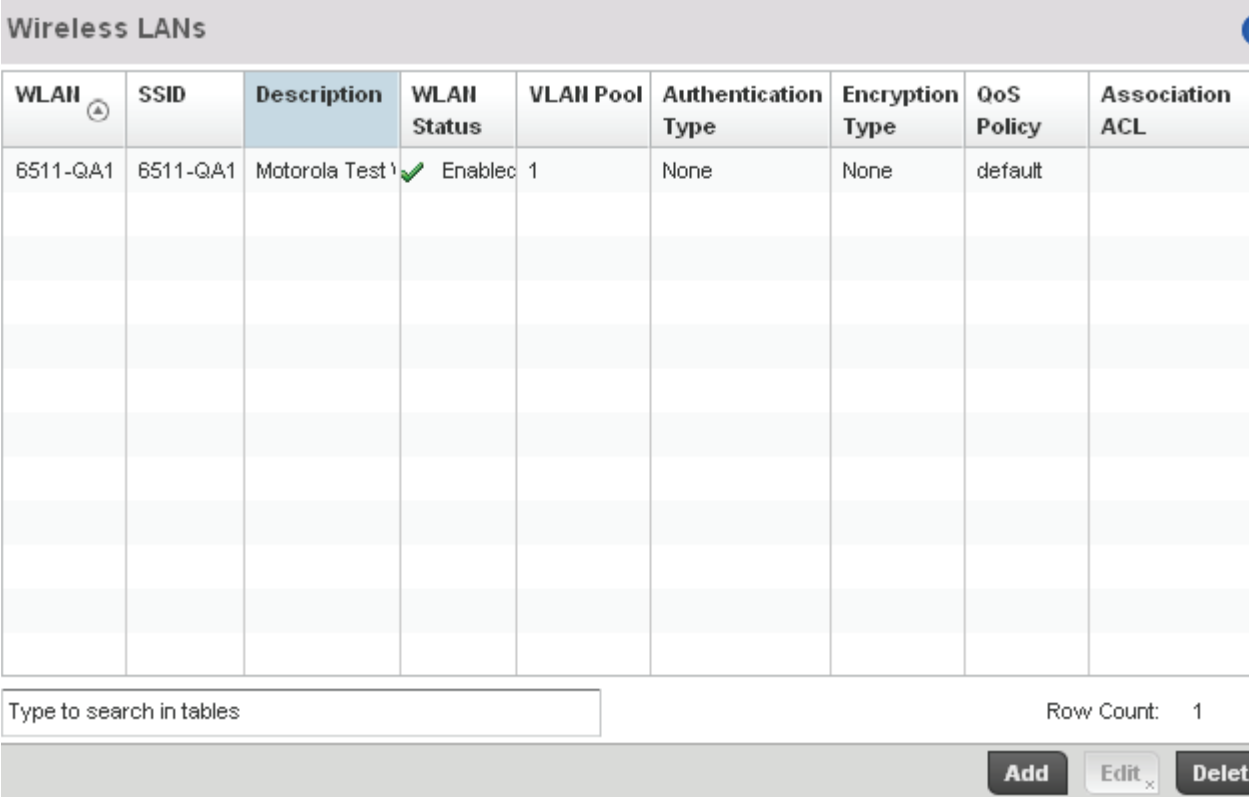


Figure 6-2 Wireless LANs screen

2. Refer to the following (read only) information to assess the attributes of each available WLAN:

- WLAN** Displays the name of each WLAN. Each WLAN can be selected and its SSID and client management properties modified.
- SSID** Displays the name of the SSID assigned to the WLAN when it was created or last modified. Optionally, select a WLAN and click the **Edit** button to update the SSID.
- Description** Displays the brief description defined for each listed WLAN when it was either created or modified.
- WLAN Status** Lists each WLANs current status as either **Active** or **Shutdown**. A green checkmark 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's not available for clients to associate and use.

VLAN Pool	Lists each WLANs 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. Keep in mind however, typical deployments only map a single VLAN to a WLAN. The use of a pool is strictly optional.
Authentication Type	Displays the name of the authentication scheme this WLAN is using to secure its client membership transmissions. None is listed if authentication is not used within this WLAN. Refer to the Encryption type column if no authentication is used to verify there is some sort of data protection used with the WLAN or risk using this WLAN with no protection at all.
Encryption Type	Displays the name of the encryption scheme this WLAN is using to secure its client membership transmissions. None is listed if encryption is not used within this WLAN. Refer to the Authentication type column if no encryption is used to verify 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 <i>Access Control List</i> (ACL) that either prevents or allows wireless clients from connecting to a WLAN. The mapping of an Association ACL is strictly optional.

Use the sequential set of WLAN screens to define a unique configuration for each WLAN. Refer to the following to set WLAN configurations:

- [Basic WLAN Configuration](#)
- [Configuring WLAN Security](#)
- [Configuring WLAN Firewall Support](#)
- [Configuring Client Settings](#)
- [Configuring WLAN Accounting Settings](#)
- [Configuring Advanced WLAN Settings](#)

6.1.1 Basic WLAN Configuration

▶ [Wireless LAN Policy](#)

When creating or modifying a WLAN, the first screen that displays as part of the WLAN configuration screen flow is the Basic Configuration screen. Use this screen to enable a WLAN and define its SSID, client behavior and VLAN assignments.



1. Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.
2. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.

WLAN Configuration

SSID *

Description

WLAN Status Disabled Enabled

QoS Policy *  

Other Settings

Broadcast SSID

Answer Broadcast Probes

WLAN Assignment

Single VLAN

VLAN

RADIUS VLAN Assignment

Allow RADIUS Override

OK x Reset x Exit

Figure 6-3 WLAN Policy Basic Configuration screen

3. Refer to the **WLAN Configuration** field to define the following:

WLAN Policy

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 that can be used for the SSID is 32.

Description

Provide a textual description for the WLAN to help differentiate it from others with similar configurations. A description can be up to 64 characters in length.

WLAN Status

Select the **Enabled** radio button to make this WLAN active and available to clients on all radios where it has been mapped. Select the **Disabled** radio button to make this WLAN inactive, meaning even if the WLAN is mapped to radios, it's not available for clients to associate and use.

QoS Policy

Use the drop-down menu to assign an existing QoS policy to the WLAN or select the **Create** icon to define a new QoS policy or select the **Edit** icon to modify the configuration of the selected QoS Policy. QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or per the proportion configured. For information on creating a QoS policy that can be applied to WLAN, see [Configuring WLAN QoS Policies on page 6-34](#).

4. 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 will display 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.

5. Refer to the **VLAN Assignment** field to add or remove VLANs for the selected WLAN, and define the number of clients permitted. Remember, users belonging to separate VLANs can share the same WLAN. It's not necessary to create a new WLAN for every VLAN in the network.

Single VLAN

Select the **Single VLAN** radio button to assign just one VLAN to this WLAN. Enter the name of the VLAN within the VLAN parameter field 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.

6. Select the **Allow Radius Override** radio button to allow an Access Point to override the WLAN configuration based VLAN assigned to a wireless client and use the VLAN assigned by a RADIUS Server. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN configuration (defined above) is used.
7. Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen back to the last saved configuration.

6.1.1.0.1 WLAN Basic Configuration Deployment Considerations

▶ [Basic WLAN Configuration](#)

Before defining a WLAN's basic configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola Solutions recommends one VLAN be deployed for secure WLANs, while separate VLANs be defined for each WLAN providing guest access.

6.1.2 Configuring WLAN Security

▶ [Wireless LAN Policy](#)

A WLAN can be assigned a security policy supporting authentication, captive portal (hotspot) or encryption schemes.

Select Authentication

Authentication Type EAP EAP-PSK EAP-MAC MAC PSK / None

Kerberos Configuration [Settings](#)

AAA Policy

Reauthentication 30 (30 to 86,400)

Captive Portal

Enforcement Captive Portal Enable Captive Portal if Primary Authentication Fails

Captive Portal Policy

Select Encryption

WPA/WPA2-TKIP WEP 128 WEP 64 Open

WPA2-CCMP

No Encryption

OK Reset Exit

Figure 6-4 WLAN Policy Security screen

Authentication ensures only known and trusted users or devices access a WLAN. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.

A client must authenticate to an Access Point to receive resources from the network. *802.1x EAP*, *802.1x EAP PSK*, *MAC* and *PSK/None* authentication options are supported.

Refer to the following to configure an authentication scheme for a WLAN:

- [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 guests temporary and restrictive access to the wireless network. The primary means of securing such guest access is the use of a hotspot. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

A captive portal policy's hotspot configuration provides secure authenticated access using a standard Web browser. Hotspots 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 hotspot, additional Agreement, Welcome and Fail pages provide the administrator with a number of options on the hotspot's screen flow and user appearance.

Refer to [Captive Portal on page 6-11](#) for information on assigning a captive portal policy to a WLAN. A captive portal is a guest access configuration policy that can be applied to a WLAN to provide strategic access to the WLAN.

Encryption is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, *Wired Equivalent Privacy* (WEP) was the primary encryption mechanism. WEP has since been interpreted as flawed in many ways, and is not considered an effective standalone encryption scheme for securing a WLAN. WEP is typically used in WLAN deployments designed to support legacy clients. New device deployments should use either WPA or WPA2 encryption.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized hacking. Decryption applies the algorithm in reverse, to restore the data to its original form. A sender and receiver must employ the same encryption/decryption method to interoperate. When both TKIP and CCMP are both enabled a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

Refer to the following to configure an encryption scheme for a WLAN:

- [WPA/WPA2-TKIP](#)
- [WPA2-CCMP](#)
- [WEP 64](#)
- [WEP 128](#)

6.1.2.1 802.1x EAP, EAP PSK and EAP MAC

▶ [Configuring WLAN Security](#)

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 device 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 AP-6511. 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 AP-6511 and authenticating device must use the same authenticating algorithm and passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP. The only encryption types supported with this are TKIP, CCMP and TKIP-CCMP. EAP-MAC is useful when in a hotspot environment, as some clients support EAP and an administrator may want to authenticate based on just the MAC address of the device. The only encryption type supported with this is None.

To configure EAP on a WLAN:

1. Select **Configuration > Wireless > Wireless LAN Policy** to display a high-level display of the existing WLANs.
2. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the security properties of an existing WLAN.
3. Select **Security**.
4. Select **EAP, EAP PSK or EAP MAC** as the Authentication Type.

Either option enables the radio buttons for various encryption options as an additional measure of security with the WLAN that can be used with EAP.

5. 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 the selected AAA policy.

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 6-50](#).

6. Select the **Reauthentication** radio button to force EAP supported clients to reauthenticate. Use the spinner control to set the number of seconds (between 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate to use the resources supported by the WLAN.
7. Select **OK** when completed to update the WLAN's EAP configuration. Select **Reset** to revert the screen 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:

- Motorola Solutions recommends 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, Motorola Solutions recommends the round trip delay over the WAN does not exceed 150ms. Excessive delay over a WAN can cause authentication and roaming issues and impact wireless client performance.

6.1.2.2 MAC Authentication

▶ [Configuring WLAN Security](#)

MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.

MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions.

MAC authentication can only identify devices, not users. MAC authentication only references a client wireless interface card MAC address when authenticating the device, it does not distinguish the device's

user credentials. MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provide a device MAC address to mimic a trusted device within the wireless controller managed network.

MAC authentication is enabled per WLAN profile, augmented with the use of a RADIUS server to authenticate each device. A device's MAC address can be authenticated against the local RADIUS server built into the device or centrally (from a datacenter). For RADIUS server compatibility, the format of the MAC address can be forwarded to the RADIUS server in non-delimited and or delimited formats:

To configure MAC on a WLAN:

1. Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display a high-level display of the existing WLANs available.
2. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the security properties of an existing WLAN.
3. Select **Security**.
4. Select **MAC** as the Authentication Type.

Selecting MAC enables the radio buttons for each encryption option as an additional measure of security for the WLAN.

5. 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 6-50](#).

6. Select the **Reauthentication** radio button to force MAC supported clients to reauthenticate. Use the spinner control set the number of minutes (between 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate to use the resources supported by the WLAN.
7. 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.

6.1.2.3 PSK / None

► [Configuring WLAN Security](#)

Open-system authentication can be referred to as no authentication, since no actual authentication takes place. 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).

6.1.2.4 Captive Portal

► [Configuring WLAN Security](#)

A *captive portal* is guest access policy for providing guests temporary and restrictive access to the wireless network. The primary means of securing such guest access is the use of a hotspot. 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 9-2](#).

To assign a captive portal policy to a WLAN:

1. Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless network.
2. Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Security**.
4. Refer to the **Captive Portal** field within the WLAN Policy security screen
Select the **Captive Portal Enable** option if authenticated guess access is required with the selected WLAN. This feature is disabled by default.
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 9-2](#).
5. 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.

6.1.2.5 WPA/WPA2-TKIP

► [Configuring WLAN Security](#)

Wi-Fi Protected Access (WPA) is an encryption scheme specified in the IEEE *Wireless Fidelity* (Wi-Fi) standard, 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

The encryption method is *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.

Wi-Fi Protected Access 2 (WPA2) is an enhanced version of WPA. WPA2 uses the Advanced Encryption Standard (AES) instead of TKIP. AES supports 128-bit, 192-bit and 256-bit keys. WPA/WPA2 also provide strong user authentication based on 802.1x EAP.

To configure WPA/WPA2 encryption on a WLAN:

1. Select **Configuration > Wireless > Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless network.
2. Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify the properties of an existing WLAN.
3. Select **Security**.
4. Select the **WPA/WPA2-TKIP** radio button from within the Select Encryption field.

The screen populates with the parameters required to define a WLAN WPA/WPA2-TKIP configuration for the new or existing WLAN.

Select Encryption

WPA/WPA2-TKIP WEP 128 WEP 64 Open

WPA2-CCMP

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key ASCII ▾

Key Rotation

Unicast Rotation Interval 30 (30 to 86,400 seconds)

Broadcast Rotation Interval 30 (30 to 86,400 seconds)

Fast Roaming

Pre-Authentication

Advanced

TKIP Countermeasure Hold Time Minutes ▾ (0 to 1,093)

Exclude WPA2 TKIP

>> OK Reset Exit

Figure 6-5 WPA/WPA2-TKIP screen

5. Define **Key Settings**.

Pre-Shared Key

Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The wireless controller converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

6. Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an access point, and one broadcast key, the common key for all the clients in that subnet.

Motorola recommends rotating these keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

Unicast Rotation Interval

Define an interval for unicast key transmission in seconds (30 -86,400). 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 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 feature is disabled by default.

7. Define the **Fast Roaming** configuration used with the WPA/WPA2-TKIP policy.

Using 802.11i can speed up the roaming process from one AP to another. Instead of doing a complete 802.1x authentication each time a client roams between APs, 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 APs, Opportunistic Key Caching allows multiple APs to share PMKs amongst themselves. This allows a client to roam to an AP it has not previously visited and reuse a PMK from another AP to skip 802.1x authentication.

Pre-Authentication

Selecting the Pre-Authentication option enables an associated client to carry out an 802.1x authentication with another wireless controller (or device) before it roams to it. This enables the 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 providing faster re-association. This feature is enabled by default.

8. Set the following **Advanced** settings for the WPA/WPA2-TKIP encryption scheme

TKIP Countermeasure Hold Time The TKIP countermeasure hold-time is the time during which the use of the 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 60 seconds.

Exclude WPA2-TKIP Select this option for an Access Point to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with the newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Motorola recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.

9. Select **OK** when completed to update the WLAN's WPA/WPA2-TKIP encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.
-
-



NOTE: WPA-TKIP is not supported on radios configured to exclusively use 802.11n.

WPA-TKIP Deployment Considerations

Before defining a WPA-TKIP supported configuration on a wireless controller WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Though TKIP offers better security than WEP, it can be vulnerable to certain attacks.
- 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.

6.1.2.6 WPA2-CCMP

► *Configuring WLAN Security*

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 keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any for associated clients.

To configure WPA2-CCMP encryption on a WLAN:

1. Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.

2. Select the **Add** button to create an additional WLAN or select an existing WLAN and choose **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Security**.
4. 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 new or existing WLAN.

Select Encryption

WPA/WPA2-TKIP
 WEP 128
 WEP 64
 Open

WPA2-CCMP

Key Settings

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key ASCII ▾

Key Rotation

Unicast Rotation Interval 30 (30 to 86,400 seconds)

Broadcast Rotation Interval 30 (30 to 86,400 seconds)

Fast Roaming

Pre-Authentication

Advanced

TKIP Countermeasure Hold Time Minutes ▾ (0 to 1,093)

Exclude WPA2 TKIP

>> OK Reset Exit

Figure 6-6 WPA2-CCMP screen

5. Define **Key Settings**.

Pre-Shared Key

Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The wireless controller converts the string to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

6. Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. Broadcast messages are addressed to multiple devices. When using WPA2-CCMP, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an AP, and one broadcast key, the common key for all the clients in that subnet.

Motorola recommends rotating these keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

Unicast Rotation Interval Define an interval for unicast key transmission in seconds (30 -86,400). Some clients have issues using unicast key rotation, so ensure you know which kind of 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 an interval for broadcast key transmission in seconds (30-86,400). Key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.

7. Define the **Fast Roaming** configuration used with the WPA2-CCMP policy.

Using 802.11i can speed up the roaming process from one AP to another. Instead of doing a complete 802.1x authentication each time a client roams between APs, 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 APs, Opportunistic Key Caching allows multiple APs to share PMKs amongst themselves. This allows a client to roam to an AP it has not previously visited and reuse a PMK from another AP to skip 802.1x authentication.

Pre-Authentication Selecting the Pre-Authentication option enables an associated client to carry out an 802.1x authentication with another wireless controller (or device) before it roams to it. This enables the roaming client to send and receive data sooner by not having to conduct an 802.1x authentication after roaming. With pre authentication, a wireless 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 AP, the device is already authenticated on the access point providing faster re-association. This feature is enabled by default.

8. Set the following **Advanced** for the WPA2-CCMP encryption scheme.

TKIP Countermeasure Hold Time The TKIP countermeasure hold-time is the time during which the use of the 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 60 seconds.

Exclude WPA2-TKIP Select this option for an Access Point to advertise and enable support for only WPA-TKIP. Select this option if certain older clients are not compatible with the newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. *Motorola* recommends enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.

9. 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:

- Motorola recommends WPA2-CCMP be configured for all new (non visitor) WLANs requiring encryption, as it's supported by the majority of the hardware and client vendors using Motorola 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.

6.1.2.7 WEP 64

▶ Configuring WLAN Security

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 802.1X 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 that are 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 **Configuration > Wireless > Wireless LAN Policy** to display a high-level display of the existing WLANs.
2. Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Security**.
4. Select the **WEP 64** radio button from within the Select Encryption field.

The screen populates with the parameters required to define a WEP 64 configuration for the WLAN.

Select Encryption

WPA/WPA2-TKIP
 WEP 128
 WEP 64
 Open

WPA2-CCMP

Enter 4 to 32 Characters

Generate Keys **Generate**

Enter 10 HEX or 5 ASCII Characters Transmit Key

Key 1

Key 2

Key 3

Key 4

Restore Default WEP Keys

Figure 6-7 WEP 64 screen

5. Configure the following WEP 64 settings:

- Generate Keys** Specify a 4 to 32 character Pass Key and click the **Generate** button. The pass key can be any alphanumeric string. The wireless controller, other proprietary routers, and Motorola clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.
- Keys 1-4** Use the Key #1-4 fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button.
- Restore Default WEP Keys** If you feel it necessary to restore the WEP algorithm back to its default settings, click the **Restore Default WEP Keys** button.

Default WEP 64 keys are as follows:

- Key 1 1011121314
- Key 2 2021222324
- Key 3 3031323334

- Key 4 4041424344
6. Select **OK** when completed to update the WLAN's WEP 64 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

WEP 64 Deployment Considerations

Before defining a WEP 64 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Motorola recommends 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.

6.1.2.8 WEP 128

► *Configuring WLAN Security*

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 802.1X 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 uses 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 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.

To configure WEP 128 encryption on a WLAN:

1. Select **Configuration > Wireless > Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless controller managed network.
2. Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Security**.
4. Select the **WEP 128** radio button from within the Select Encryption field.

The screen populates with the parameters required to define a WEP 128 configuration for the WLAN.

Figure 6-8 WEP 128 screen

5. Configure the following WEP 128 settings:

Generate Keys Specify a 4 to 32 character Pass Key and click the **Generate** button. The pass key can be any alphanumeric string. The wireless controller, other proprietary routers, and Motorola clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers.

Keys 1-4 Use the Key #1-4 areas to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button.

Restore Default WEP Keys If you feel it necessary to restore the WEP algorithm back to its default settings, click the **Restore Default WEP Keys** button.

Default WEP 128 keys are as follows:

- Key 1 101112131415161718191A1B1C
- Key 2 202122232425262728292A2B2C
- Key 3 303132333435363738393A3B3C
- Key 4 404142434445464748494A4B4C

6. 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:

- Motorola recommends 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.

6.1.3 Configuring WLAN Firewall Support

▶ Wireless LAN Policy

A Firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the Motorola wireless 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 wireless network. For an overview of Firewalls, see [Wireless Firewall on page 8-2](#).

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 wireless controller 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 access policies, create a new access policy or edit the properties of a new WLAN Firewall policy.



1. Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.
2. Select the **Add** button to create a new WLAN or **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Firewall** from the Wireless LAN Policy options.



IP Firewall Rules

Inbound IP Firewall Rules  



Outbound IP Firewall Rules  

MAC Firewall Rules


Inbound MAC Firewall Rules  

Outbound MAC Firewall Rules  

Association ACL

Association ACL  


Trust Parameters

ARP Trust 

Validate ARP Header Mismatch

DHCP Trust

Wireless Client Deny

Wireless Client Denied Traffic Threshold  (1 to 1,000,000 packets per second)

Action

Blacklist Duration (0 to 86,400 seconds)

Advanced

Firewall Session Hold Time (1 to 300)

>> OK **Reset** **Exit**

Figure 6-9 WLAN Policy Firewall screen

The screen displays editable fields for IP Firewall Rules, MAC Firewall Rules, Trust Parameters and Client Deny Limits.

Select an existing inbound and outbound **IP Firewall Rule** using the drop-down menu. If no rules exist, select the **Create** icon to display a screen where Firewall rules can be created. Select the **Edit** icon to modify the configuration of a selected Firewall policy configuration.

If creating a new rule, providing a name up to 64 characters long.

4. Select the **+ Add Row** button.
5. Select the added row to expand it into configurable parameters.

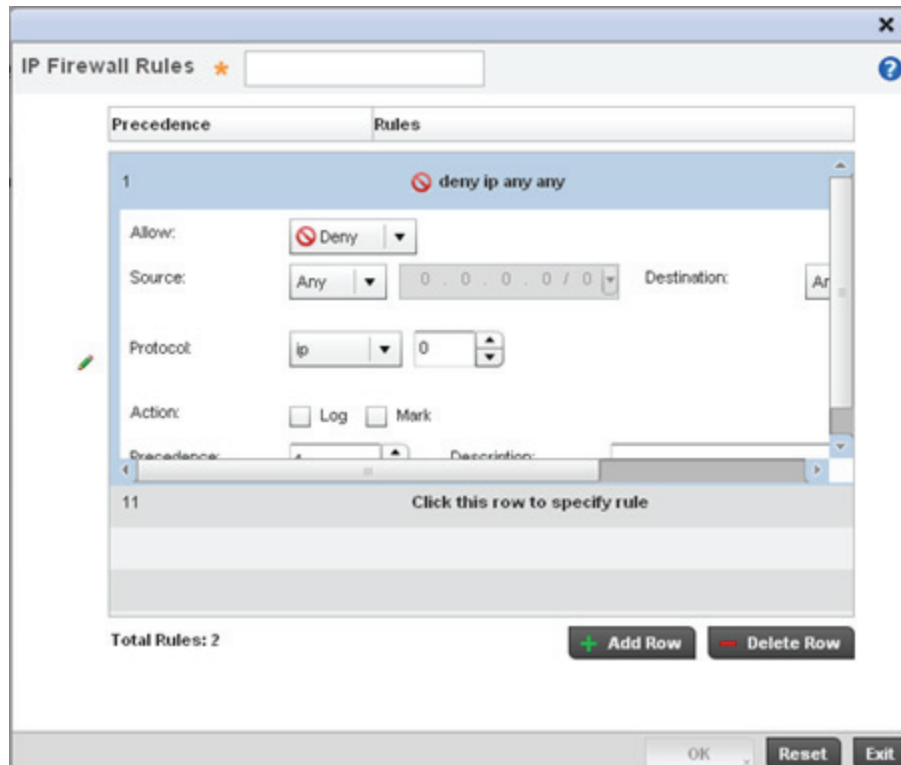


Figure 6-10 IP Firewall Rules screen

6. Define the following parameters for either the inbound or outbound IP Firewall Rules:

Allow

Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:

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

Enter both **Source** and **Destination** IP addresses. The device uses the source IP address, destination IP address and IP protocol type as basic matching criteria. The access policy filter can also include other parameters specific to a protocol type (like source and destination port for TCP/UDP protocol. Provide a subnet mask if needed.

Protocol

Select the protocol used with the IP access policy from the drop-down menu. IP is selected by default. Selecting ICMP displays an additional set of ICMP specific Options for ICMP Type and code. Selecting either TCP or UDP displays an additional set of specific TCP/UDP source and destinations port options.

- Action** The following actions are supported:
- Log*—Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted.
 - Mark*—Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.
 - Mark, Log*— Conducts both mark and log functions.
- Precedence** Use the spinner control to specify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied first to packets.
- Description** Provide a description up to characters long for rule to help differentiate it from others with similar configurations.

7. Select existing inbound and outbound **MAC Firewall Rules** using the drop-down menu. If no rules exist, select **Create** to display a screen where Firewall rules can be created.
8. Select the **+ Add Row** button.
9. Select the added row to expand it into configurable parameters.

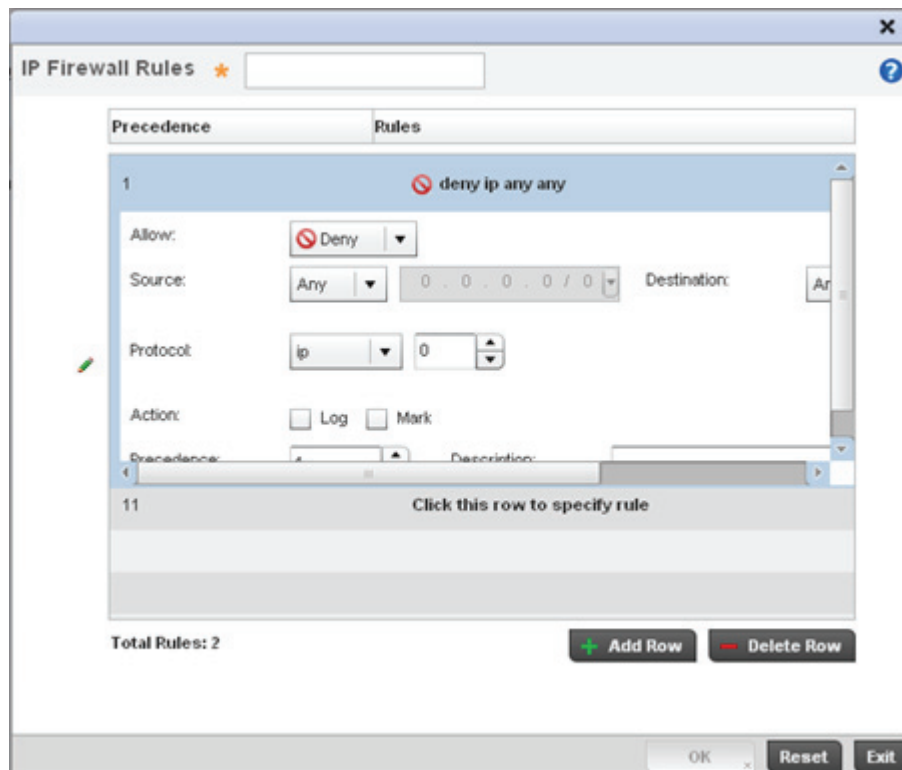


Figure 6-11 MAC Firewall Rules screen

10. Define the following parameters for either the inbound or outbound MAC Firewall Rules:

Allow	<p>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:</p> <p><i>Deny</i>— Instructs the Firewall to not to allow a packet to proceed to its destination.</p> <p><i>Permit</i>— Instructs the Firewall to allow a packet to proceed to its destination.</p>
Source and Destination MAC	<p>Enter both Source and Destination MAC addresses. The wireless controller uses the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.</p>
Action	<p>The following actions are supported:</p> <p><i>Log</i>— Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted.</p> <p><i>Mark</i>— Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.</p> <p><i>Mark, Log</i>— Conducts both mark and log functions.</p>
Precedence	<p>Use the spinner control to specify a precedence for this MAC Firewall rule between 1-1500. Access policies with lower precedence are always applied first to packets.</p>
VLAN ID	<p>Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be between 1 and 4094.</p>
Match 802.1P	<p>Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0-7.</p>
Ethertype	<p>Use the drop-down menu to specify an EtherType of either ipv6, arp, wisp, monitor 8021q. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame.</p>
Description	<p>Provide a description (up to 64 characters) for the rule to help differentiate the it from others with similar configurations.</p>

11. Save the changes to the new MAC rule or reset to the last saved configuration as needed.

12. Set the following **Trust Parameters**:

ARP Trust	<p>Select the 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.</p>
DHCP Trust	<p>Select the radio button to enable DHCP trust on this WLAN. This setting is disabled by default.</p>

13. Set the following **Wireless Client Deny** configuration:

Wireless Client Denied Traffic Threshold	If enabled, any associated client which exceeds the thresholds configured for storm traffic is either deauthenticated or blacklisted depending on the selected Action. The threshold range is 1-1000000 packets per second. This feature is disabled by default.
Action	If enabling a wireless client threshold, use the drop-down menu to determine whether clients are deauthenticated when the threshold is exceeded or blacklisted from connectivity for a user defined interval. Selecting None applies no consequence to an exceeded threshold.
Blacklist Duration	Select the checkbox and define a setting between 0 - 86,400 seconds. Once the blacklist duration has been exceeded, offending clients can reauthenticate.

14. 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 10 seconds.

15. 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 guidelines to ensure the configuration is optimally effective:

- IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

6.1.4 Configuring Client Settings

▶ *Wireless LAN Policy*

Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations.

1. Select **Configuration > Wireless > Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless network.
2. Select the **Add** button to create an additional WLAN, or select an existing WLAN and **Edit** to modify the properties of an existing WLAN.
3. Select the **Client Settings** tab.

Client Settings

Disallow Client-to-Client Communication

Wireless Client Power (0 to 20 dBm)

Wireless Client Idle Time Minutes (1 to 1,440)

Max Firewall Sessions per Client (10 to 10,000)

Enforce Client Load Balancing

Enforce DHCP Client Only

Proxy ARP Mode

Enforce DHCP-Offer Validation

Figure 6-12 WLAN Policy Client Settings screen

4. Define the following **Client Settings** for the WLAN:

Disallow Client-to-Client Communication

Select this option to disallow client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting also disabled on that WLAN, the clients are not permitted to interoperate.

Wireless Client Power

Use this parameter to set the maximum transmit power (between 0 - 20 dBm) communicated to wireless clients for transmission. The default value is 20 dBm.

Wireless Client Idle Time

Set the maximum amount of time wireless clients are allowed to be idle within this WLAN. Set the idle time in either *Seconds* (60 - 86,400), *Minutes* (1 - 1,440), *Hours* (0 - 24) or *Days* (0 - 1). When this setting is exceeded, the client is no longer able to access resources and must re-authenticate. The default value is 1,800 seconds.

Max Firewall Sessions per Client

Select this option to set the maximum amount of sessions (between 10 - 10,000 clients) 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.

Enforce Client Load Balancing

Select the checkbox to distribute clients evenly amongst associated Access Point radios. This feature is enabled by default.

- | | |
|--------------------------------------|--|
| Enforce DHCP Client Only | Select the checkbox to enforce that the firewall only allows packets from clients if they used DHCP to obtain an IP address, disallowing static IP addresses. This feature is disabled by default. |
| Proxy ARP Mode | Use the drop-down menu to define the proxy ARP mode as either <i>Strict</i> or <i>Dynamic</i> . 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. |
| Enforce DHCP-Offer Validation | Select the checkbox to enforce DHCP offer validation. The default setting is disabled. |

7. Select **OK** when completed to update the WLAN's client setting configuration. Select **Reset** to revert the screen back to the last saved configuration.

6.1.5 Configuring WLAN Accounting Settings

Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports and logs user activity to a RADIUS security server in the form of accounting records. 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 location outside of the switch for periodic network and user permission administration.

To configure WLAN accounting settings:

1. Select **Configuration > Wireless LANs > Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless controller managed network.
2. Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Accounting**.

Figure 6-13 WLAN Policy Accounting screen

4. Set the following **Syslog Accounting** information:

Enable System Log Accounting	Use 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.
Syslog Port	Use the spinner control to set the destination UDP port number of the external syslog host where the accounting records are routed.

5. Select the **Enable RADIUS Accounting** radio button 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.
6. Select **OK** when completed to update this WLAN's accounting settings. Select **Reset** to revert the screen back to its last saved configuration.

6.1.5.1 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, Motorola Solutions recommends the WAN port round trip delay not exceed 150ms. Excessive delay over a WAN can cause authentication and roaming issues. When excessive delays exist, a distributed RADIUS service should be used.
- Motorola Solutions recommends 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.

6.1.6 Configuring Advanced WLAN Settings

► Wireless LAN Policy

To configure advanced settings on a WLAN:

1. Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display a high-level display of the existing WLANs available to the wireless controller managed network.
2. Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing wireless controller WLAN.
3. Select **Advanced**.

Protected Management Frames

Mode Disabled Optional Mandatory

SA Query Attempts (1 to 15)

SA Query Retry Timeout (100 to 6,000 milliseconds)

Advanced RADIUS Configuration

NAS Identifier

NAS Port

RADIUS Dynamic Authorization

Radio Rates

Rates for 2.4 GHz WLAN **Select** ▾

Rates for 5.0 GHz WLAN **Select** ▾

OK Reset Exit

Figure 6-14 WLAN Policy Advanced screen

4. Refer to the **Protected Management Frames** field to set a frame protection mode and security association for the WLAN's advanced configuration.

During a *security association (SA)* negotiation, the wireless controller and recipient gateways agree to use a particular transform set to protect data flow. A transform set is a combination of security protocols and algorithms. During an IPSec security association negotiation, peers agree to use a particular transform set for protecting the wireless controller managed data flow.

Mode

Select a radio button option to determine whether management frames are continually or optionally protected. Disabled is the default setting.

-
- SA Query Attempts** Use the spinner control to set the number of security association query attempts between 1-15. The default value is 3.
- SA Query Retry Timeout** The timeout value is the configurable interval used to timeout association requests that exceed the defined interval. Set the timeout value between 100-6000 milliseconds. The default value is 1000 milliseconds.
5. Refer to the **Advanced RADIUS Configuration** field to set the WLAN's NAS configuration and RADIUS Dynamic Authorization.
- NAS Identifier** Specify what should be included in the RADIUS NAS-Identifier field for authentication and accounting packets relating to this WLAN. Configuring a value here is optional, and defaults are used if this is not configured per WLAN.
- 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 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. Set the numeric port value between 0-4,294,967,295.
- RADIUS Dynamic Authorization** Select the radio button to enable a mechanism that extends the RADIUS protocol to support unsolicited messages sent from the RADIUS server. These messages allow wireless network administrators to issue *change of authorization* (CoA) messages, which affect session authorization, or *Disconnect Message (DM)*, which cause a session to be terminated immediately. This feature is disabled by default.
6. Refer to the **Radio Rates** field to define selected data rates for both the 2.4 and 5.0 GHz bands.

Rate Settings 2.4GHz-wlan

Radio Transmission Data Rates

b-only rates
 bg rates
 bgn rates
 Default
 g-only rates
 gn rates
 Custom Rates

802.11 b rates

	1Mbps	2Mbps	5.5Mbps	11Mbps
Basic:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

802.11 g rates

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

802.11 n rates

	MCS0-7	MCS8-15
Basic:	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Reset Cancel

Figure 6-15 Advanced WLAN Rate Settings 2.4 GHz screen

Rate Settings 5GHz-wlan

Radio Transmission Data Rates

a-only rates
 Default
 an rates
 Custom Rates

802.11 a rates

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

802.11 n rates

	MCS0-7	MCS8-15
Basic:	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK Reset Cancel

Figure 6-16 Advanced WLAN Rate Settings 5 GHz screen

Define both minimum Basic and optimal Supported rates as required for the 802.11b rates, 802.11g rates and 802.11n 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 WLAN.

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).

The selected rates apply to associated client traffic within this WLAN only.

7. Select **OK** when completed to update this WLAN's advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

6.2 Configuring WLAN QoS Policies

▶ *Wireless LAN Policy*

QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Management, 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. Each QoS policy has its own radio button that can be selected to edit its properties. If none of the existing QoS policies supports an ideal QoS configuration for the intended data traffic of 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) Policy* screen to add a new QoS policy or edit the attributes of an existing policy.



NOTE: WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these access point radios support.

1. Select **Configuration > Wireless > WLAN QoS Policy** to display existing QoS policies available to WLANs.

WLAN Quality of Service (QoS) ?					
WLAN QoS Policy ⌵	Wireless Client Classification	SVP Prioritization	WMM Power Save	Multicast Mask Primary	Multicast Mask Secondary
default	WMM	✗	✓	00-00-00-00-00-00/	00-00-00-00-00-00/

Row Count: 1

Add
Edit ✕
Delete

Figure 6-17 WLAN Quality of Service (QoS) screen

2. Refer to the following read-only information on each listed QoS policy to determine whether an existing policy can be used as is, an existing policy requires edit or a new policy requires creation:

WLAN QoS Policy	Displays the name assigned to this WLAN QoS policy when it was initially created. The assigned policy name cannot be modified as part of the edit process.
Wireless Client Classification	Lists each policy's <i>Wireless Client</i> Classification as defined for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to a radio. The <i>Wireless Client</i> Classification types are: <i>WMM</i> – 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. <i>Voice</i> – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. <i>Video</i> – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. <i>Normal</i> – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. <i>Low</i> – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
SVP Prioritization	A green checkmark defines the policy as having <i>Spectralink Voice Prioritization</i> (SVP) enabled to allow the wireless controller to identify and prioritize traffic from Spectralink/Polycomm phones using the SVP protocol. Phones using regular WMM and SIP are not impacted by SVP prioritization. A red "X" defines the QoS policy as not supporting SVP prioritization.
WMM Power Save	Enables support for the WMM based power-save mechanism, also known as <i>Unscheduled Automatic Power Save Delivery</i> (U-APSD). This is primarily used by voice devices that are WMM capable. 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, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Mask Secondary	Displays the secondary multicast mask defined for each listed QoS policy.



NOTE: When using a wireless client classification other than WMM, only legacy rates are supported on that WLAN.

3. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration. Existing QoS policies can 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 a WLAN's QoS WMM Settings](#)
- [Configuring a WLAN's QoS Rate Limit Settings](#)
- [Configuring a WLAN's QoS Wireless Client Rate Limit Settings](#)

6.2.1 Configuring a WLAN's QoS WMM Settings

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 traffic priority.

WMM's prioritization capabilities are based on the four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over the wireless controller managed WLAN. ACs were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled wireless controllers/ 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 interframe 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 **Configuration** > **Wireless** > **Wireless LAN QoS Policy** to display existing WLANs.

- 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.

WLAN QoS Policy WLANQoS1

WMM WLAN Rate Limit Wireless Client Rate Limit

Wireless Client Classification: WMM

Enable Voice Prioritization:

Enable SVP Prioritization:

Enable WMM Power Save:

Video Access

Transmit Ops: 94 (0 to 65,535)

AIFSN: 2 (2 to 15)

ECW Min: 3 (0 to 15)

ECW Max: 4 (0 to 15)

Voice Access

Transmit Ops: 47 (0 to 65,535)

AIFSN: 2 (2 to 15)

ECW Min: 2 (0 to 15)

ECW Max: 3 (0 to 15)

Other Settings

Trust IP DSCP:

Trust 802.11 WMM QoS:

Multicast Mask Primary: 11 : 22 : AA : BB : AA : AA / FF : FF : FF : FF : FF : FF

Multicast Mask Secondary: 22 : 11 : AA : BB : AA : AA / FF : FF : FF : FF : FF : FF

Multicast Mask Classification: Normal

Normal (Background) Access

Transmit Ops: 25 (0 to 65,535)

AIFSN: 7 (2 to 15)

ECW Min: 4 (0 to 15)

ECW Max: 10 (0 to 15)

Low (Best Effort) Access

Transmit Ops: 25 (0 to 65,535)

AIFSN: 3 (2 to 15)

ECW Min: 4 (0 to 15)

ECW Max: 10 (0 to 15)

OK Reset Exit

Figure 6-18 WLAN QoS Policy - WMM screen

4. Configure the following 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.

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 *Motorola* VOIP phones. This feature is enabled by default.

Enable SVP Prioritization

Enabling *Spectralink Voice Prioritization (SVP)* allows the *wireless controller* to identify and prioritize traffic from Spectralink/Polycomm phones. This gives priority to voice, with voice management packets supported only on certain legacy *Motorola* VOIP phones. 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 enabled 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 voice devices that are WMM capable. 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, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.

Multicast Mask Secondary	Set a secondary multicast mask for the WLAN QoS policy.
Multicast Mask Classification	Select a drop-down menu option to determine the priority at which immediate multicast/broadcast packets go out. This setting overwrites the WLAN Client Classification. This does not affect multicast/broadcast packets going out at DTIM. The default setting (Normal) mean immediate multicast/broadcast packets go out at the classification priority. For WMM, this means Best Effort.

3. Set the following **Video Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default values is 94.
AIFSN	Set the current Arbitrary Inter-frame Space Number (AIFSN) between 2-15. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

4. Set the following **Voice Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 47.
AIFSN	Set the current <i>Arbitrary Inter-frame Space Number</i> (AIFSN) between 2-15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

5. Set the following **Normal (Background) Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 25.
AIFSN	Set the current <i>Arbitrary Inter-frame Space Number</i> (AIFSN) between 2-15. The default value is 7.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10.

6. Set the following **Low (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. For higher-priority traffic categories, this value should be set to a low number. The default value is 25.
AIFSN	Set the current AIFSN between 2-15. The default value is 3.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Low). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Low). The available range is from 0-15. The default value is 10.

7. Set the following **Other Settings** for the WLAN's QoS policy:

Trust IP DSCP	Select this option to trust IP DSCP values for WLANs. The default value is disabled.
Trust 802.11 WMM QoS	Select this option to trust 802.11 WMM QoS values for WLANs. The default value enabled.
QBSS Load Information	Select this option to enable support for a WMM QBSS Load Information Element in beacons and probe response packets. The default value is enabled.

8. Select **OK** when completed to update this WLAN's QoS settings. Select **Reset** to revert the screen back to its last saved configuration.

