



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.

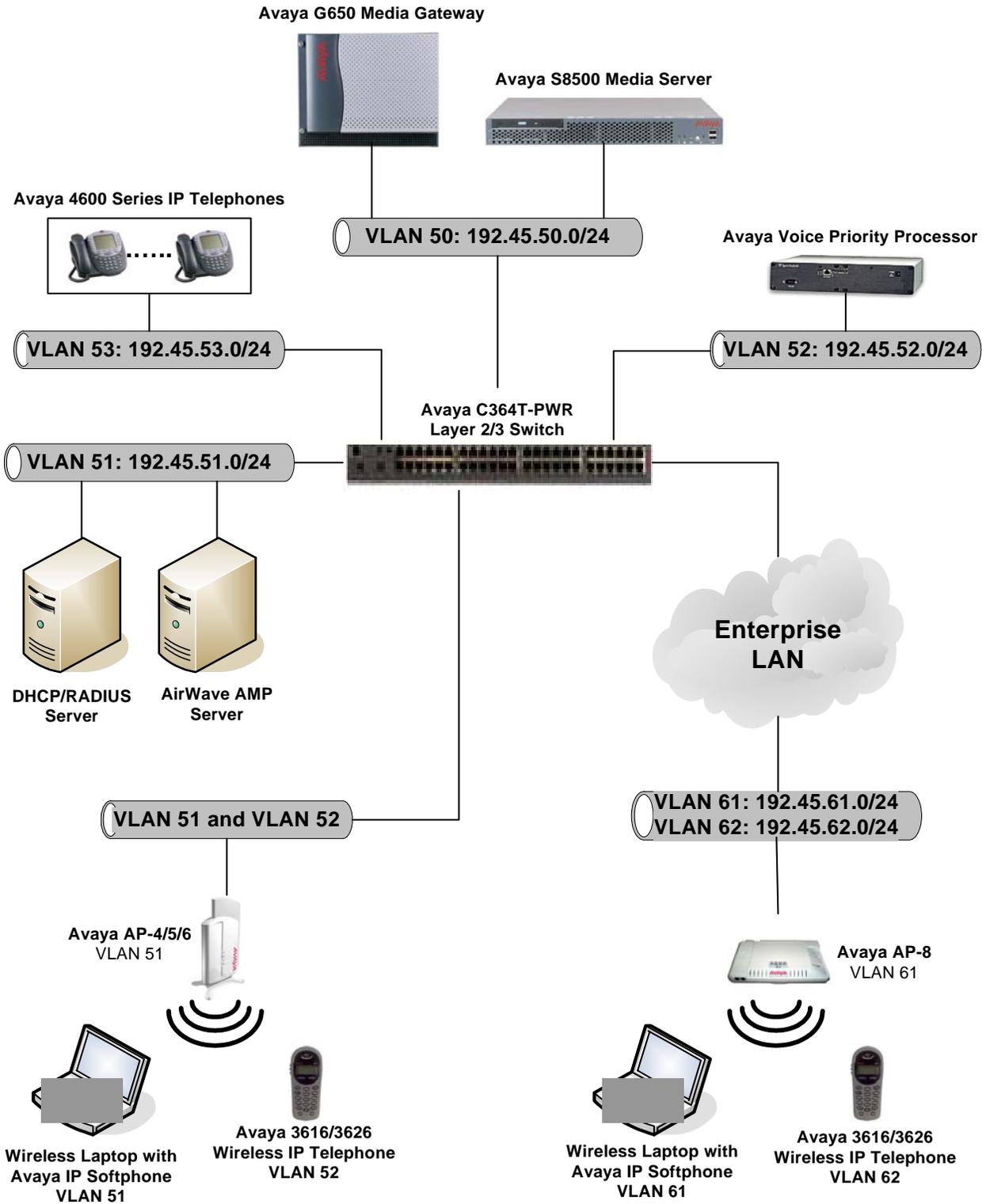


Figure 1: Sample configuration.

