



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the AirWave Wireless AirWave Management Platform to Manage Avaya Wireless Access Point Devices – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring the AirWave Wireless AirWave Management Platform (AMP) to manage and monitor Avaya Wireless Access Point (AP) Devices on a local area network. During compliance testing, the Avaya AP Devices were successfully discovered, configured, and monitored by the AMP application. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Wireless Access Point (AP) Devices and the AirWave Wireless AirWave Management Platform (AMP). Avaya APs include:

- an AP equipped with a single fixed-mode radio, such as the AP-4, AP-5, and AP-6,
- an AP-4, AP-5, or AP-6 upgraded with a single configurable-mode 802.11a/b/g radio (the AP-4/5/6),
- an AP equipped with a single configurable-mode 802.11a/b/g radio (the AP-7), and
- an AP equipped with dual radios, one a fixed-mode 802.11a radio and the other a configurable-mode 802.11b/g radio (the AP-8).

Avaya APs attach to existing wired LAN segments to extend them to wireless 802.11 clients such as wireless IP phones and computers equipped with 802.11 interface cards. AMP is a wireless network management software application that allows the network administrator to centrally manage and monitor wireless APs. AMP runs on a Linux server attached to a wired network and is accessed through a web-based user interface (UI). From the AMP UI, the network administrator may enter APs into AMP management, either through automatic discovery or manual input, define uniform configurations and policies for groups of APs, adjust the settings of individual APs, and monitor wireless utilization and performance on the APs and their clients. In addition, AMP may be configured to restrict network access from certain APs or groups of APs, enforce group policies on APs, and provide firmware updates to APs.

Figure 1 shows a sample network configuration consisting of Avaya APs, wireless clients, an AMP server, and a DHCP/RADIUS server. The Avaya AP-4/5/6 resides on the same subnet as the AMP server, whereas the AP-8 resides on a separate subnet. The wireless clients include Avaya 3616 and 3626 Wireless IP Telephones and 802.11-enabled laptops with Avaya IP Softphone. The Avaya S8500 Media Server, Avaya G650 Media Gateway, Avaya Voice Priority Processor, Avaya 4600 Series IP Telephones, and Avaya C364T-PWR Converged Stackable Switch support the verification and illustration of the solution only, and are not discussed further in these Application Notes.

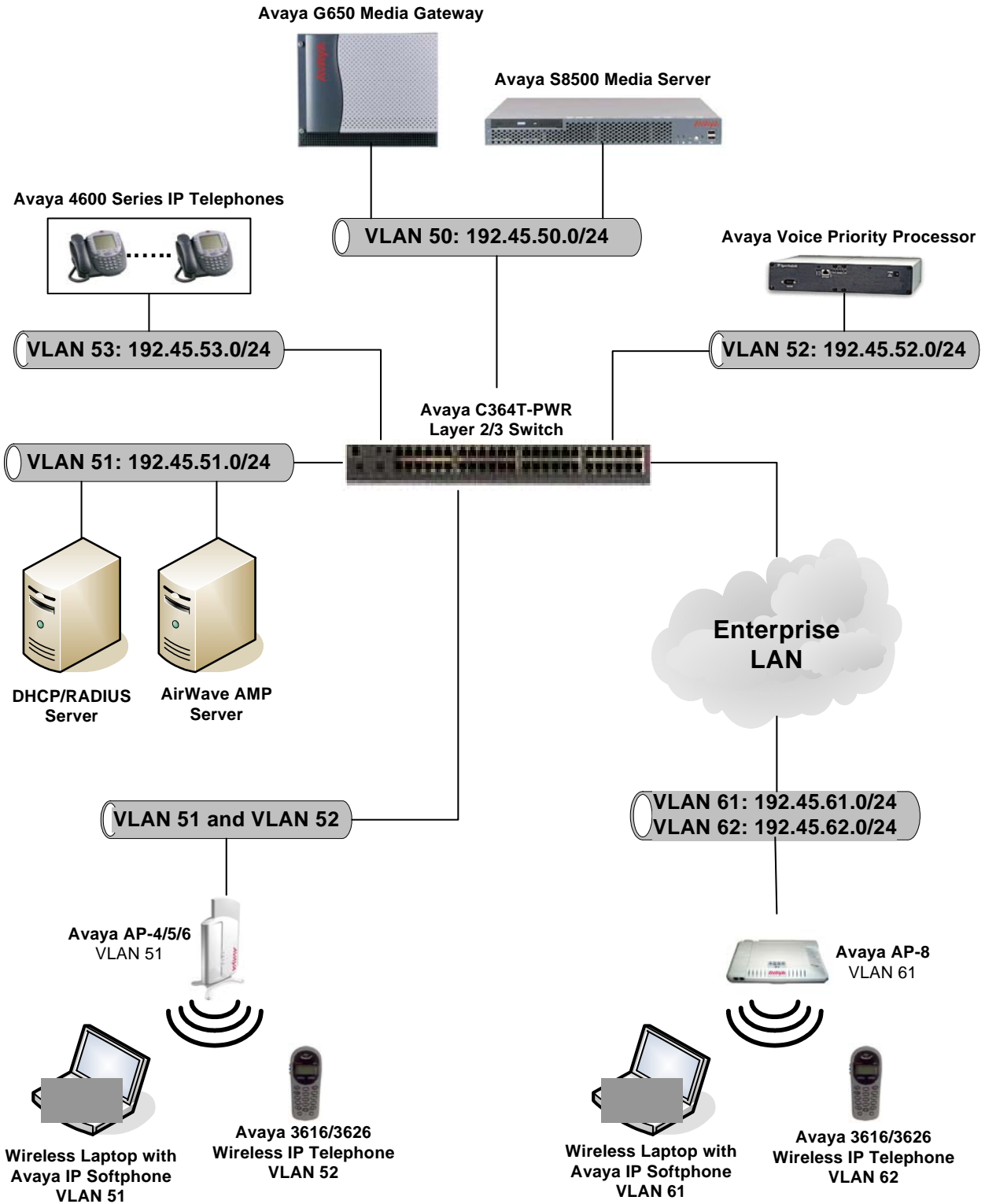


Figure 1: Sample configuration.

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment		Software/Firmware
Avaya AP-4/5/6 Wireless Access Point		2.5.3
Avaya AP-8 Wireless Access Point		2.6.0
Avaya 3616 Wireless IP Telephone		96.036
Avaya 3626 Wireless IP Telephone		96.036
Avaya Voice Priority Processor		17x.012
Avaya IP Softphone		5.2
Avaya S8500 Media Server		2.2 (R012x.02.0.111.4)
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface	12
	TN799DP C-LAN Interface	12
	TN2302AP IP Media Processor	HW11 FW95 HW03 FW93
Avaya 4600 Series IP Telephones		1.8.2 (4602SW) 2.2 (4610SW) 2.2 (4620SW) 2.0.2 (4630SW)
Avaya C364T-PWR Converged Stackable Switch		4.3.12
AirWave Wireless AirWave Management Platform (AMP)		3.3.1
802.11-enabled Laptop		Windows XP Professional SP2
DHCP/RADIUS Server		Windows 2003 Server Enterprise Edition

3. Configure Avaya AP Community Strings

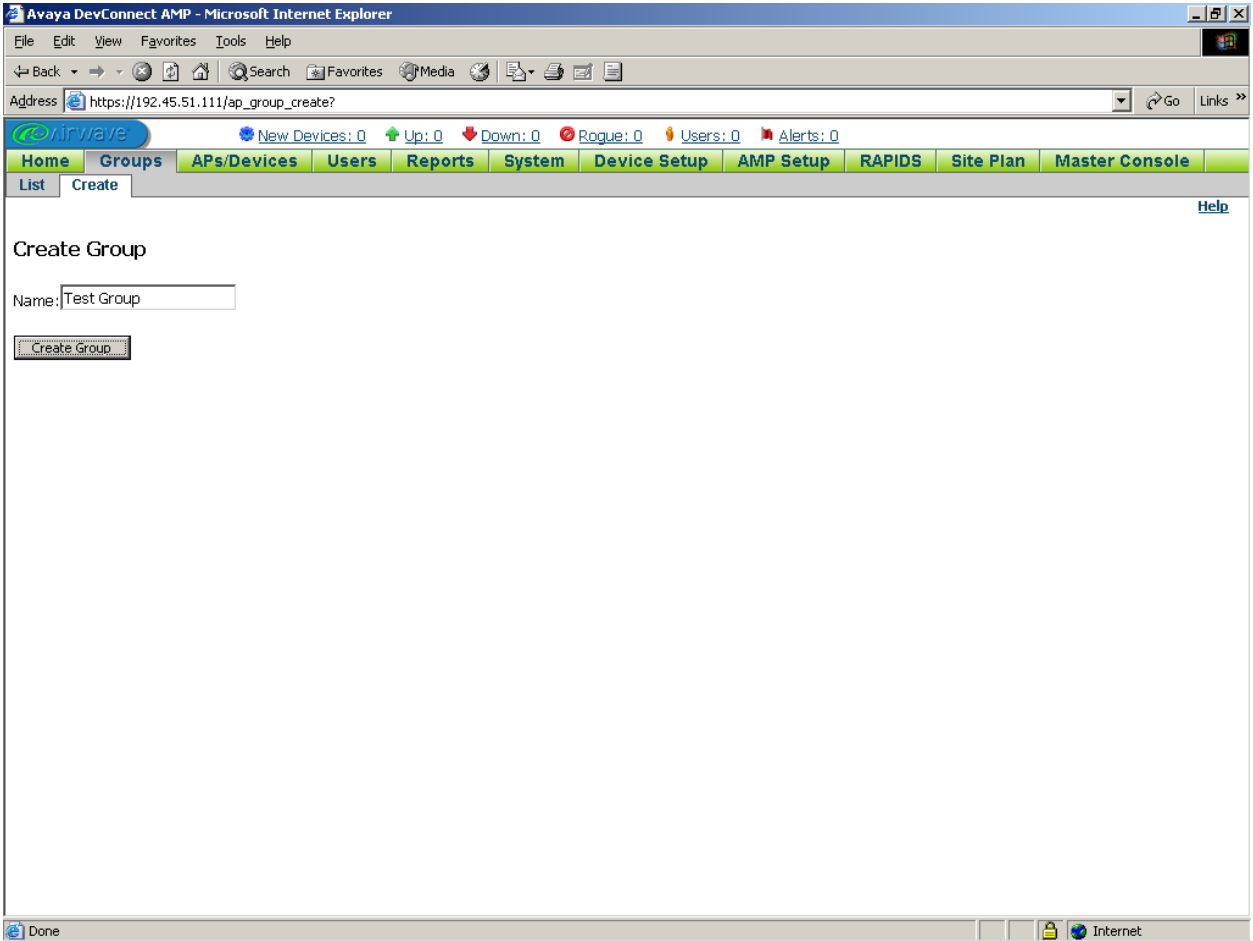
This section describes the steps for configuring community strings on Avaya APs. Repeat these steps for each Avaya AP.