6.2.2 Configuring a WLAN's QoS Rate Limit Settings

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. An administrator can set separate QoS rate limit configurations for data transmitted from the Access Point (upstream) and data transmitted from a WLAN's wireless clients back to their associated Access Point radios (downstream).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, Motorola Solutions recommends 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.

To configure a QoS rate limit configuration for a WLAN:

1. Select **Configuration > Wireless > WLAN QoS Policy** to display existing QoS policies available to WLANs.
2. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration.
3. Select the **WLAN Rate Limit** tab.

The screenshot displays the 'WLAN QoS Policy' configuration window for 'WLANQoS1'. It features three tabs: 'WMM', 'WLAN Rate Limit' (selected), and 'Wireless Client Rate Limit'. The 'WLAN Rate Limit' tab is divided into two main sections: 'WLAN Upstream Rate Limit' and 'WLAN Downstream Rate Limit'. Each section has an 'Enable' checkbox checked, a 'Rate' field set to 5000 (with a range of 50 to 1,000,000 kbps), and a 'Maximum Burst Size' field set to 320 (with a range of 2 to 1,024 kbytes). Below these are 'Upstream Random Early Detection Threshold' and 'Downstream Random Early Detection Threshold' sections, each with four rows for 'Background Traffic', 'Best Effort Traffic', 'Video Traffic', and 'Voice Traffic'. The thresholds are set to 50, 50, 25, and 0 respectively, with a range of 0 to 100 % for each. At the bottom right, there are 'OK', 'Reset', and 'Exit' buttons.

Figure 6-19 WLAN QoS Policy - WLAN Rate Limit screen

4. Configure the following parameters in respect to the intended **WLAN Upstream Rate Limit**.

Enable Select the **Enable** 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 downstream direction. This feature is disabled by default.

Rate Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Maximum Burst Size Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream 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.

5. Set the following **Upstream 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 upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Best Effort Traffic Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Video Traffic Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.

Voice Traffic Set a percentage value for voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

5. Configure the following parameters in respect to the intended **WLAN Downstream Rate Limit**, or traffic from wireless clients to associated Access Point radios:

Enable Select the **Enable** 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 between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Maximum Burst Size Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the 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.

6. Set the following **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is done when the amount of tokens for a traffic stream falls below the set threshold.

Background Traffic Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Best Effort Traffic Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.

Video Traffic Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.

Voice Traffic Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

7. Select **OK** when completed to update this WLAN's QoS rate limit settings. Select **Reset** to revert the screen back to its last saved configuration.

6.2.3 Configuring a WLAN's QoS Wireless Client Rate Limit Settings

Wireless clients can also have QoS rate limit settings defined in both the upstream and downstream direction.

To configure a QoS rate limit configuration for wireless clients:

1. Select **Configuration > Wireless > WLAN QoS Policy** to display existing QoS policies available to WLANs.
2. Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration.
3. Select the **Wireless Client Rate Limiting** tab.

Figure 6-20 WLAN QoS Policy - WLAN Client Rate Limit screen

4. Configure the following parameters in respect to the intended **Wireless Client Upstream Rate Limit**:

- Enable** Select the **Enable** radio button to enable rate limiting for data transmitted from the client to its associated access point radio. Enabling this option does not invoke client rate limiting for data traffic in the downstream direction. This feature is disabled by default.
- Rate** Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.
- Maximum Burst Size** Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

5. Set the following **Upstream Random Early Detection Threshold** settings for each access category:

- Background Traffic** Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
- Best Effort Traffic** Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.

Video Traffic Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.

Voice Traffic Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% means no early random drops will occur.

6. Configure the following parameters in respect to the intended **Wireless Client Downstream Rate Limit**:

Enable Select the **Enable** 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 upstream direction. This feature is disabled by default.

Rate Define a downstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.

Maximum Burst Size Set a maximum burst size between 2 - 64 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the wireless client. The default burst size is 6 kbytes.

7. Set the following **Downstream Random Early Detection Threshold** settings for each access category:

Background Traffic Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.

Best Effort Traffic Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.

Video Traffic Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 25%

Voice Traffic Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% means no early random drops will occur.

8. Select **OK** when completed to update this WLAN's QoS rate limit settings for wireless clients. Select **Reset** to revert the screen back to its last saved configuration.

6.2.3.1 WLAN QoS Deployment Considerations

Before defining a WLAN QoS configuration, 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 wireless 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 all 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 email are harder to estimate, since bandwidth usage varies depending on how the applications are utilized.

6.3 Radio QoS Policy

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 customizations best suited to each QoS policy's intended wireless client base.

Motorola Solutions 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, Email and file transfers). A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize the network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent the ineffective utilization of access points degrading session quality by configuring admission control mechanisms within each radio QoS policy

Within a Motorola Solutions 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 than 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 provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. An AP-6511 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.

An AP-6511 supports static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. An AP-6511 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, hotspot authentication and devices using MAC authentication.

6.3.1 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.
- Motorola Solutions recommends 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.

6.4 AAA Policy

Authentication, Authorization, and Accounting (AAA) provides the mechanism network administrators define access control within the network.

The AP-6511 can interoperate with external Radius and LDAP Servers (AAA Servers) to provide user database information and user authentication data. Each WLAN can maintain its own unique AAA configuration.

AAA provides a modular way of performing the following services:

Authentication — Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before granted access. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. Remote RADIUS servers authorize users by associating *attribute-value (AV)* pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces on the network.

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. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA.

To define unique WLAN AAA configurations:

1. Select **Configuration > Wireless > AAA Policy** to display existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA)** screen lists those AAA policies created thus far. Any of these policies can be selected and applied.

Authentication, Authorization, and Accounting (AAA) ?				
AAA Policy ⬆	Accounting Packet Type	Request Interval	IAC Policy	Server Pooling Mode
Type to search in tables Row Count: 0				
Add Edit Delete				

Figure 6-21 Authentication, Authorization, and Accounting (AAA) screen

2. Refer to the following information listed for each existing Radio QoS 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: <i>Start Only</i> - Sends a start accounting notice to initiate the user accounting process. <i>Start/Stop</i> - Sends a start accounting notice at the beginning of a process and a stop notice at the end of a process. The start accounting record is sent in the background. The requested process begins regardless of whether the start accounting notice is received by the accounting server.
Request Interval	Lists each AAA policy's interval to send a RADIUS accounting request to the RADIUS server.
NAC Policy	Lists the name <i>Network Access Control</i> (NAC) filter used to either include or exclude clients from access to the network.
Server Pooling Mode	The server pooling mode controls how requests are transmitted across RADIUS servers. Selecting <i>Failover</i> results in working down the list of servers if a server is unresponsive and unavailable. The <i>Load Balanced</i> option uses all available servers transmitting requests in round robin.

3. For information on configuring a new AAA policy or editing the attributes of an existing AAA policy, see [AAA Policy on page 6-50](#).

6.5 Association ACL

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 affords a system administrator the ability 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 Advanced WLAN Settings on page 6-30*.

To define an Association ACL deployable with a WLAN:

1. Select **Configuration > Wireless > Association ACL** to display existing Association ACLs.

The **Association Access Control List (ACL)** screen lists those Association ACL policies created thus far. Any of these policies can be selected and applied.

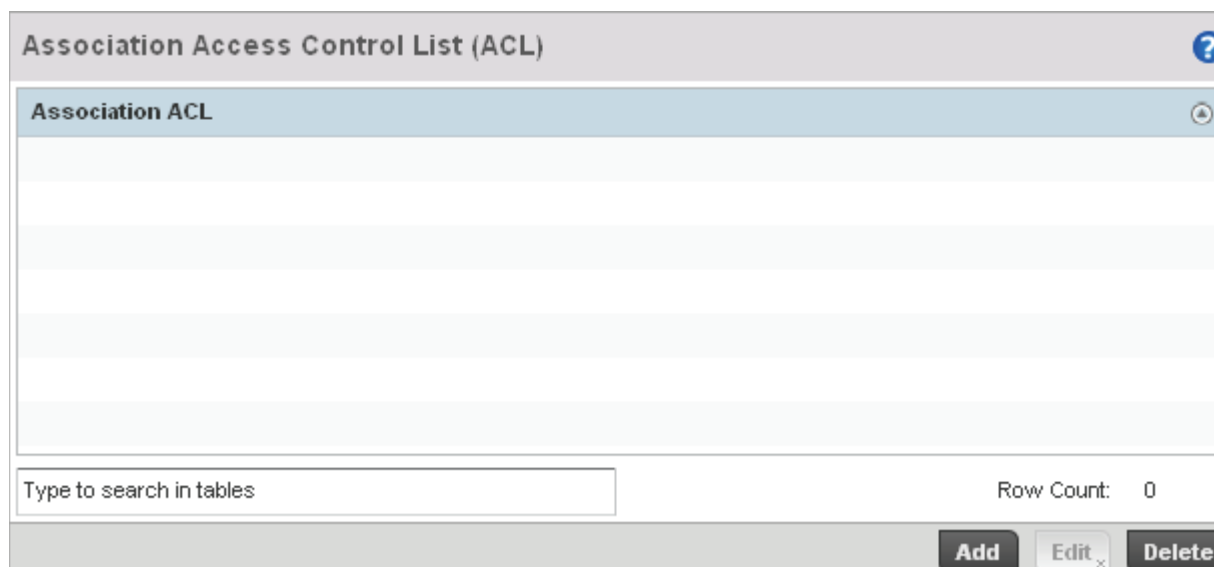


Figure 6-22 Association Access Control List (ACL) screen

2. Select **Add** to define a new ACL configuration, **Edit** to modify an existing ACL configuration or **Delete** to remove one.

A unique Association ACL screen displays for defining the new ACL or modifying the selected ACL.

Precedence	Starting MAC Address	Ending MAC Address	Allow/Deny	
* 1	00 - 00 - 00 - 00 - 00 - 00	FF - FF - FF - FF - FF - FF	Deny	🗑️

+ Add Row

Figure 6-23 Association Access Control List (ACL) screen

3. Select the **+ Add Row** button to add an association ACL template that requires configuration.
4. Set the following parameters for the creation or modification of the Association ACL:

Association ACL If creating an 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.

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 MAC address of the wireless client, for non unicast and multicast packet transmissions.

Ending MAC Address Provide an ending MAC address of the wireless client, 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.

5. Select the **+ Add Row** radio button to add MAC address ranges and allow/deny designations.
6. Select **OK** to update the Association ACL settings. Select **Reset** to revert to the last saved configuration.

6.5.1 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:

- Motorola Solutions recommends using 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.

6.6 Smart RF Policy

Self Monitoring At Run Time RF Management (Smart RF) is a Motorola innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization radio performance improvements.

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power 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 the 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 APs).

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.



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.

To define a Smart RF policy:

1. Select **Configuration** > **Wireless** > **Smart RF Policy** to display existing Smart RF policies.

The Smart RF screen lists those Smart RF policies created thus far. Any of these policies can be selected and applied.

The user has the option of displaying the configurations of each Smart RF Policy defined thus far, or referring to the **Smart RF Browser**.

SMART RF ?				
SMART RF Policy ⌵	SMART RF Policy Enable	Interference Recovery	Coverage Hole Recovery	Neighbor Recovery
Moto-6511-dependantR	✓	✗	✓	✓

Type to search in tables Row Count: 1

Add Edit x Delete

Figure 6-24 Smart RF Policy screen

2. Refer to the following configuration data for existing Smart RF policies:

- Smart RF Policy** Displays the name assigned to the Smart RF policy when it was initially created. The name cannot be modified as part of the edit process.
- Smart RF Policy Enable** Displays a green check mark if Smart RF has been enabled for the listed policy. A red "X" designates the policy as being disabled.
- Interference Recovery** Displays a green check mark if interference recovery has been enabled for the listed policy. A red "X" designates coverage hole recovery being disabled.
- Coverage Hole Recovery** Displays a green check mark if coverage hole recovery has been enabled for the listed policy. A red "X" designates coverage hole recovery being disabled.
- Neighbor Recovery** Displays a green check mark if neighbor recovery has been enabled for the listed policy. A red "X" designates neighbor recovery being disabled.

3. Select **Add** to create a new Smart RF policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available.

The **Basic Configuration** screen displays by default for the new or modified Smart RF policy.

Figure 6-25 Smart RF Basic Configuration screen

4. Refer to the **Basic Settings** field to enable a Smart RF policy and define its sensitivity and detector status.

Sensitivity	Select a radio button corresponding to the desired Smart RF sensitivity. Options include <i>Low</i> , <i>Medium</i> , <i>High</i> and <i>Custom</i> . Medium, is the default setting. Select the Custom sensitivity option to enable the Interference Recovery, Coverage Hole Recovery and Neighbor Recovery options as additional Smart RF recovery options.
SMART RF Policy Enable	Select the Smart RF Policy Enable radio button to enable this Smart RF policy for immediate inclusion with a RF Domain. Smart RF is disabled by default.
Auto Assign Sensor	Select the radio button to enable an AP-651 to auto assign a sensor radio for neighbor activity monitoring within the AP-6511 Smart RF supported network.
Interference Recovery	Select the radio button to enable Interference Recovery when radio interference is detected within the Smart RF supported AP-6511 radio coverage area. 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.

Coverage Hole Recovery

Select the radio button to enable Coverage Hole Recovery 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. Coverage Hole Recovery is enabled by default when Custom is selected as the Sensitivity option.

Neighbor Recovery

Select the radio button to enable Neighbor Recovery when a failed radio is detected within the Smart RF supported radio coverage area. Smart RF can provide automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor recovery is enabled by default when **Custom** is selected as the Sensitivity option.

5. Refer to the **Calibration Assignment** field to define whether Smart RF Calibration and radio grouping is conducted by floor or building. Both options are disabled by default.
6. Select **OK** to update the Smart RF Basic Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.
7. Select **Channel and Power**.

Use the Channel and Power screen to refine Smart RF power settings over both the 5 and 2.4 GHz radio bands and select channel settings in respect to the device channel usage.

Power Settings

5.0 GHz Minimum Power: 4 (1 to 20 dBm)

5.0 GHz Maximum Power: 10 (1 to 20 dBm)

2.4 GHz Minimum Power: 4 (1 to 20 dBm)

2.4 GHz Maximum Power: 10 (1 to 20 dBm)

Channel Settings

5.0 GHz Channels: 36,40,44,48,... **Select**

5.0 GHz Channel Width: 20MHz 40MHz Automatic

2.4 GHz Channels: 1,6,11 **Select**

2.4 GHz Channel Width: 20MHz 40MHz Automatic

OK Reset Exit

Figure 6-26 Smart RF Channel and Power screen



NOTE: The Power Settings and Channel Settings parameters are only enabled when Custom is selected as the Sensitivity setting from the Basic Configuration screen.

8. Refer to the **Power Settings** to define Smart RF recovery settings for either the selected 5.0 GHz (802.11a) or 2.4 GHz (802.11bg) radio.

5.0 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 GHz band. 1 dBm is the default setting.
5.0 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 GHz band. 17 dBm is the default setting.
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. 1 dBm is the default setting.
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. 17 dBm is the default setting.

9. Set the following **Channel Settings** for the 5.0 GHz and 2.4 GHz radio bands:

- 5.0 GHz Channels** Use the **Select** drop-down menu to select the 5 GHz channels used in Smart RF scans.
- 5.0 Channel Width** 20 and 40 MHz channel widths are supported by the 802.11a radio. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the *Access Point* to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of “wider channels.” 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **Automatic** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 40MHz is the default setting.
- 2.4 GHz Channels** 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 the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of “wider channels.” 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select **Automatic** to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 20MHz is the default setting.

10. Select **OK** to update the Smart RF Channel and Power settings for this policy. Select **Reset** to revert to the last saved configuration.

11. Select **Advanced Configuration**.

The **Neighbor Recovery** tab displays by default. Use the *Neighbor*, *Interference* and *Coverage Hole* recovery tabs to define how 5 and 2.4 GHz radios compensate for failed neighbor radios, interference and coverage holes requiring neighbor radio intervention.

12. Set the following **Neighbor Recovery** variables for the Smart RF configuration:



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 Basic Configuration screen.

Neighbor Recovery	Interference Recovery	Coverage Hole Recovery
Hold Time		
Power Hold Time	0	Seconds (0 to 3,600)
Channel Hold Time	1	Hours (0 to 24)
Neighbor Recovery		
5.0 GHz Neighbor Power Threshold	-70	(-85 to -55 dBm)
2.4 GHz Neighbor Power Threshold	-70	(-85 to -55 dBm)
<p>! Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.</p>		

Figure 6-27 Smart RF Advanced 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.

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 3,660 seconds.

13. Set the following **Neighbor Recovery** parameters:

5.0 GHz Neighbor Recovery Power Threshold Use the spinner control to set a value between -85 to -55 dBm the 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 device radio within its wireless radio coverage area. The default value is -70 dBm.

2.4 GHz Neighbor Recovery Power Threshold Use the spinner control to set a value between -85 to -55 dBm the 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 device radio within its wireless radio coverage area. The default value is -70 dBm.

14. Select **OK** to update the Smart RF Neighbor Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

15. Select the **Interference Recovery** tab.



Figure 6-28 Smart RF Advanced Configuration screen - Interference Recovery tab

16. Set the following **Interference Recovery** parameters:

- Interference** Select the radio button to allow the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default.
- Noise** Select the radio button to allow the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a cleaner channel. This feature is enabled by default.
- Client Threshold** Use the spinner to set a client threshold for the Smart RF policy between 1 - 255. If threshold number of clients are connected to a radio, it does not change its channel even though it requires one, based on the interference recovery determination made by the smart master. The default setting is 50.
- 5.0 GHz Channel Switch Delta** Use the spinner to set a channel switch delta (between 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 (between 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.

17. Select **OK** to update the Smart RF Interference Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

18. Select the **Coverage Hole Recovery** tab.

Neighbor Recovery Interference Recovery Coverage Hole Recovery

Coverage Hole Recovery for 5.0 GHz

Client Threshold: 1 (1 to 255)

SNR Threshold: 20 (1 to 75 dB)

Coverage Interval: 10 Seconds (1 to 120)

Interval: 30 Seconds (1 to 120)

Coverage Hole Recovery for 2.4 GHz

Client Threshold: 1 (1 to 255)

SNR Threshold: 20 (1 to 75 dB)

Coverage Interval: 10 Seconds (1 to 120)

Interval: 30 Seconds (1 to 120)

Note: The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter

OK Reset

Figure 6-29 Smart RF Advanced Configuration screen - Coverage Hole Recovery tab

19. 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 for the Smart RF policy between 1 - 255. This is the minimum number of clients a radio should have associated in order for coverage hole recovery to trigger. The default setting is 1.
- SNR Threshold** Use the spinner control to set a signal to noise threshold (between 1 - 75 dB). This is the signal to noise threshold for an associated client as seen by its associated AP radio. When exceeded, the radio increases its transmit power in order to increase coverage for the associated client. The default value is 20 dB.
- Coverage Interval** Define the interval coverage hole recovery should be initiated after a coverage hole is detected. The default is 10 seconds for both the 2.4 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 the 2.4 and 5.0 GHz radios.

20. Select **OK** to update the Smart RF Coverage Hole Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

6.6.1 Smart RF Configuration and Deployment Considerations

▶ Smart RF Policy

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when Access Points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

Profile Configuration

Profiles enable administrators to assign a common set of configuration parameters and policies to the AP-6511 model Access Point. 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. An AP-6511 supports both default and user defined profiles implementing new features or updating existing parameters to groups of Access Points. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Profiles assign configuration parameters, applicable policies and WLANs to one or more Access Points, thus allowing smart administration across large wireless network segments. However, individual devices can still be assigned unique configuration parameters that follow the flat configuration model supported by Motorola Solutions in previous software releases. As individual device updates are made, these device no longer share the profile based configuration they originally supported. Changes made to the profile are automatically inherited by all assigned devices, but not those devices who have had their configuration customized. These devices require careful administration, as they no longer can be tracked and as profile members. Their customized configurations overwrite their profile configurations until the profile can be re-applied to the device.

Each AP-6511 model Access Point is automatically assigned a default profile. A default profile for each supported model is automatically added to a device's configuration file when the device is discovered. Default profiles can also be manually added prior to discovery when needed. Default profiles are ideal for single site deployments where Access Points may share a common configuration.

User defined profiles are manually created for each supported AP-6511. User defined profiles can be manually assigned or automatically assigned using an AP-6511 Adoption policy. AP Adoption policies provide the means to easily assign profiles to Access Points based on model, serial number, VLAN ID, DHCP option, IP address (subnet) and MAC address.

Motorola Solutions recommends using user defined profiles in larger deployments using centralized controllers when groups of devices on different floors, buildings or sites share a common configuration.

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

Review the existing profiles to determine whether a new profile requires creation, or existing profile requires edit or deletion.

To review existing profiles and assess if they can be applied to a AP-6511:

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

3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.

Profile ?							
Profile	Type	Adoption Policy	Firewall Policy	Wireless Client Role Policy	Advanced WIPS Policy	DHCP Server Policy	Management Policy ⌵
DAP-20	AP6511		default				default
default-ap651	AP6511		default				default
Controller-prf	AP6511	DAP	default				default

Row Count: 3

Add
Edit
Delete

Figure 7-1 Profile screen

4. Review the following information on existing profiles:

- Profile** Lists the user-assigned name defined for each profile when created. Profile names cannot be edited with a profiles configuration.
- Adoption Policy** Displays the AP-6511 adoption policy applied to this profile. At adoption, an AP solicits and receives multiple adoption responses from controllers available on the network. These adoption responses contain preference and loading policy information the AP uses to select the optimum controller for adoption. By default, an adoption policy generally distributes AP adoption evenly. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of this particular profile.
- Firewall Policy** Displays the existing firewall policy, if any, assigned to each listed profile. Firewall policies can be assigned when creating or editing a profile.
- DHCP Server Policy** Lists the name of the DHCP Server Policy used with each listed profile. 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.
- Management Policy** Lists the name of Management policies applied to each listed profile. A management policy is a mechanism to allow/deny management access for separate interfaces and protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Management access can be enabled/disabled as required for each policy.

5. Select the **Add** button to create a new profile, **Edit** to revise a selected profile configuration or **Delete** to permanently remove a selected profile.

The following tasks comprise required profile configuration activities:

- *General Profile Configuration*
- *Profile Interface Configuration*
- *Profile Network Configuration*
- *Profile Security Configuration*
- *Profile Services Configuration*
- *Profile Management Configuration*
- *Miscellaneous Profile Configuration*

7.1 General Profile Configuration

Each profile requires an AP-6511 unique adoption policy and clock synchronization settings as part of its general configuration. Each profile can have an adoption policy and system time.

AP-6511 model Access Points are automatically assigned a default profile unless an AP-6511 Adoption policy has been defined that specifically assigns Access Points to a user defined profile. During the general configuration process, an AP-6511 adoption policy can be assigned to a specific profile or a new AP-6511 adoption policy can be created and applied to the profile. Adoption is the process an AP uses to discover controllers available in the network, pick the most desirable one, establish an association and optionally obtain an image upgrade, obtains its configuration and considers itself provisioned.

Network Time Protocol (NTP) manages time and/or network clock synchronization within the network. NTP is a client/server implementation. The AP-6511 periodically synchronizes its clock with a master clock (an NTP server). For example, the AP-6511 resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Additionally, if the profile is supporting an Access Point, the profile's general configuration provides an option to disable the device's LEDs.

To define a profile's general configuration:

1. Select the Configuration tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **General**.

A general configuration screen displays for the new or existing profile.

The screenshot shows the 'General Profile Configuration' screen. It is divided into three main sections:

- Controller AP:** Includes a checkbox labeled 'Set as Controller AP' which is checked.
- Adoption Policy:** Features a dropdown menu currently set to 'DAP', with icons for adding a new policy and editing the current one.
- Network Time Protocol (NTP):** Contains a table with the following columns: Autokey, Key, Prefer, Server IP, Version, and a delete icon. The table is currently empty. Below the table is a '+ Add Row' button.

Figure 7-2 General Profile Configuration screen

5. If creating a new profile, provide a name (up to 32 characters long) within the **Profile** parameter field.
6. Set the AP as a **Controller AP**. A Controller AP mediates the configuration and monitoring of a multiple AP deployment. It's used to adopt other APs and provide a single point of management and control for an installation.

7. Use the **Adoption Policy** drop-down menu to select an AP-6511 adoption policy to assign a specific Profile to Access Points based on model, serial number, VLAN, DHCP option, IP address or MAC address. An Adoption Policy screen displays requiring a name be defined before the policy's configuration can be set.
8. Select **+ Add Row** below the **Network Time Protocol (NTP)** table to define the configurations of NTP server resources the used it obtain system time. Set the following parameters to define the NTP configuration:

AutoKey	Select the radio button to enable an autokey configuration for the NTP resource. The default setting is disabled.
Key	If an autokey is not being used, manually enter a 64 character maximum key the AP-6511 and NTP resource share to securely interoperate.
Prefer	Select the radio button designate this particular NTP resource as preferred. If designating multiple NTP resources, preferred resources will be given first opportunity to connect and provide NTP calibration.
Server IP	Set the IP address of each server added as a potential NTP resource.
Version	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.

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

7.1.1 General Profile Configuration and Deployment Considerations

► General Profile Configuration

Before defining a general profile configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A default profile is applied automatically to an AP-6511, and default AP profiles are applied to APs discovered and adopted by a controller.
- A central difference compared to the default-radio configurations in previous WiNG releases is default profiles are used as pointers of an AP'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 APs using that profile.
- Each user defined profile requires a unique name.
- User defined profiles can be automatically assigned to Access Points using AP adoption policies.
- Access Points are automatically assigned a default profile based on the hardware type selected when the profile is initially created.

7.2 Profile Interface Configuration

A profile's interface configuration can be defined to support separate physical Ethernet configurations that are both unique and specific to the AP-6511 Access Point.

An AP-6511 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 VLAN ID the Access Point is connected to.

If the profile is configured to support an Access Point radio, an additional Radios option is available, unique to the Access Point's radio configuration.

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

- [Ethernet Port Configuration](#)
- [Virtual Interface Configuration](#)
- [Access Point Radio 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 [Profile Interface Deployment Considerations on page 7-24](#).

7.2.1 Ethernet Port Configuration

► [Profile Interface Configuration](#)

Displays the physical port name reporting runtime data and statistics. The following ports are available on an AP-6511:

- *AP6511* - fe1, fe2, fe3, fe4, up1

To define a profile's Ethernet port configuration:

1. Select **Configuration** > **Profiles** > **Interface**.
2. Expand the Interface menu to display its submenu options.
3. Select **Ethernet Ports**.

The Ethernet Ports screen displays configuration, runtime status and statistics regarding the physical ports.

Tag Native VLAN

A green checkmark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.

Allowed VLANs

Displays the VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to Trunk.

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

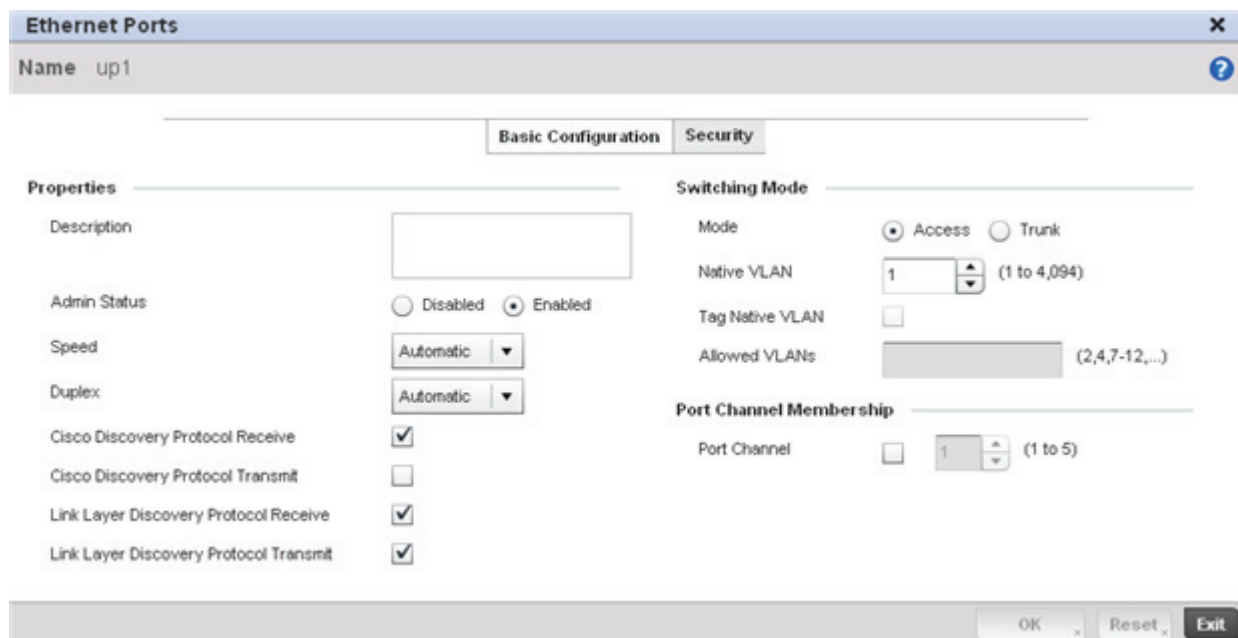


Figure 7-4 Ethernet Ports - Basic Configuration screen

- 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.
Cisco Discover Protocol Receive	Select the radio button to allow the Cisco discovery protocol for receiving data on this port.
Cisco Discover Protocol Transmit	Select the radio button to allow the Cisco discovery protocol for transmitting data on this port.
Link Layer Discovery Protocol Receive	Select this option to snoop LLDP on this port. The default setting is enabled.
Link Layer Discovery Protocol Transmit	Select this option to transmit LLDP PDUs on this port. The default setting is disabled.

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

Mode	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port. If <i>Access</i> is selected, the port accepts packets only from 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 <i>Trunk</i> , the port allows packets from a list of VLANs you add to the trunk. A port configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. <i>Access</i> is the default mode.
Native VLAN	Use the spinner control to define a numerical Native VLAN ID between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.

Tag Native VLAN

Select the radio button 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 to. 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.

8. Optionally select the **Port Channel** checkbox and define a setting between 1 - 8 using the spinner control. This sets the channel group for the port.
9. Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.
10. Select the **Security** tab.

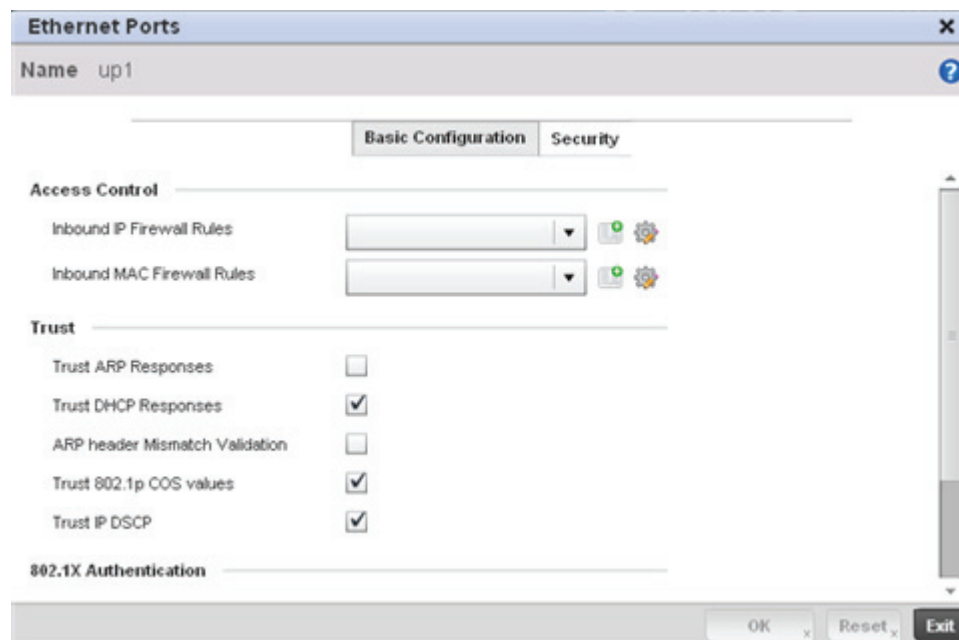


Figure 7-5 Ethernet Ports - Security screen

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

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

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

12. 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 8-2](#).

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

Trust ARP Responses	Select the radio button to enable ARP trust on this port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled.
Trust DHCP Responses	Select the radio button 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 the radio button to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
Trust 8021p COS values	Select the radio button to enable 802.1p COS values on this port. The default value is enabled.
Trust IP DSCP	Select the radio button 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.

14. Select the **Enable** checkbox within the **802.1x Authentication** field to enable a username and password pair to be used when authenticating users on this port.

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

7.2.2 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:

5. Select **Add** to define a new Virtual Interface configuration, **Edit** to modify the configuration of an existing Virtual Interface or **Delete** to permanently remove a selected Virtual Interface.

Figure 7-7 Virtual Interfaces - Basic Configuration screen

The **Basic Configuration** screen displays by default regardless of whether a new Virtual Interface is being created or an existing one is being modified.

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

8. Set the following network information from within the **IP Addresses** field:

Enable Zero Configuration	The AP-6511 can use Zero Config for IP assignments on an individual virtual interface basis. Select <i>Primary</i> to use Zero Config as the designated means of providing an IP address, this eliminates the means to assign one manually. Selecting <i>Secondary</i> is preferred when wanting the option to either use Zero Config or manual assignments.
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.

9. Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the Virtual Interface.
10. Select the **Respond to DHCP Relay Packets** option to allow the DHCP server to respond to relayed DHCP packets on this interface.

Provide IP addresses for DHCP server relay resources.

The interface VLAN and gateway should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to a DHCP Server. The interface VLAN and gateway interface cannot be the same.

11. 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 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 to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network.
- *None* - No NAT activity takes place. This is the default setting.



NOTE: Refer to [Setting the Profile's NAT Configuration on page 7-39](#) for instructions on creating a profile's NAT configuration.

-
-
12. Select **OK** button to save the changes to the Basic Configuration screen. Select **Reset** to revert to the last saved configuration.
 13. Select the **Security** tab.

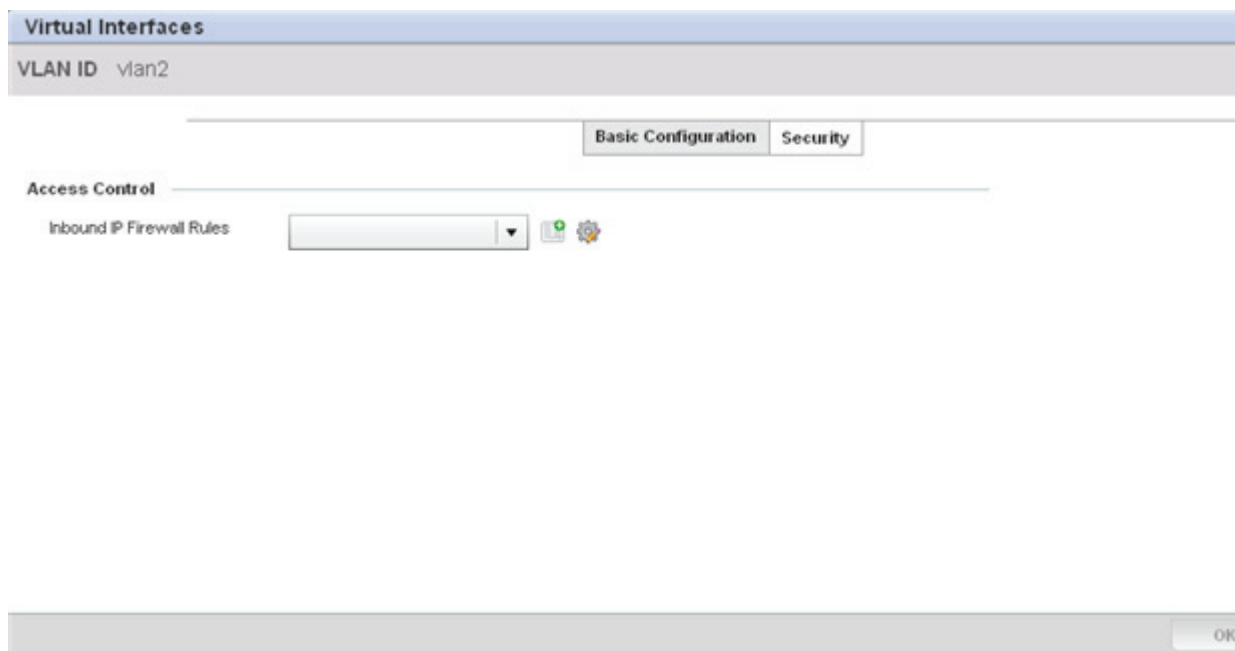


Figure 7-8 Virtual Interfaces - Security screen

14. Use the **Inbound IP Firewall Rules** drop-down menu to select the firewall rule configuration to apply to this Virtual Interface.

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 an existing configuration. For more information, see [Wireless Firewall on page 8-2](#).

15. 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.

7.2.3 Access Point Radio Configuration

► Profile Interface Configuration

An AP-6511 model Access Point can have its radio configurations modified by a connected controller once its radios have successfully associated to the network. Take care not to modify an Access Point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the Access Point having a configuration independent from the profile until the profile can be uploaded to the Access Point once again.

To define a Access Point radio configuration:

1. Select **Configuration > Profiles > Interface**.
2. Expand the Interface menu to display its submenu options.
3. Select **Radios**.

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

Figure 7-10 Access Point Radio - Radio Settings tab

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

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

- | | |
|-------------------------|---|
| Description | Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations. |
| Admin Status | Either select the Active or Shutdown radio button to define this radio's current status within the network. When defined as Active, 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 there's no existing suiting the radio's intended operation, select the Create icon to define a new QoS policy that can be applied to this profile. For more information, see Radio QoS Policy on page 6-48 . |
| 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 <i>Access Control List</i> (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. For more information, see Association ACL on page 6-52 . |

7. Set the following profile **Radio Settings** for the selected Access Point radio:

RF Mode	Set the mode to either 2.4 GHz WLAN or 5 GHz WLAN 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.
Lock Radio Band	Select the radio button to lock Smart RF 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 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.
Transmit Power	Set the transmit power of the selected Access Point radio. If using a dual or three radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value.
Antenna Gain	Set the antenna between 0.00 - 30.00 dBm. The access point's <i>Power Management Antenna Configuration File</i> (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. Motorola Solutions recommends 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. The default setting is dynamic based on the Access Point model deployed and its transmit power settings.
Dynamic Chain Selection	Select the radio button for the radio to dynamically change the number of transmit chains. This option is enabled by default.

Data Rates	Once the radio band is provided, the Data Rates drop-down menu populates with rate options depending on the 2.4 or 5 GHz band selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).
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 AP-6511 radio. The available range is between 1- 128.

8. 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 <i>Delivery Traffic Indication Messages</i> (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 Port) 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 (between 1 - 2,347 bytes) for use by the WLAN's adopted Access Point radios. RTS is a transmitting station's signal that requests a *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.
- Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold.
- Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.
- A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.
- Short Preamble** If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectralLink 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 the radio button to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

9. Select the **WLAN Mapping** tab.

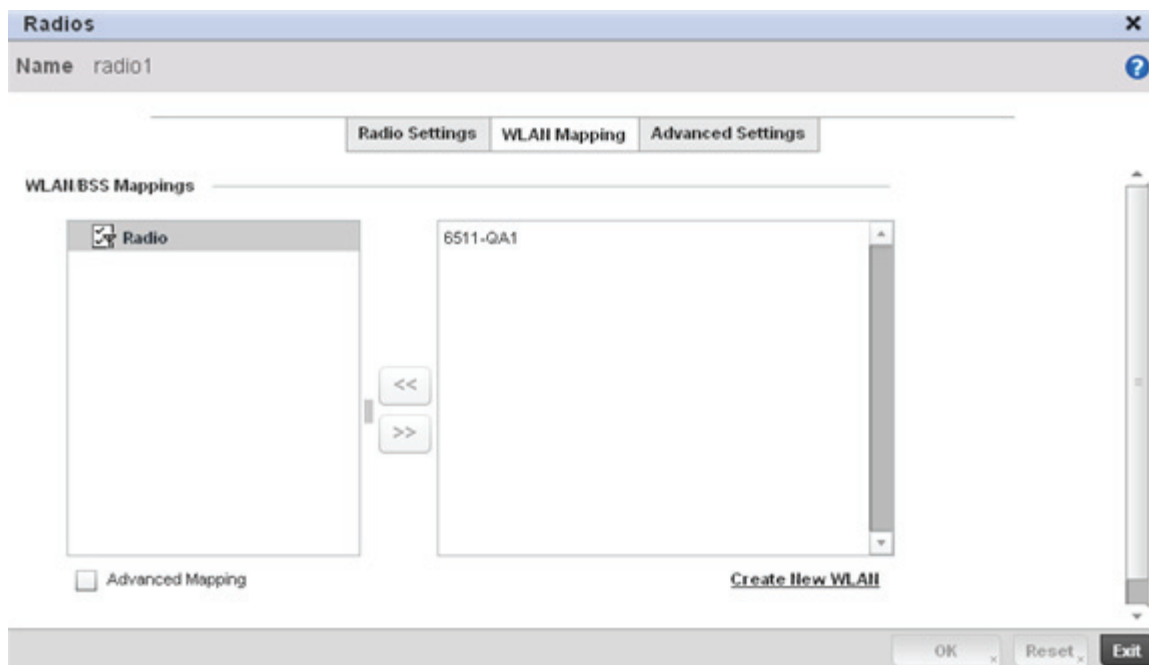


Figure 7-11 Access Point Radio - WLAN Mapping screen

10. Refer to the **WLAN/BSS Mappings** 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.

11. 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.