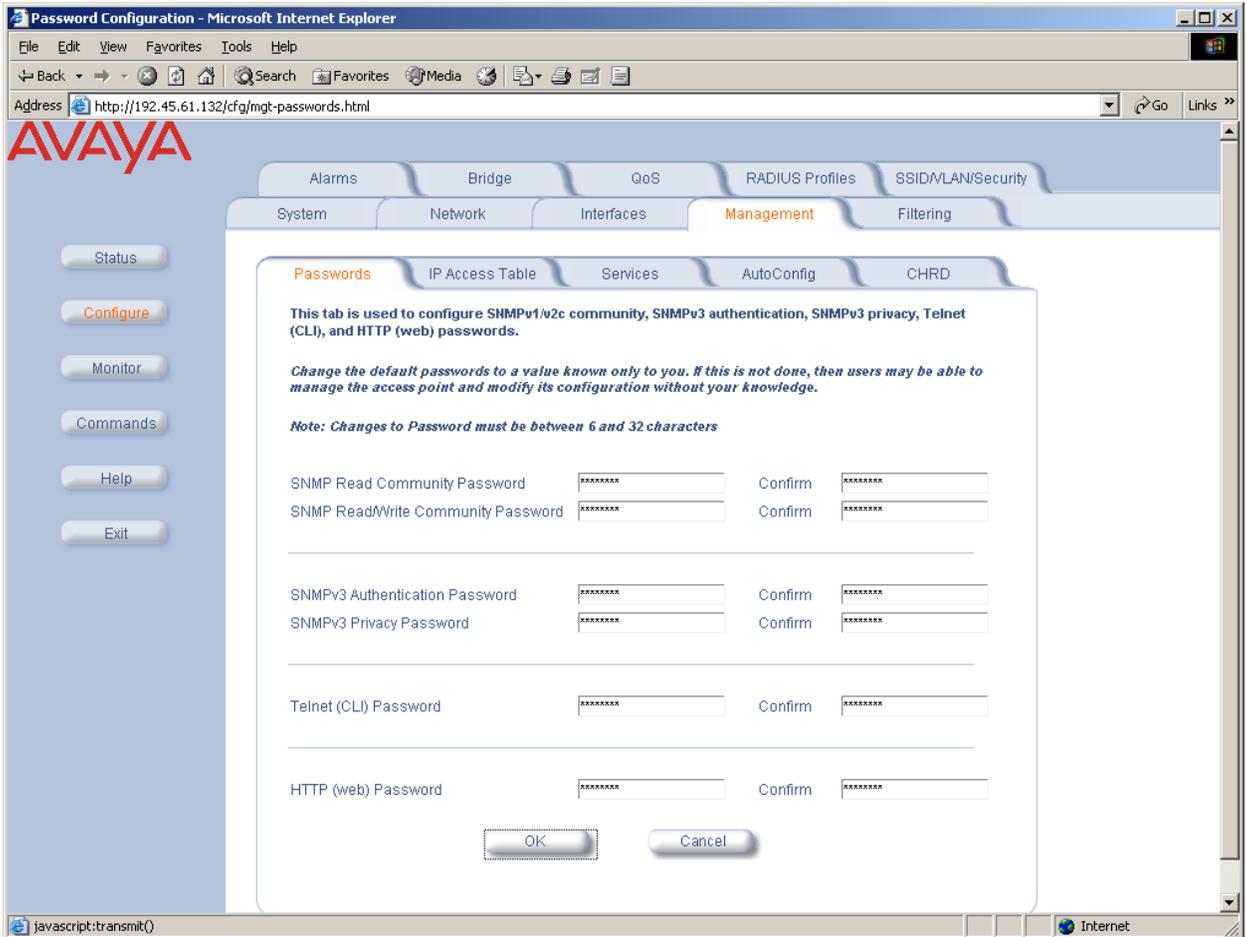
2. Equipment and Software Validated

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