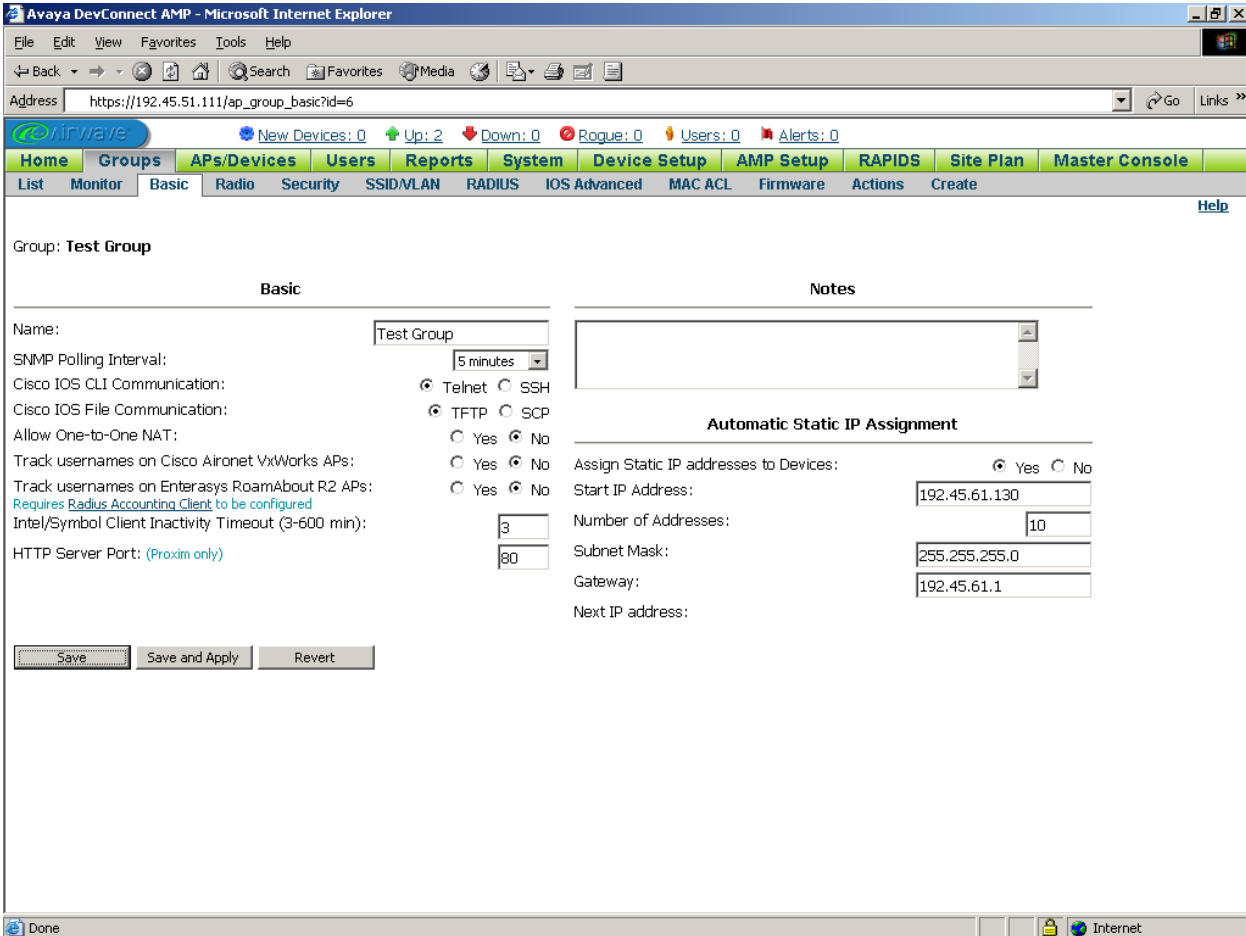
Step	Description
1.	Open a web browser and enter the AP's IP address in the URL. Log in with the appropriate credentials.
2.	Click on “ Configure ” and then the “ Management ” tab. Change the SNMP Read Community Password and SNMP Read/Write Community Password if necessary, and click on “ OK ”.

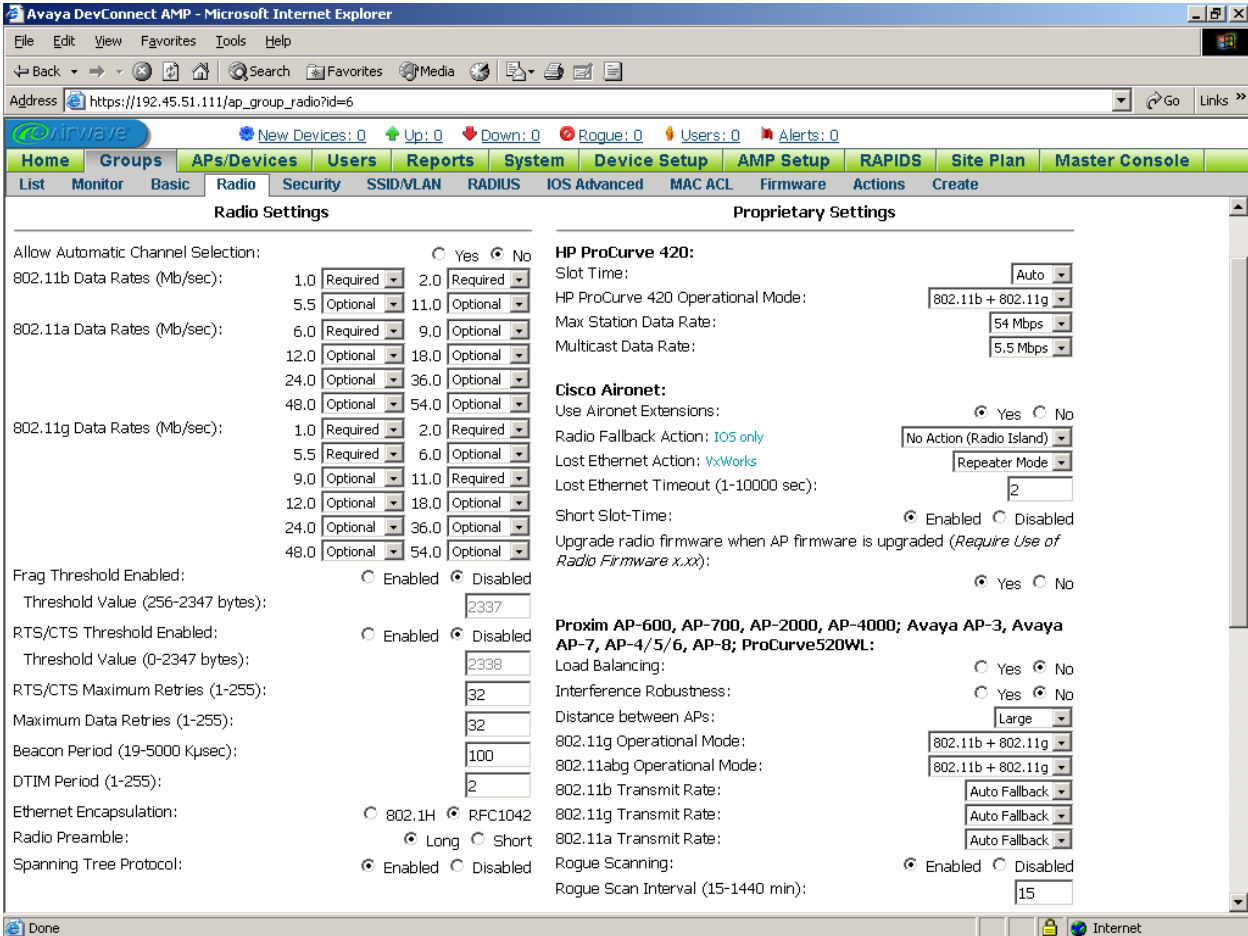
4. Configure the AirWave Wireless AirWave Management Platform (AMP)

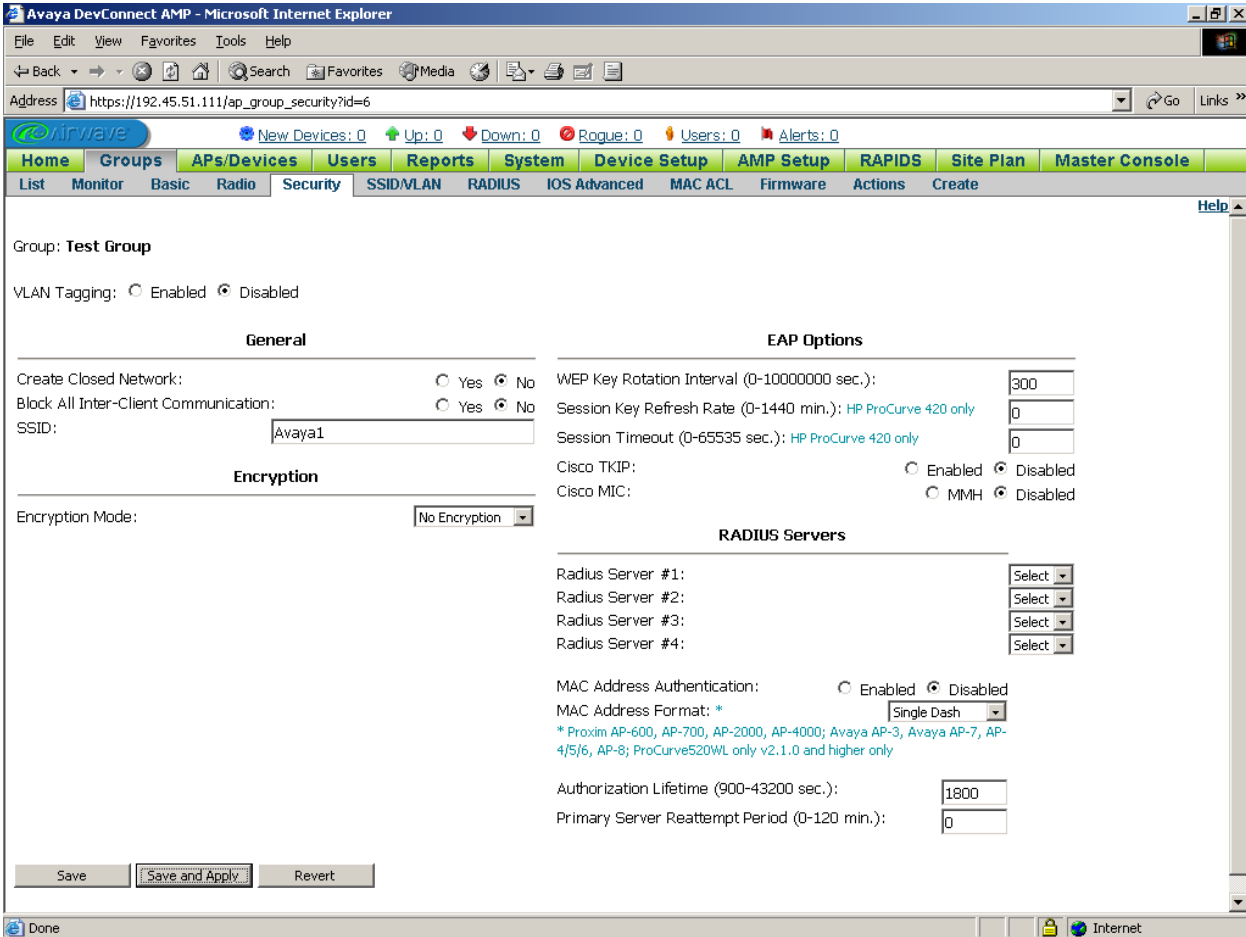
This section describes the steps for configuring the AirWave Management Platform (AMP) application. It assumes that AMP has already been installed on a Linux server.