12. Select the **Advanced Settings** tab.

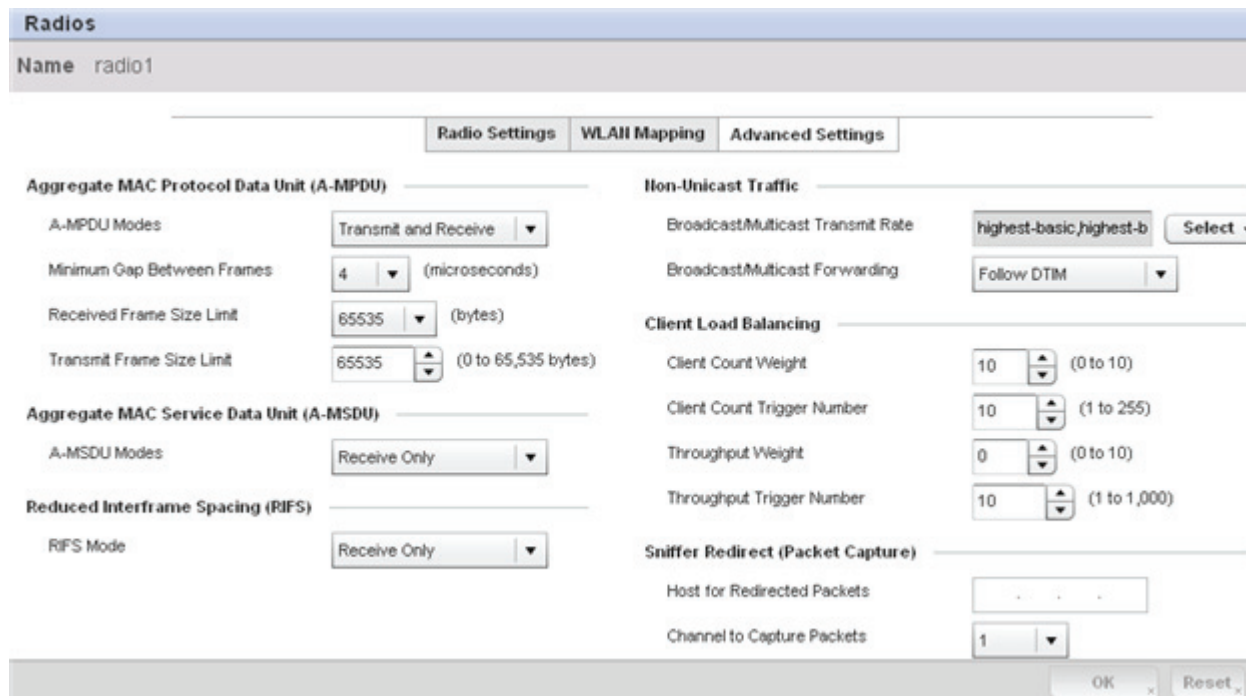


Figure 7-12 Access Point Radio - Advanced Settings screen

13. 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 4 microseconds.

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 between 0 - 65,535 bytes). The default value is 65535 bytes.

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

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

15. Define a **RIFS Mode** using the drop-down menu. This value determines whether interframe spacing is applied to Access Point 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.

16. 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.

17. Refer to the **Client Load Balancing Across APs** field to define how the Access Point radio supports clients based on a maximum count for the radio, a count trigger and throughput.

Client Count Weight Sets the client load per Access Point radio between 0 - 10. Motorola Solutions recommends considering the client load on an Access Point before defining its radio configuration. The higher the number of clients, the greater the strain on a radio's resources. The default weight is 10 clients. Setting the weight to 0 defines the weight as not considered.

Client Count Trigger Number The trigger value is the number of client association on the Access Point radio before load balancing is triggered. The configurable range is between 1 - 255. The default trigger client count is 10 clients.

Throughput Weight Set a throughput weight ratio on the Access Point radio between 0 - 10. the higher the value entered, the greater the anticipated load on the Access Point radio. The default throughput weight is 0.

Throughput Trigger Number When the average Access Point radio throughput exceeds the trigger number (as defined between 1 - 1,100), load balancing is initiated for the radio. The default throughput trigger number is 10.

18. 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.

19. 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.

7.2.4 Profile Interface Deployment Considerations

▶ Profile Interface Configuration

Before defining a profile's interface configuration (supporting Ethernet port, Virtual Interface, port channel and Access Point radio configurations) refer to the following deployment guidelines to ensure these configuration are optimally effective:

- When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when the AP-6511 is being accessed from a subnet not directly connected to the Access Point and the default route was set from DHCP.
- Take care not to modify an Access Point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the Access Point having a configuration independent from the profile until the profile can be uploaded to the Access Point once again.

7.3 Profile Network Configuration

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

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

- *Setting a Profile's DNS Configuration*
- *ARP*
- *Quality of Service (QoS)*
- *Static Routes*
- *Forwarding Database*
- *Bridge VLAN*
- *Miscellaneous Network 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 7-34*.

7.3.1 Setting a Profile's DNS Configuration

▶ *Profile 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. DNS is supported on an AP-6511 by dedicating DNS server resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (www.domainname.com).

To define the DNS configuration:

1. Select **Configuration** > **Profiles** > **Network**.
2. Expand the Network menu to display its submenu options.
3. Select **DNS**.

Figure 7-13 DNS screen

4. Provide a default **Domain Name** used when resolving DNS names. The name cannot exceed 64 characters.
5. Set the following DNS configuration data:

Enable Domain Lookup

Select the radio button to enable DNS. When enabled, human friendly domain names can be converted into numerical IP destination addresses. The radio button is selected by default.

6. In the **Name Servers** field, provide the IP addresses or hostnames of up to three DNS Server resources available to the AP-6511.
7. Select **OK** to save the changes made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

7.3.2 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 so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To define an ARP supported configuration:

1. Select **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options.
3. Select **ARP**.
4. Select **+ Add Row** from the lower right-hand side of the screen to populate the ARP table with rows used to define ARP network address information.

Address Resolution Protocol (ARP)

VLAN	IP Address	MAC Address	Device Type	
1	*	* 00 - 00 - 00 - 00 - 00 - 00	Host	

OK Reset

Figure 7-14 ARP screen

5. Set the following parameters to define the ARP configuration:

VLAN	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 (<i>Host, Router</i> or <i>DHCP Server</i>). Host is the default setting.

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

7.3.3 Quality of Service (QoS)

► Profile Network Configuration

The AP-6511 uses different *Quality of Service (QoS)* screens to define WLAN and device radio QoS configurations. The **Configuration > Profiles > Network** 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 that is applied to a packet.

To define an QoS configuration for DSCP mappings:

1. Select **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options
3. Select **Quality of Service (QoS)**.

Quality of Service (QoS)

DSCP Mapping

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

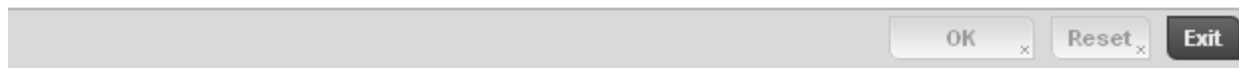


Figure 7-15 Profile QoS screen

4. 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

5. Use the spinner controls within the **802.1p Priority** field for each **DSCP** row to change its priority value.

6. 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.

7.3.4 Static Routes

► Profile Network Configuration

Use the **Static Routes** 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 create static routes:

1. Select **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options.
3. Select **Static Routes**.

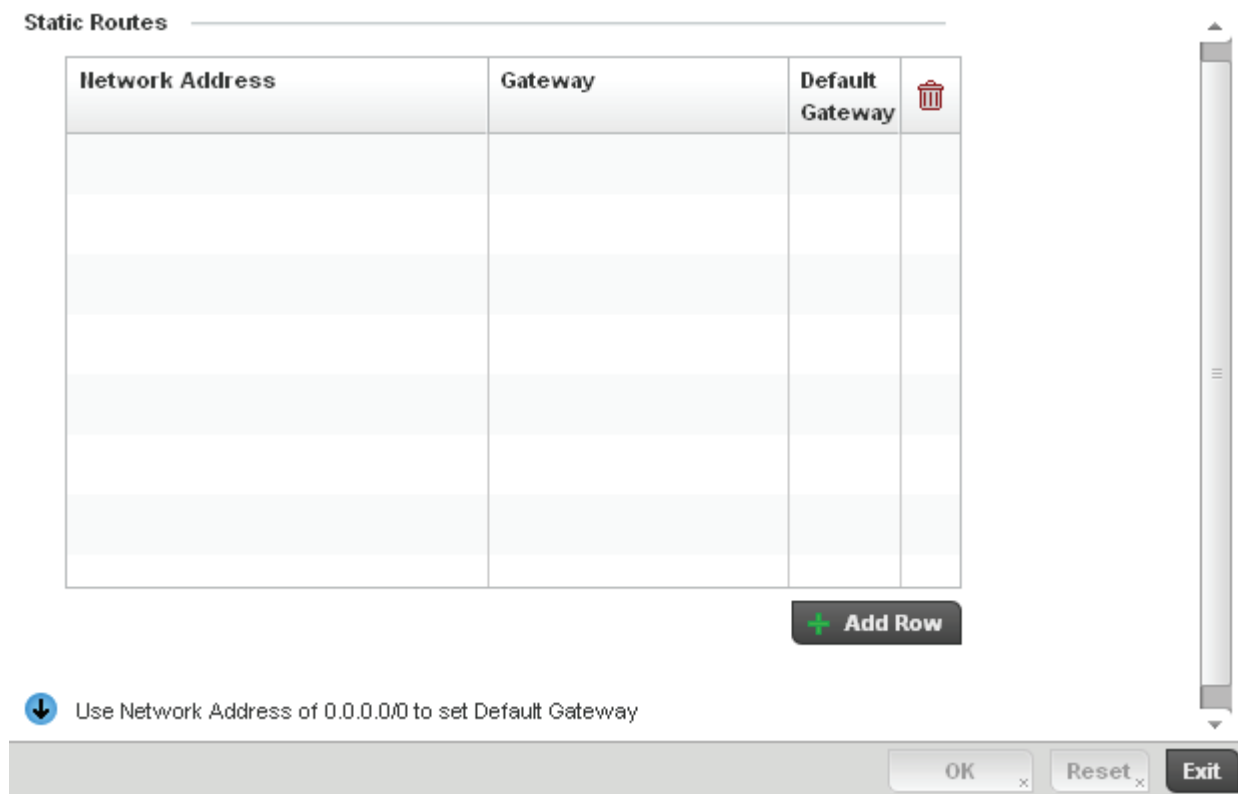


Figure 7-16 Static Routes screen

4. Select **Add Row +** as needed to include single rows in the static routes table.
5. Add IP addresses and network masks in the **Network** column.
6. Provide the **Gateway** used to route traffic.
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.

7.3.5 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 **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options.
3. Select **Forwarding Database**.

Aging Time _____

Bridge Aging Time (0,10-1000000 seconds)

Static Forwarding Table _____

MAC Address	VLAN Id	Interface Name	
* <input type="text" value="00 - 00 - 00 - 00 - 00 - 00"/>	* <input type="text"/>	* <input type="text"/>	

+ Add Row

OK **Reset** **Exit**

Figure 7-17 Forwarding Database screen

4. Define a **Bridge Aging Time** between 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 being deleted due to lack of activity. If an entry replenishes a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

5. Use the **+ Add Row** button to create a new row within the MAC address table.
6. Set a destination **MAC Address** address. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).
7. Define the target **VLAN ID** if the destination MAC is on a different network segment.
8. Provide an **Interface Name** used as the target destination interface for the target MAC address.
9. Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

7.3.6 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 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 device, but ignore the systems that aren't using same VLAN ID.

Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the Bridge VLAN forwards the data frame on the appropriate port(s). VLAN's are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. 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 **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options.
3. Select **Bridge VLAN**.
4. Review the following VLAN configuration parameters:

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 Response	When ARP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks.
Trust DHCP Responses	When DHCP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible within the network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.

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

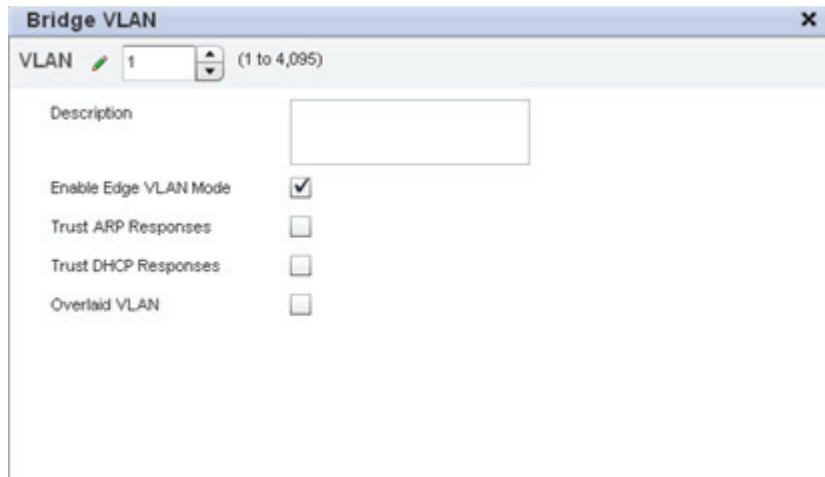


Figure 7-18 Bridge VLAN screen - General Tab

The **General** tab displays by default.

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

Description	If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
Enable Edge VLAN Mode	Select the radio button to enable edge VLAN mode. When selected, the IP address in the VLAN is not used for normal operations, as its now designated to isolate devices and prevent connectivity. This feature is enabled by default.
Trust ARP Response	Select the radio button 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 the radio button 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.
Overlaid VLAN	Select this checkbox to separate this VLAN from the wired VLAN. This feature is disabled by default.

8. 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.

7.3.7 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 a hostnames in DHCP request:

1. Select **Configuration > Profiles > Network**.
2. Expand the Network menu to display its submenu options
3. Select **Miscellaneous**.

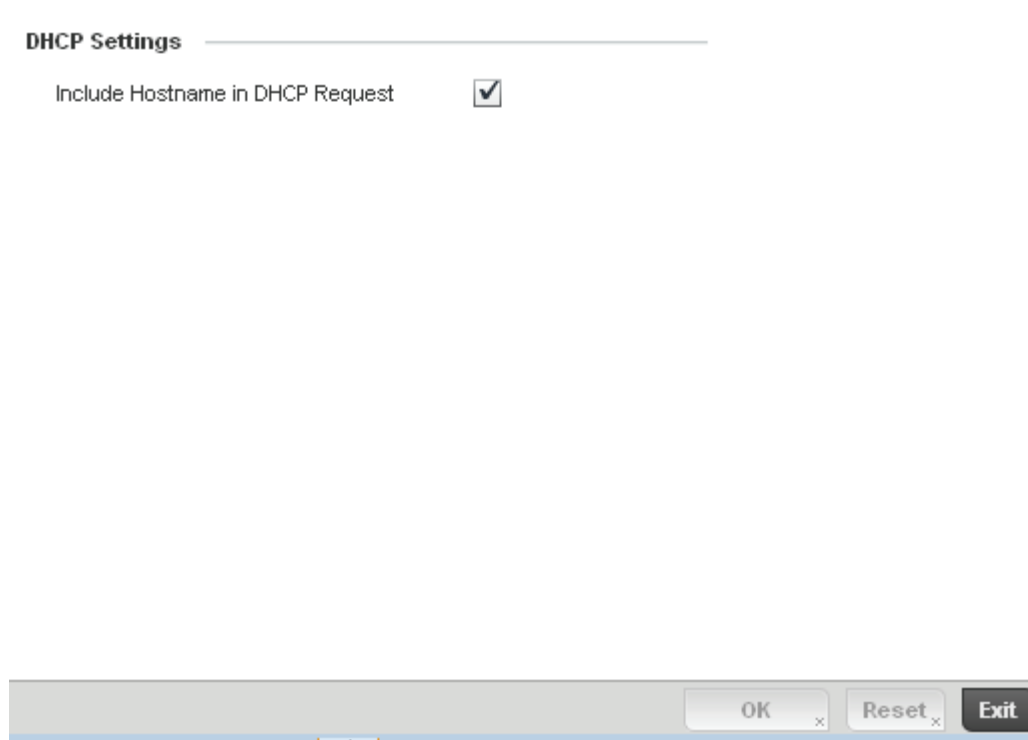


Figure 7-19 Profile Miscellaneous screen

4. Select the **Include Hostname in DHCP Request** checkbox to include a hostname in a DHCP lease for a requesting device. This feature is disabled by default.
5. Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

7.3.8 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 needing to be configured. If you have N number of routers and a route between each router is needed, then you must configure $N \times N$ routes. Thus, for a network with nine routers, you'll need a minimum of 81 routes ($9 \times 9 = 81$).

7.4 Profile Security Configuration

An Access Point profile can have its own firewall policy, wireless client role policy, WEP shared key authentication and NAT policy applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can be navigated from the **Configuration > Profiles** section of the UI to the **Configuration > Security** portion of the UI to create the required security policy configuration. Once created, separate policies can be applied to the profile to best support the data protection and security requirements in respect to the Access Point model supported by the profile.

For more information, refer to the following sections:

- [Defining Profile Security Settings](#)
- [Setting the Certificate Revocation List \(CRL\) Configuration](#)
- [Setting the Profile's NAT Configuration](#)

7.4.1 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 that profile.

To define a profile's security settings:

1. Select the Configuration tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Security**.
5. Select **Settings**.

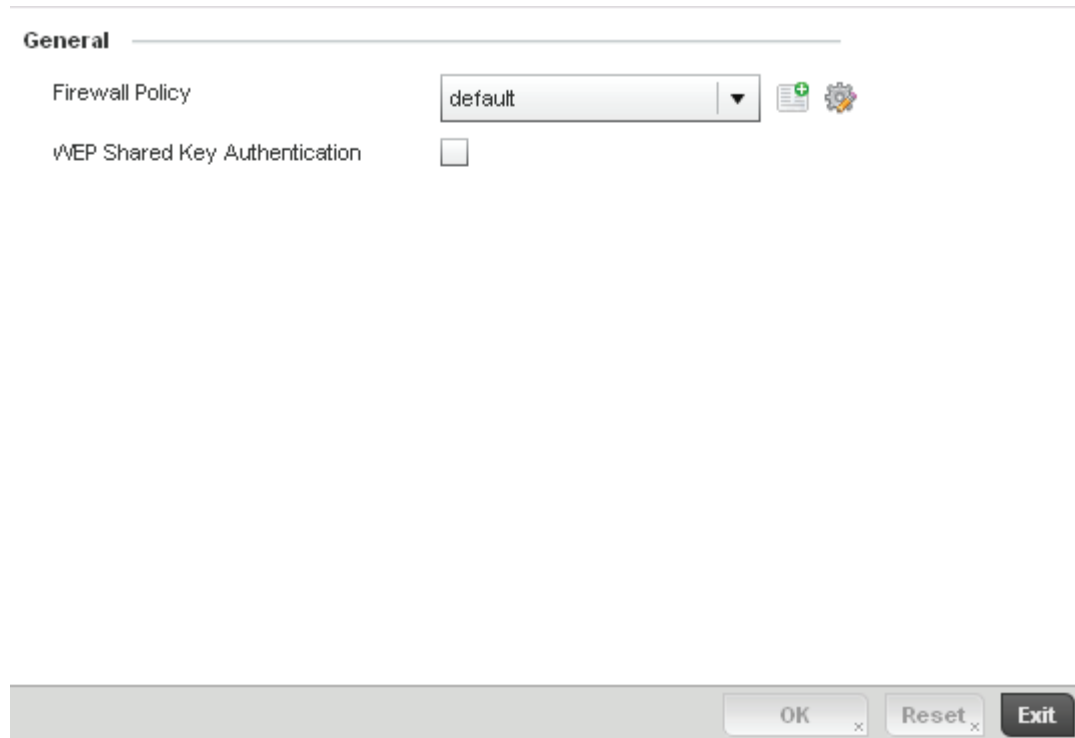


Figure 7-20 Profile Security - Settings screen

6. Refer to the **General** field to assign or create the following security policy's to the profile:

Firewall Policy

Use the drop-down menu to select an existing Firewall Policy to use as an additional security mechanism with this profile. All devices using this profile must meet the requirements of the firewall policy to access the network. A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both 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. For more information, see [Wireless Firewall on page 8-2](#) and [Configuring a Firewall Policy on page 8-2](#).

WEP Shared Key Authentication

Select the radio button to require devices using this profile to use a WEP key to access the network using this profile. The Access Point, other proprietary routers, and Motorola clients use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without Motorola adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

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

7.4.2 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 **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Security**.
5. Select **Certificate Revocation**.

Certificate Revocation List (CRL) Update Interval

Trustpoint Name	URL	Hours	
 <input type="text"/>	<input type="text"/>	 1 	
			

 **Add Row**


OK  **Reset** **Exit**

Figure 7-21 Security 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.

- a. Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.
- b. Enter the resource ensuring the trustpoint's legitimacy within the URL field.
- c. Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.

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

7.4.3 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 AP-6511. 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 **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Security**.
5. Select **NAT**.

Figure 7-23 Security NAT Pool screen

7. 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.
Prefix Length	Use the spinner control to set the netmask (between 1 - 30) of the network the pool address belongs to.
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.

8. Select the **+ Add Row** button as needed to append additional rows to the IP Address Range table.
9. Select **OK** to save the changes made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.
10. Select the **Static NAT** tab.
The Source tab displays by default.

IIAT Pool Static IIAT Dynamic IIAT

Source Destination

Source

Source IP	IIAT IP	Network	
*	*	*	

+ Add Row

OK Reset Exit

Figure 7-24 Static NAT screen

11. To map a source IP address from an internal network to a NAT IP address click the **+ Add Row** button. Enter the internal network IP address in **Source IP** field. Enter the NAT IP address in the **NAT IP** field.
12. Use the **Network** drop-down menu to set the NAT type either *Inside* or *Outside*. 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.

IAT Pool Static IAT Dynamic IAT

Source Destination

Protocol	Destination IP	Destination Port	IAT IP	IAT Port	Network
UDP	157.235.223.42	1	157.235.255.245	53	inside

Row Count: 1

Add Edit Delete Exit

Figure 7-25 NAT Destination screen

14. Select **Add** to create a new NAT destination configuration, **Edit** to modify the attributes of an existing configuration or **Delete** to permanently remove a NAT destination.

Destination
✕

Add Destination NAT
?

Settings

Protocol ★

Destination IP ★

Destination Port ★ (1 to 65,535)

NAT IP ★

NAT Port (1 to 65,535)

Network ★

OK Reset Exit

Figure 7-26 NAT Destination Add screen

15. 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 available options. TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The <i>User Datagram Protocol</i> (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. Inside is the default setting.

16. Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

17. 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.

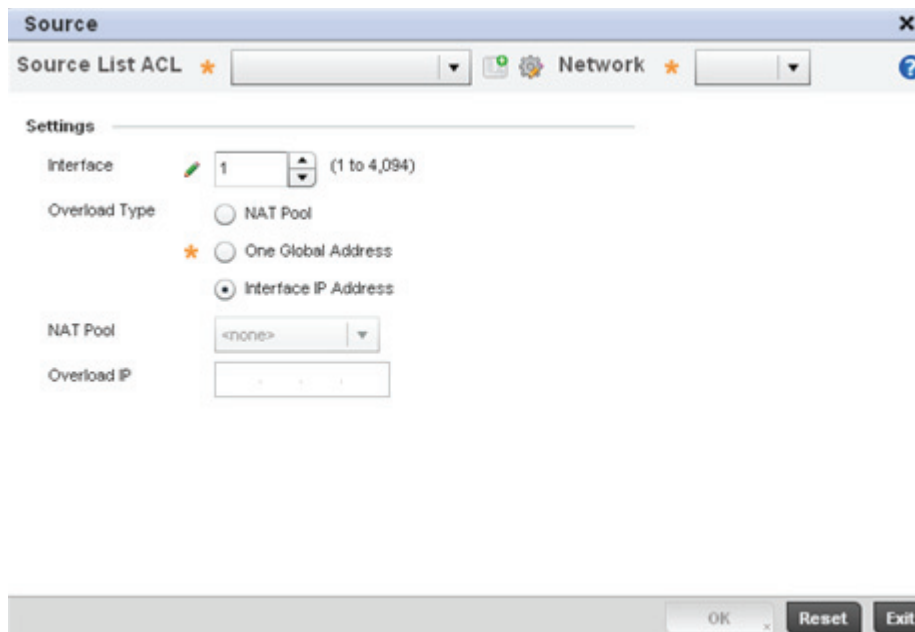


Figure 7-28 Source ACL List screen

20. 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) 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.
- Interface** Use the drop-down menu to select the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
- Overload Type** Select the radio button of Overload Type used with the listed IP ACL rule. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.
- NAT Pool** Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
- Overload IP** Enables the use of one global address for numerous local addresses.

21. Select **OK** to save the changes made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

7.4.4 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.

7.5 Profile Services Configuration

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 a profile's services configuration:

1. Select the Configuration tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Services**.

Captive Portal Hosting

Captive Portal Policies

[Create](#)

DHCP Server

DHCP Server Policy

OK x Reset x Exit

Figure 7-29 Profile 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 AP-6511 managed network. The primary means of securing such guest access is a hotspot.

A captive portal policy's hotspot configuration provides secure authenticated access using a standard Web browser. Hotspots 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 hotspot, additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on the hotspot'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 this profile. For more information, see [Configuring Captive Portal Policies on page 9-2](#).

6. Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP policy. If an existing DHCP policy does not meet the profile's requirements, select the **Create** button to create a new policy configuration that can be applied to this profile.

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after a pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

Either select an existing captive portal policy or select the **Create** button to create a new captive portal configuration that can be applied to this profile. Existing policies can be modified by selecting the **Edit** icon. For more information, see [Setting the DHCP Server Configuration on page 9-14](#).

7. Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

7.5.1 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.

7.6 Profile Management Configuration



The AP-6511 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 **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Management**.
5. Expand the Management menu item to display additional *Settings*, *Firmware* and *Heartbeat* Management options.
6. Select **Settings** from the Management menu.

Management Policy

Management Policy  

Message Logging

Enable Message Logging 

Remote Logging Host

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

Facility to Send Log Messages

Syslog Logging Level

Console Logging Level

Buffered Logging Level

Time to Aggregate Repeated Messages (0 to 60)

Forward Logs to Controller

System Event Messages

Enable System Events

Enable System Event Forwarding

Figure 7-30 Profile Management Settings screen

7. Refer to the **Management Policy** field to select or set a management configuration for use with this profile. A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If no management policies exist meeting the data access requirements of this profile, select the **Create** icon to access a series of screens used to define administration, access control and SNMP configurations. Select an existing policy and select the **Edit** icon to modify the configuration of an existing management policy. For more information, see [Viewing Management Access Policies on page 10-2](#).

8. Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to discern an overall pattern that may be negatively impacting performance using the configuration defined for this profile.

Enable Message Logging	Select the radio button 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 as needed 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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . 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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . 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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . The default logging level is 4.
Time to Aggregate Repeated Messages	Define the interval (duration) system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged. Either define an interval in Seconds (0 - 60) or Minutes (0 -1). The default value is 0 seconds.
Forward Logs to Controller	Select the checkbox to define a log level for forwarding event logs to the control. Log levels include <i>Emergency</i> , <i>Alert</i> , <i>Critical</i> , <i>Error</i> , <i>Warning</i> , <i>Notice</i> , <i>Info</i> and <i>Debug</i> . The default logging level is Error.

9. Refer to the **System Event Messages** field to define 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's important to log individual events to discern an overall pattern that may be negatively impacting performance. This settings 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.

10. Select **OK** to save the changes made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.

11. Select **Firmware** from the Management menu.

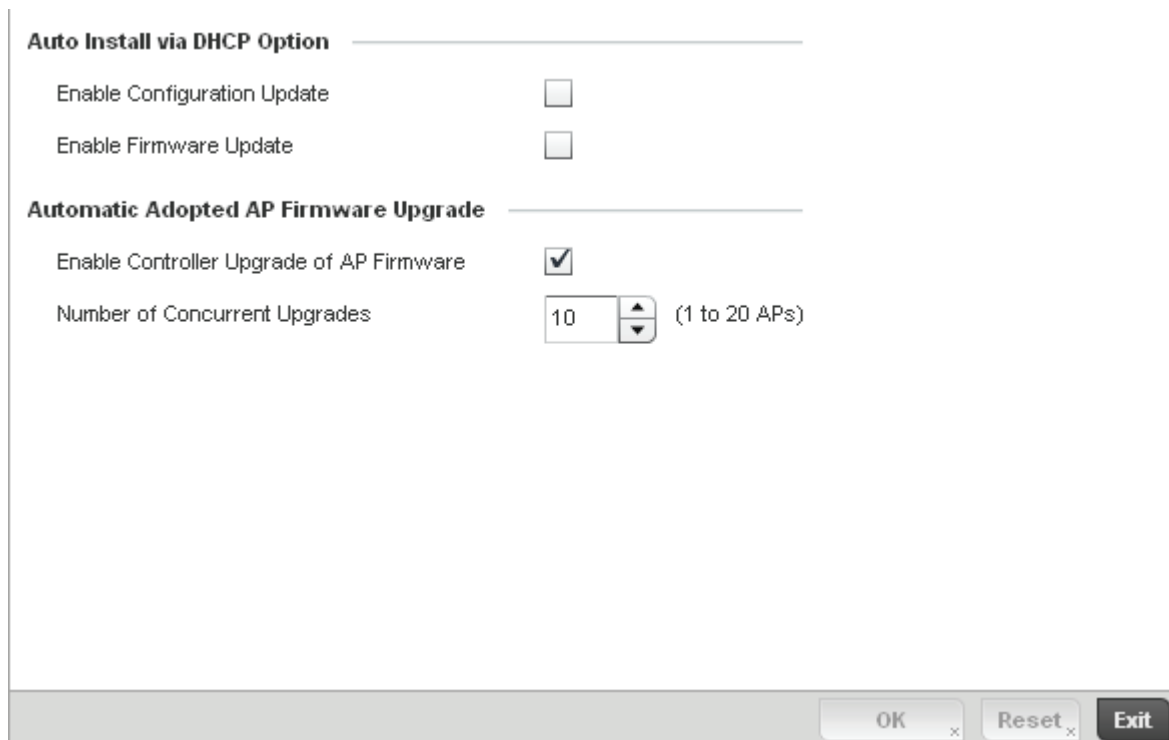


Figure 7-31 Profile Management Firmware screen

12. Refer to the **Auto Install via DHCP** field to define the configuration used by the profile to update firmware using DHCP:

Enable Configuration Upgrade

Select this option to enable automatic configuration file updates for the profile from an external location. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update. 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 Upgrade

Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. 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.

13. Use the parameters within the **Automatic Adopted AP Firmware Upgrade** field to define an automatic firmware configuration.

Enable Controller Upgrade of AP Firmware

Select this option to enable adopted Access Point radios to upgrade to a newer firmware version using its associated controller's most recent firmware file for that AP model. This parameter is disabled by default.

Number of Concurrent Upgrades.

Use the spinner control to define the maximum number (1 - 20) of adopted APs that can receive a firmware upgrade at the same time. Keep in mind that, during a firmware upgrade, the AP 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 made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.

15. Select the **Heartbeat** option from the Management menu.

Device Heartbeat Settings

Service Watchdog

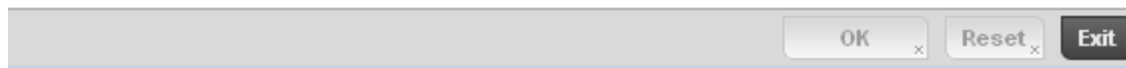


Figure 7-32 Profile Management Heartbeat screen

16. 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.

17. Select **OK** to save the changes made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

7.6.1 Profile Management Configuration and Deployment Considerations

► Profile Management Configuration

Before defining a 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.
- Motorola Solutions recommends SNMPv3 be used for management profile configurations, as it provides both encryption, and authentication.

7.7 Miscellaneous 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 users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection.

To set a profile's advanced configuration:

1. Select the Configuration tab from the Web UI.
2. Select **Profiles** from the Configuration tab.
3. Either select **Add** if creating a new profile or **Edit** if modifying the configuration on an existing profile.
4. Select **Miscellaneous**.

Device RADIUS Authentication Parameters _____

NAS-Identifier Attribute

NAS-Port-Id Attribute

LEDs (Light Emitting Diodes) _____

Turn on LEDs



Figure 7-33 Profile Miscellaneous screen

5. Set a **NAS-Identifier Attribute** up to 253 characters in length.
This is the RADIUS NAS-Identifier attribute that typically identifies the Access Point where a RADIUS message originates.
6. 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.
7. Select the **Turn on LEDs** option to keep the AP-6511's functioning as normal. Some deployments (hospitals for example) prefer to keep an Access Point's LED from illuminating, so consider this option when creating the profile configuration.

8. Select **OK** to save the changes made to the profile's Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

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 its entirety, since the chain is as weak as its weakest link. A Motorola 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 AP-6511 managed network, including:

- *Wireless Firewall*
- *Intrusion Prevention*

8.1 Wireless Firewall

A Firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the Motorola wireless 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 wireless network. Firewalls implement uniquely defined 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, and in fact could provide a false sense of network security.

With Motorola RFS series wireless controllers, Firewalls are configured to protect against unauthenticated logins from outside the wireless network. This helps prevent hackers from accessing wireless clients within the wireless network. Well designed Firewalls block traffic from outside the wireless controller managed network, but permit authorized users to communicate freely with outside the wireless network.

Firewalls can be implemented in both hardware and software, or a combination of both. All messages entering or leaving the wireless network pass through the Firewall, which examines each message and blocks those not meeting the security criteria (rules) defined by the configuration.

Firewall rules define the traffic permitted or denied within the wireless network. Rules are processed by a Firewall device from first to last. When a rule matches the network traffic a wireless controller is processing, the Firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. For example, if the 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:

- [Configuring a Firewall Policy](#)
- [Configuring IP Firewall Rules](#)
- [Configuring MAC Firewall Rules](#)
- [Firewall Deployment Considerations](#)

8.1.1 Configuring a Firewall Policy

► [Wireless Firewall](#)

To configure a Firewall:

1. Select **Configuration** > **Security** > **Wireless Firewall** to display existing Firewall policies.

The **Wireless Firewall** screen lists those Firewall policies created thus far. Any of these policies can be selected and applied. The user has the option of displaying the configurations of each Wireless Firewall Policy defined thus far, or referring to the **Wireless Firewall Browser** and either selecting individual policies.

Wireless Firewall ?		
Firewall Policy ⬆	Status	Proxy ARP
default	✓ Enabled	✓

Type to search in tables Row Count: 1

Add **Edit** **Delete**

Figure 8-1 Wireless Firewall screen

- Refer to the following configuration data for existing wireless Firewall policies:

Firewall Policy	Displays the name assigned to the Wireless Firewall policy when it was initially created. the name cannot be modified as part of the edit process.
Status	Displays a green check mark if the Wireless Firewall policy has been enabled. A red "X" designates the policy as disabled.
Proxy ARP	Displays a green check mark if Proxy ARP routing functions for the Wireless Firewall policy has been enabled. A red "X" designates Proxy ARP as disabled.

- Select **Add** to create a new Wireless Firewall policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available.
- When adding a new policy, first enter a name in the Firewall Policy field. The name must not exceed 64 characters. Once a name has been specified, click **OK** to enable the other parameters within the screen.

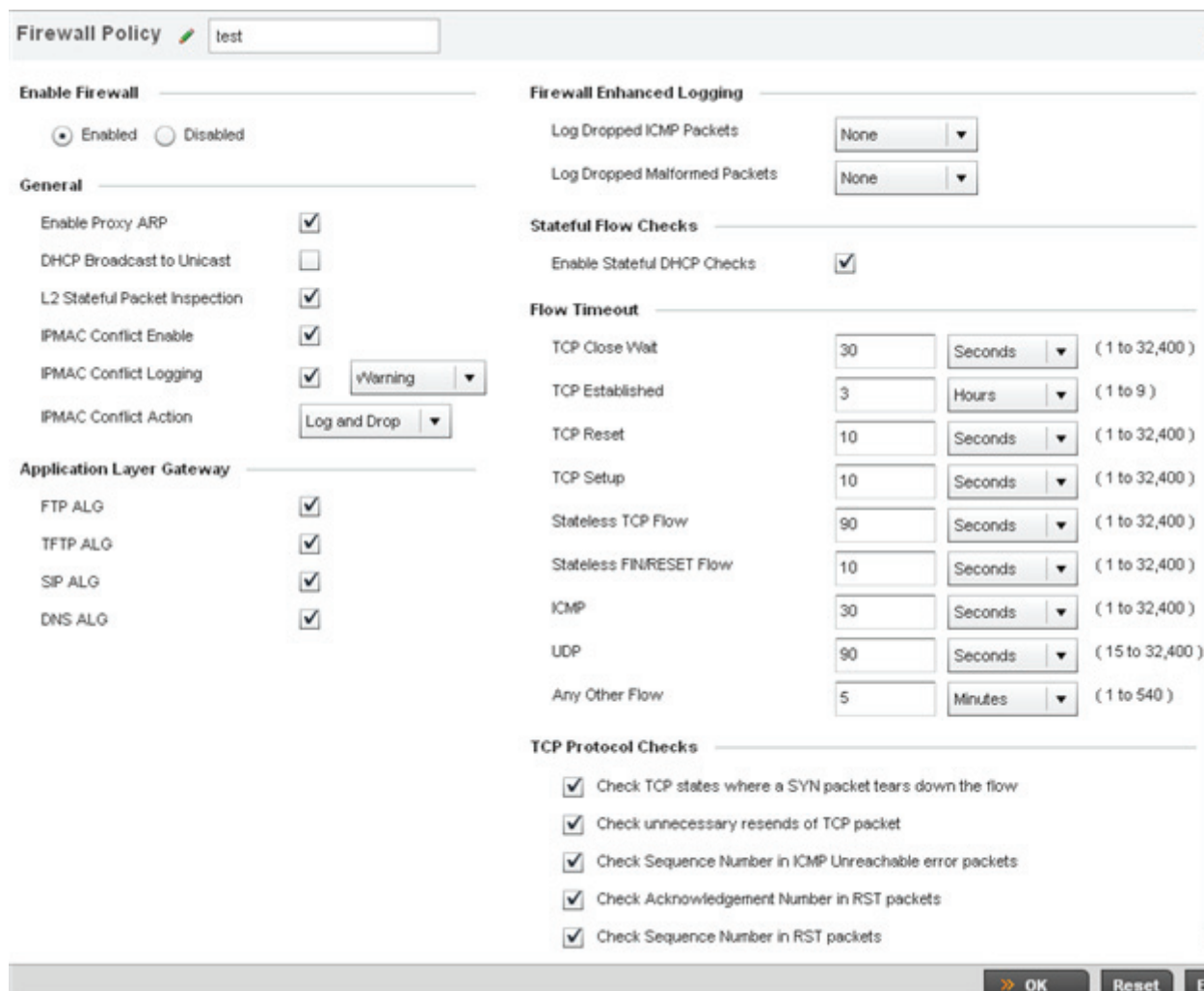


Figure 8-2 Wireless Firewall Policy Configuration screen

5. Refer to the **Enable Firewall** 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.

6. Refer to the **General** field to enable or disable the following Firewall configuration 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 disabled 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 (<i>Error, Warning, Notification, Information</i> or <i>Debug</i>) if an attack is detected. The default setting is <i>Warning</i> . |
| IPMAC Conflict Action | Use the drop-down menu to set the action taken when an attack is detected. Options include <i>Log Only, Drop Only</i> or <i>Log and Drop</i> . The default setting is <i>Log and Drop</i> . |
7. The Firewall policy allows traffic filtering at the application layer using the **Application Layer Gateway (ALG)** feature. The Application Layer Gateway provides filters for the following common protocols:
- | | |
|-----------------|---|
| FTP ALG | Check the Enable box to allow FTP traffic through the Firewall using its default ports. This feature is enabled by default. |
| TFTP ALG | Check the Enable box to allow TFTP traffic through the Firewall using its default ports. This feature is enabled by default. |
| SIP ALG | Check the Enable box to allow SIP traffic through the Firewall using its default ports. This feature is enabled by default. |
| DNS ALG | Check the Enable box to allow DNS traffic through the Firewall using its default ports. This feature is enabled by default. |
8. 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 <i>Rate Limited, All</i> or <i>None</i> . The default setting is <i>None</i> . |
| 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 <i>Rate Limited, All</i> or <i>None</i> . The default setting is <i>None</i> . |
9. 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.
10. Define **Flow Timeout** intervals for the following flow types impacting the Firewall:
- | | |
|------------------------|---|
| TCP Close Wait | Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 30 seconds. |
| TCP Established | Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10,800 seconds. |
| TCP Reset | Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds. |
| TCP Setup | Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds. |

Stateless TCP Flow	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 90 seconds.
Stateless FIN/RESET Flow	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 10 seconds.
ICMP	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 30 seconds.
UDP	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 90 seconds.
Any Other Flow	Define a flow timeout value in either <i>Seconds</i> (1 - 32,400), <i>Minutes</i> (1 - 540) or <i>Hours</i> (1 - 9). The default setting is 5 seconds.

11. 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 radio button 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 radio button 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 radio button 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 radio button 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 radio button to check the sequence number in RST packets which abort an established TCP flow. The default setting is enabled.

12. Select **OK** to update the Firewall Policy Advanced Settings. Select **Reset** to revert to the last saved configuration.

8.1.2 Configuring IP Firewall Rules

► Wireless Firewall

Devices use IP 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.

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.



NOTE: Once defined, a set of IP Firewall rules must be applied to an interface to be a functional filtering tool.

To add or edit an IP based Firewall Rule policy:

1. Select **Configuration** > **Security IP Firewall Rules** to display existing IP Firewall Rule policies.

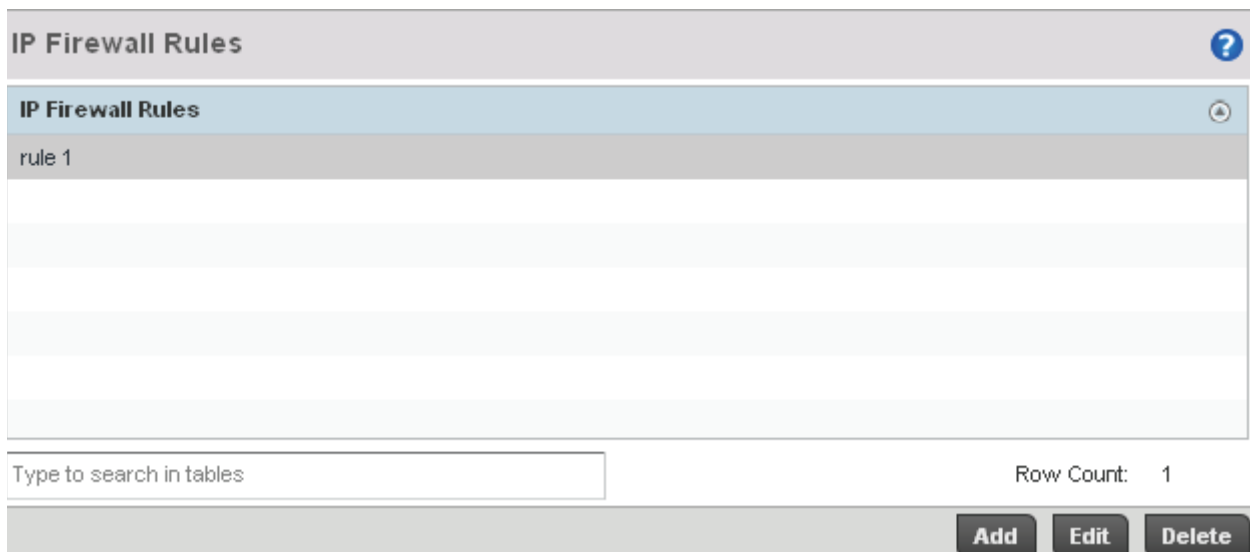


Figure 8-3 IP Firewall Rules screen

2. Select **+ Add Row** to create a new IP Firewall Rule. Select an existing policy and click **Edit** to modify the attributes of the rule's configuration.
3. Select the added row to expand it into configurable parameters for defining the rule.