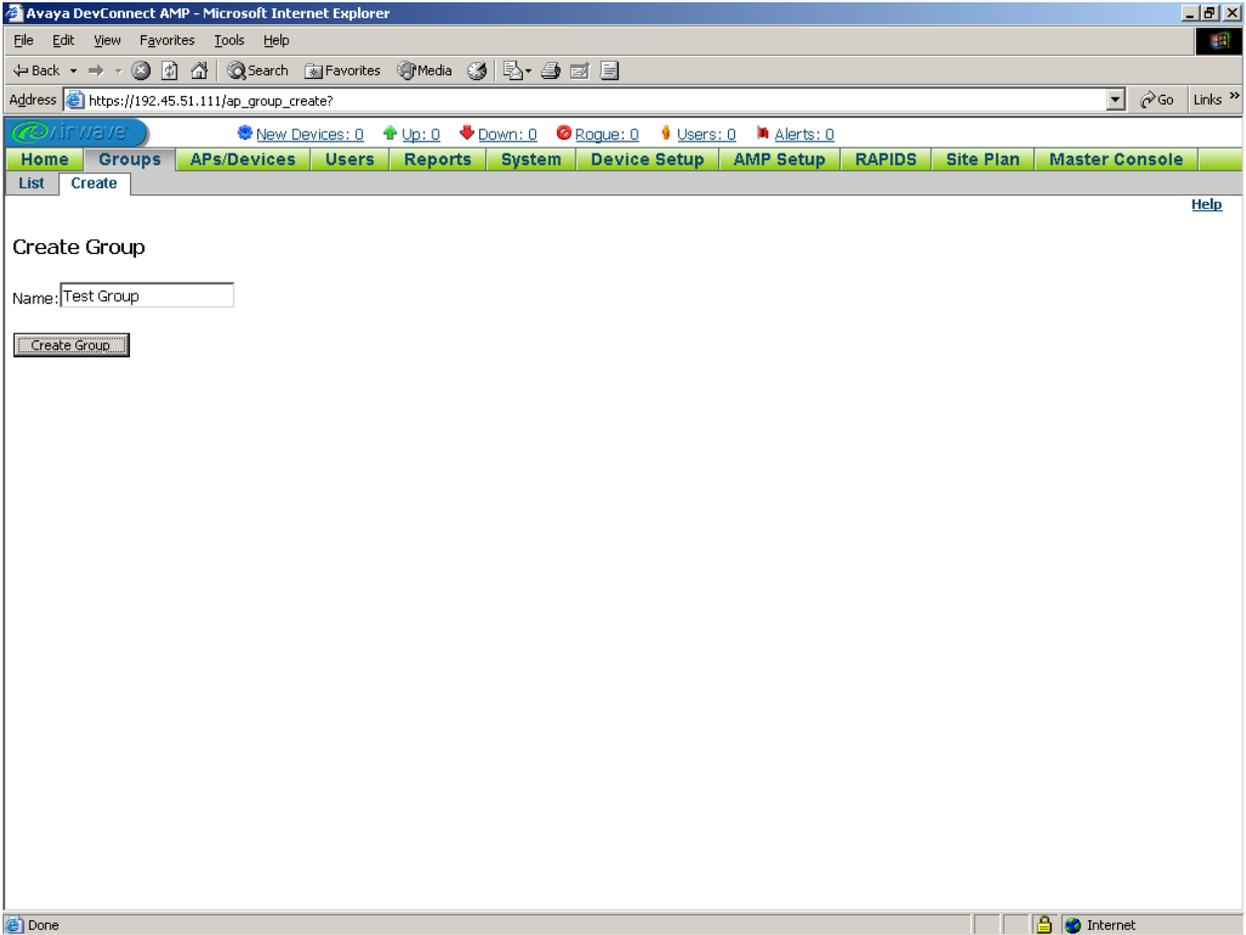
This section describes the steps for configuring community strings on Avaya APs. Repeat these steps for each Avaya AP.