4.1. Create AMP Groups

Step	Description
1.	Open a web browser and enter the AMP server IP address as the URL. Log in with the appropriate credentials.
2.	<p>Click on the “Groups” tab and then the “Create” tab. Specify a Name for the Group and click on “Create Group”.</p> 

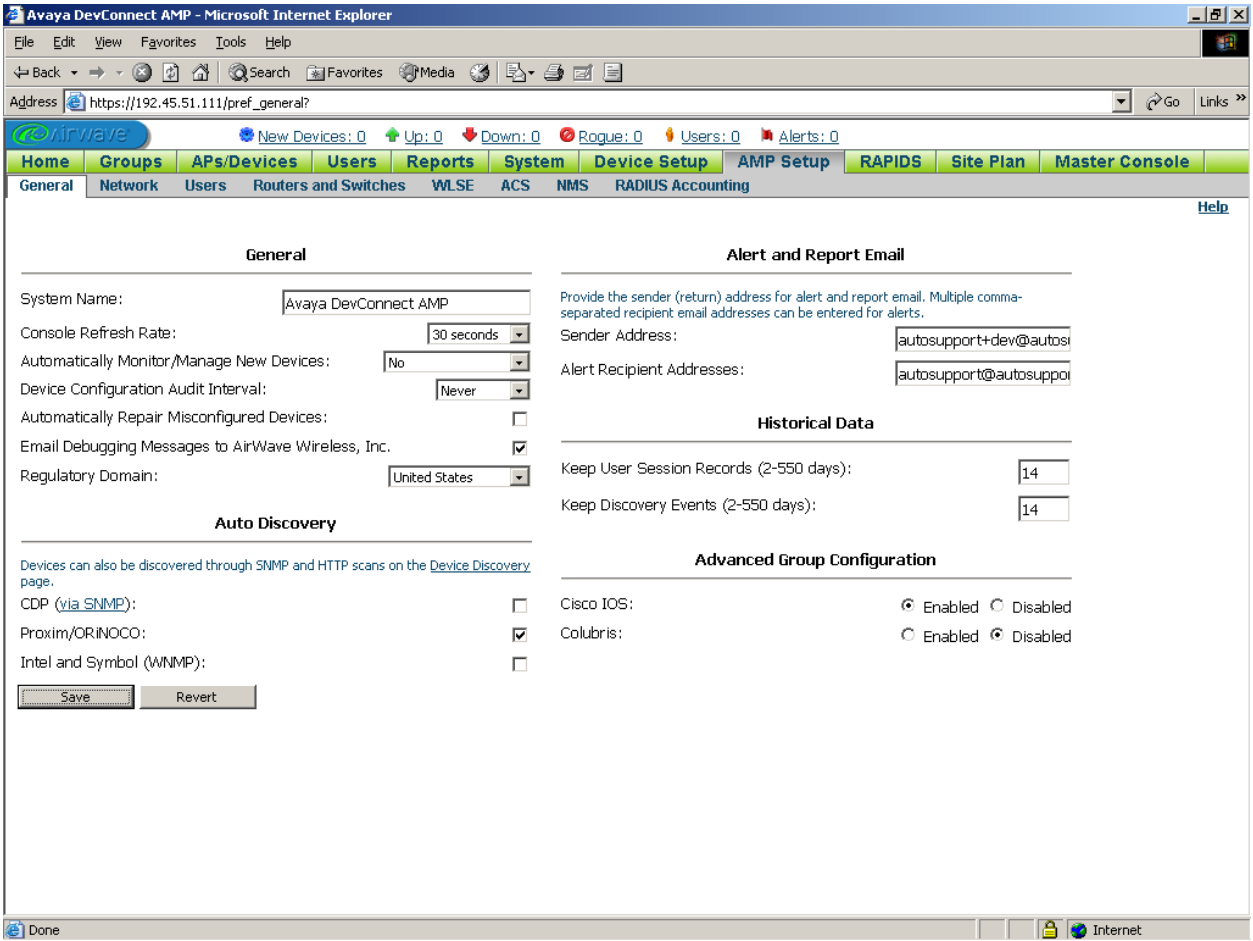
Step	Description
3.	<p>The Basic tab for the newly created Group is invoked. The default settings may be used.</p> <p>Optional: To have AMP automatically assign static IP addresses to Avaya APs that obtained IP addresses via DHCP, set Assign Static IP addresses to Devices to “Yes” and configure an IP address pool as depicted below. Click on “Save”.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows the URL: https://192.45.51.111/ap_group_basic?id=6. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/MLAN, RADIUS, IOS Advanced, MAC ACL, Firmware, Actions, and Create. The main content area is titled 'Group: Test Group' and has two sections: 'Basic' and 'Notes'. The 'Basic' section contains the following settings: Name: Test Group, SNMP Polling Interval: 5 minutes, Cisco IOS CLI Communication: Telnet (selected), Cisco IOS File Communication: TFTP (selected), Allow One-to-One NAT: No, Track usernames on Cisco Aironet VxWorks APs: No, Track usernames on Enterasys RoamAbout R2 APs: No, Intel/Symbol Client Inactivity Timeout (3-600 min): 3, and HTTP Server Port: 80. The 'Automatic Static IP Assignment' section contains the following settings: Assign Static IP addresses to Devices: Yes (selected), Start IP Address: 192.45.61.130, Number of Addresses: 10, Subnet Mask: 255.255.255.0, Gateway: 192.45.61.1, and Next IP address: (empty). At the bottom of the 'Basic' section are three buttons: Save, Save and Apply, and Revert. The 'Save' button is highlighted.</p>

Step	Description
4.	<p>Click on the “Radio” tab. Specify Radio Settings and Avaya AP settings according to customer requirements, and click on “Save” (scroll down to the bottom of the window).</p> <p>Note: Some AMP default settings, such as Allow Automatic Channel Selection, DTIM Period, Load Balancing, Interference Robustness, Rogue Scanning, and Rogue Scan Interval may be different from the equivalent default settings in the Avaya AP. The AMP default settings will overwrite the default settings of Avaya APs that are in “Managed” mode (see Section 4.2 Step 6 or Section 4.3 Step 2).</p> 

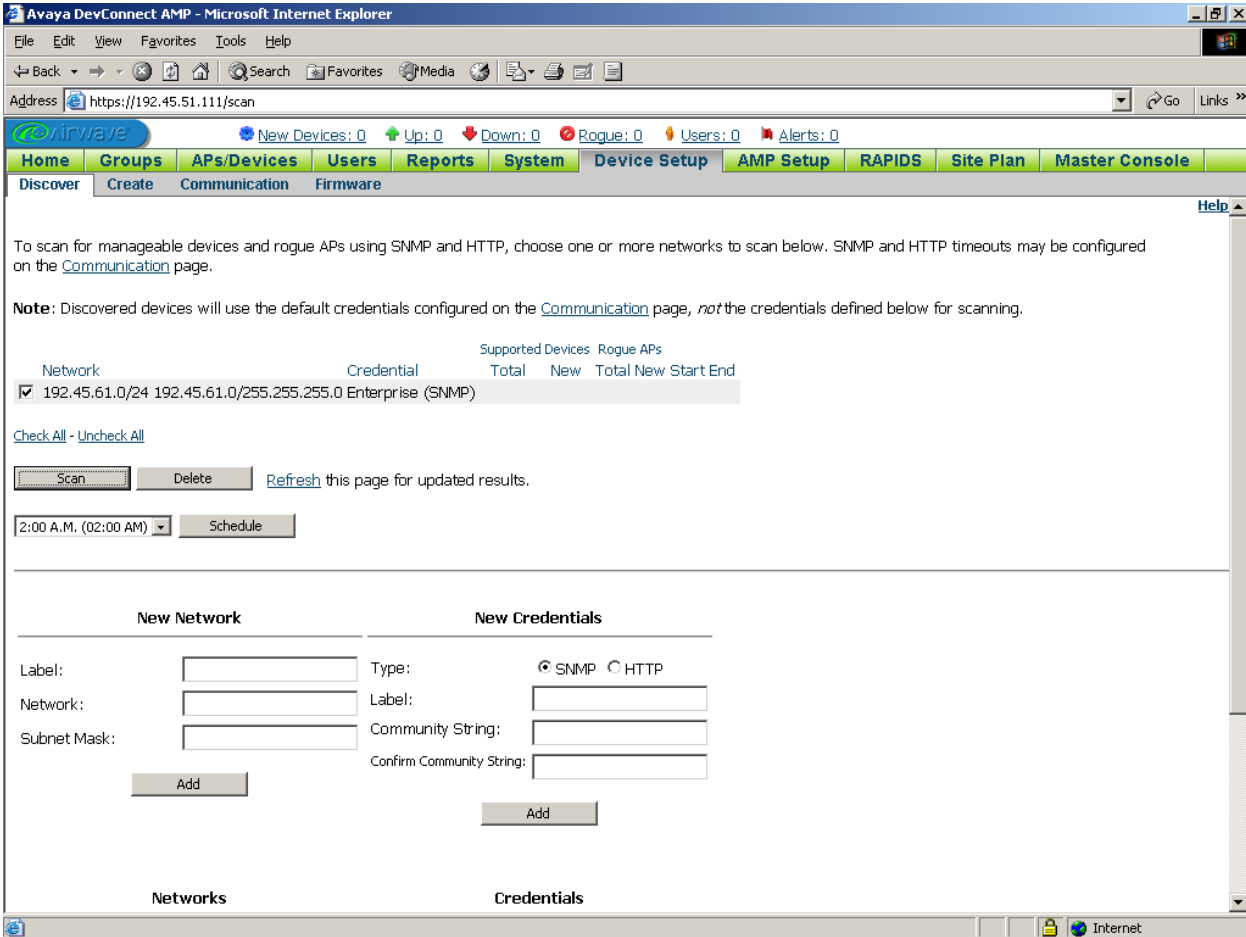
Step	Description
5.	<p>Click on the “Security” tab. Specify the SSID and other settings according to customer requirements (to configure encryption and authentication settings and RADIUS servers, see Section 4.5). Click on “Save and Apply”, and confirm the changes when prompted.</p>  <p>The screenshot displays the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows the URL: https://192.45.51.111/ap_group_security?id=6. The interface features a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/VLAN, RADIUS, IOS Advanced, MAC ACL, Firmware, Actions, and Create. The main content area is titled 'Group: Test Group' and shows 'VLAN Tagging: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled'. The 'General' section includes 'Create Closed Network: <input type="radio"/> Yes <input checked="" type="radio"/> No', 'Block All Inter-Client Communication: <input type="radio"/> Yes <input checked="" type="radio"/> No', and 'SSID: Avaya1'. The 'Encryption' section shows 'Encryption Mode: No Encryption'. The 'EAP Options' section includes 'WEP Key Rotation Interval (0-10000000 sec.): 300', 'Session Key Refresh Rate (0-1440 min.): HP ProCurve 420 only 0', 'Session Timeout (0-65535 sec.): HP ProCurve 420 only 0', 'Cisco TKIP: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled', and 'Cisco MIC: <input type="radio"/> MMH <input checked="" type="radio"/> Disabled'. The 'RADIUS Servers' section shows four servers with dropdown menus for selection. The 'MAC Address Authentication' section includes 'MAC Address Authentication: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled' and 'MAC Address Format: * Single Dash'. The 'Authorization Lifetime (900-43200 sec.): 1800' and 'Primary Server Reattempt Period (0-120 min.): 0' are also visible. At the bottom, there are 'Save', 'Save and Apply', and 'Revert' buttons.</p>

4.2. Enable AMP Discovery of Avaya APs

AMP can be configured to discover Avaya APs on the wired network. The steps below describe how to configure AMP to discover Avaya APs on its local subnet and other specific subnets.