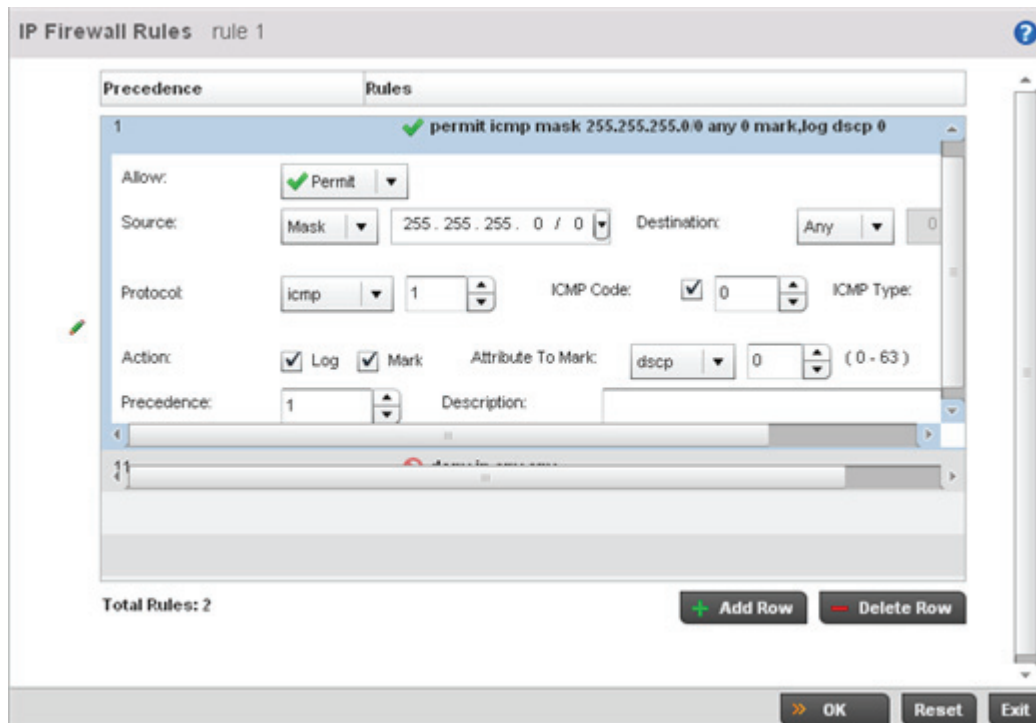


Figure 8-4 IP Firewall Rules Add screen

4. If adding a new rule, provide a name up to 32 characters in length.
5. Define the following parameters for the IP Firewall Rule:

Allow

Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with a 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

Enter both **Source** and **Destination** IP addresses. The Access Point uses the source IP address, destination IP address and IP protocol type as basic matching criteria. The access policy filter can also include other parameters specific to a protocol type (like source and destination port for TCP/UDP protocol. Provide a subnet mask if needed.

Protocol

Select the protocol used with the IP rule from the drop-down menu. IP is selected by default. Selecting ICMP displays an additional set of ICMP specific Options for ICMP Type and code. Selecting either TCP or UDP displays an additional set of specific TCP/UDP source and destinations port options.

Action	The following actions are supported: <i>Log</i> —Events are logged for archive and analysis. <i>Mark</i> —Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. - VLAN 802.1p priority. - DSCP bits in the IP header. - TOS bits in the IP header. <i>Mark, Log</i> — Conducts both mark and log functions.
Precedence	Use the spinner control to specify a precedence for this IP policy between 1-1500. Rules with lower precedence are always applied first to packets.
Description	Provide a description to help differentiate it from others with similar configurations.

6. Select **+ Add Row** as needed to add additional IP Firewall Rule configurations. Select the **- Delete Row** icon as required to remove selected IP Firewall Rules.
7. Select **OK** when completed to update the IP Firewall rules. Select **Reset** to revert the screen back to its last saved configuration.

8.1.3 Configuring MAC Firewall Rules

► Wireless Firewall

Devices 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 > Security > MAC Firewall Rules** to display existing MAC Firewall Rule policies.

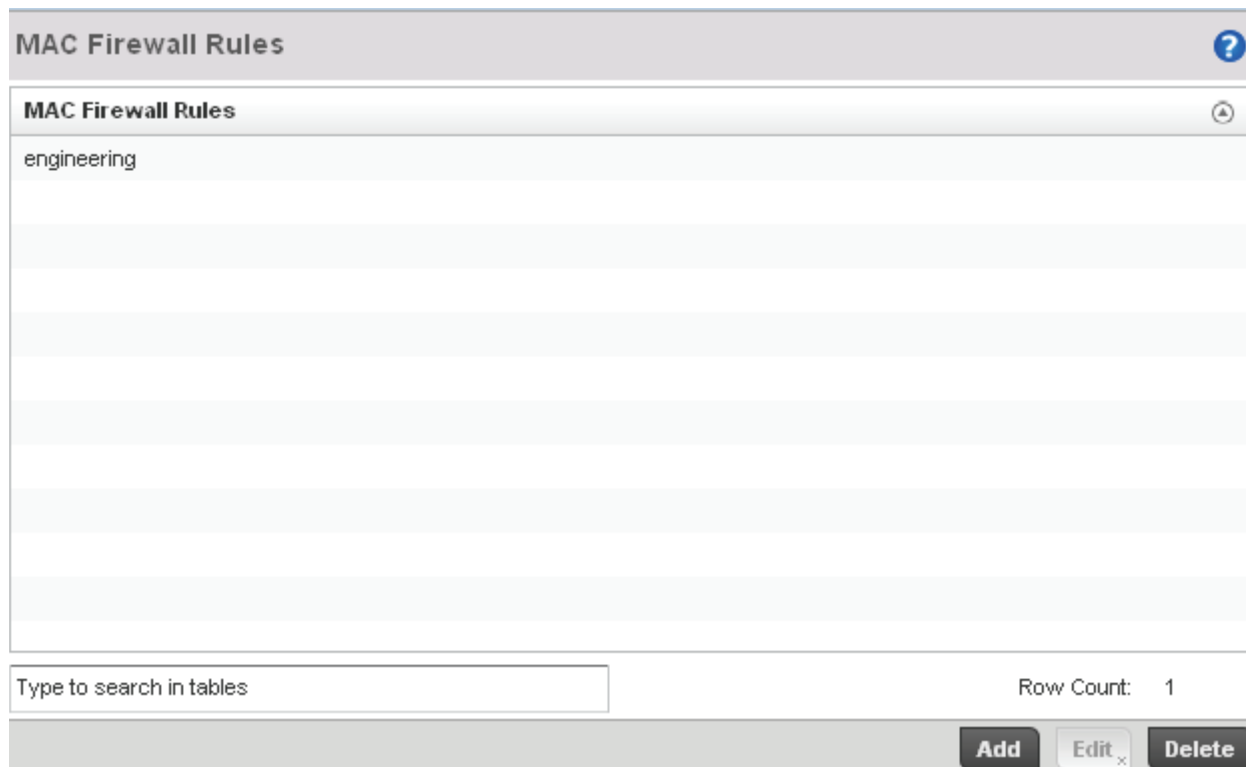


Figure 8-5 MAC Firewall Rules screen

2. Select **+ Add Row** to create a new MAC Firewall Rule. Select an existing policy and click **Edit** to modify the attributes of the rule's configuration.
3. Select the added row to expand it into configurable parameters for defining the MAC based Firewall rule.

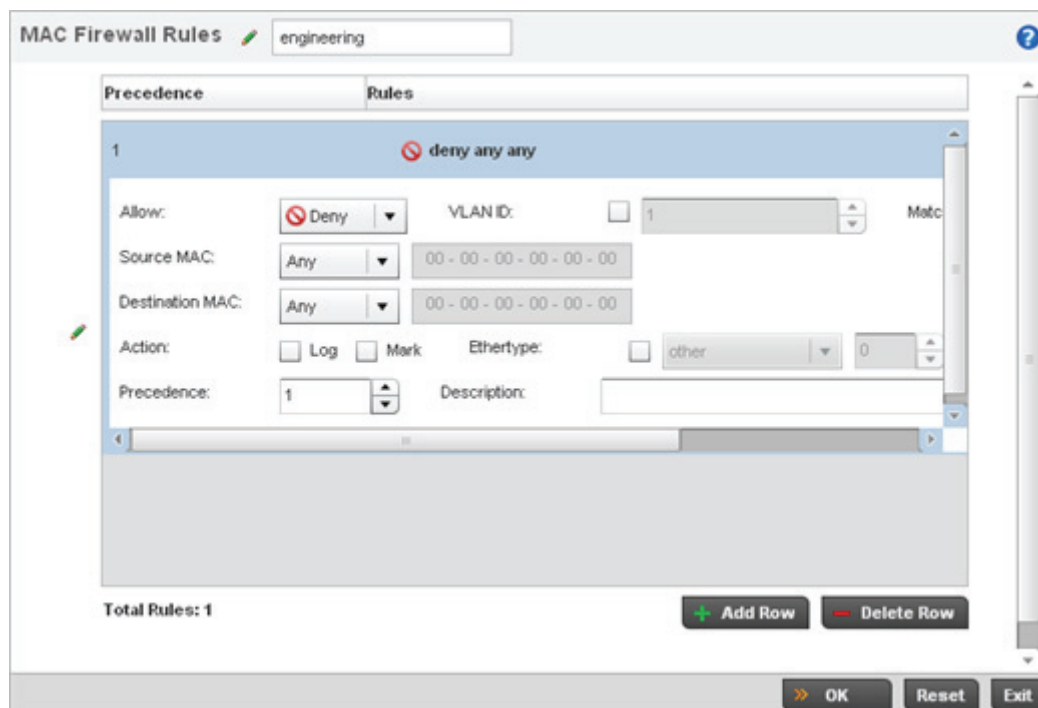


Figure 8-6 MAC Firewall Rules screen

4. If adding a new **MAC Firewall Rule**, provide a name up to 32 characters in length.
5. Define the following parameters for the IP Firewall Rule:

Allow	Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: <i>Deny</i> — Instructs the Firewall to not to allow a packet to proceed to its destination. <i>Permit</i> —Instructs the Firewall to allow a packet to proceed to its destination.
Source and Destination MAC	Enter both Source and Destination MAC addresses. Devices use the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.
Action	The following actions are supported: <i>Log</i> —Events are logged for archive and analysis. <i>Mark</i> —Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. - VLAN 802.1p priority. - DSCP bits in the IP header. - TOS bits in the IP header. <i>Mark, Log</i> — Conducts both mark and log functions.
Precedence	Use the spinner control to specify a precedence for this MAC Firewall rule between 1-1500. Rules with lower precedence are always applied first to packets.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the RADIUS server). The VLAN ID can be between 1 and 4094.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0-7.
Ethertype	Use the drop-down menu to specify an Ethertype of either ipv6, arp, wisp, monitor 8021q. An EtherType is a two-octet field within an Ethernet frame. It's 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.

6. Select **+ Add Row** as needed to add additional MAC Firewall Rule configurations. Select the **- Delete Row** icon as required to remove selected MAC Firewall Rules.
7. Select **OK** when completed to update the MAC Firewall Rules. Select **Reset** to revert the screen back to its last saved configuration.

8.1.4 Firewall Deployment Considerations

► Configuring a Firewall Policy

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.
- 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 Hotspot guest access. Firewall policies should be applied to Hotspot enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.

8.2 Intrusion Prevention

The AP-6511 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 AP-6511 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 support is not supported natively by an AP-6511 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 APs. WIPS identifies threatening versus non-threatening APs by segregating APs attached to the network (unauthorized APs) from those not attached to the network (neighboring APs). 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 APs.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues through 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.

8.2.1 Configuring a WIPS Policy

► *Intrusion Prevention*

To define a WIPS configuration:

1. Select **Configuration > Security > WIPS Policy**

The Wireless IPS screen lists those WIPS policies created thus far. Any of these existing WIPS policies can be selected and applied.

Wireless IPS ?		
WIPS Policy ⬆	Status	Interval to Throttle Duplicates
Moto-do-not delete	✔ Enabled	10m 0s

Type to search in tables Row Count: 1

Add **Edit** **Delete**

Figure 8-7 Wireless IPS screen

2. Refer to the following configuration data for existing Wireless IPS policies:

WIPS Policy	Displays the name assigned to the WIPS policy when it was initially created. The name cannot be modified as part of the edit process.
Status	Displays a green checkmark if the listed WIPS policy is enabled and ready for use with a profile. A red "X" designated the listed WIPS policy as disabled.
Interval to Throttle Duplicates	Displays the duration in seconds when traffic meeting the criteria defined in the selected WIPS policy is prevented/throttled.

3. Select **Add** to create a new WIPS policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

If adding or editing an existing WIPS policy, the WIPS Policy screen displays with the *Settings* tab displayed by default.

WIPS Policy Moto-do-not delete

Settings | WIPS Events | WIPS Signatures

Wireless IPS Status

Status Enabled Disabled

Duplicate Events

Interval to Throttle Duplicates Minutes (1 to 1,440)

Rogue AP Detection

Enable Rogue AP Detection

Wait Time to Determine AP Status Minutes (1 to 10)

Ageout for AP Entries Minutes (1 to 1,440)

OK Reset Exit

Figure 8-8 WIPS Policy screen - Settings tab

- If creating a new **WIPS Policy**, assign it name to help differentiate it from others that may have a similar configuration. The policy name cannot exceed 64 characters. The name cannot be modified as part of the edit process.
- Within the **Wireless IPS Status** field, select either the **Enabled** or **Disabled** radio button to either activate or de-activate the WIPS policy for use with a profile. The default setting is disabled.
- Enter the **Interval to Throttle Packets** in either *Seconds* (1 - 86,400), *Minutes* (1 - 1,400), *Hours* (1 - 24) or *Days* (1). This interval represents the duration event duplicates are *not* stored in history. The default setting is 120 seconds.
- Refer to the **Rogue AP Detection** field to define the following detection settings for this WIPS policy:

Enable Rogue AP Detection	Select the checkbox 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 <i>Seconds</i> (10 - 600) or <i>Minutes</i> (1 - 10) before a detected AP is interpreted as a rogue (unsanctioned) device, and potentially removed. The default interval is 1 minute.
Ageout for AP Entries	Set the interval the WIPS policy uses to ageout rogue devices. Set the policy in either <i>Seconds</i> (30 - 86,400), <i>Minutes</i> (1- 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). The default setting is 5 minutes.

- Select **OK** to update the settings. Select **Reset** to revert to the last saved configuration.
- Select the **WIPS Events** tab to enable events, filters and threshold values for this WIPS policy. The **Excessive** tab displays by default.

WIPS Policy Moto-do-not delete

Settings | **WIPS Events** | WIPS Signatures

Excessive | **MU Anomaly** | AP Anomaly

Excessive Actions Events

Name	Enable	Filter Expiration	Client Threshold	Radio Threshold
Aggressive Scanning	✗	0s	30	
Decryption Failures	✗	0s	25	
DoS Unicast Deauthentication or Dis	✓	0s	25	
DoS Association or Authentication F	✗	0s	25	
EAP Flood	Enabled	0	15	40
802.11 Replay Check Failure	✗	0s	10	
Authentication Server Failures	✗	0s	5	

Figure 8-9 WIPS Events screen - Excessive tab

The Excessive tab lists a series of events that can impact the performance of the network. An administrator can enable or disable the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action applied.

An Excessive Action Event is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the *Excessive Action Events* table to select and configure the action taken when events are triggered.

10. Set the configurations of the following **Excessive Action Events**:

- Name** Displays the name of the excessive action event. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
- Enable** Displays whether tracking is enabled for each Excessive Action Event. Use the drop-down menu to enable/disable events as required. A green 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 the anomaly causing 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 events history.











11. Select **OK** to save the updates to the Excessive Actions configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration.

12. Select the **MU Anomaly** tab:

Settings WIPS Events WIPS Signatures

Excessive MU Anomaly AP Anomaly

MU Anomaly Events

Name	Enable	Filter Expiration
 Crackable WEP IV Key Used	✗	0s
 DoS Broadcast Deauthentication	✗	0s
 All Zero MAC Address Observed	✗	0s
 Invalid Frame Type Detected	✗	0s
 Invalid Management Frame	✗	0s
 Invalid Sequence Number	✗	0s
 Identical Source/Destination Address	✗	0s
 Invalid 802.1X Frame Detected	✗	0s
 Netstumbler (v3.2.0, 3.2.3, 3.3.0)	✗	0s
 Non-Changing WEP IV	✗	0s

OK Reset

Figure 8-10 WIPS Events screen - MU Anomaly tab

MU Anomaly events are suspicious events performed by wireless clients that can compromise the security and stability of the network. Use this MU Anomaly screen to configure the intervals clients can be filtered upon the generation of each defined event.

13. Set the configurations of the following **MU Anomaly Events** configurations:

Name	Displays the name of the MU Anomaly event. 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 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 the anomaly causing client is filtered. This creates a special ACL entry and frames coming from the client are silently dropped. The default setting is 0 seconds. For each violation, define a time to filter value in seconds which determines how long received packets are ignored from an attacking device once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.

14. 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.

15. Select the **AP Anomaly** tab.

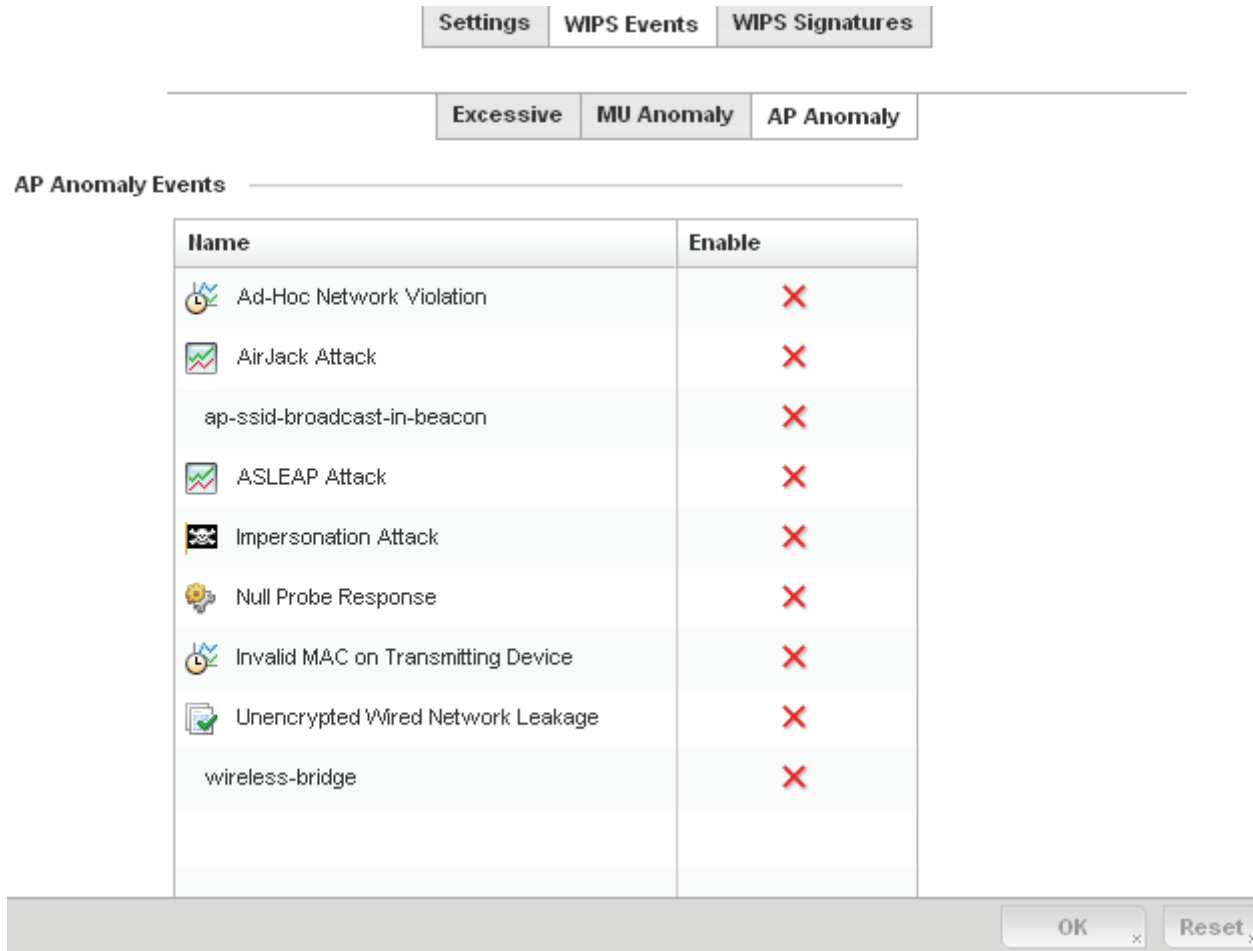


Figure 8-11 WIPS Events screen - AP Anomaly tab

AP Anomaly events are suspicious frames sent by a neighboring APs. Use this screen to determine whether an event is enabled for tracking.

16. Set the configurations of the following MU Anomaly Events configurations:

Name	Displays the name of the MU Anomaly event. 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 values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default.

17. 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.

18. Select the **WIPS Signatures** tab.

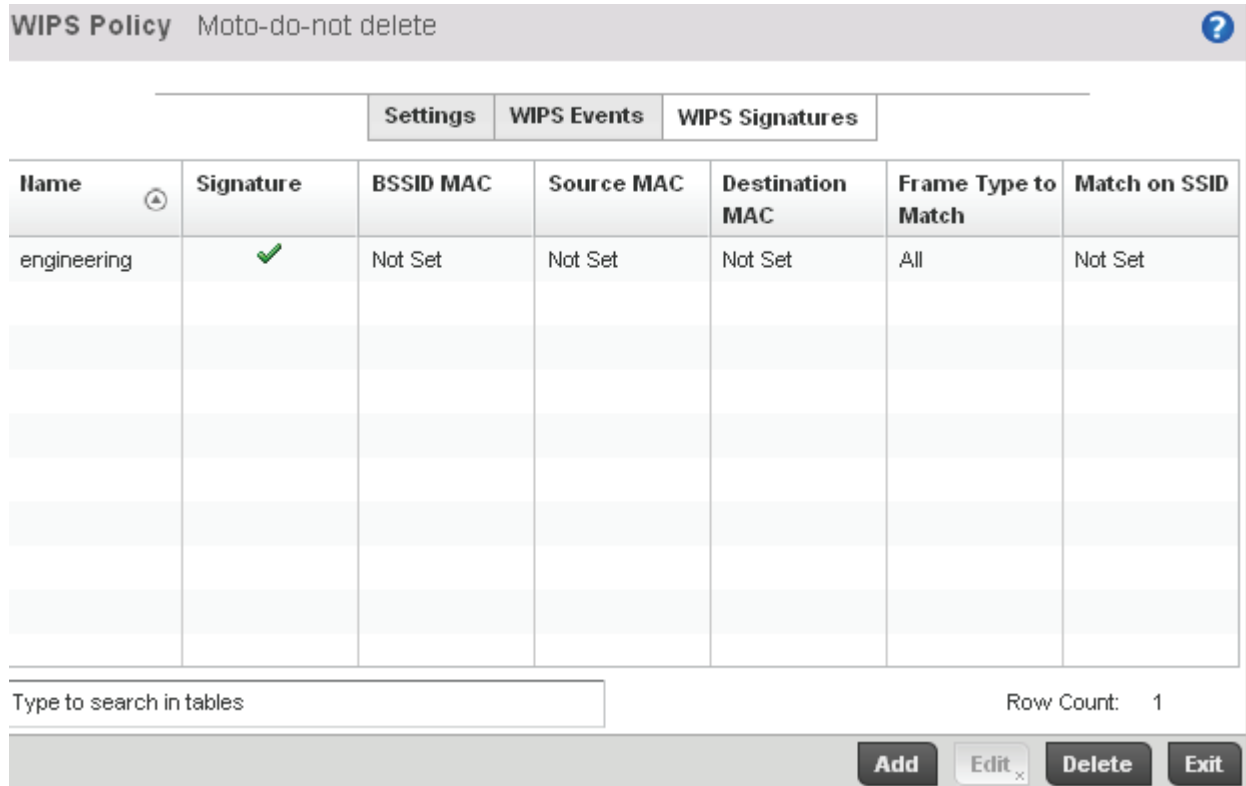


Figure 8-12 WIPS Signatures screen

The WIPS Signatures tab displays the following read-only configuration data:

- Name** Lists the name assigned to each signature as 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 MAC address of the packet examined for matching purposes.
- Destination MAC** Displays each destination MAC address of the packet examined 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.

19. 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 8-13 WIPS Signatures Configuration screen

20. If adding a new WIPS signature, define a **Name** to distinguish it from others with similar configurations. The name cannot exceed 64 characters.

21. 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 purposes.
- Source MAC** Define a source MAC address for the packet examined for matching purposes.
- Destination MAC** Set a destination MAC address for the packet examined for matching purposes.
- Frame Type to Match** Use the drop-down menu to select a frame type matching with the WIPS signature.
- Match on SSID** Sets the SSID used for matching. Ensure it's 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.

22.Refer to **Thresholds** field to set the thresholds used as filtering criteria.

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.

23.Set a **Filter Expiration** between 1 - 86,400 seconds that specifies the duration a client is excluded from radio association when responsible for triggering a WIPS event.

24.Refer to the **Payload** table to set a numerical index and offset for the WIPS signature.

25.Select **OK** to save the updates to the WIPS Signature configuration. Select **Reset** to revert to the last saved configuration.

8.2.2 Intrusion Detection Deployment Considerations

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 investigated and minimize the need for network monitoring.
- It's 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?
- Motorola Solutions recommends trusted and known Access Points be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.

Services Configuration

The AP-6511 supports services providing guest user access and leased DHCP IP addresses to requesting clients.

For more information, refer to the following:

- *[Configuring Captive Portal Policies](#)*
- *[Setting the DHCP Server Configuration](#)*

-
3. 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	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	Lists the IP address (or DNS hostname) of the external (centralized) server validating guest user permissions for the listed captive portal policy.
Captive Portal Server Mode	Lists each policy's hosting mode as either <i>Internal (Self)</i> or <i>External (centralized)</i> . If the mode is Internal (Self), the AP-6511 is maintaining the captive portal internally, while External (centralized) means the captive portal is being supported on an external server.
Connection Mode	Lists each policy's connection mode as either HTTP or HTTPS. However, Motorola Solutions recommends the use of HTTPS, as it offers client transmissions some measure of data protection HTTP cannot provide.
Simultaneous Users	Displays the number of users permitted at one time for each listed policy.
Web Page Source	Displays whether the captive portal HTML pages are maintained <i>Internally</i> , <i>Externally</i> (on an external system you define) or are <i>Advanced</i> 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 hotspot authentication. When a captive portal policy is created or modified, a AAA policy must be defined and applied to effectively authorize, authenticate and account user requests.

4. Select **Add** to create a new captive portal policy, **Edit** to modify an existing policy or **Delete** to remove an existing captive portal policy.

A **Basic Configuration** screen displays by default. Define the policy's security, access and whitelist basic configuration before actual HTML pages can be defined for guest user access.

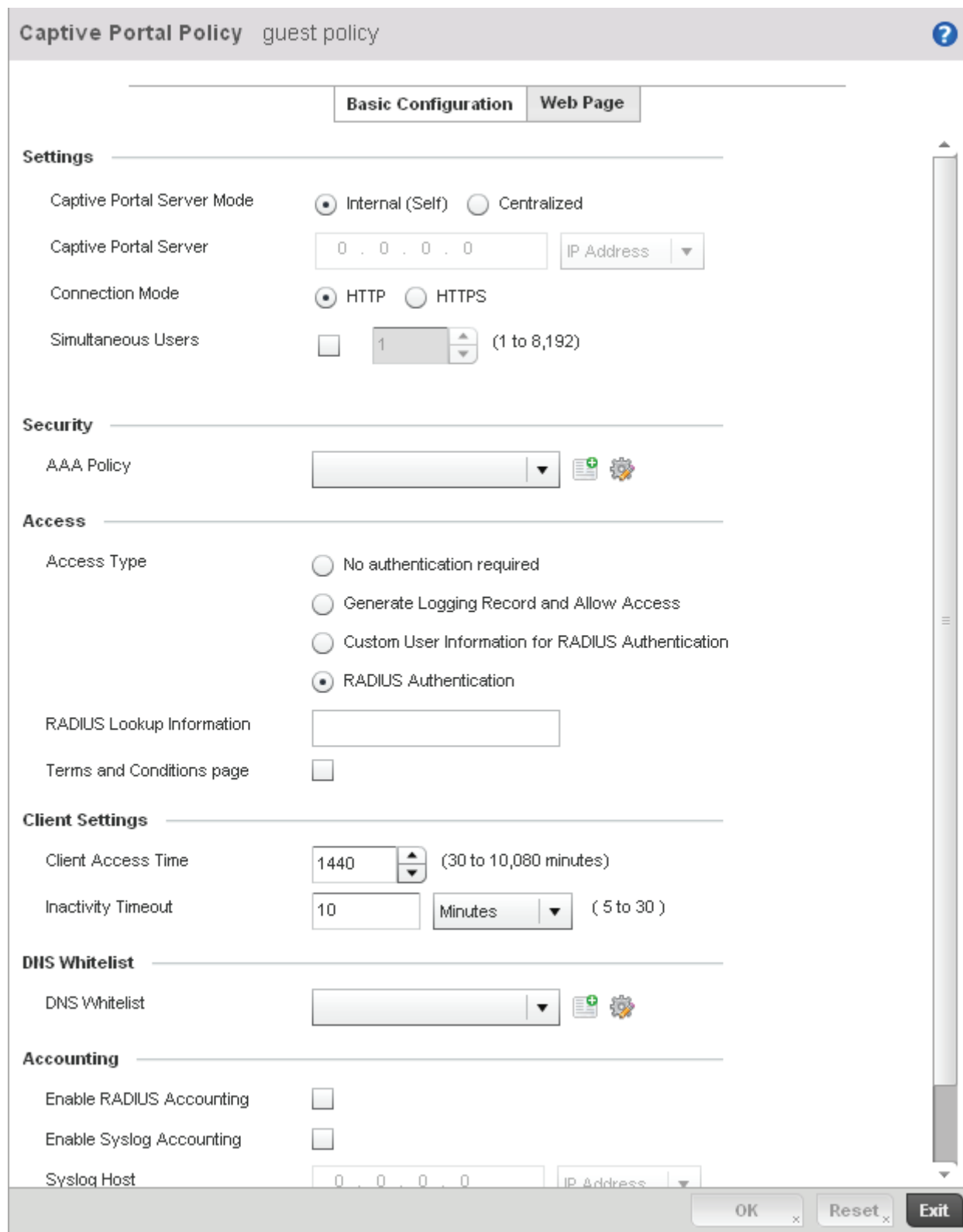


Figure 9-2 Captive Portal Policy Basic Configuration screen

5. Define the following **Settings** for the captive portal policy:

Guest Access 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 either **Internal (Self)** or **External (Centralized)**. Select the Internal (Self) radio button to maintain the captive portal configuration (Web pages) internally. Select the External (Centralized) radio button if the captive portal is supported on an external server. The default value is Internal (Self).

Captive Portal 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 the HTTP or HTTPS radio button to define the connection medium. Motorola Solutions recommends the use of HTTPS, as it offers additional data protection HTTP cannot provide. The default value however is HTTP.

Simultaneous Users Select the checkbox and use the spinner control to set between 0-8192 users (client MAC addresses) allowed to simultaneously access and use the captive portal.

6. 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 it from the drop-down menu and selecting the **Edit** icon. For information on creating a AAA policy that can be applied to a captive portal configuration, see [AAA Policy on page 6-50](#).

7. Set the following **Access** parameters to define how hotspot access is permitted, RADIUS lookup information and whether the hotspot's login pages contain agreement terms that must be accepted before access is granted to resources:

Access Type Select the radio button for the authentication scheme applied to wireless clients using the captive portal for guest access. Options include:
No authentication required - Clients can freely access the captive portal Web pages without authentication.
Generate Logging Record and Allow Access - Access is provided without authentication, but a record of the accessing client is logged.
Custom User Information for RADIUS Authentication - When selected, accessing clients are required to provide a 1-32 character lookup data string used to authenticate client access.
RADIUS Authentication - An accessing client's user credentials require authentication with an external RADIUS resource before access to the captive portal is granted. This is the default setting.

RADIUS Lookup Information When **Custom User Information for RADIUS Authentication** is selected as the access type, provide a 1-32 character lookup information string used as a customized authentication mechanism.

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 Agreement page when *No authentication required* is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled.

8. Set the following **Client Settings** to define the duration clients are allowed captive portal access and when they're timed out due to inactivity:

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 between 30 - 10,800 minutes. The default interval is 1,440 minutes.

Inactivity Timeout Use the drop-down menu to specify an interval in either *Minutes* (5 - 30) or *Seconds* (300 - 1,800) that, when exceeded, times out clients that have not transmitted a packet within the captive portal.

9. Use the **DNS White List** parameter to create a set of allowed destination IP addresses. These allowed DNS destination IP addresses are called a *Whitelist*.

To effectively host hotspot 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. If no DNS Whitelist entries exist, select the **Create** or **Edit** icons and follow the sub-steps below:

- a. If creating a new Whitelist, assign it a name up to 32 characters in length. Use the **+ Add** button to populate the Whitelist table with Host and IP Index parameters that must be defined for each Whitelist entry.

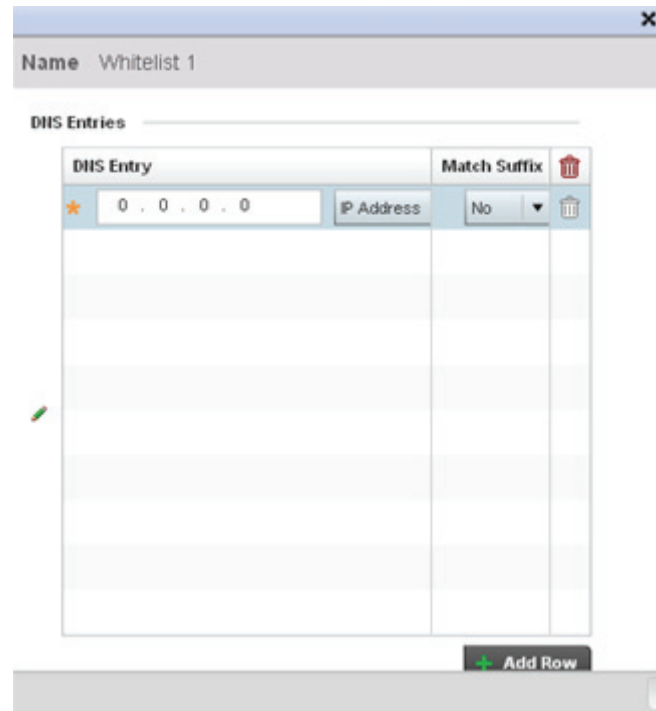


Figure 9-3 Captive Portal DNS Whitelist screen

- b. Provide a numerical IP address or Hostname within the **DNS Entry** parameter for each destination IP address or host included in the Whitelist.
 - c. Use the **Match Suffix** parameter to match any hostname or domain name as a suffix. The default setting is disabled.
 - d. If necessary, select the radio button of an existing Whitelist entry and select the - **Delete** icon to remove the entry from the Whitelist.
10. Set the following **Accounting** parameters to define how accounting is conducted for the 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 the **Enable RADIUS Accounting** 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 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 host name of an external server resource is required to route captive portal syslog events to that destination.

Syslog Port Define the numerical syslog port to route traffic with the external syslog server.

11. Select **OK** to save the changes made within the Basic Configuration screen. Selecting **Reset** reverts the settings back to the last saved configuration.

12. Select the **Web Page** tab to create HTML pages requesting wireless clients use to login and navigate within a hotspot.

The **Login** page displays by default.

Captive Portal Policy *guest policy* ?

Basic Configuration **Web Page**

Web Page Source Internal Advanced Externally Hosted

Login **Terms and Conditions** **Welcome** **Fail**

Title Text

Header Text

Login Message

Footer Text

Main Logo URL

Small Logo URL

A simple auto-generated set of web pages are created based on the provided fields.
 Three separate web pages are provided for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt

OK Reset **Exit**

Figure 9-4 Captive Portal Policy Basic Web Page screen

The *Login* screen prompts the user for a username and password to access the hotspot 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 hotspot. The *Fail* page asserts the hotspot authentication attempt has failed, and the user is not allowed to access the Internet (using this captive portal policy) and must provide the correct login information again to access the Internet.

13. Provide the following required information if creating Basic **Login, Agreement, Welcome** and **Fail** pages maintained internally (when the **Basic** radio button is selected as the Web Page Source). The Basic (internally hosted) captive portal is the default setting.


Title Text	Set the title text displayed on the Login, Agreement, 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, agreement, welcome and fail function.
Header Text	Provide header text unique to the function of each page.
Message	Specify a message containing unique instructions or information for the users who access the Login, Agreement, Welcome or Fail pages. In the case of the Agreement 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 hotspot Web pages.
Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the Login, Agreement, 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, Agreement, Welcome and Fail pages. Use the Browse button to navigate to the location of the target file.

14. Select **OK** to save the changes made within the Internal Pages screen. Selecting **Reset** reverts the settings back to the last saved configuration.

15. If hosting the captive portal on an external system, select the **Externally Hosted** tab.

Captive Portal Policy guest policy ?

Basic Configuration **Web Page**

Web Page Source  Internal Advanced Externally Hosted

Login URL

Agreement URL

Welcome URL

Fail URL

A set of pre-existing web pages outside of the switch are specified by the provided URLs.
Three separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

>> OK **Reset** **Exit**

Figure 9-5 Captive Portal Policy Externally Hosted Web Page screen

16. Set the following external URL destinations for the captive portal policy's hotspot 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. |

17. Select **OK** when completed to update the captive portal policy settings. Select **Reset** to revert the screen back to its last saved configuration.


18. Select **Advanced** to use a custom directory of Web pages copied to and from the AP-6511 for captive portal support.

Captive Portal Policy guest policy ?

Basic Configuration | Web Page

Web Page Source  Internal Advanced Externally Hosted

File/s	URL	Advanced
	<input type="text"/>	Advanced

Export  Import Reset

A custom-developed directory full of web page content can be copied in and out of the switch. File transfers occur immediately.
There are minimal requirements that the custom web pages must comply with in order to work. Refer to this device's documentation for more details.

>> OK Reset Exit

Figure 9-6 Captive Portal Policy Advanced Web Page screen

19. Set the following external URL destinations for the captive portal policy's hotspot pages.

- URL** Define the complete URL for the location of the custom captive portal pages.
- Advanced** Select the **Advanced** link to display additional parameters for accessing the remote server used to support the advanced captive portal configuration. The following parameters are required:
- Protocol* - Select the file transfer method used between the AP-6511 and the resource maintaining the custom captive portal files.
 - Port* - Use the spinner control to set the port used on the external Server maintaining the custom captive portal files.
 - Host* - Set the IP address or hostname of the destination server supporting the captive portal's advanced files set. Use the drop-down menu to specify whether an IP address or hostname is used.
 - Path* - Provide a complete and accurate path to the location where the captive portal file set resides on the external server resource.

Export	Select the Export button to upload target captive portal files to the designated external resource. The exported files display within the File/s table.
Import	Select the Import button to download target captive portal files from the designated external resource to the AP-6511. The imported files display within the File/s table.

20. Select **OK** when completed to update the captive portal's advanced configuration. Select **Reset** to revert the screen back to its last saved configuration.

9.1.2 Captive Portal Deployment Considerations

Before defining a captive portal configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The architecture should consider the number of wireless clients allowed on the guest network and the services provided. Each topology has benefits and disadvantages which should be taken into consideration to meet each deployment's requirements.
- Hotspot authentication uses secure HTTPS to protect user credentials, but doesn't typically provide encryption for user data once they have been authenticated. For private access applications, Motorola Solutions recommends WPA2 (with a strong passphrase) be enabled to provide strong encryption.
- Motorola Solutions recommends guest user traffic be assigned a dedicated VLAN, separate from other internal networks.
- Guest access services should be defined in a manner whereby end-user traffic doesn't cause network congestion.
- Motorola Solutions recommends a valid certificate be issued and installed on all devices providing Hotspot access to a WLAN and wireless network. The certificate should be issued from a public certificate authority ensuring guests can access the Hotspot without browser errors.

9.2 Setting the DHCP Server 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.

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.

To access and review the DHCP server configuration:

1. Select **Configuration > Services > DHCP Server Policy**.

The **DHCP Server** screen displays. 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 then compared against classes.

DHCP Server Policy	Ignore BOOTP Requests	Ping Timeout
engineering	✘	1s

Type to search in tables Row Count: 1

Figure 9-7 DHCP Server screen

- 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 network. BOOTP messages are encapsulated inside UDP messages and are forwarded. 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.

- Select **Add** to create a new DHCP 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 **DHCP Server Policy** screen by default.

9.2.1 Defining DHCP Pools

A pool (or range) of IP network addresses and DHCP options can be created for each IP interface configured. This range of addresses can be made available to DHCP enabled wireless devices 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 of characters (or octets) that has a meaning specified by the vendor of the DHCP client

To define the parameters of a DHCP pool:

- Select **Configuration > Services > DHCP Server Policy**. The DHCP Server Policy screen displays the DHCP Pool tab by default.

The screenshot shows the 'DHCP Server Policy' configuration page for the 'engineering' user. The page has three tabs: 'DHCP Pool', 'Global Settings', and 'Class Policy'. The 'DHCP Pool' tab is active, displaying a table with the following columns: 'DHCP Pool', 'Subnet', 'Domain Name', 'Boot File', and 'Lease Time'. The table is currently empty. Below the table is a search bar labeled 'Type to search in tables' and a 'Row Count: 0' indicator. At the bottom right of the page are four buttons: 'Add', 'Edit', 'Delete', and 'Exit'.

DHCP Pool	Subnet	Domain Name	Boot File	Lease Time

Figure 9-8 DHCP Server Policy screen - DHCP Pool tab

- Review the following DHCP pool configurations to determine if an existing pool can be used as is, a new one requires creation or edit, or a pool requires deletion:

DHCP Pool	Displays the name assigned to the network pool when created. The DHCP pool name represents the group of IP addresses used to assign to DHCP clients upon request. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted.
Subnet	Displays the network address and mask used by clients requesting DHCP resources.
Domain Name	Displays the domain name used with this network pool. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A <i>fully qualified domain name</i> (FQDN) consists of a host name plus a domain name. For example, <i>computername.domain.com</i> .

Boot File

Boot files (*Boot Protocol*) are used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed.

Lease Time

If a lease time has been defined for a listed network pool, it displays in an interval between 1 - 9,999,999 seconds. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another DHCP supported client.

3. Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool's properties or **Delete** to remove a pool from amongst those available.