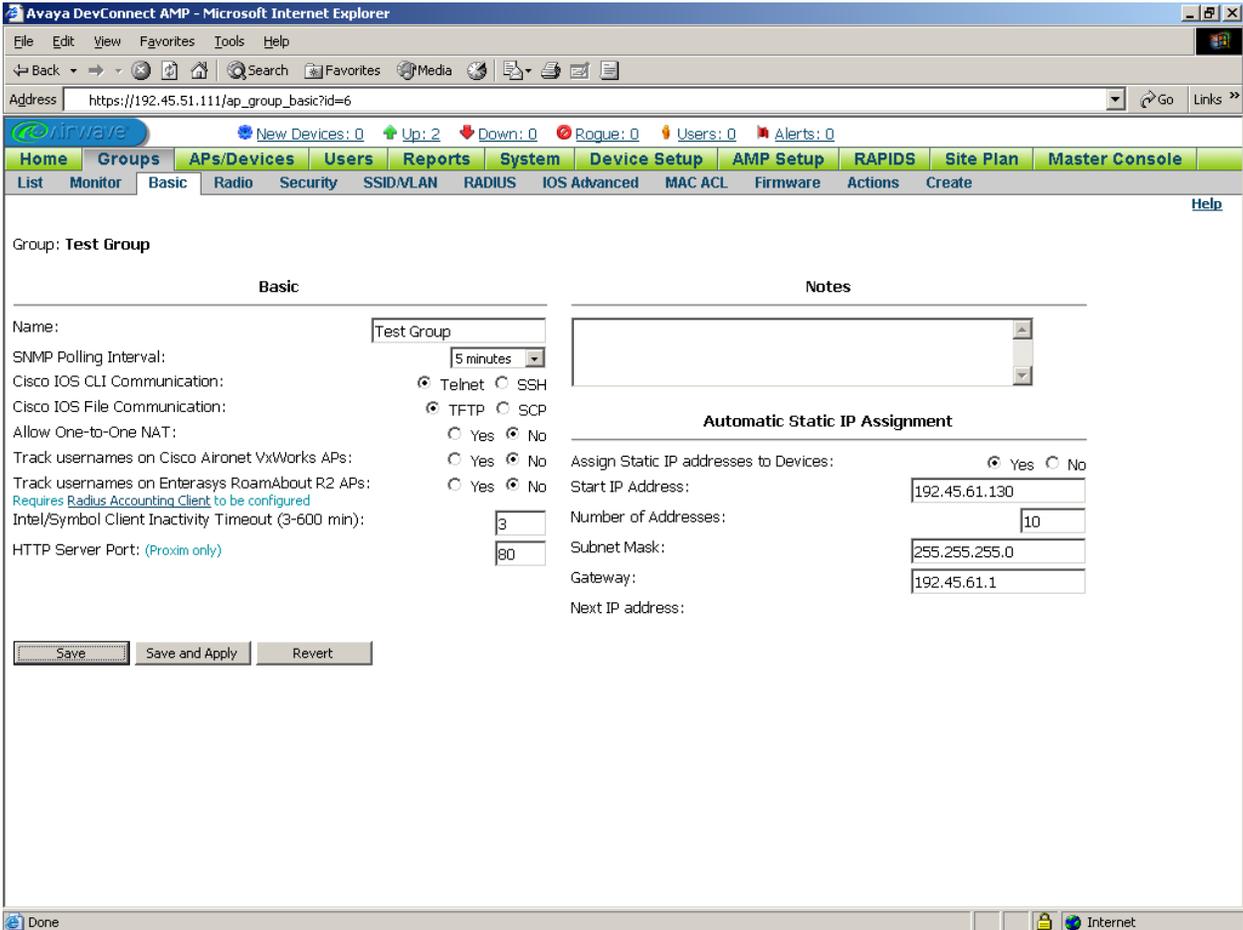
Step	Description
1.	Open a web browser and enter the AP's IP address in the URL. Log in with the appropriate credentials.
2.	<p>Click on “Configure” and then the “Management” tab. Change