Step	Description
1.	<p>In the AMP web interface, click on the “AMP Setup” tab and then the “General” tab. Check the Proxim/OriNOCO checkbox and click on “Save”. This allows AMP to automatically discover Avaya APs on its local subnet.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows 'https://192.45.51.111/pref_general?'. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup (selected), RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: General (selected), Network, Users, Routers and Switches, WLSE, ACS, NMS, and RADIUS Accounting. The main content area is divided into several sections: 'General' with fields for System Name (Avaya DevConnect AMP), Console Refresh Rate (30 seconds), Automatically Monitor/Manage New Devices (No), Device Configuration Audit Interval (Never), Automatically Repair Misconfigured Devices (unchecked), Email Debugging Messages to AirWave Wireless, Inc. (checked), and Regulatory Domain (United States); 'Alert and Report Email' with fields for Sender Address (autosupport+dev@autosupport.com) and Alert Recipient Addresses (autosupport@autosupport.com); 'Historical Data' with fields for Keep User Session Records (2-550 days) and Keep Discovery Events (2-550 days), both set to 14; 'Auto Discovery' with checkboxes for CDP (via SNMP) (unchecked), Proxim/ORINOCO (checked), and Intel and Symbol (WNMP) (unchecked); and 'Advanced Group Configuration' with radio buttons for Cisco IOS (Enabled) and Colubris (Disabled). At the bottom of the 'Auto Discovery' section are 'Save' and 'Revert' buttons.</p>

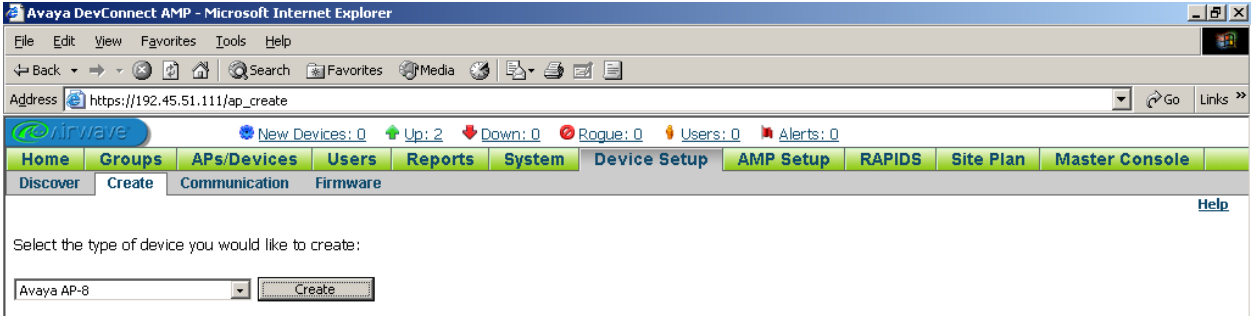
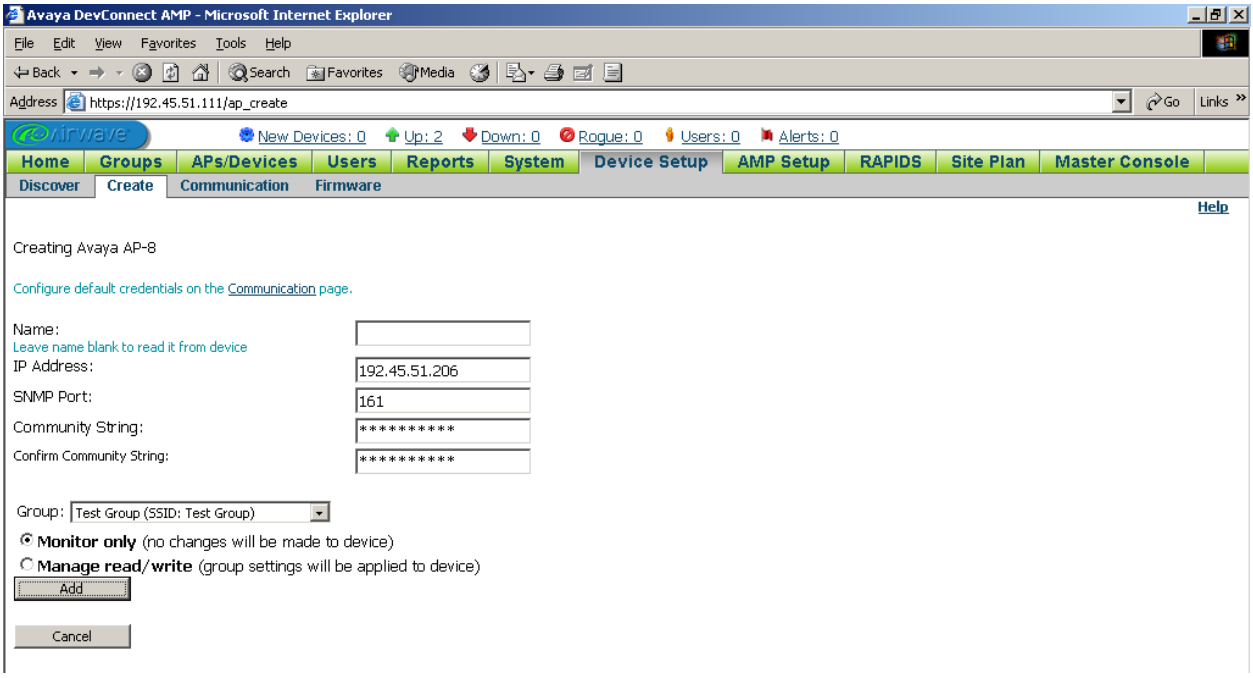
Step	Description								
2.	<p>Click on the “Device Setup” tab and then the “Discover” tab. In the New Network section, for each subnet that contains one or more Avaya APs, enter its Network address and Subnet Mask, assign a Label, and click on “Add”.</p> <div data-bbox="722 373 1063 562" data-label="Form"> <p style="text-align: center;">New Network</p> <hr/> <p>Label: <input type="text" value="192.45.61.0/24"/></p> <p>Network: <input type="text" value="192.45.61.0"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="Add"/></p> </div>								
3.	<p>In the New Credentials section, if there are Avaya APs with community strings that are neither “public” or “private, enter each community string and click on “Add”. Recall that community strings were configured on the Avaya APs in Section 3.</p> <div data-bbox="722 762 1063 982" data-label="Form"> <p style="text-align: center;">New Credentials</p> <hr/> <p>Type: <input checked="" type="radio"/> SNMP <input type="radio"/> HTTP</p> <p>Label: <input type="text" value="Enterprise"/></p> <p>Community String: <input type="text" value="*****"/></p> <p>Confirm Community String: <input type="text" value="*****"/></p> <p style="text-align: center;"><input type="button" value="Add"/></p> </div>								
4.	<p>Check the appropriate checkboxes under Networks and Credentials for each pertinent combination of subnet and community string. In the example below, a scan for Avaya APs on the 192.45.61.0/24 subnet with the community string specified for the “Enterprise” credential will be defined.</p> <div data-bbox="544 1228 1242 1465" data-label="Form"> <table border="0" style="width: 100%;"> <thead> <tr> <th style="text-align: center; border-bottom: 1px solid black;">Networks</th><th style="text-align: center; border-bottom: 1px solid black;">Credentials</th></tr> </thead> <tbody> <tr> <td style="vertical-align: top;"> <input checked="" type="checkbox"/> 192.45.61.0/24: 192.45.61.0/255.255.255.0 </td><td style="vertical-align: top;"> <input checked="" type="checkbox"/> Enterprise (SNMP) <input type="checkbox"/> admin (HTTP) <input type="checkbox"/> default (HTTP) <input type="checkbox"/> private (SNMP) <input type="checkbox"/> public (SNMP) </td></tr> <tr> <td style="text-align: center;"> Check All - Uncheck All </td><td style="text-align: center;"> Check All - Uncheck All </td></tr> <tr> <td style="text-align: center;"> <input type="button" value="Define Scan"/> </td><td style="text-align: center;"> <input type="button" value="Delete"/> </td></tr> </tbody> </table> </div>	Networks	Credentials	<input checked="" type="checkbox"/> 192.45.61.0/24: 192.45.61.0/255.255.255.0	<input checked="" type="checkbox"/> Enterprise (SNMP) <input type="checkbox"/> admin (HTTP) <input type="checkbox"/> default (HTTP) <input type="checkbox"/> private (SNMP) <input type="checkbox"/> public (SNMP)	Check All - Uncheck All	Check All - Uncheck All	<input type="button" value="Define Scan"/>	<input type="button" value="Delete"/>
Networks	Credentials								
<input checked="" type="checkbox"/> 192.45.61.0/24: 192.45.61.0/255.255.255.0	<input checked="" type="checkbox"/> Enterprise (SNMP) <input type="checkbox"/> admin (HTTP) <input type="checkbox"/> default (HTTP) <input type="checkbox"/> private (SNMP) <input type="checkbox"/> public (SNMP)								
Check All - Uncheck All	Check All - Uncheck All								
<input type="button" value="Define Scan"/>	<input type="button" value="Delete"/>								

Step	Description
5.	<p>Scroll up to the top of the window. Check the checkboxes of the Network/Credential combinations to scan and click on “Scan”. The scan may take several seconds; click on “Refresh” to show the scan’s progress until completion.</p> 

Step	Description
6.	<p>The discovered Avaya APs are listed in the APs/Devices->New page.</p> <p>To assign APs to a Group as “Monitored” APs (Group configuration settings will not be applied), check the corresponding checkboxes, select the Group that the APs are to be assigned to, select the Monitor only radio button, and click on “Add”.</p>  <p>To assign APs to a Group as “Managed” APs, check the corresponding checkboxes, select the Group that the APs are to be assigned to, select the Manage read/write radio button, and click on “Add”. Note that this will apply the Group configuration settings to the APs and reboot the APs.</p> 

4.3. Manual Entry of Avaya APs into AMP Management

An alternative to discovering and scanning for Avaya APs is to manually enter Avaya APs into AMP management. An Avaya AP may also be entered as a “Monitored” or “Managed” AP.