The screenshot shows the 'DHCP Pools' configuration window with the 'Basic Settings' tab selected. The window title is 'DHCP Pools'. At the top, there is a 'DHCP Pool' label with a star icon and a question mark icon. Below this are three tabs: 'Basic Settings', 'Static Bindings', and 'Advanced'. The 'Basic Settings' tab is active and contains two 'General' sections. The left 'General' section includes a 'Subnet' field with a dropdown menu, a 'Domain Name' text box, and a 'DNS Servers' table with four rows, each containing an 'IP Address' field and a 'Clear' button. The right 'General' section includes a 'Lease Time' checkbox (checked) with a dropdown menu showing '86400', and a 'Default Routers' table with four rows, each containing an 'IP Address' field and a 'Clear' button. At the bottom of the window, there is an 'IP Address Ranges' table with three columns: 'IP Start', 'IP End', and 'Class Policy', and a trash icon. The bottom right corner of the window has 'OK', 'Reset', and 'Exit' buttons.

Figure 9-9 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 the DHCP pool.

4. Set the following **General** parameters from within the **Basic Settings** tab:

Network 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.
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. A <i>fully qualified domain name</i> (FQDN) consists of a host name plus a domain name. For example, <i>computername.domain.com</i> .
DNS Servers	Define one or a group of <i>Domain Name Servers</i> (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.
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 <i>Seconds</i> (1 - 31, 622, 399), <i>Minutes</i> (1 - 527,040), <i>Hours</i> (1 - 8,784) or <i>Days</i> (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 host names into IP addresses available to DHCP supported clients. Up to 8 default router IP addresses are supported.

5. Use the **IP and Excluded IP Address Ranges** to define the range of included (starting and ending IP addresses) addresses for this particular pool.
- Select the **+ Add Row** button at the bottom of the IP addresses 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.
 - 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.
 - Select **OK** to save the updates to the DHCP Pool Basic Settings tab. Select **Reset** to revert to the last saved configuration.

- 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.

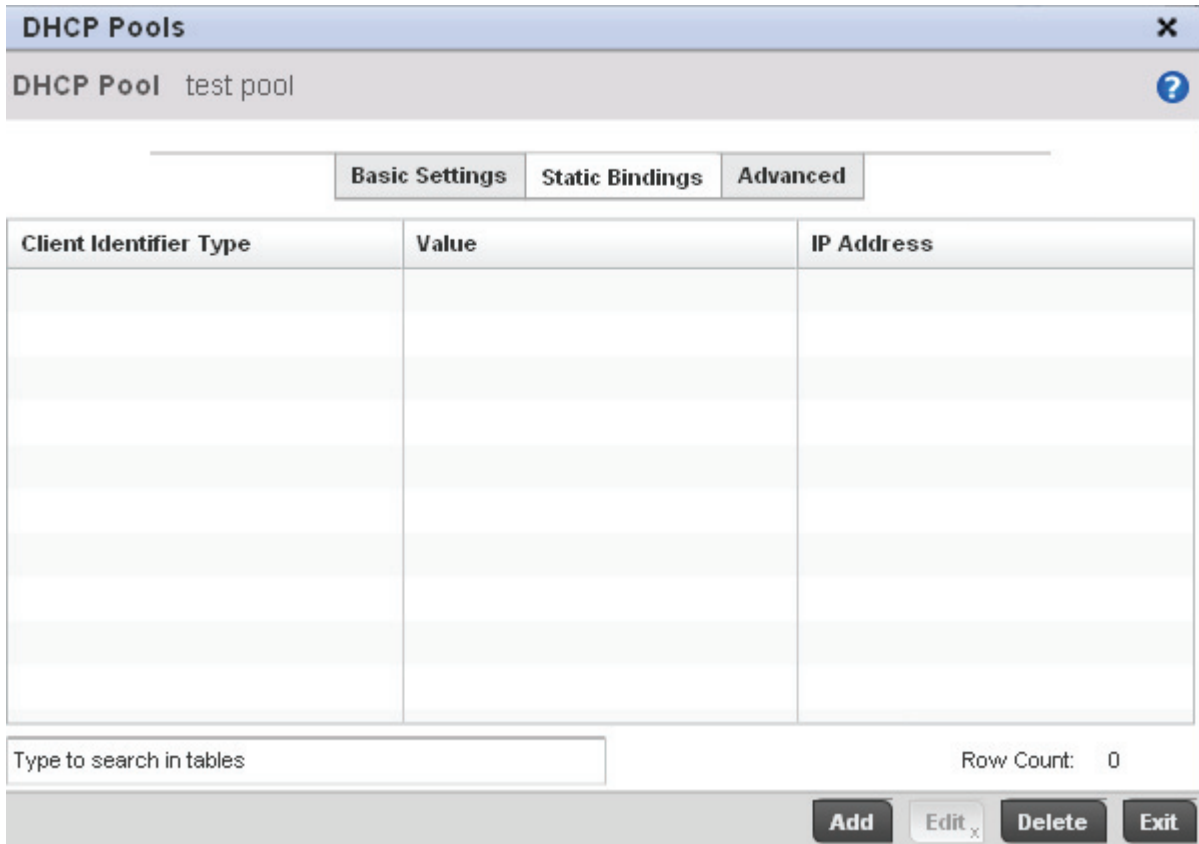


Figure 9-10 DHCP Pools screen - Static Bindings tab

- Review the following 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.

- 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 9-11 Static Bindings Add screen

9. 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 client is using a **Hardware Address** or **Client Identifier** as its identifier type.

Value

Provide a hardware address or client identifier value to the client to help differentiate from other client identifiers.

IP Address

Set the IP address of the client using this host pool.

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 host name plus a domain name. For example, *computername.domain.com*

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.
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's just one sender, and one receiver). Select this option to forward unicast messages to just a single device within this network pool.

10. 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: <i>Broadcast</i> - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name. <i>Peer-to-Peer</i> - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine. <i>Mixed</i> - A mixed node using broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. <i>Hybrid</i> - A combination of two or more nodes. <i>Undefined</i> - 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.

11. 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.

12. Refer to the **DHCP Option Values** table to set Global DHCP options. A set of global DHCP options applies to all clients, whereas a set of subnet options applies only to the clients on a specified subnet. If you configure the same option in more than one set of options, the precedence of the option type decides which the DHCP server supports a client.

- 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 1 through 254. A vendor-specific option definition only applies to the vendor class for which it is defined.

13. 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.

14. Select **OK** when completed to update the static bindings configuration. Select **Reset** to revert the screen back to its last saved configuration.
15. Select the **Advanced** tab to define additional NetBIOS and Dynamic DNS parameters.

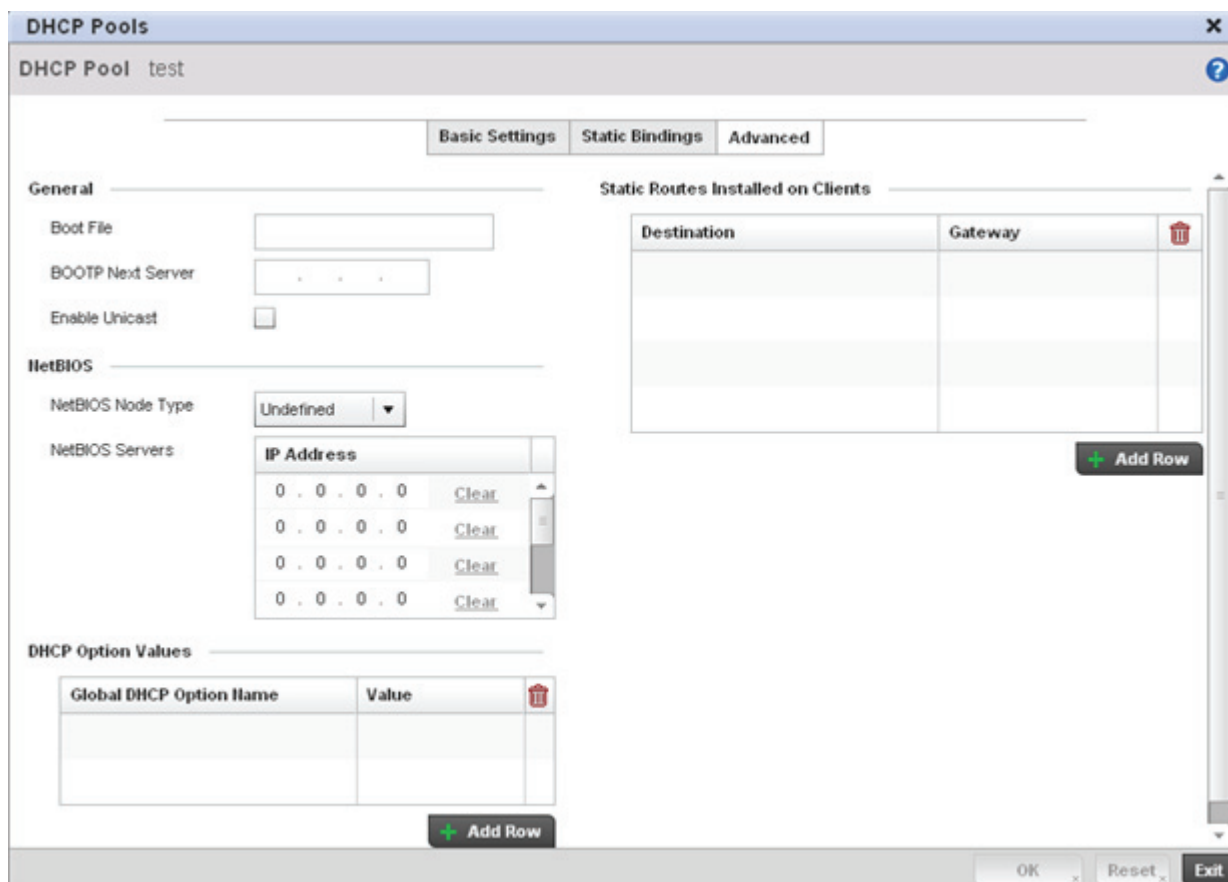


Figure 9-12 DHCP Pools screen - Advanced tab

16. The addition or edit of the network 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.
- 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.

17. Set the following **NetBIOS** parameters for the network pool:

NetBIOS Node Type	<p>Set the NetBIOS Node Type used with this pool. The following types are available:</p> <p><i>Broadcast</i> - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.</p> <p><i>Peer-to-Peer</i> - Uses directed calls to communicate with a known NetBIOS name server, such as a WINS server, for the IP address of a NetBIOS machine.</p> <p><i>Mixed</i> - Is a mixed node using broadcasted queries to find a node, and failing that, queries a known p-node name server for the address.</p> <p><i>Hybrid</i> - Is a combination of two or more nodes.</p> <p><i>Undefined</i> - No NetBIOS Node Type is used.</p>
NetBIOS Servers	<p>Specify a numerical IP address of a single or group of NetBIOS WINS servers available to DHCP supported wireless clients.</p>

18. 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.

- a. Select the **+ Add Row** button to add individual options. Assign each a **Global DHCP Option Name** to help differentiate it from others with similar configurations. 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.
- b. 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's defined.

19. 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.

20. 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.

9.2.2 Defining DHCP Server Global Settings

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.

DHCP Server Policy test

DHCP Pool **Global Settings** **Class Policy**

Configuration

Ignore BOOTP Requests

Ping Timeout seconds (1 to 10)

Global DHCP Server Options

Name	Type	Code	

+ Add Row

OK x Reset x Exit

Figure 9-13 DHCP Server Policy screen - Global Settings tab

- Set the following parameters within the **Configuration** field:

Ignore BOOTP Requests

Select the checkbox to ignore BOOTP requests. BOOTP (boot protocol) 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.

- 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.
- Select **OK** to save the updates to the DHCP server global settings. Select **Reset** to revert the screen back to its last saved configuration.

9.2.3 DHCP Class Policy 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.

The screenshot shows the DHCP Server Policy configuration interface. At the top, there is a header 'DHCP Server Policy test' with a help icon. Below the header are three tabs: 'DHCP Pool', 'Global Settings', and 'Class Policy'. The 'Class Policy' tab is active, displaying a table with the following data:

DHCP Class Name	Multiple User Class Support
policyb 1	X

Below the table is a search bar with the text 'Type to search in tables' and a 'Row Count: 1' indicator. At the bottom of the screen are four buttons: 'Add', 'Edit', 'Delete', and 'Exit'.

Figure 9-14 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.

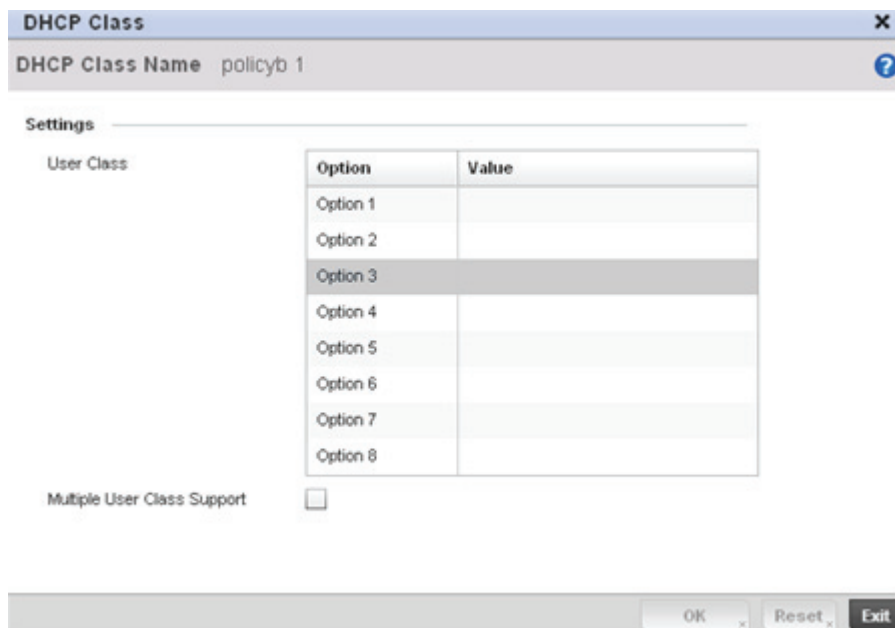


Figure 9-15 DHCP Class Name Add screen

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** 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 the screen back to its last saved configuration.

10

Management Access Policy Configuration

The AP-6511 has mechanisms to allow/deny Management 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. The Management Access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Motorola Solutions recommends disabling 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 on devices.

10.1 Viewing Management Access Policies

Management Access policies display in the lower left-hand side of the screen. Existing policies can be updated as management permissions change, or new policies can be added as needed.

To view existing Management Access policies:

1. Select **Configuration > Management > Wireless LAN Policy**.
2. Select a policy from the Management Browser or refer to the Management screen (displayed by default) to review existing Management Access policy configurations at a higher level.

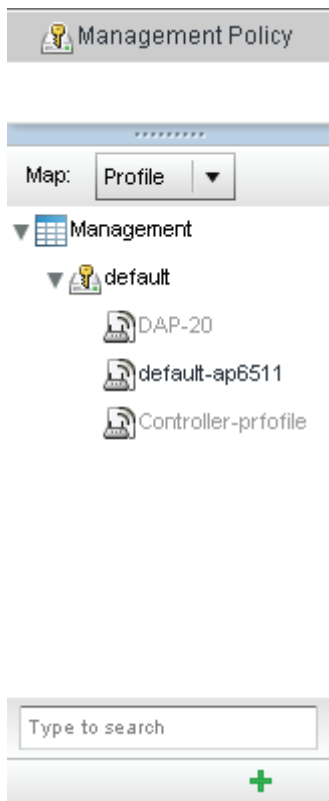


Figure 10-1 Management Browser screen

The **Management Policy** screen displays existing management policies and their unique protocol support configurations.

Management Policy	Telnet	SSHv2	HTTP	HTTPS	SNMPv2	SNMPv3	FTP
default	✓	✓	✓	✗	✗	✓	✗

Type to search in tables Row Count: 1

Add **Edit** **Delete**

Figure 10-2 Management screen

3. Refer to the following Management Access policy parameters to discern whether these policies can be used as is, require modification or a new policy requires creation:

A green check mark indicates device access is allowed using the protocol. A red X indicates device access is denied using the protocol.

Management Policy	Displays the name of the Management Access policy assigned when initially created. The name cannot be updated when modifying a policy.
Telnet	Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication.
SSH v 2	SSH (<i>Secure Shell</i>) version 2, like Telnet, provides a command line interface to a remote host. However, all SSH transmissions are encrypted, increasing the security of the transmission.
HTTP	HTTP (<i>Hypertext Transfer Protocol</i>) provides access to the device's GUI using a Web browser. This protocol is somewhat unsecure.
HTTPS	HTTPS (<i>Hypertext Transfer Protocol Secure</i>) provides fairly secure access to the device's GUI using a Web browser. Unlike HTTP, HTTPS uses encryption for transmission, and is therefore more secure than HTTP.
SNMPv 2	SNMP (<i>Simple Network Management Protocol</i>) exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified. However, SNMP is generally used to monitor a system's performance and other parameters.

SNMPv 3

SNMP (*Simple Network Management Protocol*) exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified. However, SNMP is generally used to monitor system performance and other parameters.

FTP

FTP (*File Transfer Protocol*) is a standard protocol for files transfers over a TCP/IP network.

4. If it's determined a Management Access policy requires creation or modification, refer to [Adding or Editing a Management Access Policy on page 10-4](#). If necessary, select an existing Management Access policy and select **Delete** to permanently remove it from the list of those available.

10.1.1 Adding or Editing a Management Access Policy

▶ [Viewing Management Access Policies](#)

To add a new Management Access policy or edit an existing configuration:

1. Select **Configuration** > **Management**.
2. Existing policies can be modified by either selecting a policy from the **Management Browser** and selecting the green **+** button located on the bottom right-hand side of the Browser or by selecting an existing policy from the Management screen and selecting the **Edit** button.

New policies can also be created by selecting the **Add** button from the bottom right-hand side of the Management screen.

3. A name must be supplied to the new policy before the *Administrators*, *Access Control*, *Authentication*, *SNMP* and *SNMP Traps* tabs become enabled and the policy's configuration defined. The name cannot exceed 32 characters in length.
4. Select **OK** to commit the new policy name.

Once the new name is defined, the screen's tabs become enabled with the contents of the **Administrators** tab displayed by default. Refer to the following to define the configuration of the new Management Access policy:

- [Creating an Administrator Configuration](#) - Use this tab to create users, assign them permissions to specific protocols and set specific administrative roles for the network.
- [Setting the Access Control Configuration](#) - Use this tab to enable/disable specific protocols and interfaces. Again, this kind of access control is not meant to function as an ACL, but rather as a means to enable/disable specific protocols (HTTP, HTTPS, Telnet etc.) for each Management Access policy.
- [Setting the Authentication Configuration](#) - Refer to this tab to set the authentication scheme for the policy.
- [Setting the SNMP Configuration](#) - Refer to this tab to enable SNMPv2, SNMPv3 or both and define specific community strings for this policy.
- [SNMP Trap Configuration](#) - Use this tab to enable trap generation for the policy and define trap receiver configurations.
- For deployment considerations and recommendations impacting a Management Access policy configuration, refer to [Management Access Deployment Considerations on page 10-15](#).

10.1.1.1 Creating an Administrator Configuration

► *Adding or Editing a Management Access Policy*

Use the **Administrators** tab to review existing administrators, their access medium and their administrative role within the network. New administrators can be added, existing administrative configurations modified or deleted as required.

Management Policy default

Administrators Access Control Authentication SHMP SHMP Traps

User Name	Access Type	Role
admin	All	Superuser
operator	All	Monitor

Type to search in tables Row Count: 2

Add Edit Delete Exit

Figure 10-3 Management Policy screen - Administrators tab

Refer to the following to review the high-level configurations of existing administrators:

User Name	Displays the name assigned to the administrator upon creation. the name cannot be modified as part of the administrator configuration edit process.
Access Type	Lists the <i>Web UI</i> , <i>Telnet</i> , <i>SSH</i> or <i>Console</i> access type assigned to each listed administrator. A single administrator can have any one or all of these roles assigned at the same time.
Role	Lists the <i>Superuser</i> , <i>System</i> , <i>Network</i> , <i>Security</i> , <i>Monitor</i> , <i>Help Desk</i> or <i>Web User</i> role assigned to each listed administrator. An administrator can only be assigned one role at a time.

1. Select the **Add** button to create a new administrator configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove an Administrator from the list of those available.

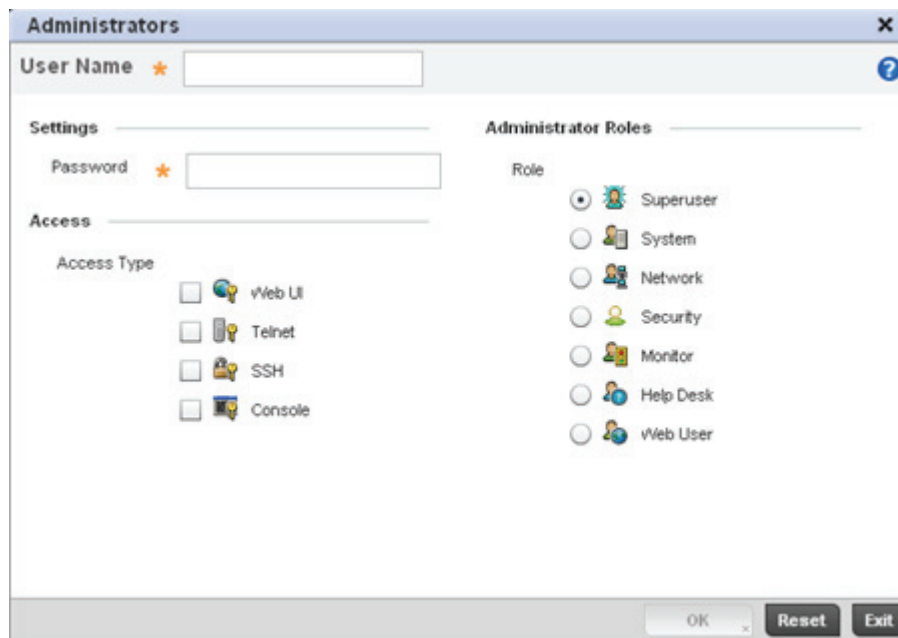


Figure 10-4 Administrators screen

2. If creating a new administrator, enter a user name in the **User Name** field. This is a mandatory field for new administrators and cannot exceed 32 characters. Optimally assign a name representative of the user and role.
3. Provide a strong password for the administrator in the **Password** field, once provided, **Reconfirm** the password to ensure its accuracy. This is a mandatory field.
4. Select **Access** options to define the permitted access for the user. If required, all four options can be selected and invoked simultaneously.

Web UI Select this option to enable access to the device's Web UI.

Telnet Select this option to enable access to the device using TELNET.

SSH Select this option to enable access to the device using SSH.

Console Select this option to enable access to the device's console.

5. Select the **Administrator Role** for the administrator using this profile. Only one role can be assigned.

Superuser Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles.

System Select System 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 Security to set the administrative rights for a security administrator allowing the configuration of all security parameters.

Monitor	Select Monitor to assign permissions without administrative rights. The Monitor option provides read-only permissions.
Help Desk	Assign this role 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 AP-6511.
Web User	Select Web User to assign the administrator privileges needed 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 9-2 .

6. Select the **OK** button to save the administrator's configuration. Select **Reset** to revert to the last saved configuration.

10.1.1.2 Setting the Access Control Configuration

► *Adding or Editing a Management Access Policy*

Refer to the **Access Control** tab 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. Motorola Solutions recommends disabling unused interfaces to reduce unnecessary security holes. The Access Control tab is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

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 an access control configuration for the Management Access policy:

1. Select the **Access Control** tab from the Management Policy screen.

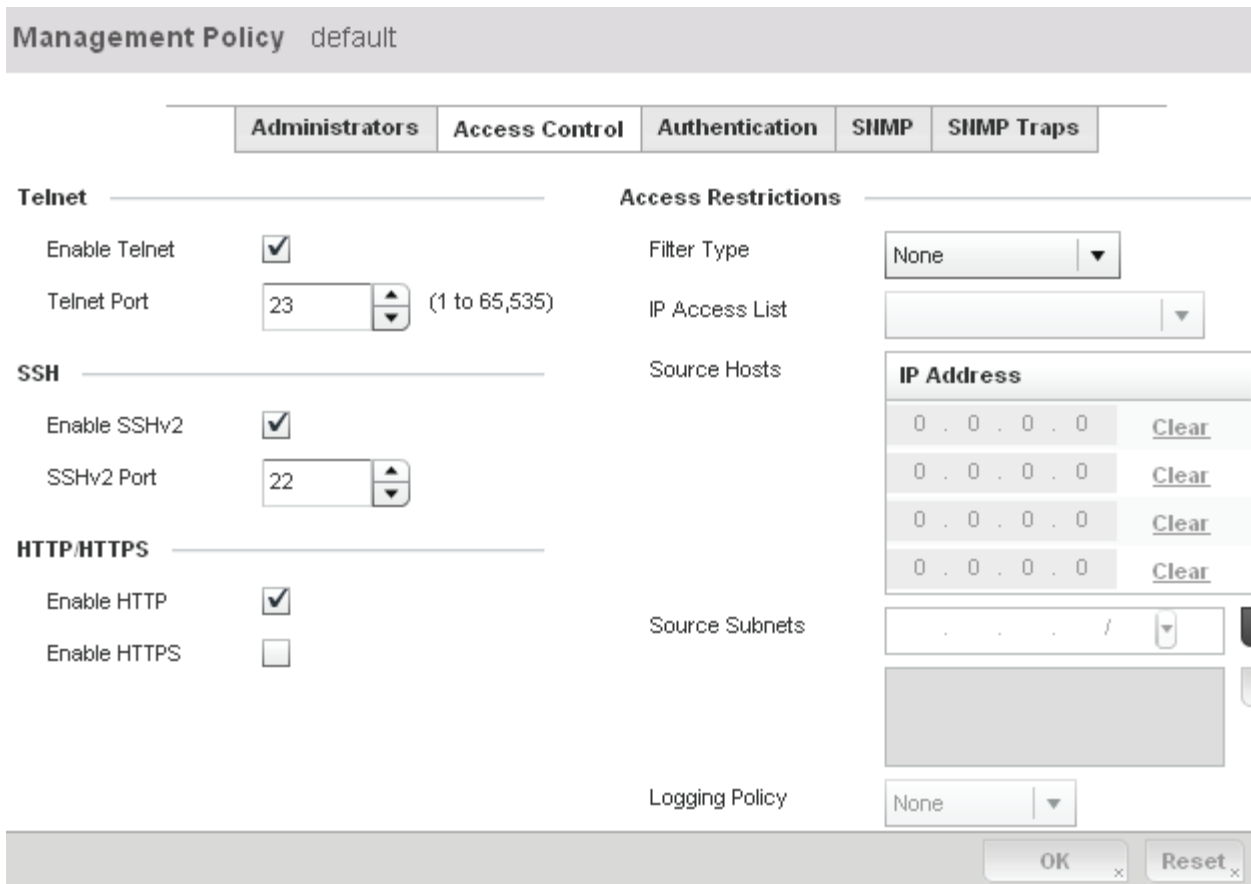


Figure 10-5 Management Policy screen - Access Control tab

2. Set the following parameters required for **Telnet** access:

Enable Telnet	Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.
Telnet Port	Set the port on which Telnet connections are made (1 - 65,535). The default port is 23. Change this value using the spinner control next to this field or by entering the port number in the field.

3. Set the following parameters required for **SSH** access:

Enable SSHv2	Select the checkbox to enable SSH device access. SSH (<i>Secure Shell</i>) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.
SSHv2 Port	Set the port on which SSH connections are made. The default port is 22. Change this value using the spinner control next to this field or by entering the port number in the field.

4. Set the following **HTTP/HTTPS** parameters:

Enable HTTP	Select the checkbox to enable HTTP device access. HTTP provides limited authentication and no encryption.
Enable HTTPS	Select the checkbox to enable HTTPS device access. HTTPS (<i>Hypertext Transfer Protocol Secure</i>) is more secure than plain HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication



NOTE: If the external RADIUS server is not reachable, HTTPS or SSH management access to Access Point may be denied.

5. Set the following **Access Restrictions**:

Filter Type	Use the drop-down menu to select the filter mechanism used as the management policy access restriction. Options include <i>source-address</i> , <i>ip-access-list</i> and <i>None</i> .
Source Hosts	Set multiple source host IP address resources.
Source Subnets	Define a list of subnets allowed administrative access.
Logging Policy	Use the drop-down menu to set the logging policy for administrative access. Select from <i>None</i> , <i>denied-only</i> and <i>All</i> .

6. Select **OK** to update the access control configuration. Select Reset to the last saved configuration.

10.1.1.3 Setting the Authentication Configuration

▶ *Adding or Editing a Management Access Policy*

To configure an external authentication resource:

1. Select the **Authentication** tab from the Management Policy screen.

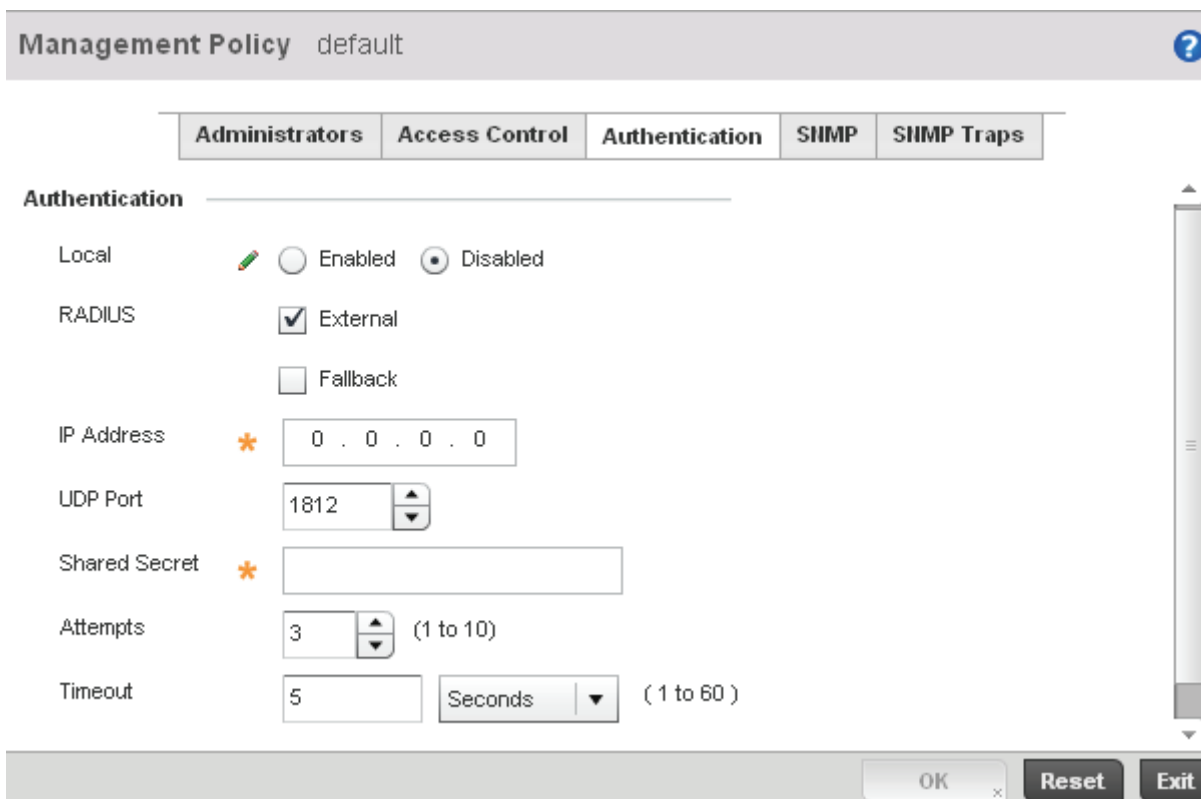


Figure 10-6 Management Policy screen - Authentication tab

2. Set the following AP-6511 external resource settings to authenticate management access requests:

Local	Set to disabled to provide the AP-6511 and external RADIUS server resource for authentication requests.
IP Address	Define the numerical IP address of the AP-6511's external RADIUS authentication resource.
UDP Port	Use the spinner control to set the port number where the RADIUS server is listening. The default setting is 1812.
Shared Secret	Define a shared secret password between the AP-6511 and the RADIUS server that must be provided to secure the external RADIUS resource.
Attempts	Set the number of times an authentication request is sent to the RADIUS server before giving up. The available range is 1- 10, with a default of 3.
Timeout	Set a timeout setting in <i>Seconds</i> (1-60) after which requests to the RADIUS server will be retries.

3. Select **OK** to update the configuration. Select **Reset** to revert to the last saved configuration.

10.1.1.4 Setting the SNMP Configuration

► *Adding or Editing a Management Access Policy*

The AP-6511 can use *Simple Network Management Protocol* (SNMP) to communicate 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 the management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather 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 configure SNMP Management Access within the network:

1. Select the **SNMP** tab from the Management Policy screen.

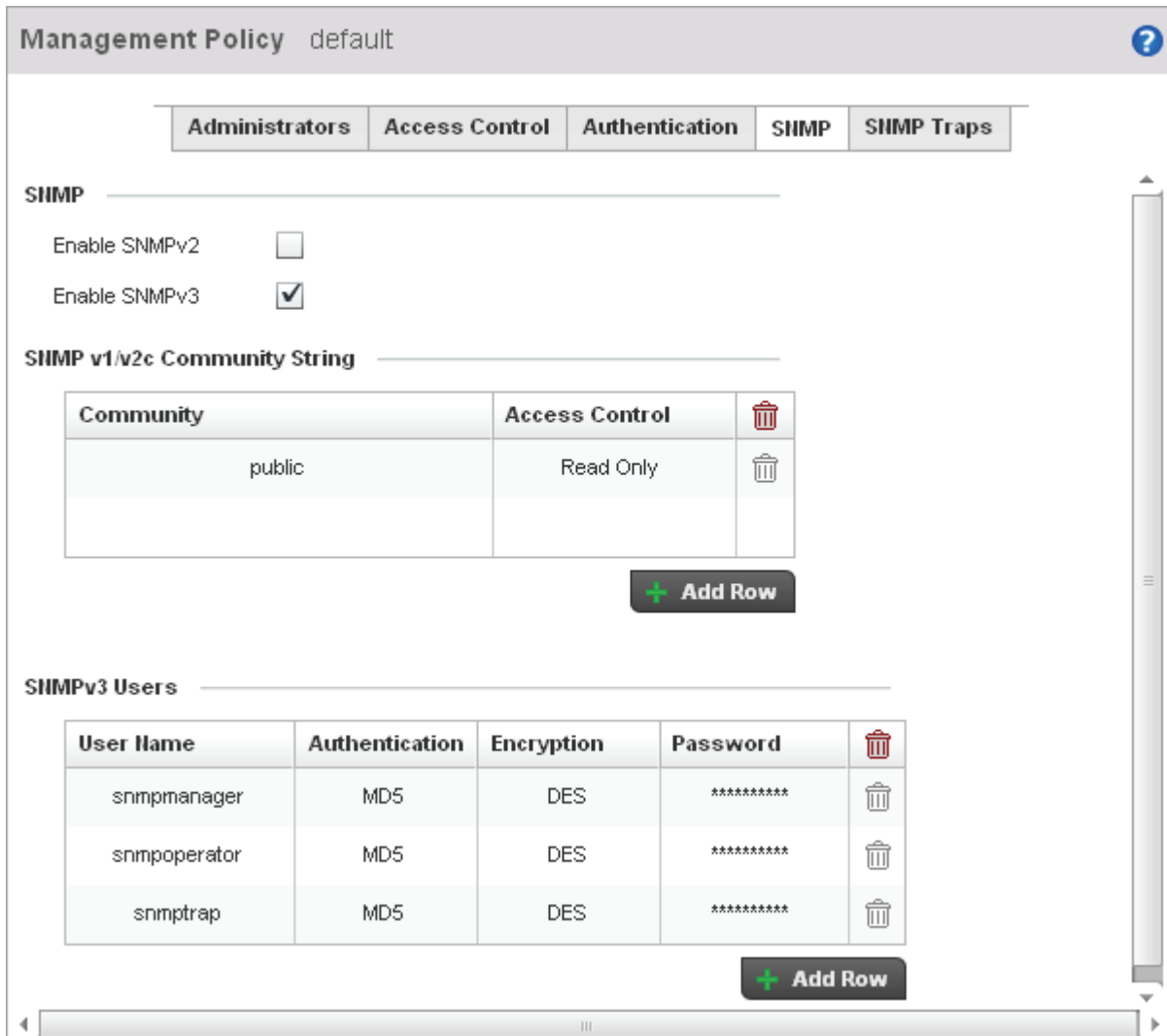


Figure 10-7 Management Policy screen - SNMP tab

2. Enable or disable SNMPv2 and SNMPv3.

Enable SNMPv2

Select the checkbox to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses *Get*, *GetNext*, and *Set* operations for data management. SNMPv2 is enabled by default.

Enable SNMPv3

Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *User-based Security Model* (USM) for message security and the *View-based Access Control Model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

3. Set the **SNMP v1/v2 Community String** configuration. Use the **+ Add Row** function as needed to add additional SNMP v1/2 community strings, or select an existing community string's radio button and select the **Delete** icon to remove it.

Community Define a *public* or *private* community designation. By default, SNMPv2 community strings on most devices are set to *public* for the read-only community string and *private* for the read-write community string.

Access Control Set the access permission for each community string used by devices to retrieve or modify information. The available options include:
Read Only - Allows a remote device to retrieve information
Read-Write - Allows a remote device to modify settings

4. Set the **SNMPv3 Users** configuration. Use the **+ Add Row** function as needed to add additional SNMP v3 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 "*" .

5. Select **OK** to update the SNMP configuration. Select **Reset** to revert to the last saved configuration.

10.1.1.5 SNMP Trap Configuration

► *Adding or Editing a Management Access Policy*

The AP-6511 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 the **SNMP Traps** tab from the Management Policy screen.

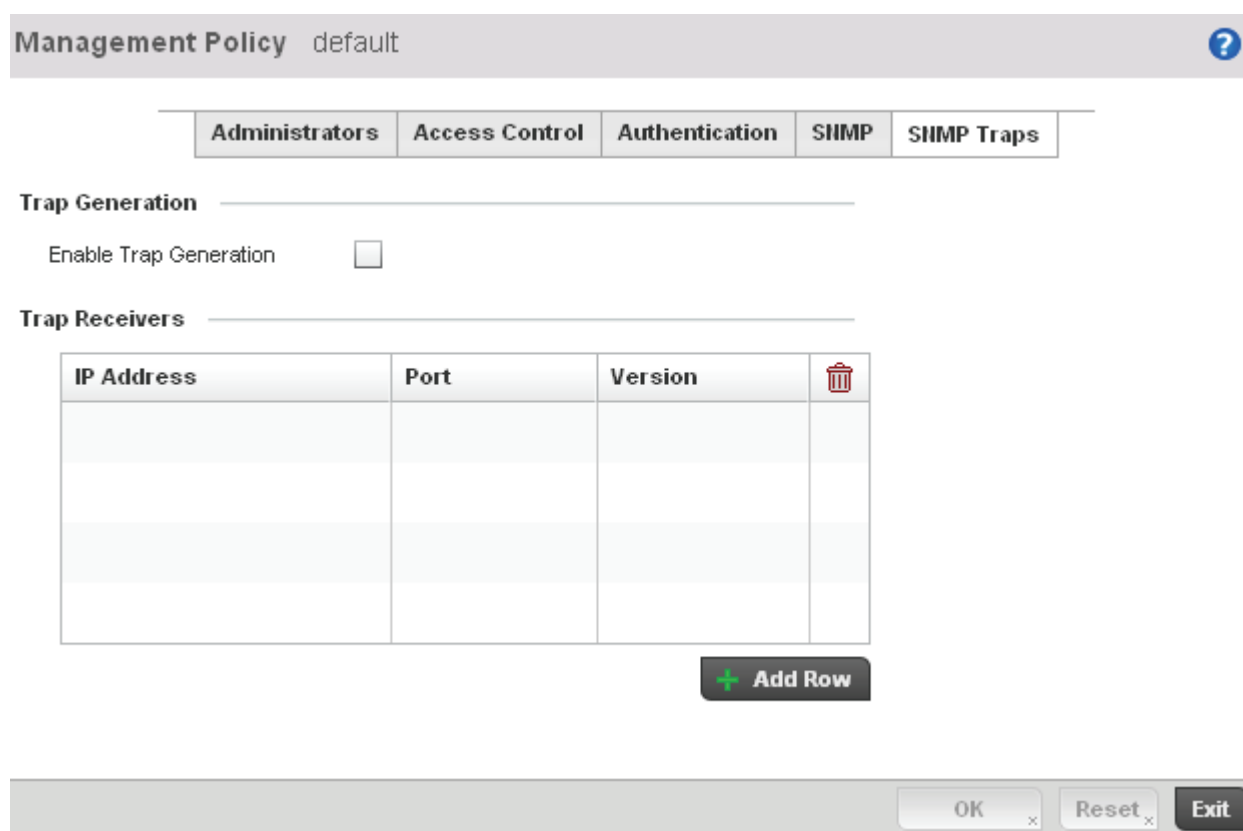


Figure 10-8 Management Policy screen - SNMP Traps tab

2. Select the **Enable Trap Generation** checkbox to enable trap creation using the trap receiver configuration. This feature is disabled by default.
3. 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.

Port	Set the server port dedicated to receiving SNMP traps. The default port is port 162.
Version	Set the SNMP version for sending SNMP traps. SNMPv2 is the default.

4. Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

10.1.2 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. Legacy Motorola Solutions devices may use other community strings by default.
- Motorola Solutions recommends 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.

Diagnostics

An AP-6511'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 allowing you to manage files generated when hardware or software issues are detected.

AP-6511 diagnostics include:

- *Fault Management*
- *Snapshots*
- *Advanced Diagnostics*

11.1 Fault Management

Fault management enables user's administering multiple sites to assess device performance and issues that may be effecting the network. Use the Fault Management screens to view and administrate errors generated by an Access Point or wireless client.

1. Select **Diagnostics > Fault Management**.

The **Configure 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.

Configure Events
?

Customize Event Filters

Severity

Module

Source

Device

Add to Active Filters

Active Event Filters

Severity	Module	Source	Device	Remove Filter
All Severities	All Modules	Allow All	Allow All	Click to Remove

Enable All Events
Disable All Events
Activate Defined Filter(s)

Figure 11-1 Fault Management Configure Events screen

Use the **Configure Events** screen to create filters for managing AP-6511 events. Events can be filtered based on severity, the module received, the source MAC of the event, the device MAC of the event and the MAC address of the wireless client.

2. Define the following **Customize Event Filters** for the Fault Management configuration:

Severity	Set the severity of the event being filtered. Select from the following: <i>All Severities</i> – All events are displayed irrespective of their severity <i>Critical</i> – Only critical events are displayed <i>Error</i> – Only errors are displayed <i>Warning</i> – Only warnings are displayed <i>Informational</i> – Only informational events are displayed
Module	Select the module from which events are tracked. When a module is selected, events from other modules are not tracked. Remember this when interested in events generated by a particular module. Individual modules can be selected (such as TEST, LOG, FSM etc.) or all modules can be tracked by selecting All Modules.
Source	Set the MAC address of the source device being tracked. Setting a MAC address of 00:00:00:00:00:00 allows all devices to be tracked.
Device	Set the device MAC address for the device from which the source MAC address is tracked. Setting a MAC address of 00:00:00:00:00:00 allows all devices.
Remove Filter	To remove a filter, click the Click to Remove link located in every row of the table.