the SNMP Read Community Password and SNMP Read/Write Community Password if necessary, and click on “OK”.</p> 

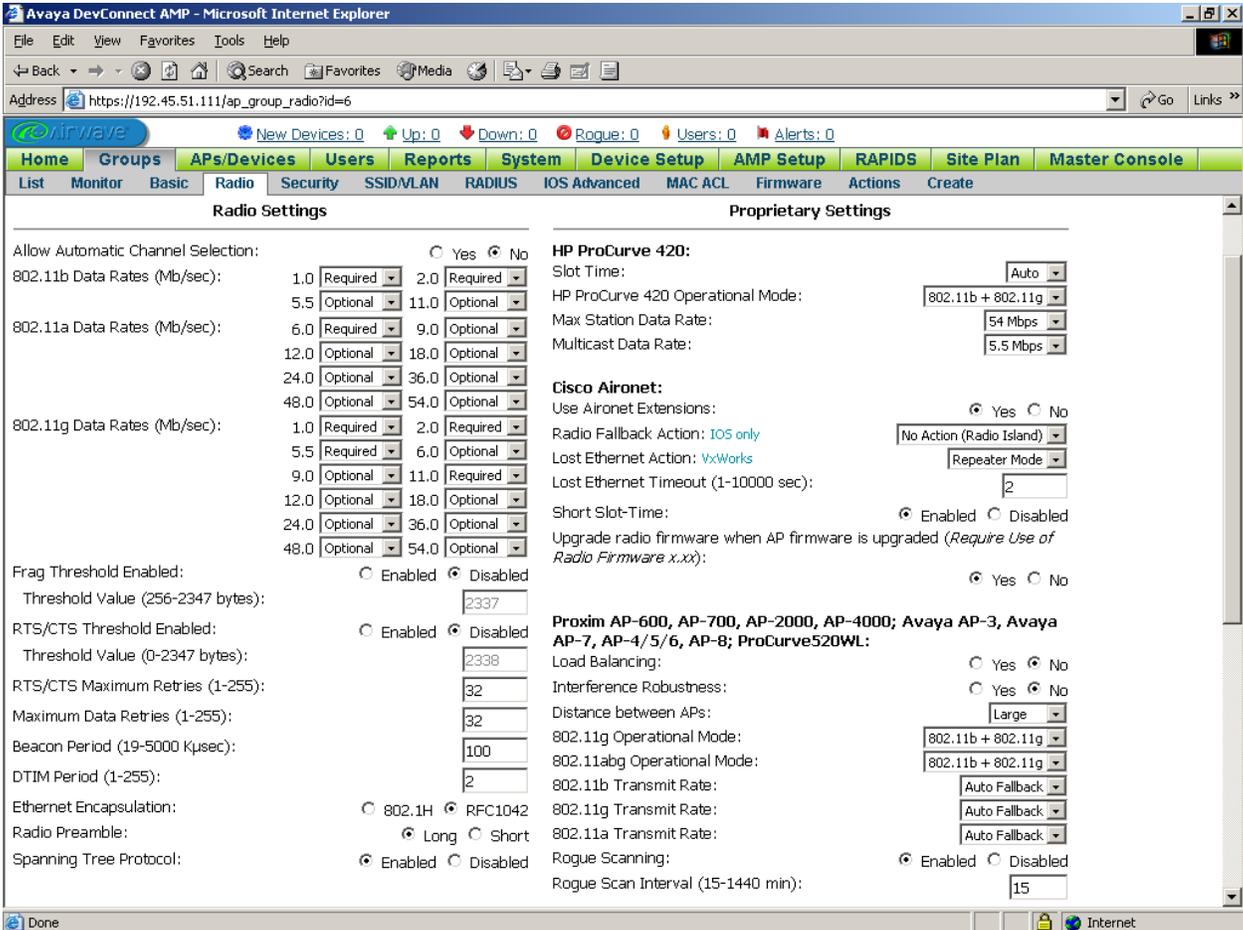
4. Configure the AirWave Wireless AirWave Management Platform (AMP)