Step	Description
1.	<p>In the AMP web interface, click on the “Device Setup” tab and then the “Create” tab. Select the type of Avaya AP to add and click on “Create”.</p> 
2.	<p>Enter the IP Address and Community String of the Avaya AP, select the Group to assign the Avaya AP to, select either “Monitor only” or “Manage read/write”, and click on “Add”.</p> <p>Note: The Community String should be set to the SNMP Read/Write Community String of the Avaya AP (see Section 3 Step 2).</p> 

4.4. Individual AP Settings

To view and change certain settings on an individual Avaya AP from the AMP web interface, click on the “**APs/Devices**” tab, click on an Avaya AP from the resulting list, and click on the “**Manage**” tab. The relevant configurable parameters are:

- **Management Mode** – change the Avaya AP to a “Monitored” or “Managed” AP.
- **Device Communication** – specifies the **IP Address**, **SNMP Port**, and **Community String** that AMP must use to retrieve from and change settings on the Avaya AP.
- **Radio** – set the **Transmit Power** and **Channel**.

Avaya DevConnect AMP - Microsoft Internet Explorer

Address: https://192.45.51.111/ap_manage?id=2

New Devices: 0 Up: 2 Down: 0 Rogue: 0 Users: 0 Alerts: 0

Home Groups **APs/Devices** Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console

All Monitor **Manage** Detail New Up Down Ignored Help

General

Name: **Avaya-AP4-AP5-AP6-4b-61-3f**
Status: Up (OK)
Configuration: Good
Last Contacted: 6/9/2005 7:41 PM
Type: Avaya AP-4/5/6
Firmware: 2.5.3
Current Group: [Test Group](#)
Management Mode: ☒ Manage Read/Write ☐ Monitor Only
Notes (optional):

Settings

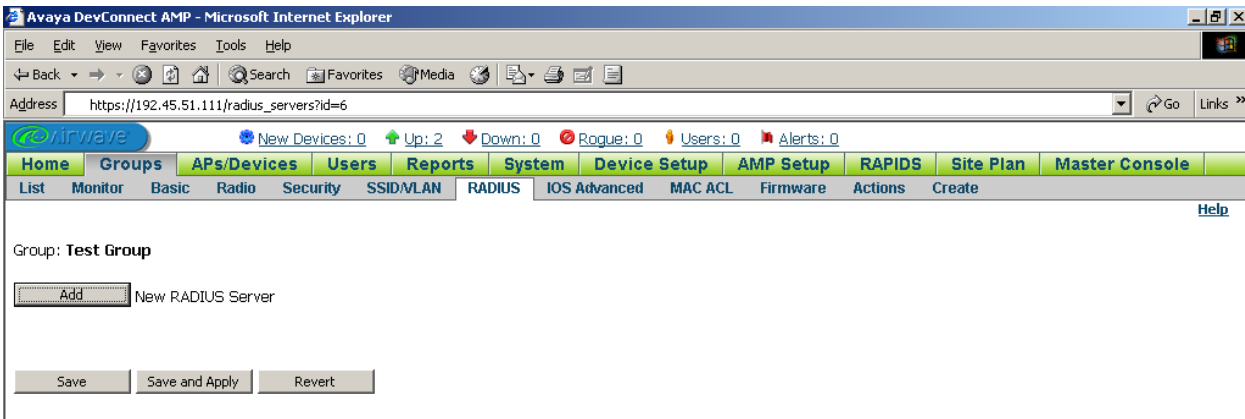
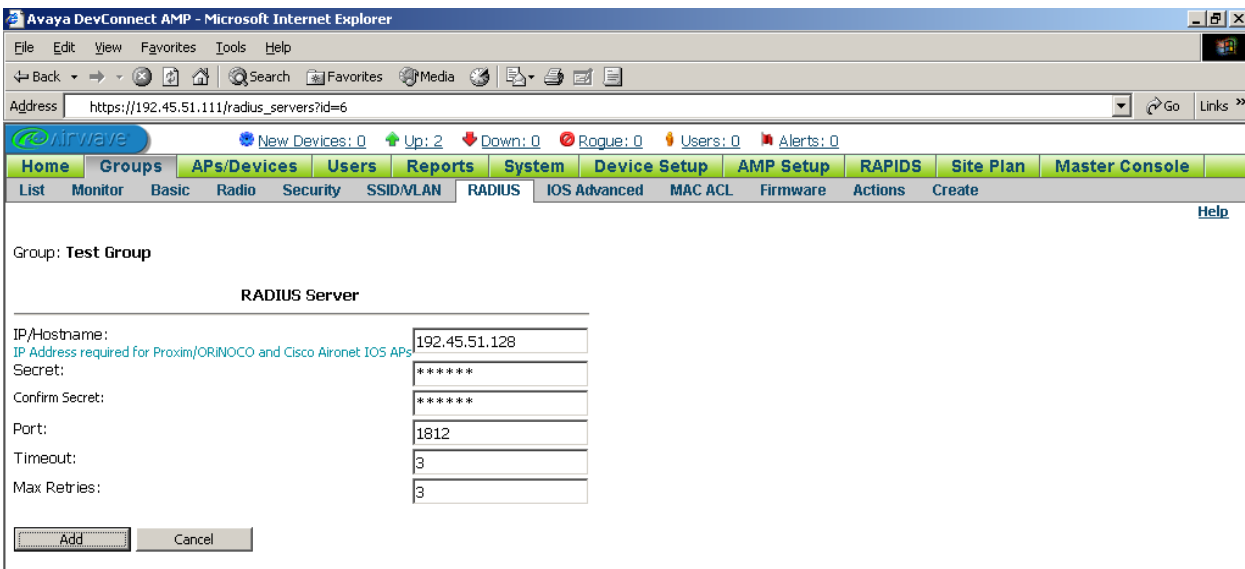
Name:
Location:
Contact:
Group:
802.11abg ('bg' mode) Radio
Transmit Power:
Channel:
Neighboring APs: No neighbors have been discovered yet.
DHCP: ☐ Yes ☒ No
LAN IP:
Subnet Mask:
Gateway:

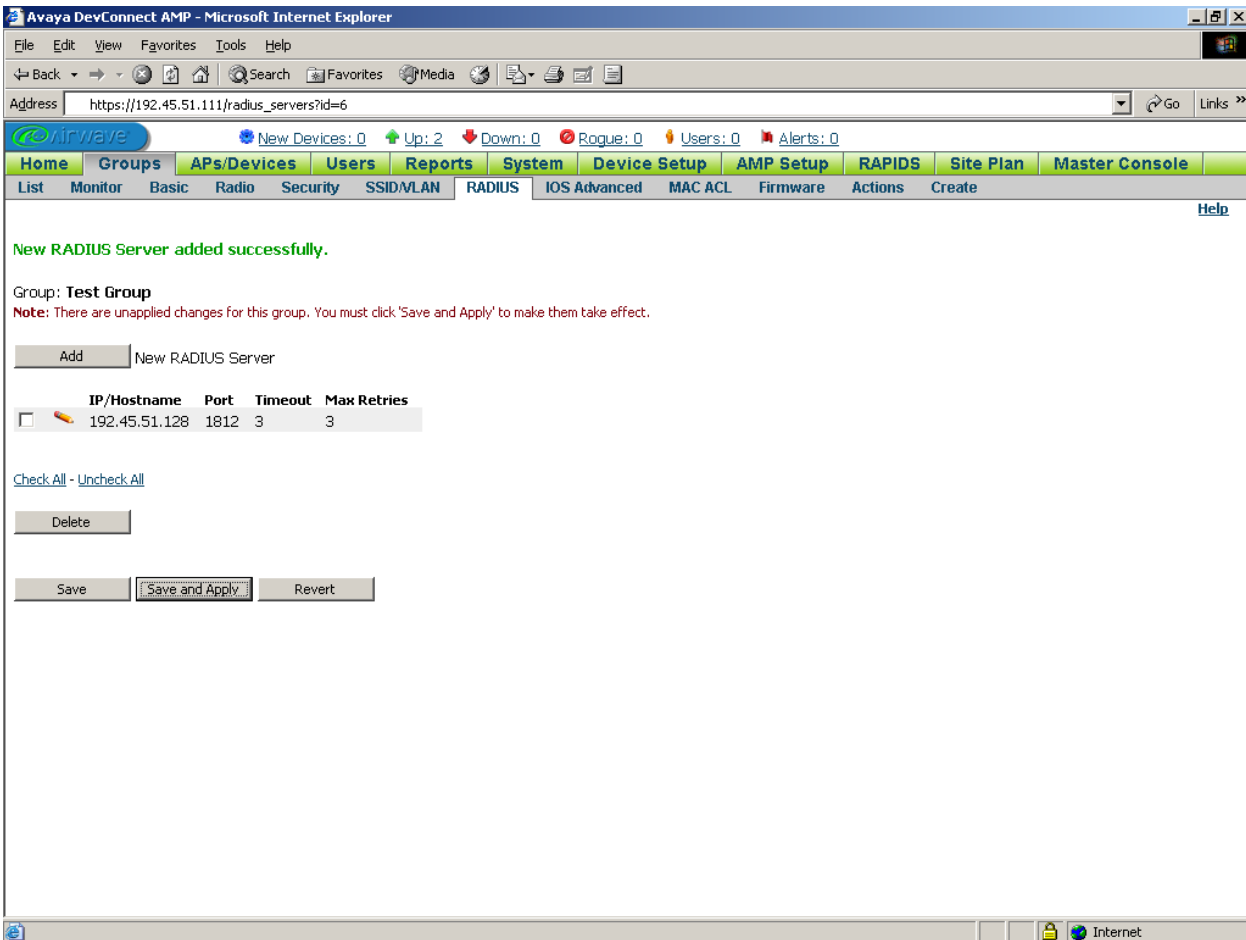
Device Communication

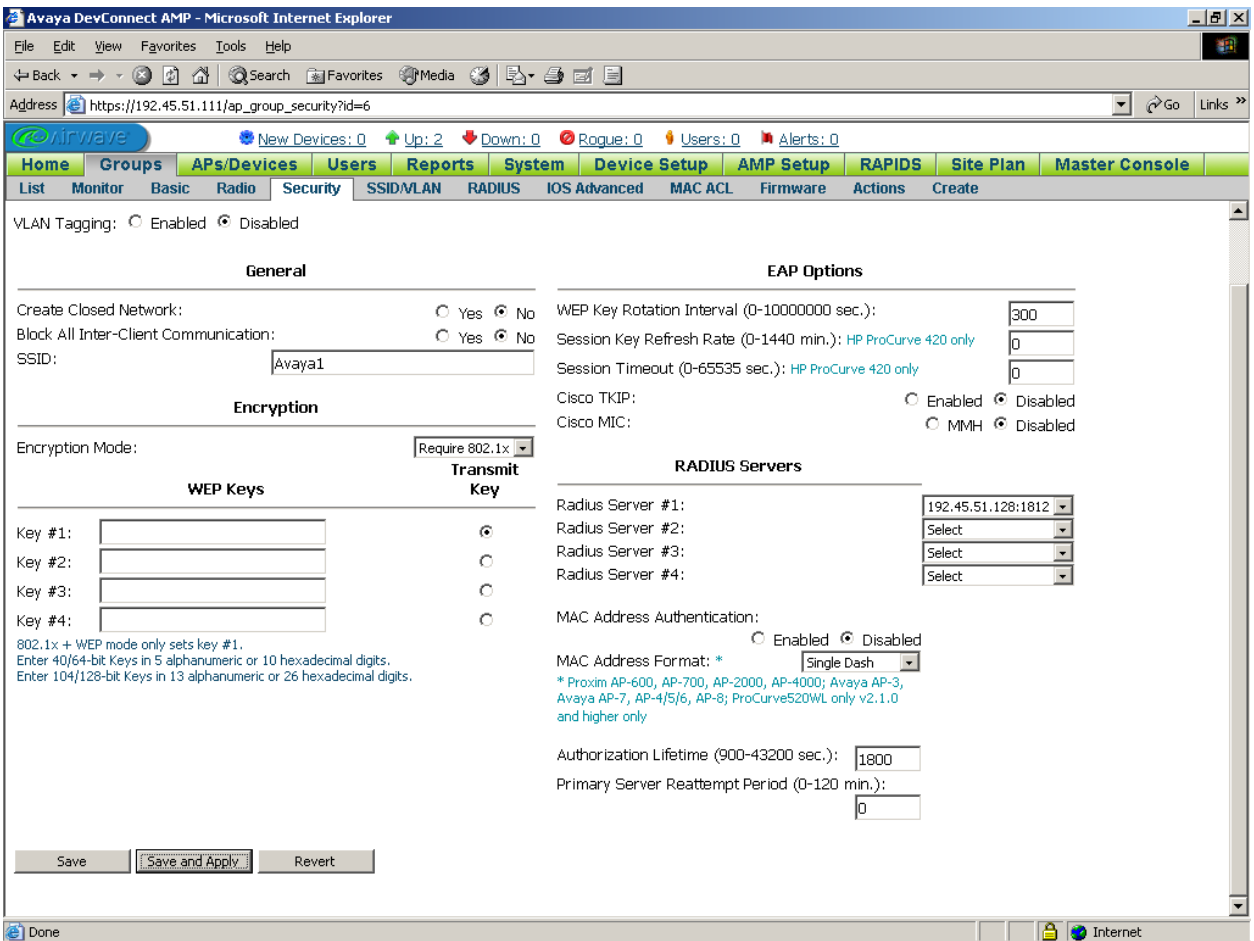
[View Device Credentials](#)
If this device is down because its IP address or management ports have changed, update the fields below with the correct information.
IP Address:
SNMP Port:
If this device is down because the credentials on the device have changed, update the fields below with the correct information.
Community String:
Confirm Community String:

4.5. Encryption and Authentication

This section describes the configuration of RADIUS servers, and encryption and authentication policies in AMP Groups. Skip to Step 5 if RADIUS authentication is not required.

Step	Description
1.	<p>In the AMP web interface, select a Group and click on its RADIUS tab. Click on “Add”.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows the URL https://192.45.51.111/radius_servers?id=6. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/LAN, RADIUS, IOS Advanced, MAC ACL, Firmware, Actions, and Create. The main content area shows 'Group: Test Group' and a 'New RADIUS Server' section with an 'Add' button highlighted.</p>
2.	<p>Enter the information for a RADIUS server and click on “Add”.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows the URL https://192.45.51.111/radius_servers?id=6. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/LAN, RADIUS, IOS Advanced, MAC ACL, Firmware, Actions, and Create. The main content area shows 'Group: Test Group' and a 'RADIUS Server' configuration form. The form has fields for IP/Hostname (192.45.51.128), Secret (*****), Confirm Secret (*****), Port (1812), Timeout (3), and Max Retries (3). The 'Add' button is highlighted.</p>
3.	<p>Repeat steps 1-2 to enter information about additional RADIUS servers to be used by Avaya APs in the Group.</p>

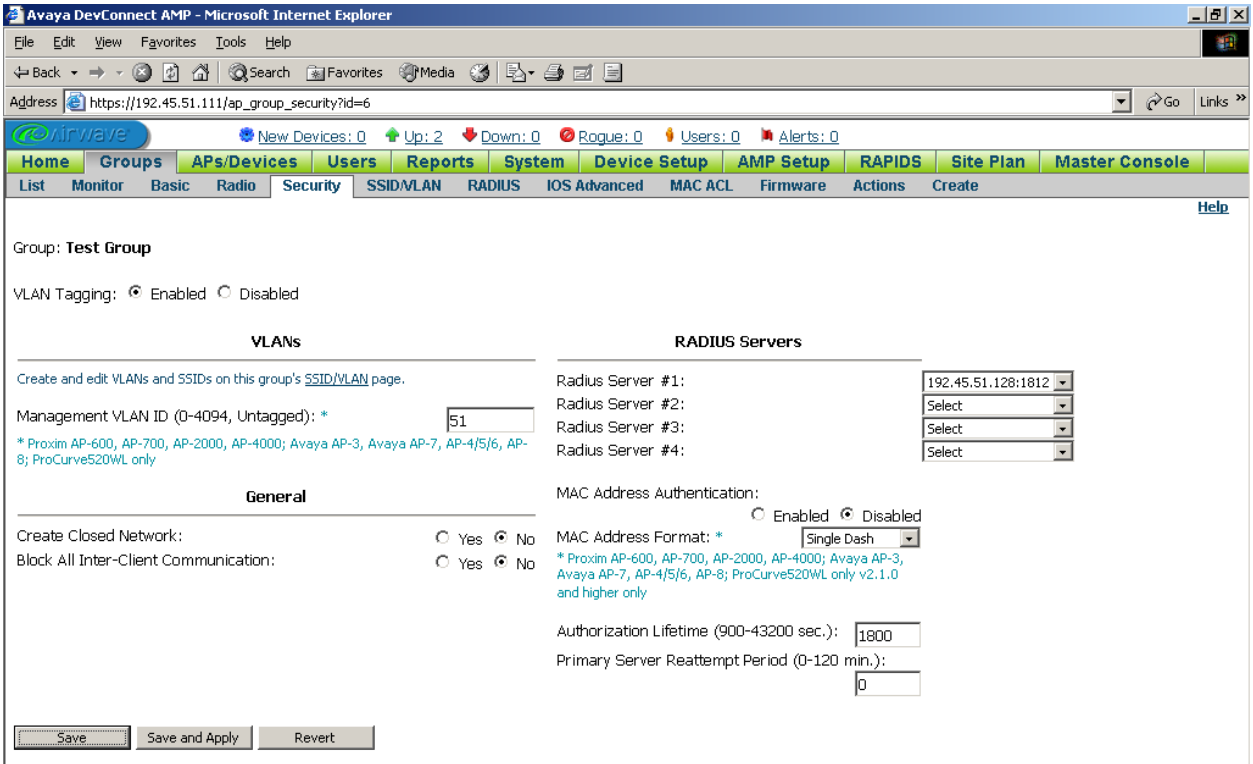
Step	Description
4.	<p>Click on “Save and Apply” when finished, and confirm the changes when prompted.</p> 

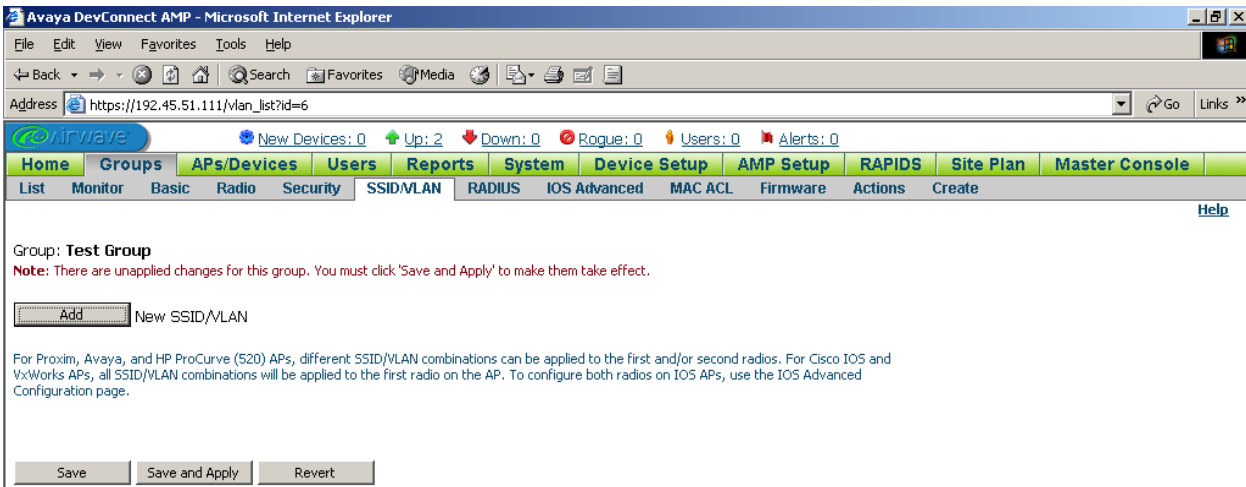
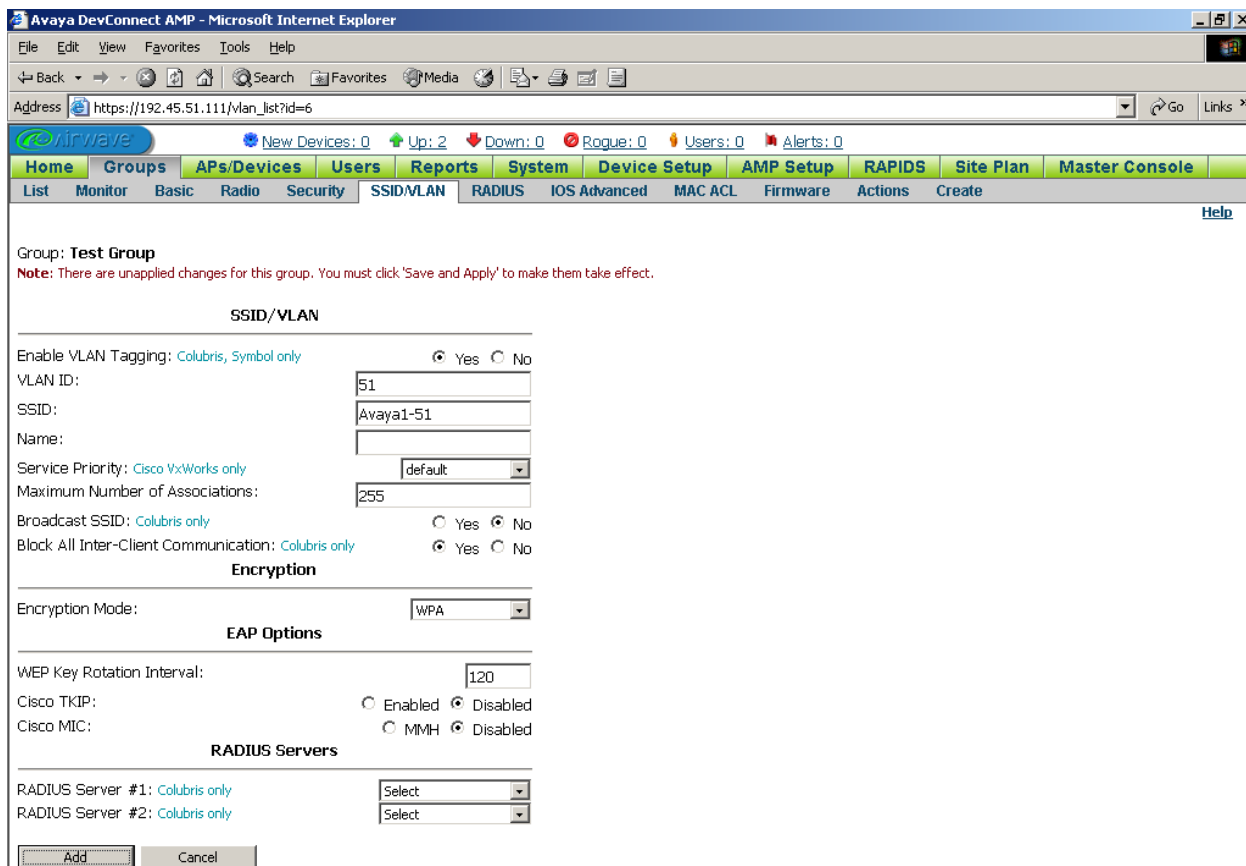
Step	Description
5.	<p>Click on the Security tab, and set the Encryption Mode to one of the encryption/authentication options from the pull-down list.</p> <p>For encryption/authentication options that use WEP, enter the WEP Keys and select one as a Transmit Key. In the example below, however, WEP Keys are not required for 802.1x encryption/authentication.</p> <p>For WPA encryption/authentication, specify the WPA Cipher (AES or TKIP) and in the case of WPA/PSK also the WPA Preshared key.</p> <p>For RADIUS-based authentication options, select a RADIUS server for Radius Server #1, and optionally Radius Server #2.</p> <p>Click on “Save and Apply”, and confirm the changes when prompted.</p> 