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.

-
-
3. 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.
 4. 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, click the event, then select the **Activate Defined Filter** button.



NOTE: Filters cannot be persisted across sessions. They must be created every time a new session is established.

-
-
5. Select **View Events** from the upper, left-hand, side of the Fault Management browser.

View Events ?				
Timestamp	Module	Message	Severity	Source
Sun Nov 21 4:23:	SYSTEM	Logged out User: 'admin' with privilege 'superuser'	Warning	5C-0E-8B-08-35-

Clear All

Figure 11-2 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.

6. 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 or fault 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: <i>All Severities</i> – All events are displayed regardless of their severity <i>Critical</i> – Only critical events are displayed <i>Error</i> – Only errors are displayed <i>Warning</i> – Only warnings are displayed <i>Informational</i> – Only informational events are displayed
Source	Displays the MAC address of the source device tracked by the selected module.

7. Select **Clear All** to clear the events displayed on this screen and begin a new event data collection.

11.2 Snapshots

Use the Snapshots screens to review *panic* and *core* dump files created when a device encounters a critical error or malfunction.

11.2.1 Core Snapshots

► Snapshots

Refer to the **Core Snapshots** screen to view core dump files (system events and process failures with a .core extension) to troubleshoot issues specific to the device on which the core event was generated. Core snapshots are issues impacting the core (distribution layer). Once reviewed, core files can be deleted or transferred for archive. Core files can be sent to a support team to expedite issues with the reporting device.

To review core snapshots impacting the network:

1. Select **Diagnostics > Snapshots**.

The Core Snapshots screen displays by default. This screen displays a list of device MAC addresses impacted by core dumps.

2. Select a device from those displayed in the lower, left-hand, side of the UI.

Core Snapshots ?		
Device ⌵	System Name	Type
5C-0E-8B-08-35-59	CONTROLLER-A20	AP6511
5C-0E-8B-08-35-71	ap6511-083571	AP6511
5C-0E-8B-08-42-40	ap6511-084240	AP6511
5C-0E-8B-08-42-8E	ap6511-08428E	AP6511

Type to search in tables Row Count: 4

Figure 11-3 Core Snapshots screen

3. The screen expands to display the following parameters for each reported core snapshot:

Device	Displays the factory encoded MAC address assigned to the device reporting the core event.
System Name	Lists the name assigned to each listed AP-6511 managed device.
Type	Displays the device type (model) of each device providing the core event.

11.2.2 Panic Snapshots

▶ *Snapshots*

Refer to the **Panic Snapshots** screen to view panic dump files used to troubleshoot issues specific to the device on which it was generated. When necessary for issue evaluation, panic files can be sent to the support team to expedite issues with the reporting device.

To review panic snapshots impacting the network:

1. Select **Diagnostics > Snapshots**.
2. Select **Panic Snapshots** from the upper, left-hand, side of the UI. A list of device MAC addresses impacted by panic events displays.
3. Select a device from those displayed in the lower, left-hand, side of the UI.

Panic Snapshots		
Device	System Name	Type
5C-0E-8B-08-35-59	CONTROLLER-A20	AP6511
5C-0E-8B-08-35-71	ap6511-083571	AP6511
5C-0E-8B-08-42-40	ap6511-084240	AP6511
5C-0E-8B-08-42-8E	ap6511-08428E	AP6511

Type to search in tables Row Count: 4

Figure 11-4 Panic Snapshots screen

4. The screen expands to display the following parameters for each reported panic snapshot:

- Device** Displays the factory encoded MAC address assigned to the device reporting the panic.
- System Name** Lists the name assigned to each listed managed device.
- Type** Displays the device type (model) of each device providing a panic.

11.3 Advanced Diagnostics

Refer to the Advanced UI Diagnostics to review and troubleshoot any potential issue with the resident *User Interface* (UI). The UI Diagnostics screen provides a large number of diagnostic tools to effectively identify and correct issues. Diagnostics can also be performed at the device level for connected clients.

To access the UI diagnostics:

1. Select **Diagnostics > Advanced** to display the UI Debugging and View UI Logs menu options.

The UI Debugging screen displays by default.

The lower, left-hand, corner of the UI displays a browser view. Select a device from amongst those displayed to debug its configuration.

2. To view specific device debugging information, select the target device from the browser. Information about the device is populated automatically in the main UI window.

The UI Diagnostics browser is available with each diagnostic screen. This enables you to view and filter diagnostic information on a per-device basis throughout the Diagnostics screen flow.

11.3.1 UI Debugging

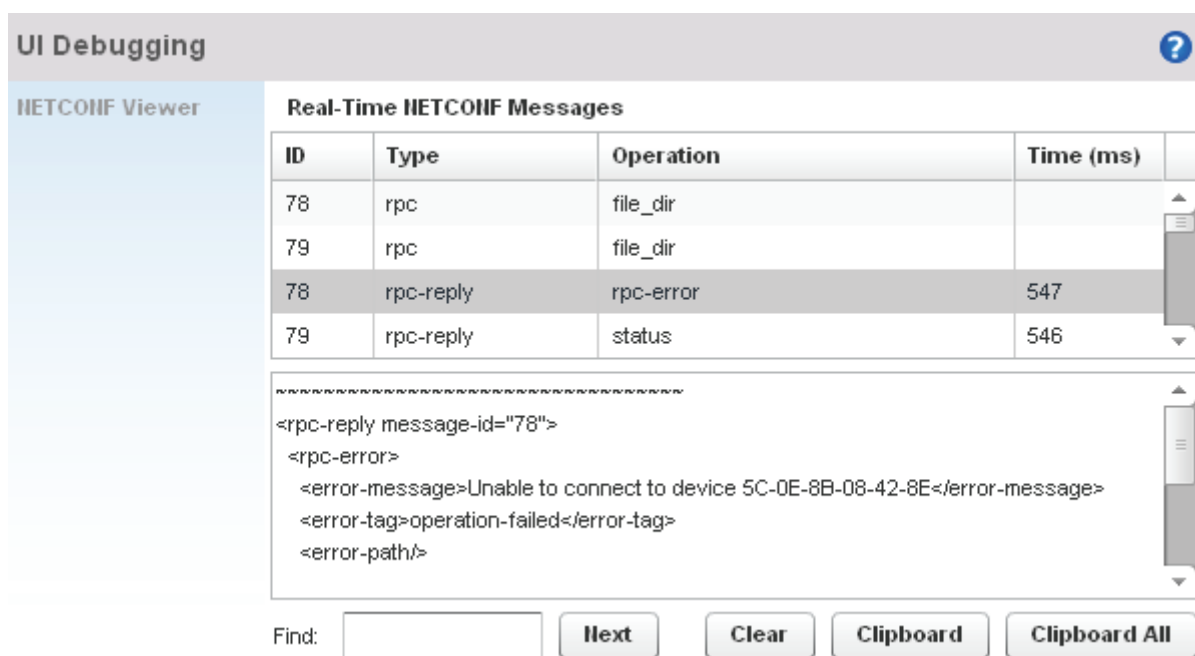
► Advanced Diagnostics

Use the UI Debugging screen to view debugging information for a selected device.

To review device debugging information:

1. Select **Diagnostics > Advanced** to display the UI Debugging menu options.

Once a target device has been selected, its debugging information displays within the **NETCONF Viewer** by default.



UI Debugging

NETCONF Viewer

Real-Time NETCONF Messages

ID	Type	Operation	Time (ms)
78	rpc	file_dir	
79	rpc	file_dir	
78	rpc-reply	rpc-error	547
79	rpc-reply	status	546

```

<rpc-reply message-id="78">
  <rpc-error>
    <error-message>Unable to connect to device 5C-0E-8B-08-42-8E</error-message>
    <error-tag>operation-failed</error-tag>
    <error-path/>
  </rpc-error>
</rpc-reply>

```

Find: **Next** **Clear** **Clipboard** **Clipboard All**

Figure 11-5 UI Debugging screen - NETCONF Viewer

2. Use the **NETCONF Viewer** to review NETCONF information. NETCONF is a tag-based configuration protocol. Messages are exchanged using XML tags.

The **Real Time NETCONF Messages** area lists an XML representation of any message generated by the system. The main display area of the screen is updated in real time.

Refer to the **Request Response** and **Time Taken** fields on the bottom of the screen to assess the time taken to receive and respond to requests. The time is displayed in microseconds.

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.

3. Select **View UI Logs** from the upper, left-hand, side of the browser to view *Application Logs*, *Flex Logs* and *Error Logs*.

The *Sequence* (order of occurrence), *Date/Time*, *Type*, *Category* and *Message* items display for each log option selected.

Sequ	Date/Time	Type	Category	Message
3	1/27/2011 09:5	INFO	com.motorola.wing.ui.framework.sei	Changes saved
4	1/27/2011 09:5	INFO	com.motorola.wing.ui.framework.vie	Saving data...
5	1/27/2011 09:5	ERRC	com.motorola.wing.ui.framework.sei	Error on write
6	1/27/2011 09:5	ERRC	com.motorola.wing.ui.framework.sei	Error on write
7	1/27/2011 09:5	INFO	com.motorola.wing.ui.framework.sei	Changes saved
8	1/27/2011 09:5	INFO	com.motorola.wing.ui.framework.vie	Saving data...
9	1/27/2011 10:0	ERRC	com.motorola.wing.ui.framework.vie	Table error: invalid entry in 'Destination', 'Gateway...
10	1/27/2011 10:0	ERRC	com.motorola.wing.ui.framework.vie	Table error: invalid entry in 'Destination', 'Gateway...
11	1/27/2011 10:0	ERRC	com.motorola.wing.ui.framework.vie	Table error: invalid entry in 'Destination', 'Gateway...
12	1/27/2011 10:0	ERRC	com.motorola.wing.ui.framework.vie	Table error: invalid entry in 'Destination', 'Gateway...
13	1/27/2011 10:0	ERRC	com.motorola.wing.ui.framework.vie	Table error: invalid entry in 'Destination', 'Gateway...

Figure 11-6 View UI Logs screen - Application Logs tab

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 a Motorola Solutions 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:

- [*Device Operations*](#)
- [*Certificates*](#)
- [*Smart RF*](#)

12.1 Device Operations

▶ *Operations*

Motorola Solutions periodically releases updated device firmware and configuration files to the Motorola Solutions Support Web site. If an Access Point's (or its associated device's) firmware is older than the version on the Web site, Motorola Solutions recommends updating to the latest firmware version for full feature functionality and optimal utilization. Additionally, selected devices can either have a primary or secondary firmware image applied or fallback back to a selected firmware image if an error were to occur in the update process.

Device update activities include:

- *Managing Firmware and Config Files*
- *Managing File Transfers*
- *Using the File Browser*
- *AP Upgrade*

These tasks can be performed on individual, Access Points and wireless clients.

12.1.1 **Managing Firmware and Config Files**

▶ *Device Operations*

The **Device Details** screen displays by default when the **Operations** menu item is selected from the main menu bar.

The Device Details screen displays firmware information for a specific device selected from either the RF Domain or Network tabs on the right-hand side of the screen.

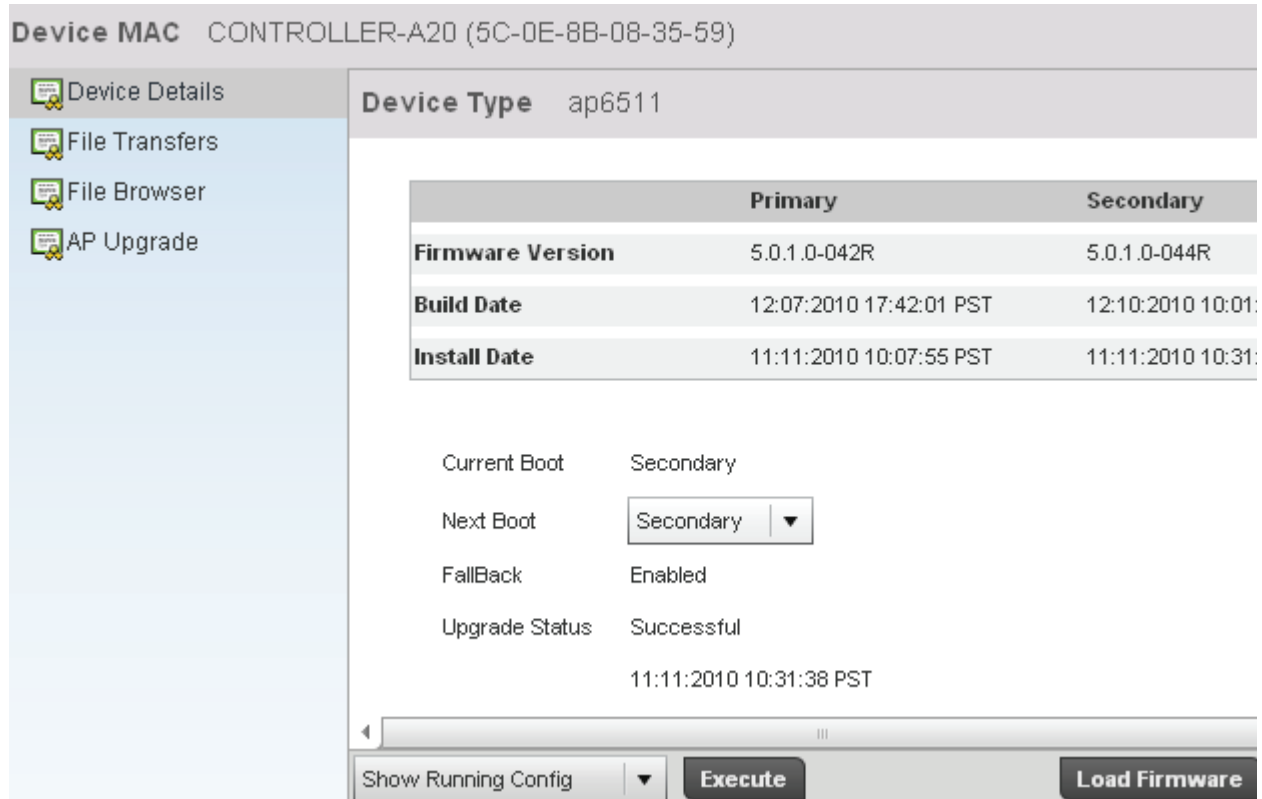


Figure 12-1 Device Details screen

Refer to the following to determine whether a firmware image needs to be updated for the selected device, or a device requires a restart or revert to factory default settings.

- Device MAC** Displays the factory assigned hardware MAC address (in the banner of the screen) for the selected device. The Device Type also displays in the banner of the screen.
- Firmware Version** Displays the primary and secondary firmware image version form the AP6511.
- Build Date** Displays the date the primary and secondary firmware image was built for the selected device.
- Install Date** Displays the date the firmware was installed for the selected device.
- Current Boot** Lists whether the primary or secondary firmware image is to be applied to the device the next time the device boots.
- Next Boot** Use the drop-down menu to select the firmware image to boot the next time the device reboots. Select either the **Primary** or the **Secondary** image.
- 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.

Upgrade Status	Displays the status of the last firmware upgrade performed for each listed device. For information on upgrading device firmware, see Upgrading Device Firmware on page 12-5 .
Show Startup Config	Select this option (from the drop-down menu on the bottom of the screen) to display the startup configuration of the selected device. The startup configuration is displayed in a separate window. Select the Execute button to perform the function.
Show Running Config	Select this option (from the drop-down menu on the bottom of the screen) to display the running configuration of the selected device. The running configuration is displayed in a separate window. Select the Execute button to perform the function.
Restart	Select this option (from the drop-down menu on the bottom of the screen) to restart the selected device. Selecting this option restarts the target device using its last saved configuration and does not apply factory defaults to the target device. Restarting a device resets all data collection values to zero. Select the Execute button to perform the function.
Restart (factory default)	Select this option (from the drop-down menu on the bottom of the screen) to restart the selected device and apply the device's factory default configuration. Selecting this option restarts the target device and applies all of its configurable parameters to their factory default values. Consider exporting the device's current configuration to a secure location for archive and potential import back to the device before reverting the device to its default configuration. Select the Execute button to perform the function.
Halt	Select this option (from the drop-down menu on the bottom of the screen) to stop the selected device. Select the Execute button to perform the function.

For information on conducting a device firmware upgrade, see [Upgrading Device Firmware on page 12-5](#). For information on file transfers, see [Managing File Transfers on page 12-6](#).

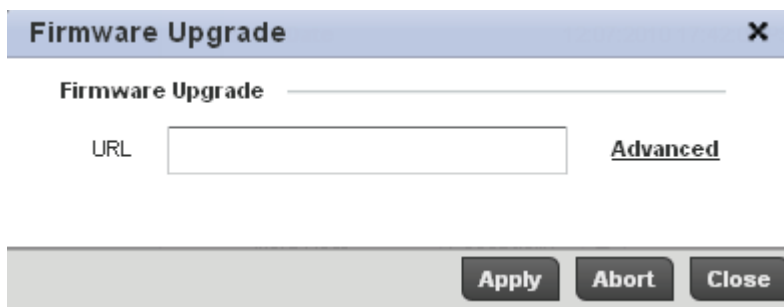
12.1.1.1 Upgrading Device Firmware

► *Managing Firmware and Config Files*

The AP-6511 has the ability to conduct firmware updates for managed devices.

To update the firmware of a managed device:

1. Select a device from either the RF Domain or Network tabs.
2. Select the **Load Firmware** button from within the Device Details screen.



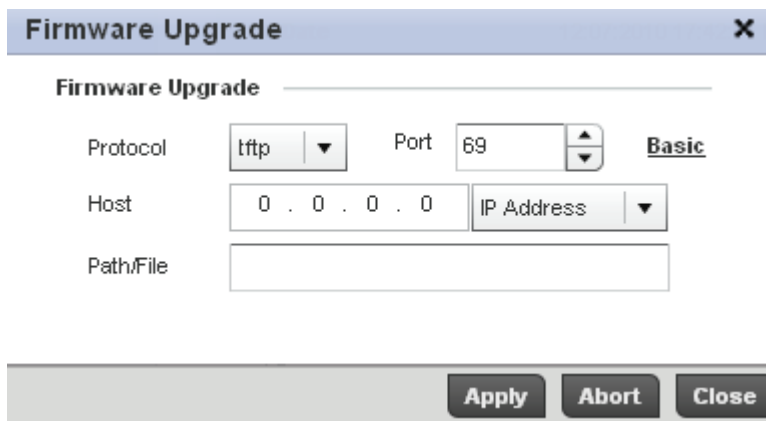
The screenshot shows a dialog box titled "Firmware Upgrade" with a close button (X) in the top right corner. Below the title bar, the text "Firmware Upgrade" is followed by a horizontal line. Underneath, there is a label "URL" next to an empty text input field. To the right of the input field is the word "Advanced" in a bold, italicized font. At the bottom of the dialog, there are three buttons: "Apply", "Abort", and "Close".

Figure 12-2 *Firmware Upgrade screen*

By default, the **Firmware Upgrade** screen displays a **URL** field to enter the URL (destination location) of the target device firmware file.

Enter the complete path to the firmware file for the target device.

3. If needed, select **Advanced** to expand the dialog to display network address information to the location of the target device firmware. The number of additional fields that populate the screen is also dependent on the selected protocol.



The screenshot shows the "Firmware Upgrade" dialog box in its expanded "Advanced" mode. The title bar and close button are the same. Below the title bar, the text "Firmware Upgrade" is followed by a horizontal line. The form contains several fields: "Protocol" is a dropdown menu set to "tftp"; "Port" is a numeric input field set to "69"; "Host" is a dotted IP address input field set to "0 . 0 . 0 . 0" with a dropdown menu labeled "IP Address" to its right; and "Path/File" is an empty text input field. To the right of the "Port" and "Host" fields is the word "Basic" in a bold, italicized font. At the bottom of the dialog, there are three buttons: "Apply", "Abort", and "Close".

Figure 12-3 *Advanced Firmware Upgrade screen*

4. Provide the following information to accurately define the location of the target device firmware file:

Protocol	Select the protocol used for updating device firmware. Available options include: <ul style="list-style-type: none">• <i>tftp</i>• <i>ftp</i>• <i>sftp</i>• <i>http</i>• <i>cf</i>• <i>usb1</i>• <i>usb2</i>
Port	Use the spinner control or manually enter the value to define the port used by the protocol for firmware updates. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to update the firmware. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to update the firmware. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
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 <i>ftp</i> or <i>sftp</i> .
Password	Specify the password for the user account to access a FTP or a SFTP server. This field is only available if the selected protocol is <i>ftp</i> or <i>sftp</i> .

5. Select **OK** 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.

12.1.2 Managing File Transfers

▶ Device Operations

Transfer files from a device to this AP-6511, to a remote server or from a remote server. An administrator can transfer logs, configurations and crash dumps.

To administrate files for managed devices:

1. Select the **Operations > Devices > File Transfers**

Figure 12-4 File Transfers screen

- Set the following file management source and target directions as well as the configuration parameters of the required file transfer activity:

Source

Select the source of the file transfer.

Select *Server* to indicate the source of the file is a remote server.

Select *Access Point* to indicate the source of the file is the AP-6511.

File

If the source is *Access Point*, enter the name of the file to be transferred.

Protocol

Select the protocol for file management. Available options include:

- *tftp*
- *ftp*
- *sftp*
- *http*
- *cf*
- *usb1*
- *usb2*

This parameter is required only when *Server* is selected as the **Source** and **Advanced** is selected.

Port	Specify the port for transferring files. This option is not available for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> . Enter the port number directly or use the spinner control. This parameter is required only when <i>Server</i> is selected as the Source .
IP Address	Specify the IP address of the server used to transfer files. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> . If IP address of the server is provided, a Hostname is not required. This parameter is required only when <i>Server</i> is selected as the Source .
Hostname	If needed, specify a Hostname of the server transferring the file. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> . If a hostname is provided, an IP Address is not needed. This field is only available when <i>Server</i> is selected in the From field.
Path	Define the path to the file on the server. Enter the complete relative path to the file. This parameter is required only when <i>Server</i> is selected as the Source .
User Name	Provide a user name to access a FTP or SFTP server. This parameter is required only when <i>Server</i> is selected as the Source , and the selected protocol is <i>ftp</i> or <i>sftp</i> .
Password	Provide a password to access the FTP or SFTP server. This parameter is required only when <i>Server</i> is selected as the Source , and the selected protocol is <i>ftp</i> or <i>sftp</i> .
Target	Select the target destination to transfer the file. <ul style="list-style-type: none">• Select <i>Server</i> 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 <i>Access Point</i> if the destination is an AP-6511.

3. Select **Copy** to begin the file transfer. Selecting **Reset** reverts the screen to its last saved configuration.

12.1.3 Using the File Browser

► Device Operations

The AP-6511 maintains a File Browser enabling an administrator to review the files currently residing on any internal or external memory locations. Directories can be created and maintained for each File Browser location and folders and files can be moved and deleted as an administrator interprets necessary.

To administrate files for managed devices and memory resources:

1. Select the **Operations > Devices > File Browser**.

Device MAC ap6511-083571 (5C-0E-8B-08-35-71) ?

- Device Details
- File Transfers
- File Browser
- AP Upgrade

File Browser

flash
system
nvrAm

Path: flash:/

	File Name	Size	Last Modified
crashinfo			
log	mcn1.cfg	1864	01:01:2010 00:03:41
cache			
hotspot			

Add New Folder

Create Folder

Rename File

Rename File

Delete Folder Delete File

Figure 12-5 File Browser screen - flash

- Refer to the following to determine whether a file needs to be deleted or included in a new folder for the selected memory resource. The following display for each of the available memory resources.

File Name	Displays the name of the file residing on the selected <i>flash</i> , <i>system</i> , <i>nvrAm</i> , <i>usb1</i> or <i>usb2</i> location. The name cannot be modified from this location.
Size	Displays the size of the file in kb. Use this information to help determine whether the file should be moved or deleted.
Last Modified	Lists a timestamp for the last time each listed file was modified. Use this information to help determine the file's relevance and whether it should be deleted.

- If needed, use the **Add New Folder** utility to create a folder that servers as a directory for some or all of the files for a selected memory resource. Once defined, select the **Create Folder** button to implement.
- Optionally, use the **Delete Folder** or **Delete File** buttons to remove a folder or file from within the memory resource.

12.1.4 AP Upgrade

► Device Operations

To configure an AP upgrade for an AP-6511:

1. Select the **Operations > Devices > AP Upgrade**.

The screenshot shows the 'AP Upgrade' configuration page. At the top, there are three tabs: 'AP Upgrade List', 'AP Image File', and 'Status'. Below the tabs, the 'AP Type List' is set to 'AP6511'. The 'Scheduled Upgrade Time' is set to 'Now' with a date of '01/27/2011' and a time of '00:00'. The 'Scheduled Reboot Time' is also set to 'Now' with the same date and time. There is a 'No Reboot' checkbox which is currently unchecked. Below these settings are two tables: 'All Devices' and 'Upgrade List', both with columns for 'Hostname' and 'MAC'. Between the tables are two buttons: '>>|' and '>>'. At the bottom right, there are 'Cancel' and 'Update Fi' buttons.

Figure 12-6 AP Upgrade screen - AP Upgrade List

2. Refer to the following to configure AP Upgrade parameters.

AP Type List

Select the Access Point model from the drop-down to specify which model types should be available to upgrade. Available options are:

All - All supported models are available to upgrade.

AP6511 - Only AP-6511 models are available to upgrade.

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 in the appropriate boxes. 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.

Now

To reboot the APs being upgraded immediately, select the box marked **Now**. To schedule the reboot to take place at a specified time in the future, enter a date and time in the appropriate boxes. If you do not wish for the APs to reboot after they have been upgraded, select the No Reboot option.

All Devices

The All Devices table list all APs available to upgrade that match the AP Type list above. For each available AP the hostname and the primary MAC Address are listed in the table.

>>|

Using the >>| button will move all APs listed in the All Devices table to the Upgrade List table.

Upgrade List	The Upgrade List table displays all the APs that have been selected for upgrade. For each AP the hostname and the primary MAC Address are listed in the table.
Cancel	Clicking the Cancel button will clear any options in this screen and cancel AP updates in progress.
Update Firmware	Clicking the Update Firmware button will update the firmware on APs listed in the Upgrade List table.

3. Select the **AP Image** tab and refer to the following configuration parameters:

AP Image Type	Select the Access Point model from the drop-down to specify which model AP image types should be available to use during an upgrade. Available options are: <i>AP6511</i> - Only AP-6511 models are available to upgrade.
URL	Enter a URL pointing to the location of available AP image files.
Advanced	Selecting Advanced will list additional options for AP image file location including protocol, host and path to the image files.
Protocol	Select the protocol to retrieve the AP image files from a remote location. Available options are: <i>tftp</i> - 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. <i>ftp</i> - 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. <i>sftp</i> - 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. <i>http</i> - Select this option to specify a file location using Hypertext Transfer Protocol. A hostname or IP address is required. Port and path are optional.
Type/Version	This table displays the available AP Image types and their corresponding version numbers.
Load Image	When the AP Image Type and appropriate file location and protocol have been specified, click the Load Image button to load all available AP image types to the Type/Version table.

4. Select the **Status** tab and refer to the following parameters:

Type	Displays the Access Point model for each known Access Point.
MAC	Displays the primary <i>Media Access Control</i> (MAC) or hardware address for each known Access Point.

State	Displays the current upgrade status of each known Access Point. Possible states include: <ul style="list-style-type: none">• <i>Waiting</i>• <i>Downloading</i>• <i>Updating Scheduled</i>• <i>Reboot</i>• <i>Rebooting Done</i>• <i>Cancelled</i>• <i>Done</i>• <i>No Reboot</i>
Progress	Displays the current progress status for each known Access Point undergoing an upgrade.
Retries	Displays the number of retries, if any, during the Access Point upgrade process.
Last Status	Displays the time of the last status update for Access Points that are no longer upgrading.
Clear History	Clicking the Clear History button will clear the current history log page for all Access Points.
Cancel	Clicking the Cancel button will cancel the upgrade process for any selected Access Points that are upgrading.

12.2 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](#)

12.2.1 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** > **Certificates**.

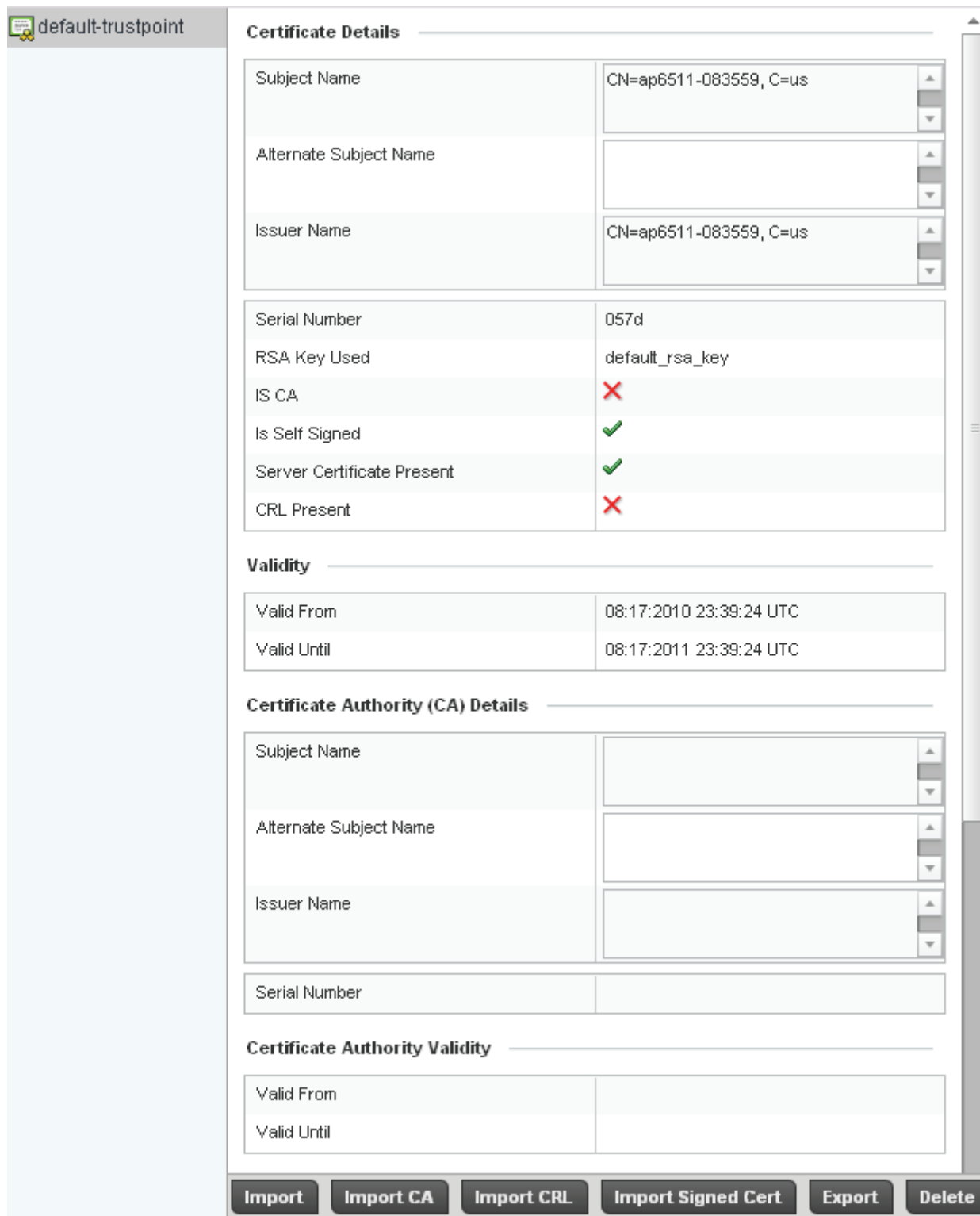


Figure 12-7 Trustpoints screen

The **Trustpoints** screen displays for the selected MAC address.

2. Refer to the **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 Trustpoints screen.

Figure 12-8 Import New Trustpoint screen

4. Define the following configuration parameters required for the **Import** 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.
- Key Passphrase** Define the key used by the target trustpoint. Select the **Show** textbox to expose the actual characters used in the key. Leaving the Show checkbox unselected displays the passphrase as a series of asterisks "***".
- 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 also dependent on the selected protocol.
- Protocol** Select the protocol used for importing the target trustpoint. Available options include:
- *tftp*
 - *ftp*
 - *sftp*
 - *http*
 - *cf*
 - *usb1*
 - *usb2*

Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to import the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the trustpoint. Enter the complete path to the file on the server.

5. Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.
6. To optionally import a CA certificate, select the **Import CA** button from the Trustpoints screen.

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*.

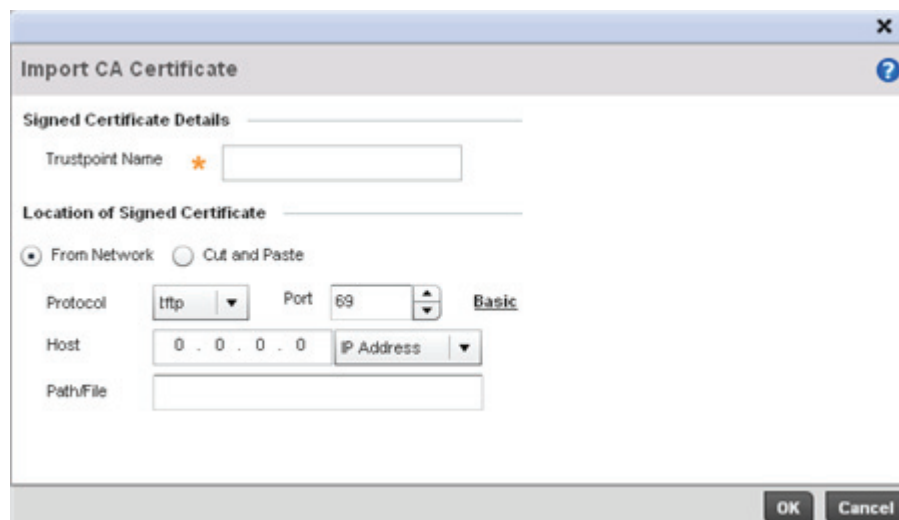


Figure 12-9 Import CA Certificate screen

7. Define the following configuration parameters required for the **Import** of the CA certificate:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
From Network	Select the From Network radio button to provide network address information to the location of the target CA certificate. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
Cut and Paste	Select the Cut and Paste radio button to simply copy an existing CA certificate into the cut and past field. When pasting a valid CA certificate, no additional network address information is required.

Protocol	Select the protocol used for importing the target CA certificate. Available options include: <ul style="list-style-type: none"> • <i>tftp</i> • <i>ftp</i> • <i>sftp</i> • <i>http</i> • <i>cf</i> • <i>usb1</i> • <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to import the CA certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the CA certificate. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the CA certificate. Enter the complete relative path to the file on the server.

8. Select **OK** to import the defined CA certificate. Select **Cancel** to revert the screen to its last saved configuration.
9. To optionally import a CRL, select the **Import CRL** button from the Trustpoints screen.

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 certificates that have been revoked or are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

Figure 12-10 Import CRL screen

10. Define the following configuration parameters required for the **Import** of the CRL:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
From Network	Select the From Network radio button to provide network address information to the location of the target CRL. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
Cut and Paste	Select Cut and Paste to copy an existing CRL into the cut and past field. When pasting a CRL no additional network address information is required.
URL	Provide the complete URL to the location of the CRL. If needed, select Advanced to expand the dialog to display network address information to the location of the target CRL. The number of additional fields that populate the screen is also dependent on the selected protocol.
Protocol	Select the protocol used for importing the CRL. Available options include: <ul style="list-style-type: none">• <i>tftp</i>• <i>ftp</i>• <i>sftp</i>• <i>http</i>• <i>cf</i>• <i>usb1</i>• <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to import the CRL. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to import the CRL. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the CRL. Enter the complete relative path to the file on the server.

11. Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.

12. To import a signed certificate, select the **Import Signed Cert** button from the Trustpoints screen.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

Self-signed certificates cannot be revoked which may allow an attacker who has already gained access to monitor and inject data into a connection to spoof an identity if a private key has been compromised. However, CAs have the ability to revoke a compromised certificate, which prevents its further use.

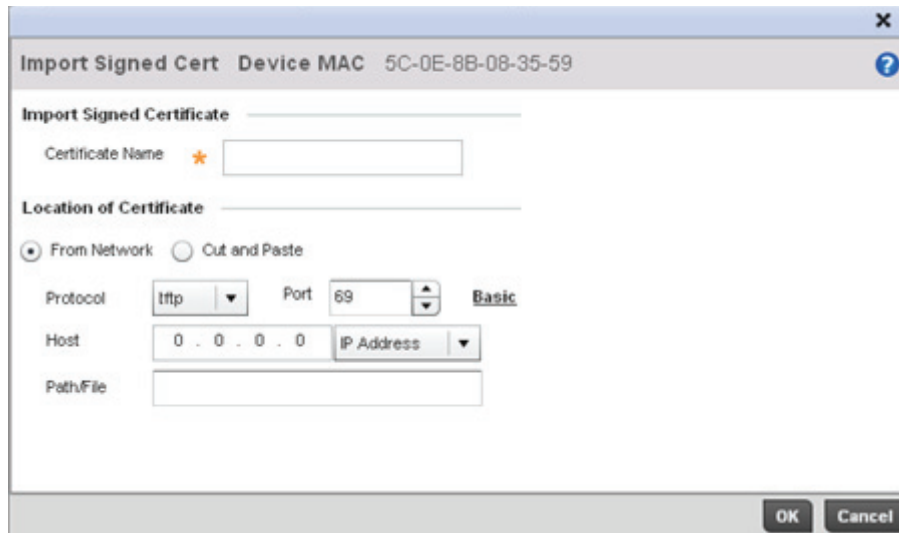


Figure 12-11 Import Signed Cert screen

13. Define the following configuration parameters required for the **Import** of the CA certificate:

- Certificate Name** Enter the 32 character maximum name of the trustpoint with which the certificate should be associated
- From Network** Select the **From Network** radio button to provide network address information to the location of the target signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
- Cut and Paste** Select the **Cut and Paste** radio button to simply copy an existing signed certificate into the cut and past field. When pasting a signed certificate, no additional network address information is required.
- URL** Provide the complete URL to the location of the signed certificate. If needed, select **Advanced** to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol.
- Protocol** Select the protocol used for importing the target signed certificate. Available options include:
- *tftp*
 - *ftp*
 - *sftp*
 - *http*
 - *cf*
 - *usb1*
 - *usb2*
- Port** Use the spinner control to set the port. This option is not valid for *cf*, *usb1*, and *usb2*.

- IP Address** Enter IP address of the server used to import the signed certificate. This option is not valid for *cf*, *usb1*, and *usb2*.
- Hostname** Provide the hostname of the server used to import the signed certificate. This option is not valid for *cf*, *usb1*, and *usb2*.
- Path** Specify the path to the signed certificate. Enter the complete relative path to the file on the server.

14. Select **OK** to import the signed certificate. Select **Cancel** to revert the screen to its last saved configuration

15. 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's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

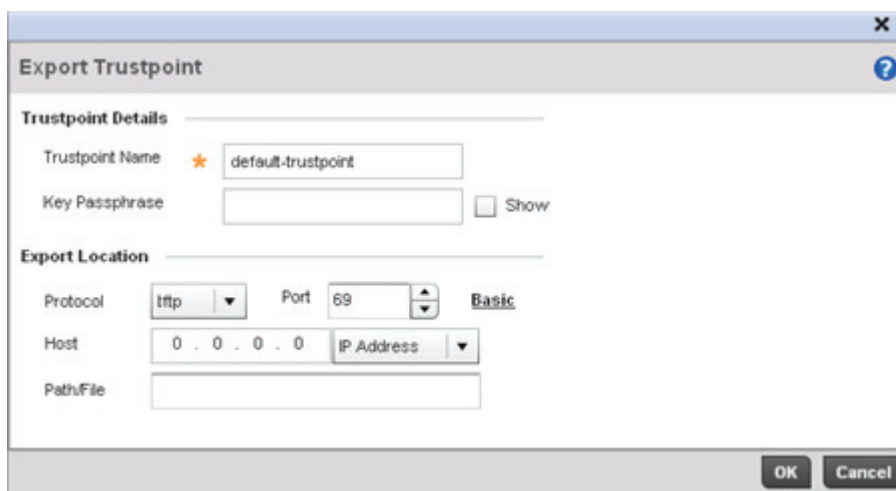


Figure 12-12 Export Trustpoint screen

16. 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.
- Key Passphrase** Define the key used by both the Access Point and the server (or repository) of the target trustpoint. Select the **Show** textbox to expose the actual characters used in the key. Leaving the Show checkbox unselected displays the passphrase as a series of asterisks "***".

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 also dependent on the selected protocol.
Protocol	Select the protocol used for exporting the target trustpoint. Available options include: <ul style="list-style-type: none">• <i>tftp</i>• <i>ftp</i>• <i>sftp</i>• <i>http</i>• <i>cf</i>• <i>usb1</i>• <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to export the trustpoint. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the trustpoint. Enter the complete relative path to the file on the server.

17. Select **OK** to export the trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

18. 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** checkbox 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.

12.2.2 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's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1. Select **Operations** > **Certificates**.
2. Select **RSA Keys**.