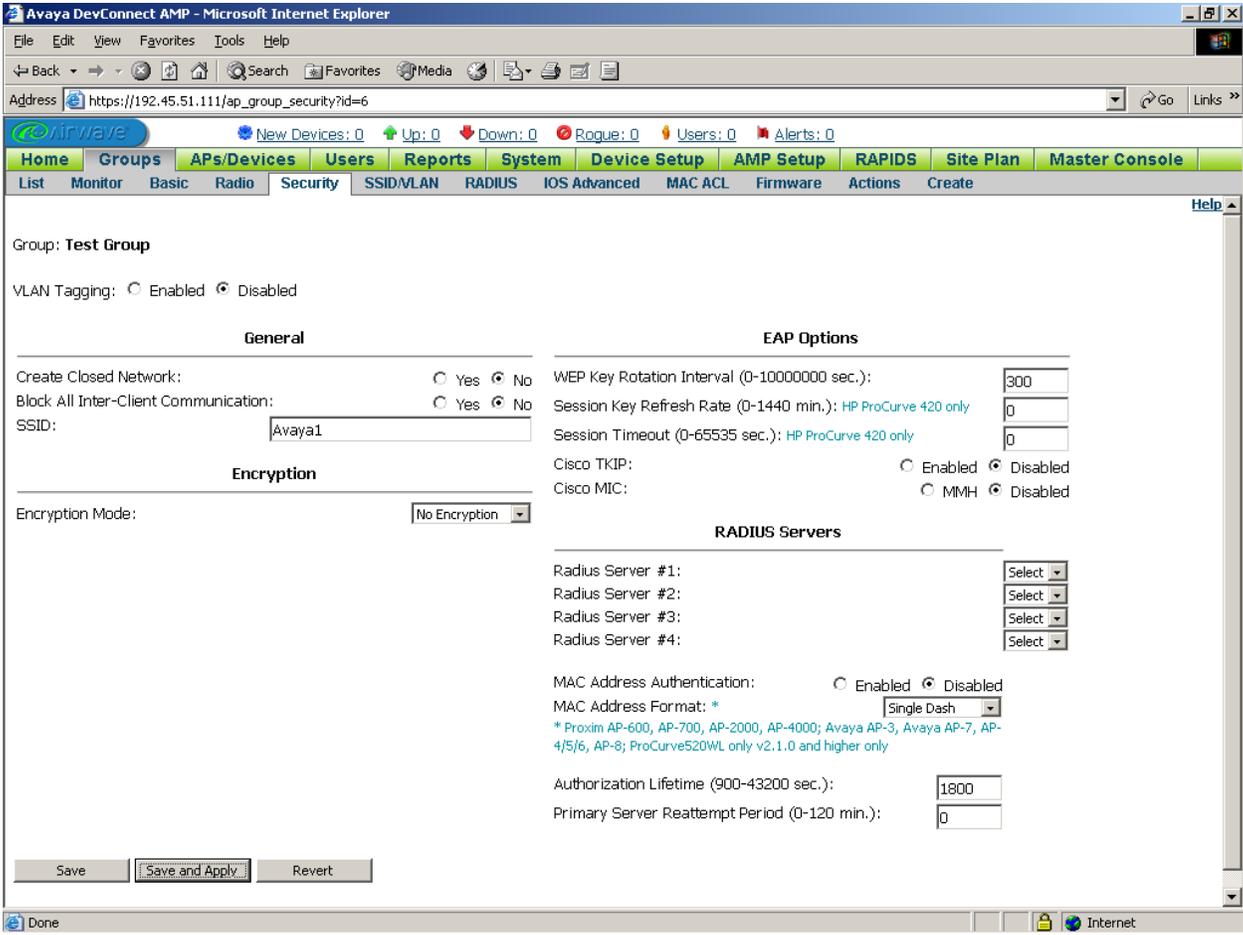
This section describes the steps for configuring the AirWave Management Platform (AMP) application. It assumes that AMP has already been installed on a Linux server.