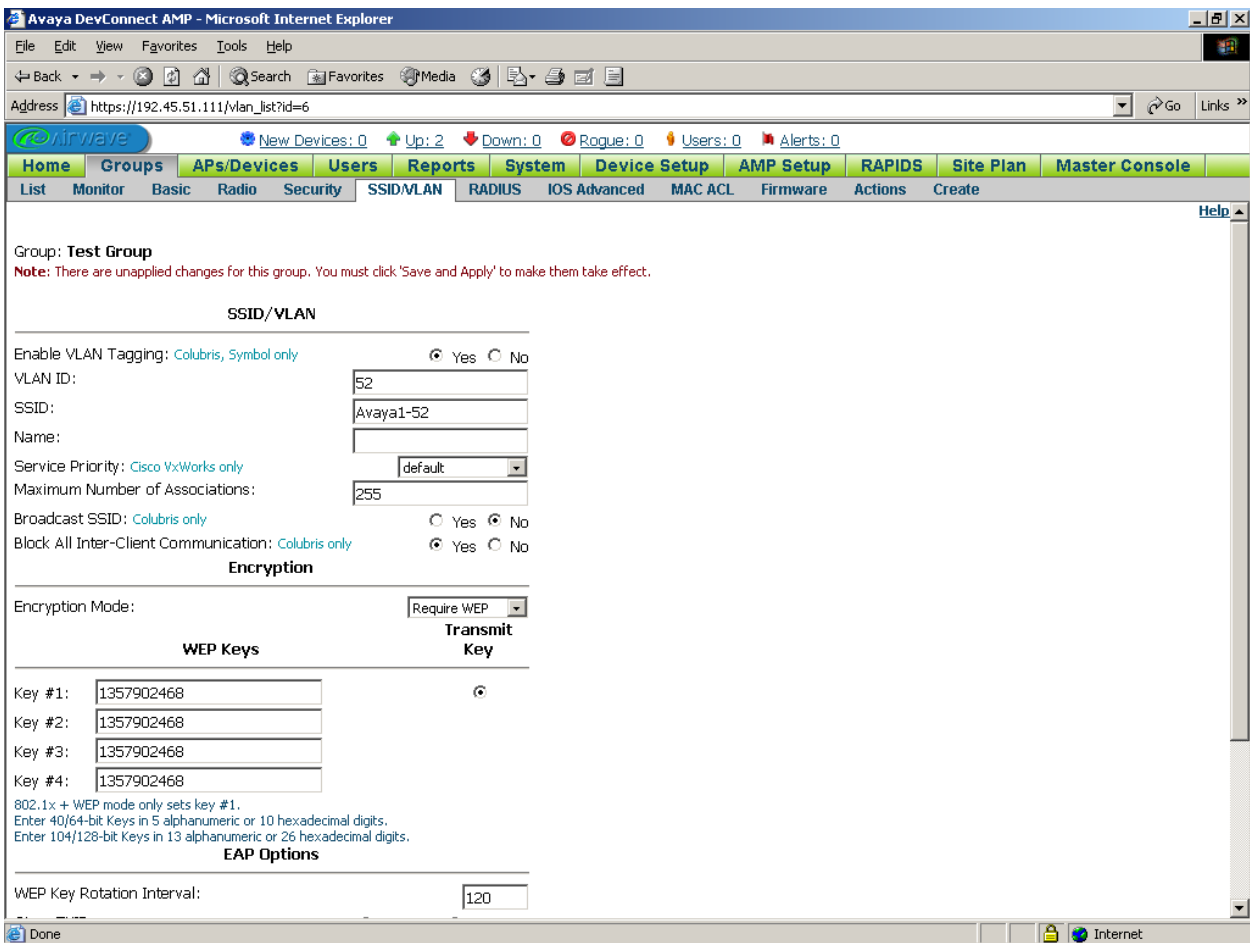
4.6. Multiple VLANs

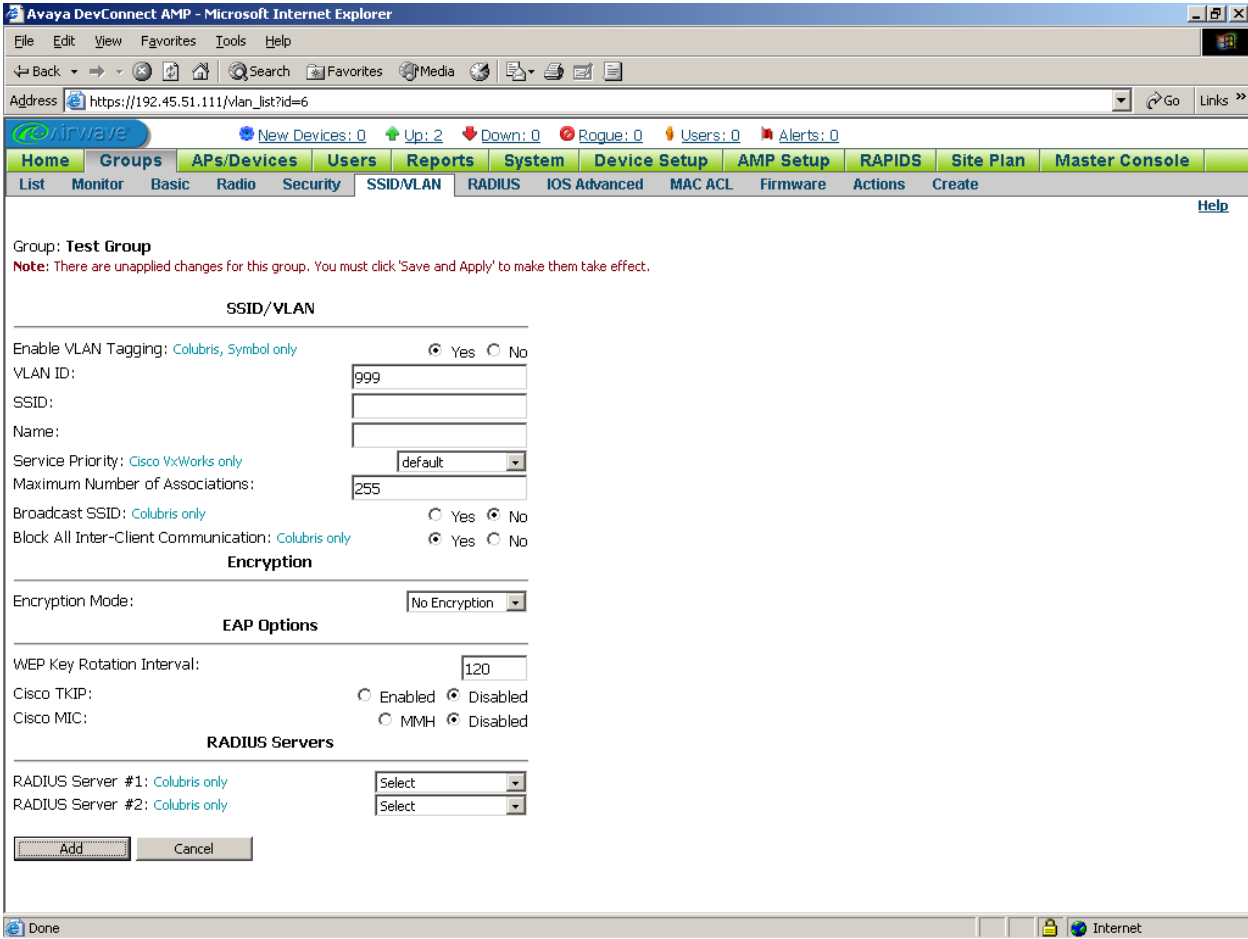
Avaya APs support multiple VLANs on each wireless interface with the following requirements:

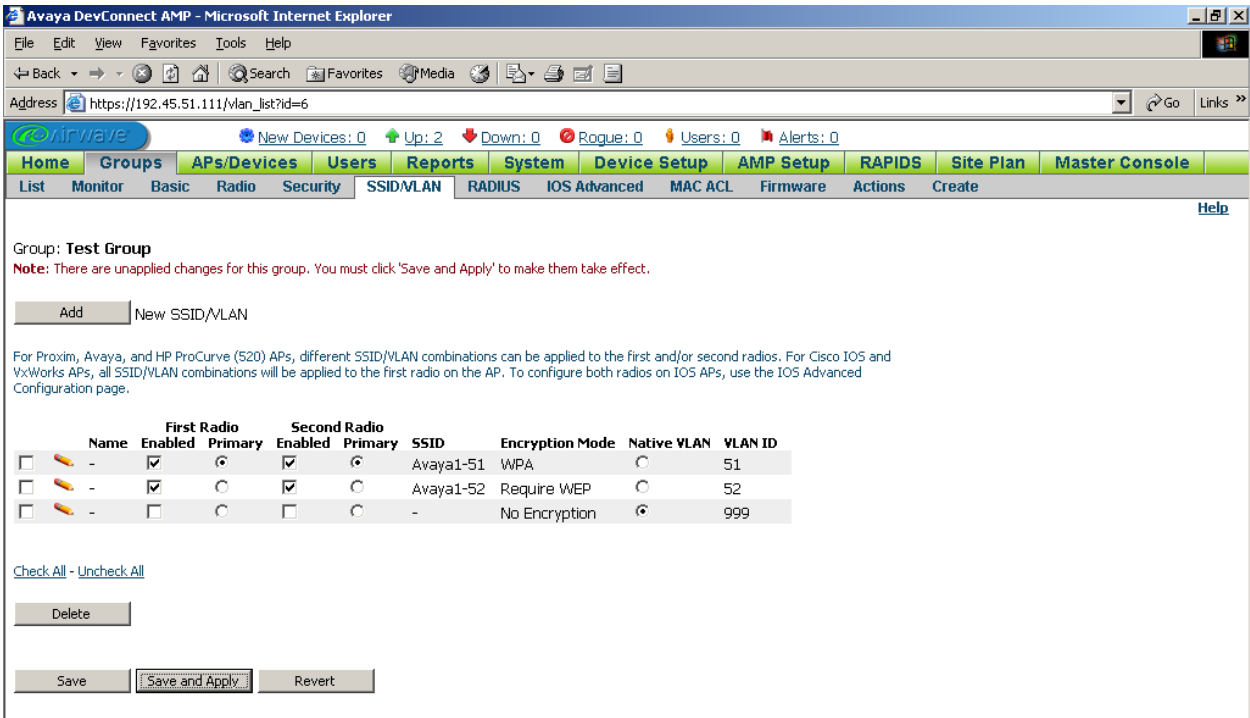
1. The Ethernet switch port to which the AP is connected must tag all VLANs. For example, on the Avaya C364T-PWR in **Figure 1**, the port trunking mode must be set to “dot1q”.
2. All VLANs on the wireless interfaces must be tagged.