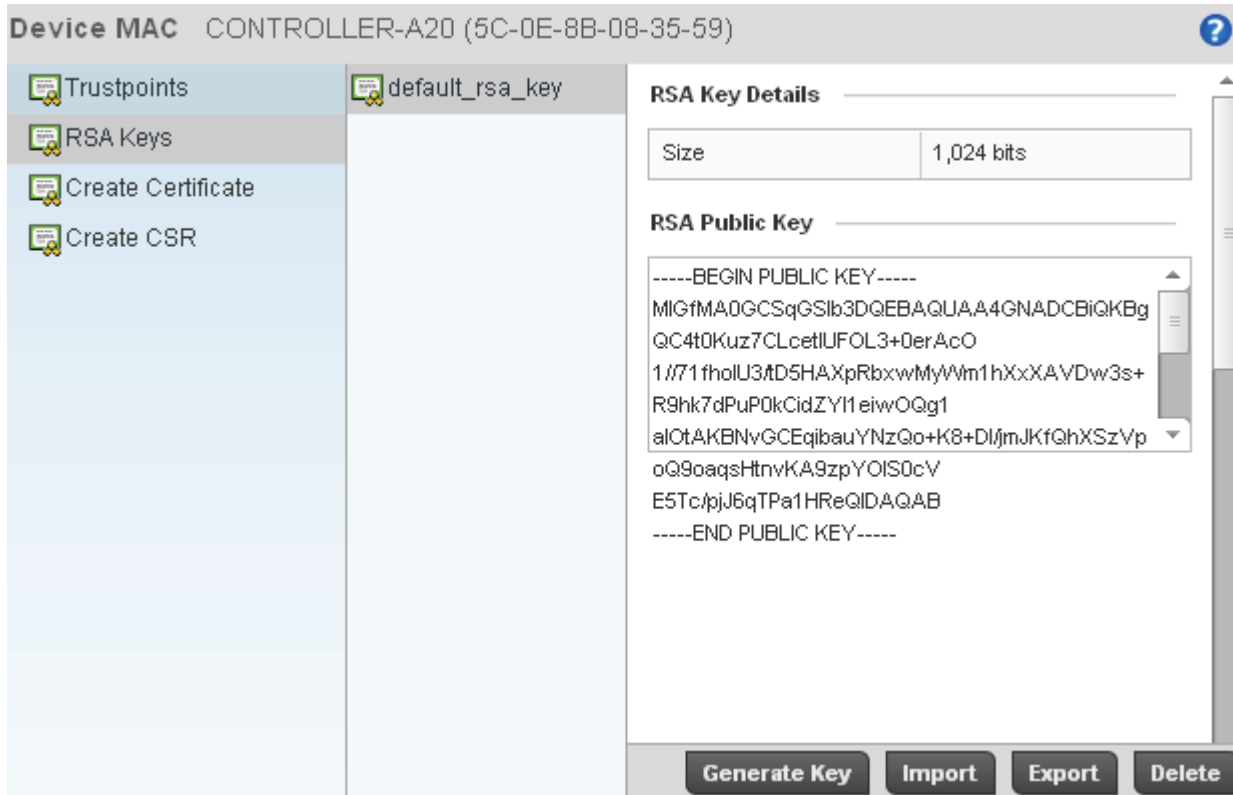


Figure 12-13 RSA Keys screen

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.

3. Select **Generate Key** to create a new key with a defined size.

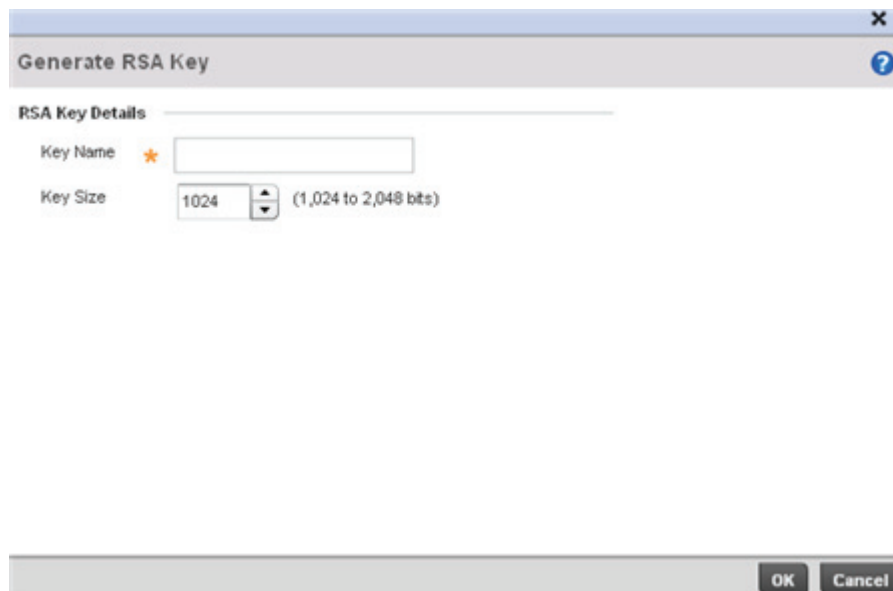


Figure 12-14 Generate RSA Key screen

4. 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). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality.

5. To optionally import a CA certificate, select the Import button from the RSA Keys screen.

Figure 12-15 Import New RSA Key screen

6. 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 Show checkbox 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 also 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*

- Port** Use the spinner control to set the port. This option is not valid for *cf*, *usb1*, and *usb2*.
- IP Address** Enter IP address of the server used to import the RSA key. This option is not valid for *cf*, *usb1*, and *usb2*.
- Hostname** Provide the hostname of the server used to import the RSA key. This option is not valid for *cf*, *usb1*, and *usb2*.
- Path** Specify the path to the RSA key. Enter the complete relative path to the key on the server.

7. Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.
8. To optionally export a RSA key to a remote location, select the **Export** button from the RSA Keys screen.
9. Export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

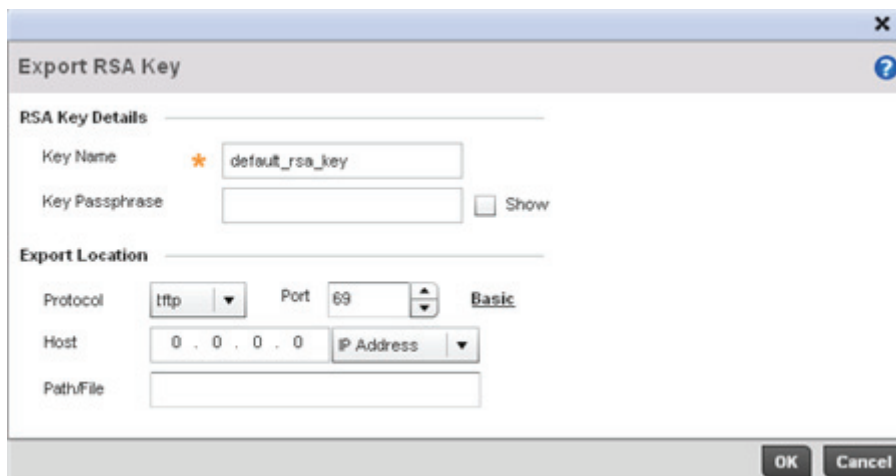


Figure 12-16 Export RSA Key screen

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 Show checkbox 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: <ul style="list-style-type: none"> • <i>tftp</i> • <i>ftp</i> • <i>sftp</i> • <i>http</i> • <i>cf</i> • <i>usb1</i> • <i>usb2</i>
Port	Use the spinner control to set the port. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
IP Address	Enter IP address of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Hostname	Provide the hostname of the server used to export the RSA key. This option is not valid for <i>cf</i> , <i>usb1</i> , and <i>usb2</i> .
Path	Specify the path to the key. Enter the complete relative path to the key on the server.

10. Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to the last saved configuration.

11. 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** checkbox to remove the certificate the key supported. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the last saved configuration.

12.2.3 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** > **Certificates**.
2. Select **Create Certificate**.

Device MAC CONTROLLER-A20 (5C-0E-8B-08-35-59)

- Trustpoints
- RSA Keys
- Create Certificate
- Create CSR

Create New Self-Signed Certificate

Certificate Name *

RSA Key Create New Use Existing

* 1025 (1,02)

Certificate Subject Name

Certificate Subject Name * auto-generate user-configured

Country (C)

State (ST)

City (L)

Organization (O)

Organizational Unit (OU)

Common Name (CN)

Additional Credentials

Email Address

Domain Name

IP Address

Figure 12-17 Create Certificate screen

3. Define the following configuration parameters required to Create New Self-Signed Certificate:

Certificate Name

Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

Use an Existing RSA Key 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.

Create a New RSA Key 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 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality. For more information on creating a new RSA key, see [RSA Key Management on page 12-21](#).

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-defined* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.

Country (C) Define the Country used in the certificate. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.

State (ST) Enter 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 Org. Unit for the name of the organization unit used in the certificate. This is a required field.

Common Name (CN) If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Select the following Additional Credentials required for the generation of the self signed certificate:

Email Address Provide an email address used as the contact address for issues relating to this certificate request.

Domain Name) Enter a *fully qualified domain name (FQDN)* 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.

6. Select the **Generate Certificate** button at the bottom of the Create Certificate screen to produce the certificate.

12.2.4 Generating a Certificate Signing Request

► 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** > **Certificates**.
2. Select **Create CSR**.

Device MAC CONTROLLER-A20 (5C-0E-8B-08-35-59)

Trustpoints

RSA Keys

Create Certificate

Create CSR

Create New Certificate Signing Request (CSR)

RSA Key Create New Use Existing

* 1024 (1,024)

Certificate Subject Name

Certificate Subject Name auto-generate user-configured

*

Country (C)

State (ST)

City (L)

Organization (O)

Organizational Unit (OU)

Common Name (CN)

Additional Credentials

Email Address

Domain Name

IP Address

Figure 12-18 Create CSR screen

3. Define the following configuration parameters required to Create New Certificate Signing Request (CSR):

Use an Existing RSA Key

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 or use an existing key by selecting the appropriate radio button. Use the spinner control to set the size of the key (between 1,024 - 2,048 bits). Motorola Solutions recommends leaving this value at the default setting of 1024 to ensure optimum functionality. For more information, see [RSA Key Management on page 12-21](#).

4. Set the following Certificate Subject Name parameters required for the creation of the certificate:

Certificate Subject Name	Select either the <i>auto-generate</i> radio button to automatically create the certificate's subject credentials or select <i>user-defined</i> 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 Org. Unit for the name of the organization unit used in the CSR. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5. Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an email address used as the contact address for issues relating to this CSR.
Domain Name)	Enter a <i>fully qualified domain name</i> (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.

6. Select the **Generate CSR** button at the bottom of the screen to produce the CSR.

12.3 Smart RF

► Operations

Self Monitoring At Run Time RF Management (Smart RF) is a Motorola 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, which typically require manual reconfiguration to resolve.

Within the Operations node, Smart RF is managed using the Access Points that comprise the AP-6511's RF Domain and their respective radio and channel configurations as the basis to conduct Smart RF calibration operations.

12.3.1 Managing Smart RF for an RF Domain

► Smart RF

When calibration is initiated, Smart RF instructs adopted radios (within a selected RF Domain) to beacon on a specific legal channel, using a specific transmit power setting. Smart RF measures the signal strength of each beacon received from both managed and unmanaged neighboring APs to define a RF map of the neighboring radio coverage area. Smart RF uses this information to calculate each managed radio's RF configuration as well as assign radio roles, channel and power.

Within a well planned AP-6511 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, unmanaged 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 for the AP-6511's RF Domain:

1. Select **Operations** > **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.

Old Power	Lists the transmit power assigned to each listed Access Point MAC address within this RF Domain. The power level may have been increased or decreased as part an Interactive Calibration process applied to this RF Domain. Compare this Old Power level against the Power value to right of it (in the table) to determine whether a new power level was warranted to compensate for a coverage hole.
Power	This column displays the transmit power level for the listed Access Point MAC address after an Interactive Calibration resulted in 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: <i>Normal</i> , <i>Offline</i> and <i>Sensor</i> .
Type	Displays the radio type (802.11an, 802.11bgn etc.) of each listed Access Point radio within the selected RF Domain.

3. Select the **Refresh** button to (as required) to update the contents of the Smart RF screen and the attributes of the devices within the selected RF Domain.
4. Select the **Interactive Calibration** button to initiate a Smart RF calibration using the Access Points within the selected RF Domain. The results of the calibration display within the Smart RF screen. Of particular interest are the channel and power adjustments made by the 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 launch a sub screen used to determine the actions taken based on the results of the Interactive Calibration. The results of an Interactive calibration are not applied to radios directly, the administrator has the choice to select one of following options.

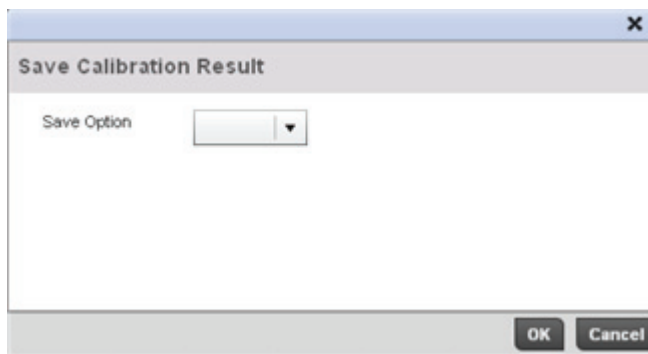


Figure 12-20 Save Calibration Result screen

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.

13

Statistics

This chapter describes the statistical information displayed by the AP-6511 GUI.

Statistics can be exclusively displayed to validate active Access Points, their VLAN assignments and the current authentication and encryption schemes.

Wireless client statistics are available for each connected client to provide 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.

The contents of this chapter are arranged as follows:

- *System Statistics*
- *RF Domain*
- *Access Point Statistics*
- *Wireless Client Statistics*

13.1 System Statistics

The **System** screen displays information about the different devices managed by the Access Point. Use this information to obtain an overall view of the state of the devices in the network. The data is organized as follows:

- [Health](#)
- [Inventory](#)

13.1.1 Health

▶ [System Statistics](#)

The *Health* screen displays information on the overall performance of the wireless network. This includes information on the device availability, overall RF quality, utilization of available resources and the threat perception for the networks and devices.

To display the health statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and select the **System** node.
3. Select **Health**.

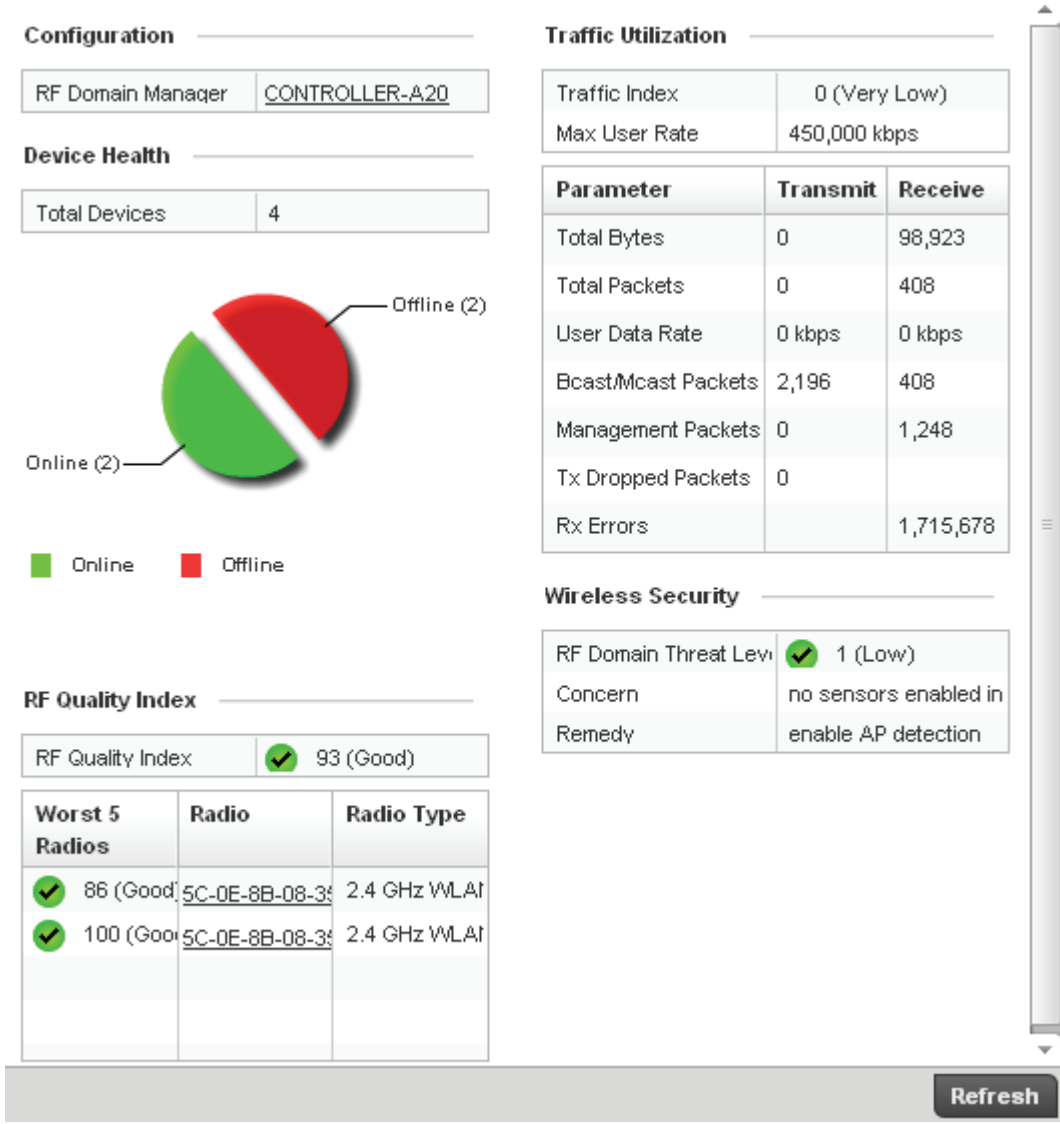


Figure 13-1 System screen

This screen displays fields supporting **Device Health**, **RF Quality Index**, **Utilization**, and **Wireless Security**.

The **Device Health** field displays a table showing the total number of devices in the network. The pie chart illustrates a proportional view of how many devices are functional and are currently online. Green indicates online devices and the red offline devices.

The **RF Quality Index** field displays the overall RF performance of the network. Quality indices are:

- 0–50 (Poor)
- 50–75 (Medium)
- 75–100 (Good).

This area displays the following information:

- Worst 5** Displays the lowest quality indices in the wireless network. The values 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.

The **Utilization Index** field displays a table with a list of RF Domain with the most effective resource utilization. Utilization is dependent on the number of devices connected to the RF Domain.

- Best 5** Utilization index is a measure of how efficiently the domain is utilized. This value is defined as a percentage of current throughput relative to the maximum possible throughput. The values are:
- 0-20 – Very low utilization
 - 20-40 – Low utilization
 - 40-60 – Moderate utilization
 - 60 and above – High utilization
- RF Domain** Displays the name of the RF Domain.
- Client Count** Displays the number of wireless clients associated with the RF Domain.

The **Utilization Index** field also displays packet transmit and receive data:

- Total Packets** Displays the total number of data packets transmitted and received by the system.
- Total Bcast/Mcast Packets** Displays the total number of broadcast/multicast packets processed by the system.
- Total Management Packets** Displays the total number of management packets processed by the system.

The **Wireless Security** field defines device security in each RF domain. The Average Threat Index is an integer value indicating the threat to the system as a whole.

The **Wireless Security** field also displays a table that displays the top 5 in terms of threat perception.

- Top 5** 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 RF Domain for which the threat level is displayed.
- Concern** Describes the top most threat to the devices in this RF domain.

13.1.2 Inventory

► *System Statistics*

The *Inventory* screen displays information about the physical hardware managed by the AP-6511. Use this information to assess the overall performance of managed devices.

To display the inventory statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select **System**.
3. Select **Inventory**.

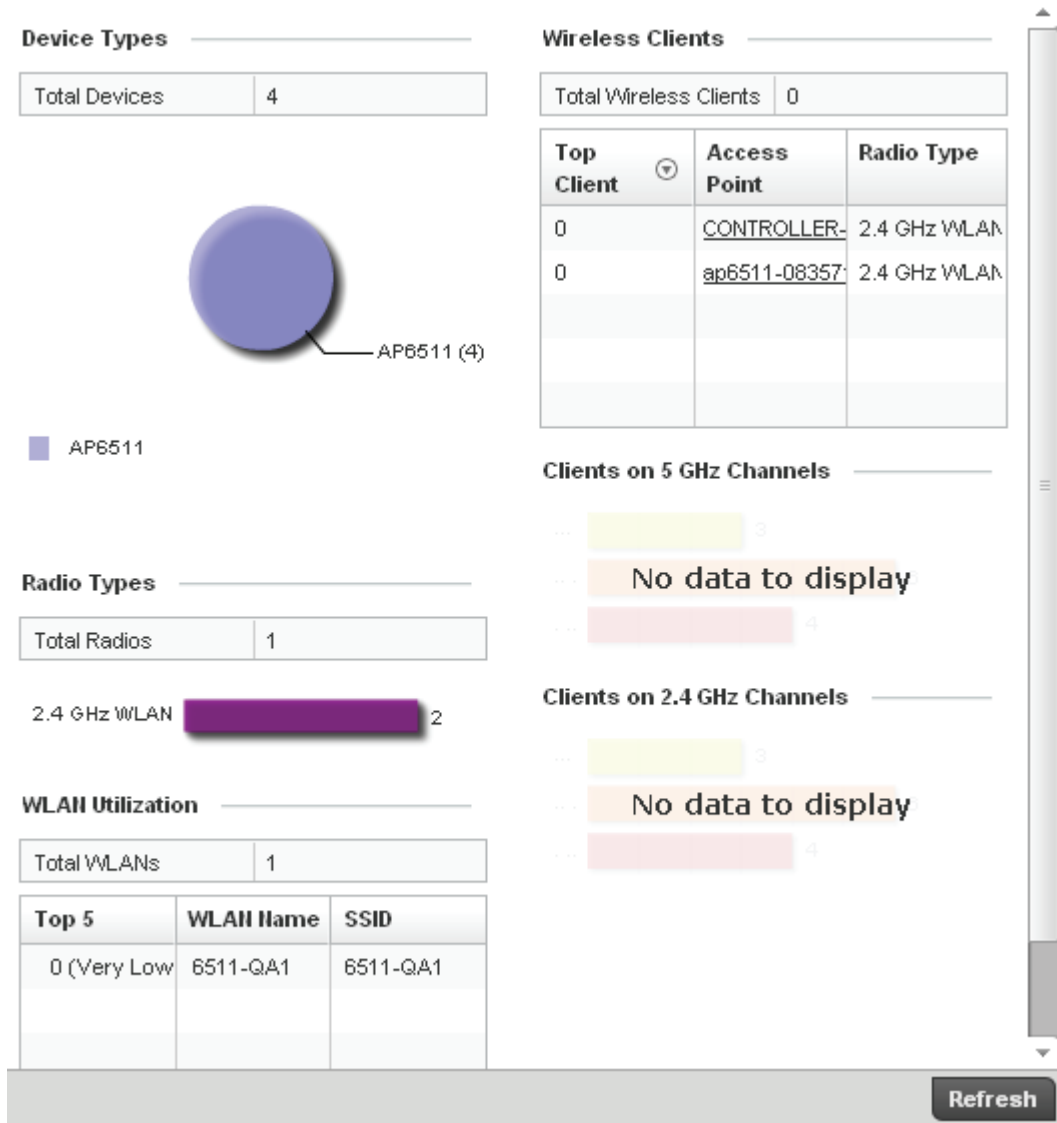


Figure 13-2 System Inventory screen

The **Device Types** field displays an exploded pie chart depicting the distribution of the different device types that are members of this network.

The **Wireless Clients** field displays the total number of wireless clients. This **Top Client Count** table lists the top in terms of the number of wireless clients adopted:

Top Client Count	Displays the number of wireless clients adopted by the RF Domain.
RF Domain	Displays the name of the RF Domain.
Last Update	Displays the UTC timestamp when the client count was last reported.

The **Radios** field displays information on the radios in use throughout the wireless network. This area displays the total number of managed radios and top 5 in terms of radio count. The **Total Radios** value is the total number of radios in this system.

Top Radio Count	Displays the number of radios in the RF Domain.
RF Domain	Displays the name of the RF domain these radios belong.
Last Update	Displays the UTC timestamp when this value was reported.

The Clients on 5 GHz Channels area displays the number of clients using 5 GHz radios.

The Clients on 2.4 GHz Channels area displays the number of clients using 2.4 GHz radios.

13.2 RF Domain

▶ *Statistics*

The **RF Domain Statistics** screens display status within the AP-6511's RF domain. This includes the AP-6511's health and device inventory, wireless clients and Smart RF feature. Use the information to obtain an overall view of the performance of the selected RF Domain and troubleshoot the domain or any member device.

Refer to the following:

- *Access Points*
- *AP Detection*
- *Wireless Clients*
- *Wireless LANs*
- *Radio*
- *SMART RF*
- *WIPS*
- *Captive Portal*
- *Historical Data*


13.2.1 **Access Points**

▶ *RF Domain*

The Access Point statistics screen displays statistical information supporting the Access Points in the RF Domain. This includes the Access Point name, MAC address, type, etc.

To display RF Domain Access Point statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **Access Points**.

Unsanctioned 	Reporting AP	SSID	AP Mode	Radio Type	Channel	Last Seen

type to search in tables Row Count: 0

Figure 13-4 AP Detection screen

The screen provides the following information:

- Unsanctioned** Displays the MAC address of the detected rogue AP.
- Reporting AP** Displays the MAC address of the AP, which detected the rogue AP.
- SSID** Displays the *Service Set ID* (SSID) of the network to which the rogue AP belongs.
- AP Mode** Displays the mode of the detected rogue device. An access point can be in two modes, either Access Point or wireless client.
- Radio Type** Displays the radio type associated with the rogue AP.
- Channel** Displays the channel of operation of the rogue AP radio.
- Last Seen** Displays the time the rogue AP was last seen (observed within the network). This value is expressed in seconds.

13.2.3 Wireless Clients

▶ *RF Domain*

The *Wireless Clients* screen displays read only device information for wireless clients. 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 the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **Wireless Clients**.

MAC Address	WLAN	Username	State	VLAN	IP Address	Vendor

Type to search in tables Row Count: 0

Refresh

Figure 13-5 Wireless Clients screen

This screen provides the following information:

- MAC Address** Displays the Hardware or *Media Access Control* (MAC) address of the wireless client. This address is hard-coded at the factory and can not be modified.
- WLAN** Displays the name of the WLAN the wireless client is currently associated with.
- Username** Displays the unique name of a user.
- State** Displays the state of the wireless client, as whether it is associating with an AP or not.
- VLAN** Displays the VLAN ID the wireless client is associated with.
- IP Address** Displays the current IP address for the wireless client.
- Vendor** Displays the vendor name of the wireless client.

13.2.4 Wireless LANs

▶ *RF Domain*

The Wireless LAN screen displays WLAN names, their SSID, traffic utilization, number of radios, etc.

Rx Bytes	Displays the average number of packets (in bytes) received on the selected WLAN.
Rx User Data Rate	Displays the average data rate per user for packets received.

13.2.5 Radio

▶ *RF Domain*

The **Radio** screens displays detailed radio information for the radios available for use in the selected RF domain. Use these screens to start troubleshooting radio related issues.


Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- *Radio Status*
- *Radio RF Statistics*
- *Radio Traffic Statistics*

13.2.5.1 Radio Status

To view the RF Domain radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and select the **RF Domain** node.
3. Expand **Radios**.
4. Select **Status** from the **Radios** menu.

Radio	Radio MAC	Radio Type	State	Channel Current (Config)	Configured Channel 	Power Current (Config)	Con
CONTROLLER-A20:R1	5C-0E-8B-06-FB-E0	2.4 GHz WLAN	On	11 (smt)	smt	23 (smt)	smt
ap6511-083571:R1	5C-0E-8B-07-04-70	2.4 GHz WLAN	Off	N/A (smt)	smt	0 (smt)	smt

Type to search in tables

Figure 13-7 Radios - Status screen

This screen provides the following information:

- Radio** Displays the name assigned to the radio as its unique identifier.
- Radio MAC** Displays the MAC address and numerical value assigned to the radio as its unique identifier.
- Radio Type** Defines whether the radio is a 802.11b, 802.11bg, 802.11bgn, 802.11a, or 802.11an.
- State** Displays the radio's current operational mode, either calibrate, normal, sensor or offline.
- Channel Current (Config)** Displays the current channel the radio is broadcasting on and the channel it is configured to use.
- Power Current (Config)** Displays the current power level the radio is broadcasting on and the power level it is configured to use.

13.2.5.2 Radio RF Statistics

To view the RF Domain radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and select the **RF Domain** node.
3. Expand the **Radios** menu item.
4. Select **RF Statistics**.

Radio	Signal	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate		Error Rate	Traffic Index	RF Quality I
ap6511-083571:R1	0 dbm	0 db	0 Mbps	0 Mbps		0	0	100 (Good)
CONTROLLER-A20:R1	-90 dbm	23 db	11 Mbps	3 Mbps		1	0	0 (Very Poor)
Type to search in tables							Row Count	

Figure 13-8 Radios - RF Statistics screen

This screen provides the following information:

- Radio** Displays the name assigned to the radio as its unique identifier.
- Signal** Displays the power of radio signals in dBm.
- SNR** Displays the signal to noise ratio of all 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.
- Error Rate** Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

- 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.
- RF Quality Index** Displays an integer that indicates overall RF performance. The RF quality indices are:
- 0–50 (poor)
 - 50–75 (medium)
 - 75–100 (good)

Tx Dropped Displays the total number of transmitted packets which have been dropped by each radio. This includes all user data as well as any management overhead packets that were dropped.

Rx Errors Displays the total number of received packets which contained errors for each radio.

13.2.6 SMART RF

► *RF Domain*

When invoked by an administrator, *Self-Monitoring At Run Time* (Smart RF) instructs radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any associated 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 Smart RF statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **SMART RF**.

Radios

AP MAC Address	MAC Address	Type	State	Channel	Power

Refresh

Figure 13-10 SMART RF screen

This screen provides the following information:

AP MAC Address Displays the MAC address of the AP (the device MAC address printed on the unit).

MAC Address This is the radio’s recognized MAC address when adopted.

Type	Identifies whether the radio is 802.11b, 802.11bg, 802.11bgn, 802.11a, or 802.11an.
State	Displays the radio's current operational mode, either calibrate, normal, sensor or offline.
Channel	Displays the operating channel assigned to the AP radio.
Power	Displays the power level in dBm for the selected radio.

13.2.7 WIPS

▶ *RF Domain*

Motorola's *Wireless Intrusion Protection Software* (WIPS) monitors for unauthorized rogue Access Points. Unauthorized attempt to access the WLAN is generally accompanied by anomalous behavior as intruding wireless clients trying to find network vulnerabilities. Basic forms of this behavior can be monitored and reported without a dedicated WIPS.

This screen displays the statistics of the WIPS events, the AP which reported the event, the unauthorized device, and so on.

13.2.7.1 WIPS Events

▶ *WIPS*

The WIPS Events screen provides details about unauthorized rogue Access Points.

To view the rogue access point statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **WIPS > WIPS Events**.

Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
dos-eapol-start-storm	AP1-ControllerA	33:44:33:44:33:44	1	Thu Jun 10 2010 12:26:2
null-probe-response	AP1-ControllerA	33:44:33:44:33:44	1	Thu Jun 10 2010 12:26:2

Figure 13-11 WIPS - Events screen

The WIPS Events screen provides the following information:

- Event Name** Displays the name of the detected intrusion.
- Reporting AP** Displays the MAC address of the AP reporting the intrusion.
- Originating Device** Displays the MAC address of the intruding device.
- Detector Radio** Displays the type of radio detecting the intrusion.
- Time Reported** Displays the time when the intruder was detected.

13.2.8 Captive Portal

▶ *RF Domain*

The captive portal technique forces an HTTP client on a network to see a special Web page (usually for authentication purposes) before using the Internet formally. A captive portal turns a Web browser into an authentication device.

To view the RF Domain captive portal statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **Captive Portal**.


Client MAC 	Client IP	Captive Portal	Authenticati on	WLAN	VLAN	Remaining Time
AA-11-11-00-00-00	1.1.1.1	default	Success	WLAN3	1	1m 40s
AA-11-12-00-00-00	1.1.1.1	default	Pending	WLAN4	2	3m 20s

Figure 13-12 Captive Portal screen

This screen provides the following information:

- Client MAC** Displays the MAC address of the wireless client.
- Client IP** Displays the IP address of the wireless client.
- Captive Portal** Displays whether the captive portal is enabled by default.
- Authentication** Displays the authentication status of the client.
- WLAN** Displays the name of the WLAN the client belongs to.
- VLAN** Displays the name of the VLAN the client belongs to.
- Remaining Time** Displays the time after which the client will be disconnected from the Internet.

13.2.9 Historical Data

► *RF Domain*

The historical data screen provides a history of Smart RF events. Smart RF enables an administrator to automatically assign the best channels to all associated devices to build an interference free environment to function in. A Smart RF event takes place when some or all of the following activities occur:

Each Smart RF event is recorded as a log entry. These events can be viewed using the Smart RF History screen.

13.2.9.1 Viewing Smart RF History

▶ *Historical Data*

To view the Smart RF history:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab from the left navigation pane and then select the **RF Domain** node.
3. Select **Historical Data > SMART RF History**.

SMART RF History

AP MAC	Radio MAC	Radio Index	Type	New Value	Old Value	Time
<u>MCN-AP1</u>	11:22:33:44:55:6	1	AP Unadopted	5	6	
<u>MCN-AP2</u>	12:22:33:44:55:6	2	AP Unadopted	55	65	
<u>MCN-AP3</u>	13:22:33:44:55:6	3	AP Unadopted	45	46	

Figure 13-13 Smart RF History

This screen displays the following information:

- AP MAC** Displays the MAC address of the selected AP.
- Radio MAC** Displays the radio MAC address of the corresponding AP.
- Radio Index** Displays the numerical identifier assigned to each detector AP used in calibration.
- Type** Displays the AP type.
- New Value** Displays the new power value as assigned by Smart RF.
- Old Value** Lists the old power value before being modified during calibration.
- Time** Displays time stamp when this event occurred.

13.3 Access Point Statistics

► *Statistics*

The Access Point Statistics screen displays an overview of the APs created for use within the network. Use this data as necessary to check all the APs that are active, their VLAN assignments and the current authentication and encryption schemes. Access Point Statistics consists of the following:

- *Health*
- *Inventory*
- *Device*
- *AP Detection*
- *Wireless Client*
- *Wireless LANs*
- *Radios*
- *Interfaces*
- *Network*
- *Firewall*
- *Certificates*
- *WIPS*
- *Captive Portal*
- *Network Time*

13.3.1 Health

► *Access Point Statistics*

The *Health* screen displays information on the selected device, such as its hardware version and software version. Use this information to fine tune the performance of the selected APs. This screen should also be the starting point for troubleshooting.

To view the access point health:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Health**.

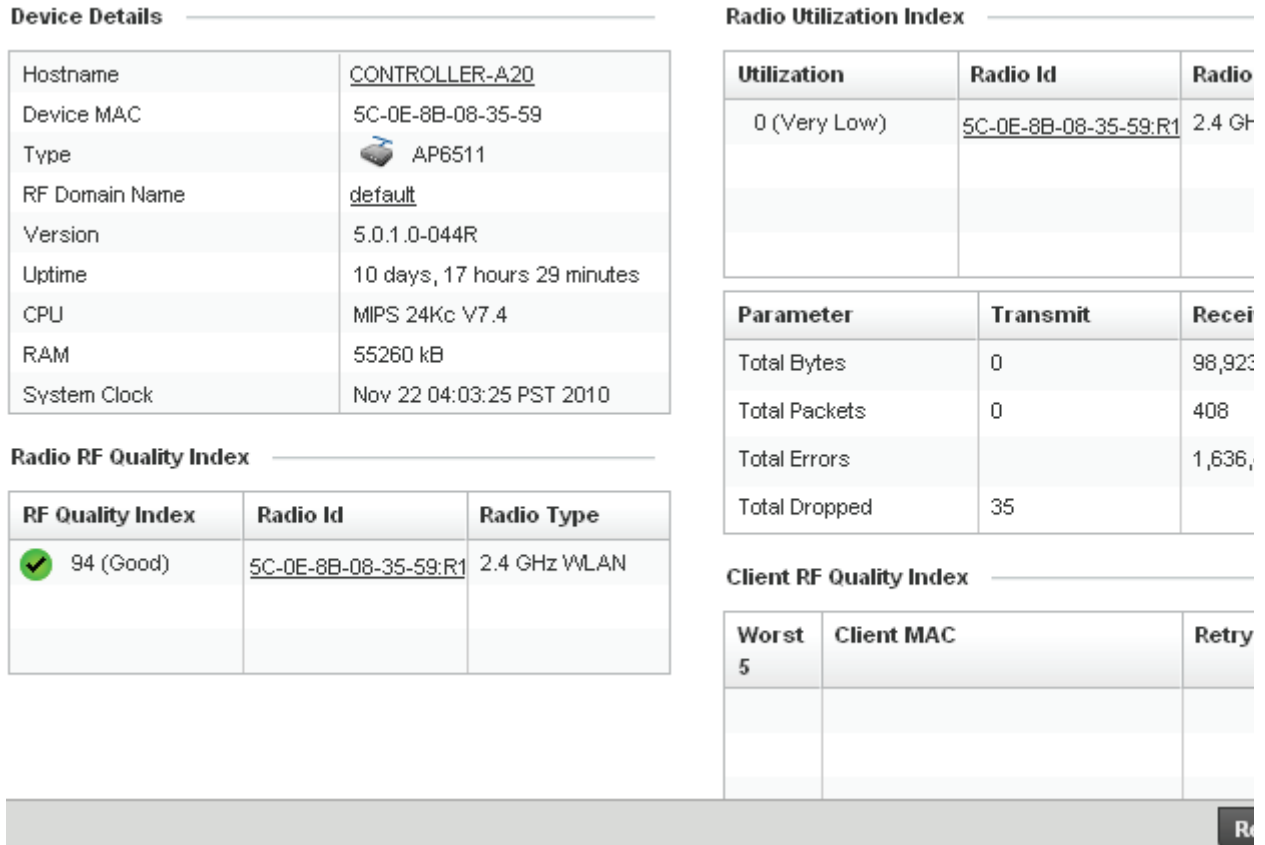


Figure 13-14 Access Point - Health screen

The **Device Details** area displays the following information:

- Hostname** Displays the AP's unique name. 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.
- Type** Displays the Access Point's model.
- RF Domain Name** Displays an AP's RF Domain membership.
- Version** Displays the AP's current firmware version. Use this information to assess whether an upgrade is required for better compatibility.
- Uptime** Displays the cumulative time since the AP 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 **RF Quality Index** field displays the following:

Bottom Radios	Displays radios having very low quality indices. RF quality index indicates the overall RF performance. The RF quality indices are: <ul style="list-style-type: none">• 0–50 (poor)• 50–75 (medium)• 75–100 (good)
Radio MAC	Displays a radio's hardware encoded MAC address.
Radio Type	Identifies whether the radio is a 802.11b, 802.11bg, 802.11bgn, 802.11a, or 802.11an.

The **Utilization Index** field displays the following:

Top Radios	Displays the traffic indices of radios, which measures how efficiently the traffic medium is used. This value is indicated as an integer.
Radio Id	Displays a numerical value assigned to the radio as a unique identifier. For example: 1, 2, or 3.
Radio Type	Identifies whether the radio is an 802.11b, 802.11bg, 802.11bgn, 802.11a, or an 802.11an.

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

Worst 5 Clients	Displays clients having low RF quality.
Client MAC	Displays a MAC address of the client having low RF indices.
Retry Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

13.3.2 Inventory

▶ Access Point Statistics

The *Inventory* screen displays information about AP physical characteristics. Use this screen to gather information on the performance of the different clients associated with the AP. Additionally, use this screen to fine tune Access Point performance.

To view the access point inventory statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Inventory**.

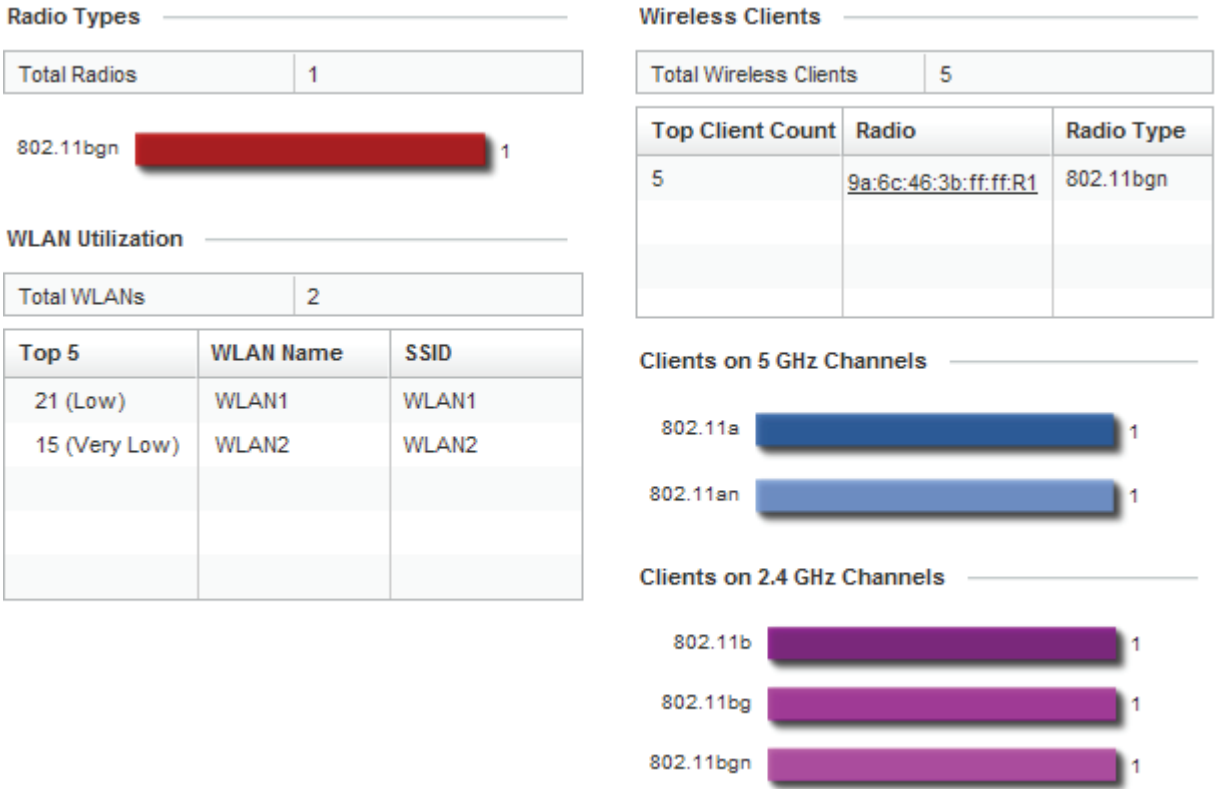


Figure 13-15 Access Point - Inventory screen

The **Radio Types** field displays the total number of radios detected. It also displays the number of radios that use the 2.4 GHz and the 5 GHz frequency bands.

The **Wireless LANs** area displays the total number of WLANs. It also displays the following:

- Top 5** Displays the maximum traffic utilization of the WLAN in which the access point is a member. The integer denotes the traffic index, which measures how efficiently the traffic medium is used. Traffic indices are:
- 0 – 20 (very low)
 - 20 – 40 (low)
 - 40 – 60 (moderate)
 - 60 and above (high).

WLAN Name Displays a name assigned to identify the WLAN.

SSID Displays the Service Set ID associated with the WLAN.

The **Wireless Clients** area displays the total number of wireless clients associated with this Access Point. It also displays the following:

Top Client Count Displays the number of clients associated with this Access Point.

Radio Displays the radio MAC address associated with the client.

Radio Type Displays the radio type.