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> 

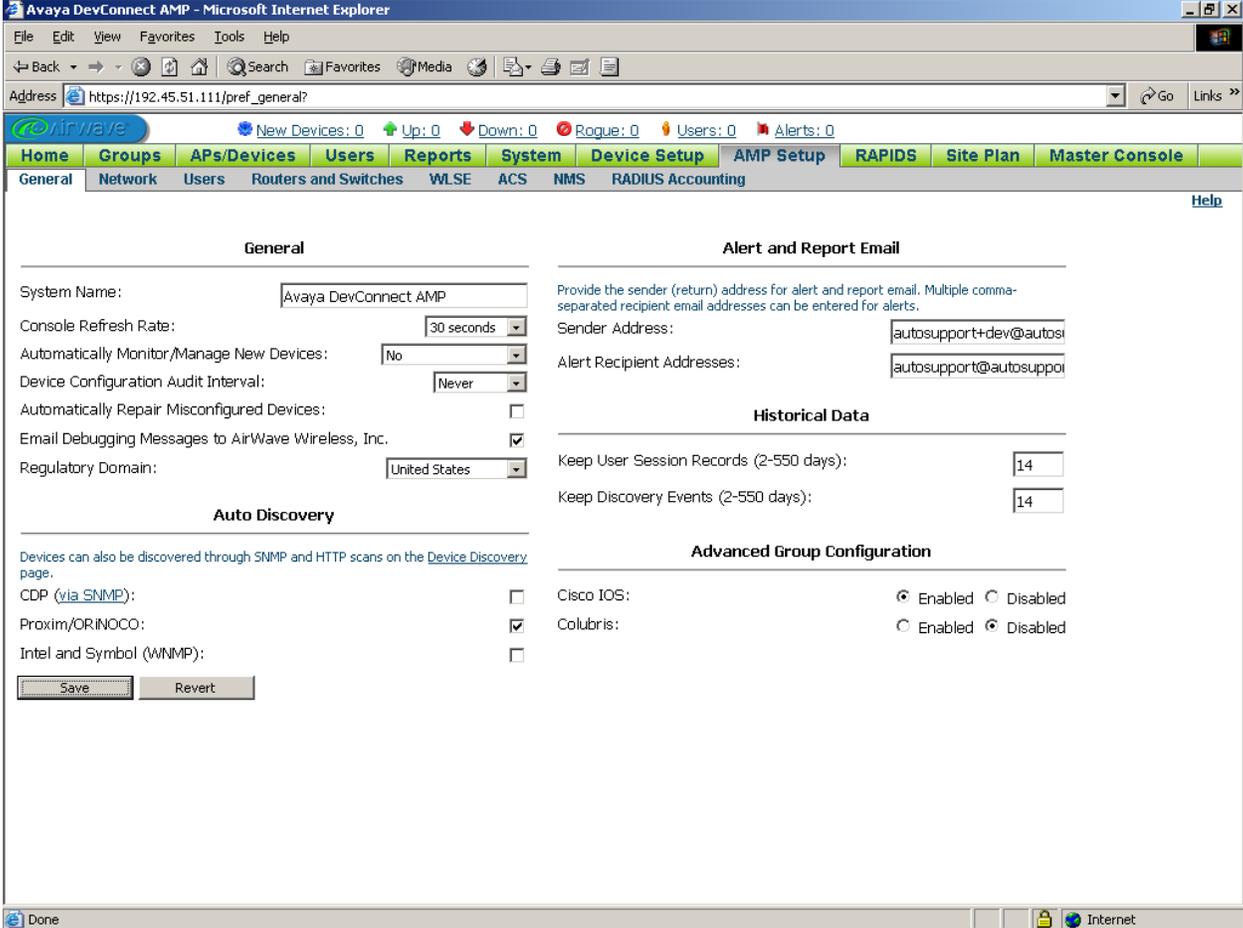
Step	Description
3.	<p>The Basic tab for the newly created Group is invoked. The default settings may be used.</p> <p>Optional: To have AMP automatically assign static IP addresses to Avaya APs that obtained IP addresses via DHCP, set Assign Static IP addresses to Devices to “Yes” and configure an IP address pool as depicted below. Click on “Save”.</p> 

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>  <p>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_radio?id=6'. The interface has a navigation menu with tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The 'Radio' tab is selected, showing 'Radio Settings' and 'Proprietary Settings' sections.</p> <p>Radio Settings:</p> <ul style="list-style-type: none"> Allow Automatic Channel Selection: <input type="radio"/> Yes <input checked="" type="radio"/> No 802.11b Data Rates (Mb/sec): 1.0 Required, 2.0 Required, 5.5 Optional, 11.0 Optional, 6.0 Required, 9.0 Optional, 12.0 Optional, 18.0 Optional, 24.0 Optional, 36.0 Optional, 48.0 Optional, 54.0 Optional 802.11a Data Rates (Mb/sec): 1.0 Required, 2.0 Required, 5.5 Required, 6.0 Optional, 9.0 Optional, 11.0 Required, 12.0 Optional, 18.0 Optional, 24.0 Optional, 36.0 Optional, 48.0 Optional, 54.0 Optional 802.11g Data Rates (Mb/sec): 1.0 Required, 2.0 Required, 5.5 Required, 6.0 Optional, 9.0 Optional, 11.0 Required, 12.0 Optional, 18.0 Optional, 24.0 Optional, 36.0 Optional, 48.0 Optional, 54.0 Optional Frag Threshold Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Threshold Value (256-2347 bytes): 2337 RTS/CTS Threshold Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Threshold Value (0-2347 bytes): 2338 RTS/CTS Maximum Retries (1-255): 32 Maximum Data Retries (1-255): 32 Beacon Period (19-5000 Kµsec): 100 DTIM Period (1-255): 2 Ethernet Encapsulation: <input type="radio"/> 802.1H <input checked="" type="radio"/> RFC1042 Radio Preamble: <input checked="" type="radio"/> Long <input type="radio"/> Short Spanning Tree Protocol: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <p>Proprietary Settings:</p> <ul style="list-style-type: none"> HP ProCurve 420: <ul