Step	Description
1.	<p>From the AMP web interface, select a Group and click on its Security tab. Set VLAN Tagging to “Enabled” and enter the VLAN number of the Avaya APs’ management interface* as the Management VLAN ID. Select a RADIUS server for Radius Server #1, and optionally Radius Server #2 if RADIUS-based authentication is to be used on any of the VLANs. Click on “Save”.</p> <p>* Since this VLAN cannot be untagged due to the first requirement for multiple VLAN support, the management interfaces of all the Avaya APs in the Group must be on the same VLAN. The AP-4/5/6 and AP-8 in the sample configuration of Figure 1 must be in different Groups, because they are in different VLANs.</p> 

Step	Description
2.	<p>Click on the “SSID/VLAN” tab and then “Add”.</p> 
3.	<p>Enter a VLAN ID, SSID, and, if desired, the Encryption Mode. In the example below, VLAN 51 is configured for the wireless laptop clients in Figure 1. Click on “Add”.</p> 

Step	Description
4.	<p>Repeat Step 3 as necessary to add additional VLANs. The example below shows the configuration of VLAN 52 for the Avaya 3616 and 3626 Wireless IP Telephones in Figure 1.</p> 

Step	Description
5.	<p>After all desired VLANs have been added, repeats Step 3 to add a “stub” VLAN. As shown below, only an unused VLAN ID is required for the “stub” VLAN. The “stub” VLAN is a placeholder for the Native (untagged) VLAN in the next step.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows 'https://192.45.51.111/vlan_list?id=6'. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/VLAN, RADIUS, IOS Advanced, MAC ACL, Firmware, Actions, and Create. The main content area is titled 'Group: Test Group' and includes a note: 'Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.' The 'SSID/VLAN' section contains the following configuration options:</p> <ul style="list-style-type: none"> Enable VLAN Tagging: Colubris, Symbol only (Yes selected, No unselected) VLAN ID: 999 SSID: (empty field) Name: (empty field) Service Priority: Cisco VxWorks only (default selected) Maximum Number of Associations: 255 Broadcast SSID: Colubris only (No selected, Yes unselected) Block All Inter-Client Communication: Colubris only (Yes selected, No unselected) <p>The 'Encryption' section shows 'Encryption Mode: No Encryption'. The 'EAP Options' section shows 'WEP Key Rotation Interval: 120', 'Cisco TKIP: Disabled' (Enabled unselected, Disabled selected), and 'Cisco MIC: Disabled' (MMH unselected, Disabled selected). The 'RADIUS Servers' section shows two 'Select' dropdown menus for 'RADIUS Server #1' and 'RADIUS Server #2'. At the bottom are 'Add' and 'Cancel' buttons.</p>

Step	Description
6.	<p>In the row for the “stub” VLAN configured in the previous step, uncheck the Enabled checkboxes under First Radio and Second Radio, and set the Native VLAN radio button. The “stub” VLAN is necessary because AMP requires that one VLAN be untagged in the Group; the stub VLAN acts as a placeholder for the untagged VLAN in the Group (recall that for multiple VLAN support, all VLANs configured on an Avaya AP wireless interface must be tagged). Note that since the “stub” VLAN is not enabled on any radio (wireless interface), it will not be configured on the Avaya APs in the Group.</p> <p>Click on “Save and Apply” and confirm the changes when prompted.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows the URL: https://192.45.51.111/vlan_list?id=6. The interface has a navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The SSID/VLAN tab is selected. Below the navigation bar, there is a section for 'Group: Test Group' with a note: 'Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.' Below this, there is a table with columns: Name, First Radio Enabled, First Radio Primary, Second Radio Enabled, Second Radio Primary, SSID, Encryption Mode, Native VLAN, and VLAN ID. The table contains three rows: 1. Name: -, First Radio Enabled: checked, First Radio Primary: radio button, Second Radio Enabled: checked, Second Radio Primary: radio button, SSID: Avaya1-51, Encryption Mode: WPA, Native VLAN: radio button, VLAN ID: 51. 2. Name: -, First Radio Enabled: checked, First Radio Primary: radio button, Second Radio Enabled: checked, Second Radio Primary: radio button, SSID: Avaya1-52, Encryption Mode: Require WEP, Native VLAN: radio button, VLAN ID: 52. 3. Name: -, First Radio Enabled: unchecked, First Radio Primary: radio button, Second Radio Enabled: unchecked, Second Radio Primary: radio button, SSID: -, Encryption Mode: No Encryption, Native VLAN: radio button selected, VLAN ID: 999. Below the table, there are buttons: Check All, Uncheck All, Delete, Save, Save and Apply (highlighted), and Revert.</p>

4.7. MAC Access Control List

To control wireless client access to the network based on wireless client MAC addresses, in the AMP web interface, select a Group and click on its **MAC ACL** tab. Set **Use MAC ACL** to “**Yes**” and enter the MAC addresses of wireless clients that are permitted to access the network. Click on “**Save and Apply**”.

The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows `https://192.45.51.111/ap_group_mac_ad?id=6`. The interface has a top navigation bar with tabs: Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below this is a sub-navigation bar with tabs: List, Monitor, Basic, Radio, Security, SSID/WLAN, RADIUS, IOS Advanced, MAC ACL (selected), Firmware, Actions, and Create. The main content area shows the MAC ACL configuration for a selected group. It includes a dropdown menu for "Use MAC ACL" set to "Yes". Below this, a list of supported devices is shown: Intel; Symbol; Cisco VxWorks; Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only. A text area for entering MAC addresses is present, with the following text: "Set a list of whitespace-separated MAC addresses that are allowed to associate to an access point. This list will not be set on Cisco VxWorks APs." Below the text area, there are three buttons: "Save", "Save and Apply", and "Revert". The status bar at the bottom shows "Done" and "Internet".

5. Interoperability Compliance Testing

The interoperability compliance testing included feature functionality and serviceability testing. The feature functionality testing evaluated AMP capabilities in discovering, configuring, auditing, monitoring, upgrading, and downgrading Avaya APs. The serviceability testing introduced failure scenarios to determine if AMP is able to resume management of Avaya APs after failure recovery.

5.1. General Test Approach

The general approach was to perform actions on Avaya APs manually and using AMP, and validate consistency between AMP and the Avaya APs. The main objectives were to verify that:

- AMP is able to discover Avaya APs on its local subnet and on specified subnets.
- Avaya APs may be entered into and deleted from AMP management.
- AMP correctly configures, upgrades, downgrades, and monitors Avaya APs.
- AMP is able to change or assign static IP addresses to Avaya APs.
- AMP audits Avaya APs and reports deviations from Group policies.
- AMP enforces Group policies on Avaya APs in “Managed” mode.
- Wireless network security policies configured in AMP are correctly applied to Avaya APs.
- AMP is able to configure multiple VLANs on Avaya AP wireless interfaces.
- AMP tracks wireless clients associated with Avaya APs.
- Information reported by AMP is accurate and consistent with the actual information on Avaya APs.

For serviceability testing, failures such as cable pulls, and AMP server and Avaya AP resets were applied to verify that AMP is able to manage Avaya APs after the failures have been resolved.

5.2. Test Results

All test cases completed successfully. AMP was able to manage and accurately monitor Avaya APs and apply Group configuration policies to the APs. Wireless client access to the network was controlled by the security policies configured in AMP and applied to the Avaya APs.

The following are notes and observations obtained from testing:

1. After changing the AMP management mode of an Avaya AP from “Manage Read/Write” to “Monitor Only” and then changing settings directly on the Avaya AP, AMP correctly shows the differences between the AMP Group settings and the actual AP settings. However, the configuration status still shows as “Good”. The AMP administrator can perform a “Fetch Device Config” to update the configuration status.
2. If an Avaya AP does not already have values stored for its four WEP keys, then if WEP encryption is to be used, the AMP administrator must configure all four WEP keys. In

addition, AMP allows only the first WEP key to be used as the Transmit key, so the other three WEP keys are just placeholders.

6. Verification Steps

The following steps may be used to verify communication between AMP and Avaya APs, and to check the configuration:

1. Ping each Avaya AP from the AMP server and verify connectivity.
2. For automatic discovery of Avaya APs on a particular subnet, verify that the scan for the subnet is defined correctly. Check the scan's subnet IP address, subnet mask, and community string.
3. In the AMP web interface, check the status of all Avaya APs in the **APs->All** page. If the status of an Avaya AP is "Down", click on the AP and look for the error message. If the error message is "ICMP Ping Failed", check reachability to the AP from the AMP server. If the error message is "SNMP Get Failed", click on the **APs->Manage** tab and ensure that the community string that AMP uses to communicate with the AP is correct.
4. From the AMP UI, check the configuration status of all "Managed" Avaya APs in the **APs->All** page. If the configuration status of an Avaya AP is "Bad", then review the differences between the Group configuration settings and the actual configuration settings of the AP. If the Group settings are desired, then instruct AMP to apply the Group settings to the AP. If the AP's actual settings are desired, then do one of the following:
 - Place the AP in "Monitored" mode.
 - Reassign the AP to another Group with settings that match those of the AP.
 - Modify the Group configuration settings to match the actual settings of the AP. Note that modifying the Group settings may affect other APs in the Group (may cause those APs with a "Good" configuration status to become "Bad").
5. From the AMP UI, check the configuration status of all "Monitored" Avaya APs in the **APs->All** page. If the configuration status of an Avaya APs is "Bad", then review the differences between the Group configuration settings and the actual configuration settings of the AP. If the Group settings are desired, then place the AP in "Managed" mode and instruct AMP to apply the Group settings to the AP.
6. Check that the authentication and encryption settings of the wireless clients are consistent with APs that the wireless clients associate with.

7. Support

For technical support on the AirWave Management Platform, contact AirWave Technical Support at:

- E-mail: support@airwave.com
- Phone: 866-WIFI-AMP (866-943-4267)

8. Conclusion

These Application Notes illustrate the procedures for configuring the AirWave Wireless AirWave Management Platform (AMP) to manage and monitor Avaya Wireless Access Point (AP) Devices on a local area network. During compliance testing, the Avaya AP Devices were successfully discovered, configured, and monitored by the AMP application.

9. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

Product documentation for the AirWave Wireless AirWave Management Platform may be found at http://www.airwave.com/prodserv_products.html.

©2005 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.