The **Clients on 5 GHz Channels** field displays the number of wireless clients with radios operating in the 5 GHz frequency band.

The **Clients on 2.4 GHz Channels** area displays the number of wireless clients with radios operating in the 2.4 GHz band.

13.3.3 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 the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Device**.

System	
Version	5.0.1.0-044R
Boot Partition	secondary
Fallback Enabled	✔ Enabled
Fallback Image Triggered	✘ False
Next Boot	secondary

Firmware Images	
Primary Build Date	12:07:2010 17:42:01 PST
Primary Install Date	11:11:2010 10:07:55 PST
Primary Version	5.0.1.0-042R
Secondary Build Date	12:10:2010 10:01:44 PST
Secondary Install Date	11:11:2010 10:31:38 PST
Secondary Version	5.0.1.0-044R

Upgrade Status	
Upgrade Status	Successful
Upgrade Status Time	11:11:2010 10:31:38 PST

Figure 13-16 Access Point - Device screen

The **System** area displays the following:

- 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 in the device 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 AP is booted.

The **Firmware Images** field displays the following:

Primary Build Date Displays the build date when this 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.

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.

13.3.4 AP Upgrade

► Access Point Statistics

The *AP Upgrade* screen displays basic information about Access Point upgrades. 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 the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **AP Upgrade**.

Upgraded By	Type	MAC	Last Update Status	Time Last Upgraded	Retries Count	S
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-2D	Update error: L	Wed Oct 20 2010 02:40:33 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3D-05	Update error: L	Wed Oct 20 2010 02:40:55 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-E1	Update error: L	Wed Oct 20 2010 02:40:44 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-2D	Update error: L	Wed Oct 20 2010 02:42:46 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-2D	Update error: L	Wed Oct 20 2010 02:46:46 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3D-05	Update error: L	Wed Oct 20 2010 02:47:09 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-E1	Update error: L	Wed Oct 20 2010 02:46:57 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-2D	Update error: L	Wed Oct 20 2010 03:00:21 PM	3	fe
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-2D	-	Thu Oct 21 2010 09:55:04 AM	0	di
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3D-05	-	Thu Oct 21 2010 09:55:27 AM	0	di
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-E1	-	Thu Oct 21 2010 09:55:15 AM	0	di
5C-0E-8B-08-35-59	mcn	5C-0E-8B-08-3C-B7	-	Thu Oct 21 2010 11:44:59 AM	0	di

Type to search in tables Row

[Clear History](#) [R](#)

Figure 13-17 Access Point - AP Upgrade screen

The **Upgrade** screen displays the following:

- Upgraded By** Displays the device that performed the upgrade.
- Type** Displays the model of Access Point.
- MAC** Displays the MAC Address of each Access Point.
- Last Update Status** Displays the error status of the last upgrade.
- Time Last Upgraded** Displays the date and time of the last upgrade.
- Retries Count** Displays the number of retries made in the current state.
- State** Displays the current state of the Access Point upgrade.

13.3.5 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 associated 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 the **System** tab from the left navigation pane and then select the **Access Point** node.

3. Select **AP Detection**.



	Unsanctioned AP 	Reporting AP	SSID	AP Mode	Radio Type	Channel	Last Seen
	11:22:33:44:55	MCN-AP1	evilbit	Ad Hoc	11a	11	10s

Figure 13-18 Access Point - AP Detection Screen

This screen provides the following:

- Unsanctioned** Displays the MAC address of the unauthorized AP.
- Reporting AP** Displays the hardware encoded MAC address of the radio used with the detecting AP.
- SSID** Displays the SSID of the WLAN to which the unsanctioned AP belongs.
- AP Mode** Displays the mode of the unsanctioned AP.
- Radio Type** Displays the type of the radio on the unsanctioned AP. The radio can be 802.11b, 802.11bg, 802.11g, 802.11a or 802.11an.
- Channel** Displays the channel the unsanctioned AP is currently transmitting on.
- Last Seen** Displays the time (in seconds) the unsanctioned AP was last seen on the network by the detecting AP.

13.3.6 Wireless Client

► [Access Point Statistics](#)

The *Wireless Clients* screen displays read only device information for wireless clients associated with the selected 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 the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Wireless Clients**.

Client MAC	WLAN	Username	State	VLAN	IP Address	Vendor

Search to search in tables Row Count

Refresh

Figure 13-19 Access Point - Wireless Clients screen

This screen provides the following:

- Client MAC** Displays the MAC address of the wireless client.
- WLAN** Displays the name of the WLAN the client is currently associated with. Use this information to determine if the client/WLAN placement best suits intended operation and the client coverage area.
- Username** Displays the unique name of the administrator or operator.
- State** Displays the working state of the client.
- VLAN** Displays the VLAN ID the client is currently mapped to.
- IP Address** Displays the unique IP address of the client. Use this address as necessary throughout the applet for filtering, device intrusion recognition, and approval.
- Vendor** Displays the name of the vendor.

13.3.7 Wireless LANs

▶ *Access Point Statistics*

The *Wireless LAN* statistics screen displays an overview of Access Point WLANs. This screen displays the WLAN names, their SSIDs, traffic utilization, number of radios etc.

To view the wireless LAN statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.

Rx Bytes	Displays the average number of packets in bytes received on the selected WLAN.
Rx User Data Rate	Displays the received user data rate.

13.3.8 Radios

▶ Access Point Statistics

The **Radio** 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 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.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- *Radio Status*
- *Radio RF Statistics*
- *Radio Traffic Statistics*

13.3.8.1 Radio Status

To view the Access Point radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Expand **Radios**.
4. Select **Status** from the **Radios** menu.

Radio ⓘ	Radio MAC	Radio Type	State	Channel Current(Config)	Power Current(Config)
<u>CONTROLLER-A20:R1</u>	5C-0E-8B-06-FB-E1	2.4 GHz WLAN	On	11 (smt)	23 (smt)

Type to search in tables Row

Figure 13-21 Access Point Radios - Status screen

This screen provides the following information:

Radio	Displays the name assigned to the radio as its unique identifier.
Radio MAC	Displays the MAC address and numerical value assigned to the radio as its unique identifier.
Radio Type	Defines whether the radio is a 802.11b, 802.11bg, 802.11bgn, 802.11a, or 802.11an.
State	Displays the radio's current operational mode, either calibrate, normal, sensor or offline.
Channel Current (Config)	Displays the current channel the radio is broadcasting on and the channel it is configured to use.
Power Current (Config)	Displays the current power level the radio is broadcasting on and the power level it is configured to use.

13.3.8.2 Radio RF Statistics

To view the Access Point radio statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Expand **Radios**.
4. Select **RF Statistics**.

Radio	Signal	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Error Rate	Traffic Index	RF Quality Index
ap6511-083571:R1	0 dbm	0 db	0 Mbps	0 Mbps	0	0	✓ 100 (Good)
CONTROLLER-A20:R1	-91 dbm	21 db	11 Mbps	3 Mbps	4	0	✓ 96 (Good)

Figure 13-22 Access Point Radios - RF Statistics screen

This screen provides the following information:

- Radio** Displays the name assigned to the radio as its unique identifier.
- Signal** Displays the power of radio signals in dBm.
- SNR** Displays the signal to noise ratio of all 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.
- Error Rate** Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
- 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.
- RF Quality Index** Displays an integer that indicates overall RF performance. The RF quality indices are:
 - 0–50 (poor)
 - 50–75 (medium)
 - 75–100 (good)

Rx User Data Rate	Displays the rate (in kbps) that user data is received by the 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 radio. This includes all user data as well as any management overhead packets that were dropped.
Rx Errors	Displays the total number of received packets which contained errors for each radio.

13.3.9 Interfaces

▶ *Access Point Statistics*

The *Interface* screen provides detailed statistics on each of the interfaces available on an Access Point. Use this screen to review the statistics for each interface. Use the following screens to review the performance of each interface on the Access Point.

The interface statistics screen consists of two tabs:

- *General Statistics*
- *Viewing Interface Statistics Graph*

13.3.9.1 General Statistics

► Interfaces

The *General* screen provides information on the interface such as its MAC address, type and TX/RX statistics.

To view the general interface statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Interfaces**. The General tab displays by default.

General
Network Graph

General

Name	fe1
Interface MAC Address	5C-0E-8B-08-35-72
IP Address	n/a
IP Address Type	n/a
Secondary IPs	0 items ▼
Hardware Type	ethernet
Index	2,001
Access VLAN	1
Access Setting	Access
Administrative Status	DOWN

Specification

Media Type	
Protocol	
MTU	1,500
Mode	
Metric	1
Maximum Speed	100M
Admin Speed	Auto
Operator Speed	
Admin Duplex Setting	Auto
Current Duplex Setting	

Errors

Bad Pkts Received	0
Collisions	0
Late Collisions	0
Excessive Collisions	0
Drop Events	0
Tx Undersize Pkts	0
Oversize Pkts	0
MAC Transmit Error	0
MAC Receive Error	0
Bad CRC	0

Receive Errors

Rx Frame Errors	0
Rx Length Errors	0
Rx FIFO Errors	0
Rx Missed Errors	0
Rx Over Errors	0

Transmit Errors

Tx Errors	0
Tx Dropped	0
Tx Aborted Errors	0
Tx Carrier Errors	0

Refresh
Exit

Figure 13-24 Access Point Interface - General tab

The **General** field describes the following:

Name	Displays the name of the interface.
Interface MAC Address	Displays the MAC address of the interface.
IP Address	IP address of the interface.
IP Address Type	Lists the IP address type of the interface
Hardware Type	Displays the hardware type.
Index	Displays the unique numerical identifier supporting the interface.
Access VLAN	Displays the interface the VLAN has access to.
Access Setting	Displays the mode of the VLAN—Access or Trunk.
Administrative Status	Displays whether the interface is currently UP or DOWN.

The **Specification** field displays the following:

Media Type	<p>Displays the physical connection type of the interface.</p> <p>Medium types are:</p> <p><i>Copper</i> - Used on RJ-45 Ethernet ports</p> <p><i>Optical</i> - Used on fibre optic gigabit Ethernet ports</p>
Protocol	Displays the name of the routing protocol adopted by the interface.
MTU	Displays the <i>maximum transmission unit</i> (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	<p>The mode can be either:</p> <p><i>Access</i>— This Ethernet interface accepts packets only from the native VLANs.</p> <p><i>Trunk</i>— This Ethernet interface allows packets from a given list of VLANs that you can add to the trunk.</p>
Metric	Displays the metric value associated with the route through this interface.
Maximum Speed	Displays the maximum speed at which the interface transmits or receives data.
Admin. Speed	Displays the speed setting used when using the administrative interface.
Operator Speed	Displays the current speed of the data transmitted and received over the interface.
Admin. Duplex Setting	Displays the administrator's duplex setting.
Current Duplex Setting	Displays the interface as either half duplex, full duplex, or unknown.

The **Traffic** field describes the following:

Good Octets Sent	Displays the number of octets (bytes) with no errors sent by the interface.
Good Octets Received	Displays the number of octets (bytes) with no errors received by the interface.
Good Pkts Sent	Describes the number of good packets transmitted.
Good Pkts Received	Describes the number of good packets received.
Mcast Pkts Sent	Displays the number of multicast packets sent through the interface.
Mcast Pkts Received	Displays the number of multicast 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 that is larger than the MTU through the interface.

The **Errors** field displays the following information:

Bad Pkts Received	Displays the number of bad packets received through the interface.
Collisions	Displays the number of collisions.
Late Collisions	A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending station. Late collisions are not normal, and are usually the result of out-of-specification cabling or a malfunctioning device.
Excessive Collisions	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point that a single Ethernet network can not handle it efficiently.
Drop Events	Displays the number of dropped packets that are transmitted or received through the interface.
Tx Undersize Pkts	Displays the number of undersize packets transmitted through the interface.
Oversize Pkts	Displays the number of oversize packets.
MAC Transmit Error	Displays the number of transmits that failed because of an internal MAC sublayer error that is not late collision, excessive collisions, or carrier sense error.

MAC Receive Error	Displays the number of received packets failed because of an internal MAC sublayer that is not late collision, excessive collisions, or carrier sense error.
Bad CRC	Displays the CRC error. The <i>Cyclical Redundancy Check</i> (CRC) is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of the frame, it's considered a bad CRC.

The **Receive Errors** field displays the following information:

Rx Frame Errors	Displays the number of frame errors received at the interface. A frame error occurs when a byte of data is received but not in the format expected.
Rx Length Errors	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was less than or exceeded the Ethernet standard.
Rx FIFO Errors	Displays the number of FIFO errors received at the interface. First-in First-out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally.
Rx Missed Errors	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store the incoming packet.
Rx Over Errors	Displays the number of overflow errors. An overflow occurs when packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following:

Tx Errors	Displays the number of packets with errors transmitted on the interface.
Tx Dropped	Displays the number of transmitted packets dropped from the interface.
Tx Aborted Errors	Displays the number of packets aborted on the interface because a clear-to-send request was not detected.
Tx Carrier Errors	Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or cabling.
Tx FIFO Errors	Displays the number of FIFO errors received at the interface. First-in first-out queueing is an algorithm that involves buffering and forwarding packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally.
Tx Heartbeat Errors	Displays the number of heartbeat errors. This generally indicates a software crash or packets stuck in an endless loop.
Tx Window Errors	Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) in the receive window field the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgement from the receiving host, it constitutes a window error.

13.3.9.2 Viewing Interface Statistics Graph

► *Interfaces*

The **Network Graph** tab displays interface statistics graphically. To view a detailed graph for an interface, select an interface and drop it on to the graph. The graph has **Port Statistics** as the Y-axis and the **Polling Interval** as the X-axis. Select different parameters on the Y-axis and different polling intervals as needed.

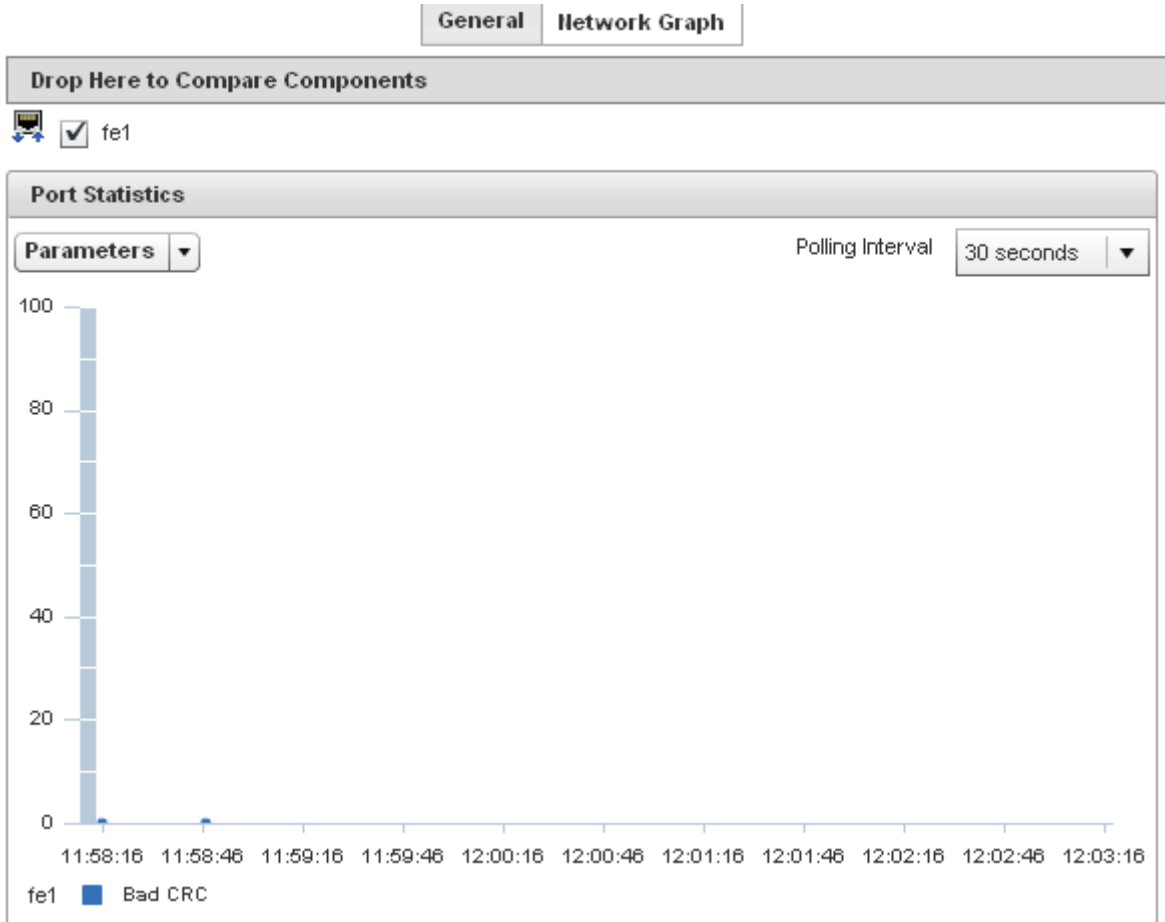


Figure 13-25 Access Point Interface - Network Graph tab

13.3.10 Network

► *Access Point Statistics*

Use the *Network* screen to view information for ARP, DHCP, Routing and Bridging. Each of these screen provide enough statistics to troubleshoot issues related to the following four features:

- *ARP Entries*
- *Route Entries*
- *DHCP Options*

13.3.10.1 ARP Entries

▶ *Network*

ARP is a networking protocol for determining a network host’s hardware address when its IP address or network layer address is known.

To view the ARP statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Network** and expand the menu to reveal its submenu items.
4. Select **ARP Entries**.

IP Address	ARP MAC Address	Type	VLAN
10.0.0.1	00:11:22:33:44:55	t1	1
10.0.0.2	00:11:22:33:44:55	t2	2

Figure 13-26 Access Port Network - ARP Entries screen

The ARP Entries screen describes the following:

- IP Address** Displays the IP address of the client being resolved.
- ARP MAC Address** Displays the MAC address corresponding to the IP address being resolved.
- Type** Defines whether the entry was added statically or dynamically in respect to network traffic. Entries are typically static.
- VLAN** Displays the name of the VLAN where an IP address was found.

13.3.10.2 Route Entries

▶ *Network*

The route entries screen provides details about 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 the route entries:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Network** and expand the menu to reveal its sub menu items.

4. Select **Route Entries**.


Destination 	FLAGS	Gateway	Interface
destination1	false	gw1	ge1
destination2	false	gw2	ge1

Figure 13-27 Access Point Network - Route Entries screen

This screen supports the following data:

- Destination** Displays the IP address of a specific destination address.
- DKEY** Displays the destination IP address.
- FLAGS** Displays the connection status for this entry. **C** indicates a connected state. **G** indicates a gateway.
- Gateway** Displays the IP address of the gateway used to route the packets to the specified destination subnet.
- Interface** Displays the name of the interface of the destination subnet.

13.3.10.3 DHCP Options

► *Network*

An AP-6511 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 the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Network** and expand the menu to reveal its sub menu items.
4. Select **DHCP Options**.

Server Information	Image File	Configuration	Cluster Configuration
n/a	n/a	n/a	n/a

Figure 13-28 Access Point Network - DHCP Options screen

The *DHCP Options* screen displays the following:

- Server Information** Displays the IP address of the DHCP server.
- 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.
- Cluster Configuration** Displays the name of the cluster configuration file on the DHCP server if the server is a part of a cluster.

13.3.11 DHCP Server

► Network

To view DHCP statistics within an AP-6511 managed network:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab from the left navigation pane and then select the **Access Point** node.
3. Select **Network > DHCP Server**.
4. Expand the DHCP Server option and select **General**.

Status _____

Interfaces	
State	Not Running

DDNS Bindings _____

IP Address	Name

DHCP Manual Bindings _____

IP Address	Client Id

Figure 13-29 Access Point Network DHCP Server - General tab

The *DHCP* screen displays the following:

- Interfaces** Displays the interface used for the newly created DHCP configuration.
- State** Displays the current state of the DHCP server.
- IP Address** Displays the IP address assigned to the client.
- Name** Displays the domain name mapping corresponding to the IP address listed.

IP Address	Displays the IP address for each client with a listed MAC address.
Client ID	Displays the MAC address (client hardware ID) of the client.

13.3.11.1 DHCP Bindings

▶ *Network*

To view a network’s DHCP Bindings:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Select **Network > DHCP Bindings**.

Expiry Time	IP Address	DHCP MAC Address

Figure 13-30 Access Point Network DHCP Server - Bindings tab

The *DHCP Bindings* screen displays the following:

- Expiry Time** Displays the expiration of the lease used by the client for DHCP resources.
- IP Address** Displays the IP address for each client whose MAC address is listed in the Client Id column.
- DHCP MAC Address** Displays the MAC address (client Id) of the client.

13.3.11.2 DHCP Networks

► [Network](#)

To view a network's DHCP Networks:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Select **Network > DHCP Networks**.

The *DHCP Networks* screen displays the following:

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.
Total Addresses	Total available addresses that can be leased to clients.

13.3.12 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's a device or set of devices configured to permit or deny computer applications based on a set of rules.

This screen is partitioned into the following:

- [Packet Flows](#)
- [IP Firewall Rules](#)
- [MAC Firewall Rules](#)
- [NAT Translations](#)
- [DHCP Snooping](#)

13.3.12.1 Packet Flows

► [Firewall](#)

The *Packet Flows* screen displays a bar graph for the different packet types flowed through the Access Point. Use this information to assess the traffic patterns supported by the Access Point.

The **Total Active Flows** graph displays the total number of flows supported. Other bar graphs display for each individual packet type.

To view the packet flows statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Expand the **Firewall** menu to reveal its sub menu options.
4. Select **Packet Flows**.

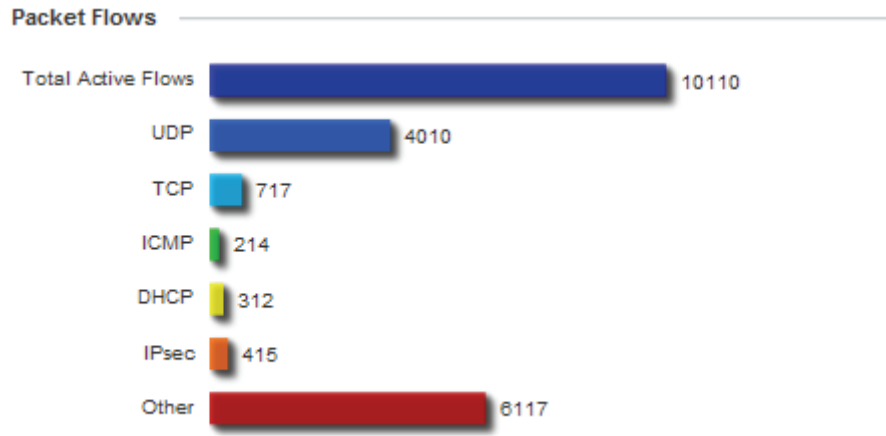


Figure 13-31 Access Point Firewall - Packet Flow screen

13.3.12.2 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 the **System** tab and then select the **Access Point** node.
3. Expand the **Firewall** menu to reveal its sub menu options.
4. Select **IP Firewall Rules**.

Precedence	⤴	Friendly String	Hit Count
1		permit tcp any any eq ftp rule-precede	0
2		permit tcp any any eq www rule-prec	0
3		permit tcp any any eq ssh rule-prec	0
4		permit tcp any any eq https rule-prec	0
5		permit udp any any eq snmp rule-prec	0
6		permit tcp any any eq telnet rule-prec	0

Row Count: 6

Refresh
Exit

Figure 13-32 Access Point Firewall - IP Firewall Rules screen

This screen displays the following:

Precedence	Displays the precedence value applied to packets. The rules within an <i>Access Control Entries</i> (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	This is a string that provides more information as to the contents of the rule.
Hit Count	Displays the number of times each WLAN ACL has been triggered.

13.3.12.3 MAC Firewall Rules

► Firewall

The ability to allow or deny a system by its MAC address ensures malicious or unwanted users are unable to bypass security filters. Firewall rules can be created to support one of the three actions listed below that match the rule's criteria:

- *Allow a connection*
- *Allow a connection only if it's secured through the MAC firewall security*
- *Block a connection*

To view the MAC Firewall Rules:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Expand the **Firewall** menu to reveal its sub menu options.
4. Select **MAC Firewall Rules**.

The *MAC Firewall Rules* screen provides the following information:

Precedence	Displays the precedence value, which are applied to packets. The rules within an <i>Access Control Entries</i> (ACL) list are based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence value.
Friendly String	Displays a string providing additional information on rule contents.
Hit Count	Displays the number of times each WLAN ACL has been triggered.

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).

13.3.12.5 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 the System tab and then select the Access Point node.
3. Expand the **Firewall** menu to reveal its sub menu options.
4. Select **DHCP Snooping**.

MAC	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since
5C-0E-8B-08-35-7*	switch-SVI	169.254.53.113		1		11d 14h 11m 44s

Search to search in tables Row |

Clear All R

Figure 13-34 Access Point Firewall - DHCP Snooping screen

The DHCP snooping screen displays the following:

- MAC Address** Displays the MAC address of the client.
- Node Type** Displays the NetBios node with the IP pool from which IP addresses can be issued to client requests on this interface.
- IP Address** Displays the IP address used for DHCP discovery, and requests between the DHCP server and DHCP clients.
- Netmask** Displays the subnet mask used for DHCP discovery, and requests between the DHCP server and DHCP clients.
- VLAN** Displays the interface used 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.
Last Updated	Displays the time the server was last updated.

13.3.13 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*

13.3.13.1 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 the **System** tab and then select the **Access Point** node.
3. Expand the Certificates menu to display its submenu items.
4. Select **Trustpoint**.

Certificate Details

Subject Name	CN=AP6511-5C-0E-8B-08-35-71
Alternate Subject Name	
Issuer Name	CN=AP6511-5C-0E-8B-08-35-71

Serial Number	049d
RSA Key Used	default_rsa_key
IS CA	✗ False
Is Self Signed	✓ True
Server Certificate Present	✓ True
CRL Present	✗ False

Validity

Valid From	01:01:2010 00:01:13 UTC
Valid Until	01:01:2011 00:01:13 UTC

Certificate Authority (CA) Details

Subject Name	
Alternate Subject Name	
Issuer Name	
Serial Number	

Certificate Authority Validity

Valid From	
Valid Until	

Refresh Exit

Figure 13-35 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 if this certificate is a authority certificate.
Is Self Signed	Displays if the certificate is self-signed. True indicates the certificate is self-signed.
Server Certificate Present	Displays if the server certificate is present. True indicates the certificate is present.
CRL Present	Displays whether this functionality is present or not. The <i>Certificate Revocation List</i> (CRL) is a method for using a public key infrastructure for maintaining access to network servers.

Refer to the **Validity** field to assess the certificate duration beginning and end dates.

Lastly, review the Certificate Authority (CA) Details and Validity information. to assess the subject and certificate duration periods.

13.3.13.2 RSA Keys

► Certificates

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption.

The *RSA Keys* screen displays a list of RSA keys installed in the selected wireless controller. 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 the **System** tab and then select the **Access Point** node.
3. Expand the Certificates menu to display its submenu items.
4. Select **RSA Keys**.

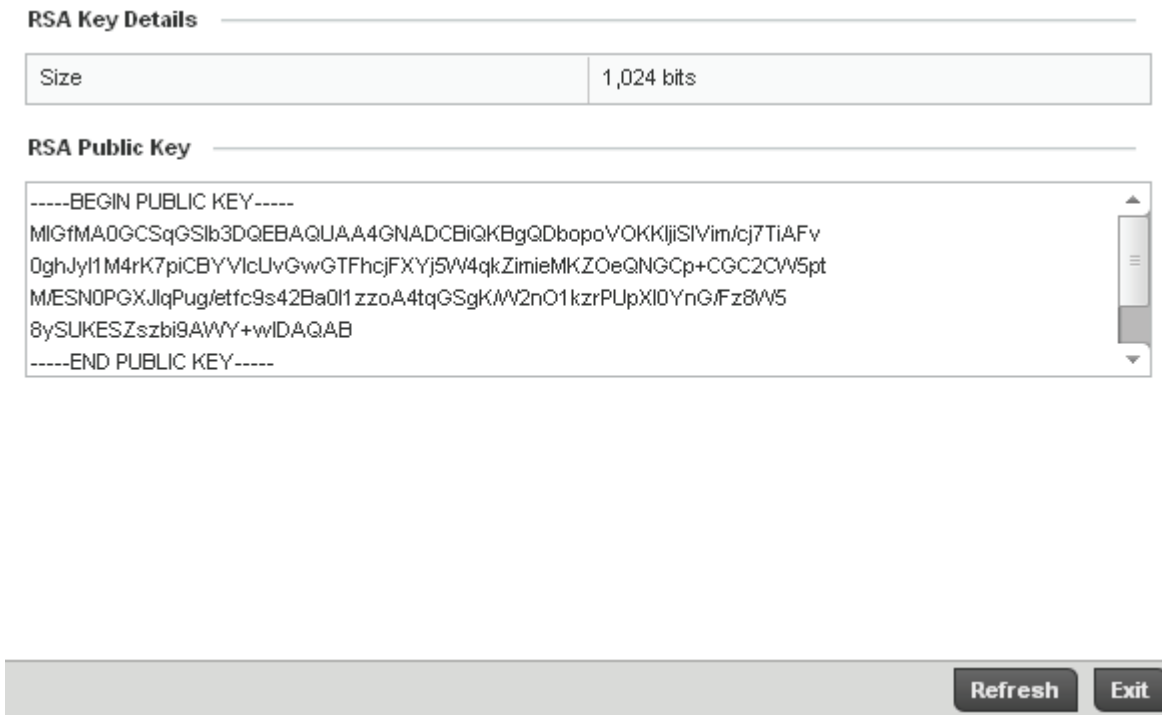


Figure 13-36 Access Point Certificates - RSA Key screen

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.

13.3.14 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 the 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 screen provides details about the blacklisted clients (unauthorized access points) intruded into the network. The 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.

13.3.14.1 WIPS Events

► WIPS

The WIPS Events screen details the wireless intrusion event by an access point.

To view the WIPS events statistics:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Expand the **WIPS** menu item and select **WIPS Events**.

Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
dos-eapol-start-storm	MCN-AP1	33-44-33-44-33-44	1	Thu Jun 10 2010 11:26:2
null-probe-response	MCN-AP1	33-44-33-44-33-44	1	Thu Jun 10 2010 11:26:2

Figure 13-37 Access Point - WIPS Events screen

The WIPS screen provides the following:

Event Name	Displays the name of the wireless intrusion detected.
Reporting AP	Displays the MAC address of the AP reporting this intrusion.
Originating Device	Displays the MAC address of the intruding device.
Detector Radio	Displays the number of sensor radios supported by the reporting AP.
Time Reported	Displays the time when the intrusion was detected.

13.3.15 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 the **System** tab and then select the **Access Point** node.
3. Select **Captive Portal**.

Client MAC	Client IP	Captive Portal	Authentication	WLAN	VLAN	Remaining Time
AA-11-11-00-00-00	1.1.1.1	default	Success	WLAN3	1	1m 40s
AA-11-12-00-00-00	1.1.1.1	default	Pending	WLAN4	2	3m 20s

Figure 13-38 Access Point - Captive Portal screen

The Captive Portal screen supporting the following:

- Client MAC** Displays the MAC address of the wireless client.
- Client IP** Displays the IP address of the wireless client.
- Captive Portal** Displays the IP address of the captive portal page.
- Authentication** Displays the authentication status of the wireless client.
- WLAN** Displays the name of the WLAN the requesting client belongs to.
- VLAN** Displays the name of the VLAN the requesting client belongs to.
- Remaining Time** Displays the time after which the client is disconnected from the Internet.

13.3.16 Network Time

► *Access Point Statistics*

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*

13.3.16.1 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 the **System** tab and then select the **Access Point** node.
3. Select **Network Time**.
4. Select the **NTP Status** tab.

		NTP Status			NTP Association				
Clock Offset	Frequency	Leap	Precision	Reference Time	Reference	Root Delay	Root Display	Status Stratum	
45	11.4	5677	111		dd	344	4566	4899	

Figure 13-39 Access Point - Network Time Status screen

The NTP Status Screen screen displays the following:

- Clock Offset** Displays the time differential between the Access Point time and the NTP resource.
- Frequency** An 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 local clock was last set 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 Display** 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.
- Status Stratum** Displays how many hops the Access Point is from its current NTP time source.

13.3.16.2 NTP Association

► *Network Time*

To view the Network Time statistics of an access point:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Access Point** node.
3. Select **Network Time**.
4. Select the **NTP Association** tab.

		NTP Status		NTP Association						
	Delay Time	Display	Offset	Poll	Reach	Reference IP Address	Server IP Address	State	Status	Time
	10	45	67	44	445	12.34.44.4	12.2.2.2	455	ss	now

Figure 13-40 Access Point - Network Time Association screen

The NTP Association screen displays the following:

- Delay Time** Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP 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 SNTP server. The Access Point adjusts its clock to match the server's time value. The offset gravitates towards zero overtime, but never completely reduces its offset to zero.
- Poll** Displays the maximum interval between successive messages in seconds to the nearest power of two.
- Reach** Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages.
- Reference IP Address** Displays the 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: <i>Synced</i> - Indicates the Access Point is synchronized to this NTP server. <i>Unsynced</i> - Indicates the Access Point has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC. <i>Selected</i> - Indicates this NTP master server will be considered the next time the Access Point chooses a master to synchronize with. <i>Candidate</i> - Indicates this NTP master server may be considered for selection the next time the Access Point chooses a NTP master server. <i>Configured</i> - 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.

13.4 Wireless Client Statistics

▶ *Statistics*

The wireless client statistics display read-only statistics for each client. It provides an overview of the health of wireless clients in the network. The wireless client statistics includes RF quality, traffic utilization, user details, etc. Use this information to assess if configuration changes are required to improve network performance.

The wireless clients statistics screen can be divided into:

- *Health*
- *Details*
- *Traffic*

13.4.1 Health

▶ *Wireless Client Statistics*

The *Health* screen displays information on the overall performance of a wireless client.

To view the health of wireless clients:

1. Select the **Statistics** menu from the Web UI.
2. Select the **System** tab and then select the **Wireless Client** node.
3. Select **Health**.

Wireless Client

Client MAC	AA-11-11-00-00-00
Vendor	Motorola
State	Roaming
IP Address	10.1.1.1
WLAN	wlan1
BSS	11-22-33-44-55-66
VLAN	1

User Details

Username	user1
Authentication	eap
Encryption	wep64
Captive Portal Auth.	✓ True

RF Quality Index

RF Quality Index	✘ 20 (Very Poor)
Retry Rate	3,452
SNR	2,456 db
Signal	2,455 dbm
Noise	2 dbm
Error Rate	24

Association

AP	MCN-AP1
Radio Number	1
Radio Type	type1

Traffic Utilization

Traffic Index		
Parameter	Transmit	Receive
Total Bytes	2,300	2,002
Total Packets	2,600	56,782
User Data Rate	2,400 kbps	1,002 kbps
Physical Layer Rate	5,677 Mbps	25,677 Mbps
Tx Dropped Packets	1,400	
Rx Errors		452

Figure 13-41 Wireless Clients - Health screen

The **Wireless Client** field displays the following:

Client MAC	Displays the MAC address of the wireless client.
Vendor	Displays the vendor name or the manufacturer of the wireless client.
State	Displays the state of the wireless client. It can be <i>idle</i> , <i>authenticated</i> , <i>associated</i> or <i>blacklisted</i> .
IP Address	Displays the IP address of the wireless client.
WLAN	Displays the WLAN name the wireless client belongs to.
BSS	Displays the basic service station ID of the network the wireless client belongs to.
VLAN	Displays the VLAN ID the wireless client is associated with.

The **User Details** field displays the following:

Username	Displays the unique name of the administrator or operator.
Authentication	Lists if any authentication is applied. If there is authentication, the status is displayed.

Encryption	Displays if encryption is applied.
Captive Portal Authentication	Displays whether captive portal authentication is enabled.

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: <ul style="list-style-type: none">• <i>0–20</i>—very poor quality• <i>20–40</i>—poor quality• <i>40–60</i>—average quality• <i>60–100</i>—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 ratio of the wireless client associated with the Access Point.
------------	---

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 that have been altered due to noise, interference, and distortion. It's a unitless performance measure.
-------------------	---

The **Association** field displays the following:

AP	Displays the name of the AP the wireless client is associated with. Click on the AP to view more information on the associated AP.
-----------	--

Radio Number	Displays the radio number on the AP to which this wireless client is associated.
---------------------	--

Radio Type	Displays the radio type. The radio can be 802.11b, 802.11bg, 802.11bgn, 802.11a or 802.11an.
-------------------	--

The **Traffic Utilization** field displays statistics on the traffic generated and received by this wireless client. This area displays the traffic 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.

Traffic indices are:

- *0–20*—very low utilization
- *20–40*—low utilization
- *40–60*—moderate utilization
- *60 and above*—high utilization

This field also displays the following:

Total Bytes	Displays the total bytes processed by the wireless client.
Total Packets	Displays the total number of packets processed by the wireless client.
User Data Rate	Displays the average user data rate.
Physical Layer Rate	Displays the average packet rate at the physical layer.
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.

13.4.2 Details

▶ *Wireless Client Statistics*

The *Details* screen provides information on a selected wireless client.

To view the details screen of a wireless client:

1. Select the **Statistics** menu from the Web UI.
2. Select the **RF Domain** tab and then select the **Wireless Clients** node.
3. Select **Details**.

Wireless Client		Association	
SSID	wlan1	AP	11-aa-bb-cc-dd-dd
RF Domain	<u>RF-Domain2</u>	BSS	11-22-33-44-55-66
User Details		Radio Number	1
Username	user1	Radio Type	type1
Authentication	eap	Rate	3457
Encryption	wep64	802.11 Protocol	
Captive Portal Auth.	✔ True	High-Throughput	✔ Supported
Connection		RIFS	✘ Unsupported
Idle Time	5m 44s	Unscheduled APSD	3377
Last Active	10	AID	22
Last Association	7m 35s	Max AMSDU Size	234
Session Time	7m 35s	Max AMPDU Size	233
SM PowerSave Mode	true	Interframe Spacing	233 microSeconds
Power Save Mode	✘ False	Short Guard Interval	✘ Unsupported
WMM Support	✔ True		
40 MHz Capable	✔ True		
Max Physical Rate	100,000 kbps		
Max User Rate	50,000 kbps		

Figure 13-42 Wireless Clients - Details screen

The **Wireless Client** area displays the following:

- SSID** Displays the Service Set ID the wireless client is associated with.
- RF Domain** Displays the RF domain name the wireless client belongs to.

The **User Details** field displays the following:

- Username** Displays the unique name of the administrator or operator.
- Authentication** Displays whether authentication is used. If there is an authentication method applied, this field displays its status.
- Encryption** Displays if any encryption is applied.
- Captive Portal Auth.** Displays whether captive portal authentication is enabled.

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 in contact with the AP.

Last Association	Displays the duration for which the wireless client was in association with the AP.
Session Time	Displays the duration for which a session can be maintained by the wireless client without it being dis-associated from the system.
SM Power Save Mode	Displays whether this feature is enabled on the wireless client. The <i>spatial multiplexing</i> (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: <i>static operation</i> and <i>dynamic operation</i> .
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 NICs. 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 this support is enabled or not.
40 MHz Capable	Displays whether the wireless client has 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.

The **Association** field displays the following:

AP	Displays the MAC address of the AP the wireless client is associated to.
BSS	Displays the basic service set the AP belongs to. A BSS is a set of all stations that can communicate with one another.
Radio Number	Displays the radio of the AP the wireless client is associated with.
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.

The **802.11 Protocol** field displays the following:

High-Throughput	Displays whether this feature is supported or not. 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 this feature is supported. This defines an unscheduled service period, which is a contiguous period of time during which the Access Point is expected to be awake.

AID	Displays the Association ID established by an AP. 802.11 association enables the access point to allocate resources and synchronize with a radio NIC. An NIC 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 NIC and the SSID of the network it wishes to associate. After receiving the request, the access point considers associating with the NIC, and reserves memory space for establishing an AID for the NIC.
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 time interval between two consecutive ethernet frames.
Short Guard Interval	Displays the guard interval in micro seconds. Guard intervals prevent interference between distinct data transmissions while.

13.4.3 Traffic

► *Wireless Client Statistics*

The traffic screen provides an overview of client traffic utilization. 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 the **RF Domain** tab and then select the **Wireless Clients** node.
3. Select **Traffic**.

Traffic Utilization

Traffic Index		45 (Medium)	
Parameter	Transmit	Receive	
Total Bytes	3,090	26,650	
Total Packets	60,905	442,660	
User Data Rate	2,199 kbps	1,664 kbps	
Packets per Second	56,965	43,660	
Physical Layer Rate	349,555 Mbps	44,595 Mbps	
Bcast/Mcast Packets	45,555	34,444	
Management Packets	53,900	1,600	
Tx Dropped Packets	45,900	---	
Tx Retries		---	
Rx Errors	---	44,466	
Rx Actions	---	33,456	
Rx Probes	---	44,755	
Rx Power Save Poll	---	4,755	

RF Quality Index

RF Quality Index	!! 30 (Poor)
Retry Rate	65,555
SNR	3,445 db
Signal	4,555 dbm
Noise	255 dbm
Error Rate	35,455
MOS Score	5.0
R-Value	20

Figure 13-43 Wireless Clients - Traffic screen

Traffic Utilization statistics provide the traffic 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 by the client.
- Total Packets** Displays the total number of data packets processed by the wireless client.
- User Data Rate** Displays the average user data rate.
- Packets per Second** Displays the packets processed per second.
- Physical Layer Rate** Displays the data rate at the physical layer level.
- Bcast/Mcast Packets** Displays the total number of broadcast/management packets processed.
- Management Packets** Displays the number of management packets processed.
- Tx Dropped Packets** Displays the number of dropped packets while transmitting.
- Tx Retries** Displays the total number of transmit retries.

Rx Errors	Displays the degree of errors encountered during data transmission. The higher the error rate, the less reliable the connection or data transfer.
Rx Actions	Displays the number of receive actions during data transmission.
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 <i>Power Save Poll</i> (PSP) mode. Power Save Poll is a protocol, which helps to reduce the amount of time a radio needs to be 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	<p>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:</p> <ul style="list-style-type: none">• 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 ratio of the wireless client associated with the Access Point.
Signal	Displays the power of the radio signals in dBm.
Noise	Displays the disturbing influences on the signal by the interference of signals.
Error Rate	Displays the number of received bit rates altered due to noise, interference, and distortion. It's a unitless performance measure.
MOS Score	Displays the average call quality using the <i>Mean Opinion Score</i> (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's likely users will not be satisfied with the voice quality.
R-Value	Displays the R-value. R-value is a number or score that is used to quantitatively express the quality of speech in communications systems. This is used in digital networks that carry <i>Voice over IP</i> (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.

MOTOROLA SOLUTIONS INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
<http://www.motorolasolutions.com>

72E-146915-01 Revision A

February 2011