style="list-style-type: none"> Slot Time: Auto HP ProCurve 420 Operational Mode: 802.11b + 802.11g Max Station Data Rate: 54 Mbps Multicast Data Rate: 5.5 Mbps Cisco Aironet: <ul style="list-style-type: none"> Use Aironet Extensions: <input checked="" type="radio"/> Yes <input type="radio"/> No Radio Fallback Action: IOS only No Action (Radio Island) Lost Ethernet Action: VxWorks Repeater Mode Lost Ethernet Timeout (1-10000 sec): 2 Short Slot-Time: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Upgrade radio firmware when AP firmware is upgraded (Require Use of Radio Firmware x.xx): <input checked="" type="radio"/> Yes <input type="radio"/> No Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL: <ul style="list-style-type: none"> Load Balancing: <input type="radio"/> Yes <input checked="" type="radio"/> No Interference Robustness: <input type="radio"/> Yes <input checked="" type="radio"/> No Distance between APs: Large 802.11g Operational Mode: 802.11b + 802.11g 802.11abg Operational Mode: 802.11b + 802.11g 802.11b Transmit Rate: Auto Fallback 802.11g Transmit Rate: Auto Fallback 802.11a Transmit Rate: Auto Fallback Rogue Scanning: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Rogue Scan Interval (15-1440 min): 15

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 shows 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 includes a navigation menu with tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The 'Security' tab is selected, and the 'SSID/VLAN' sub-tab is active. The configuration page is for a group named 'Test Group'. It features several sections: 'General' with options for 'Create Closed Network' and 'Block All Inter-Client Communication' (both set to 'No'), and a text field for 'SSID' containing 'Avaya1'. 'EAP Options' includes 'WEP Key Rotation Interval' (300), 'Session Key Refresh Rate' (0), and 'Session Timeout' (0). 'Encryption' shows 'Encryption Mode' set to 'No Encryption'. 'RADIUS Servers' has four 'Select' buttons for RADIUS Server #1 through #4. 'MAC Address Authentication' is set to 'Disabled' with a 'Single Dash' format. 'Authorization Lifetime' is 1800 and 'Primary Server Reattempt Period' is 0. 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.

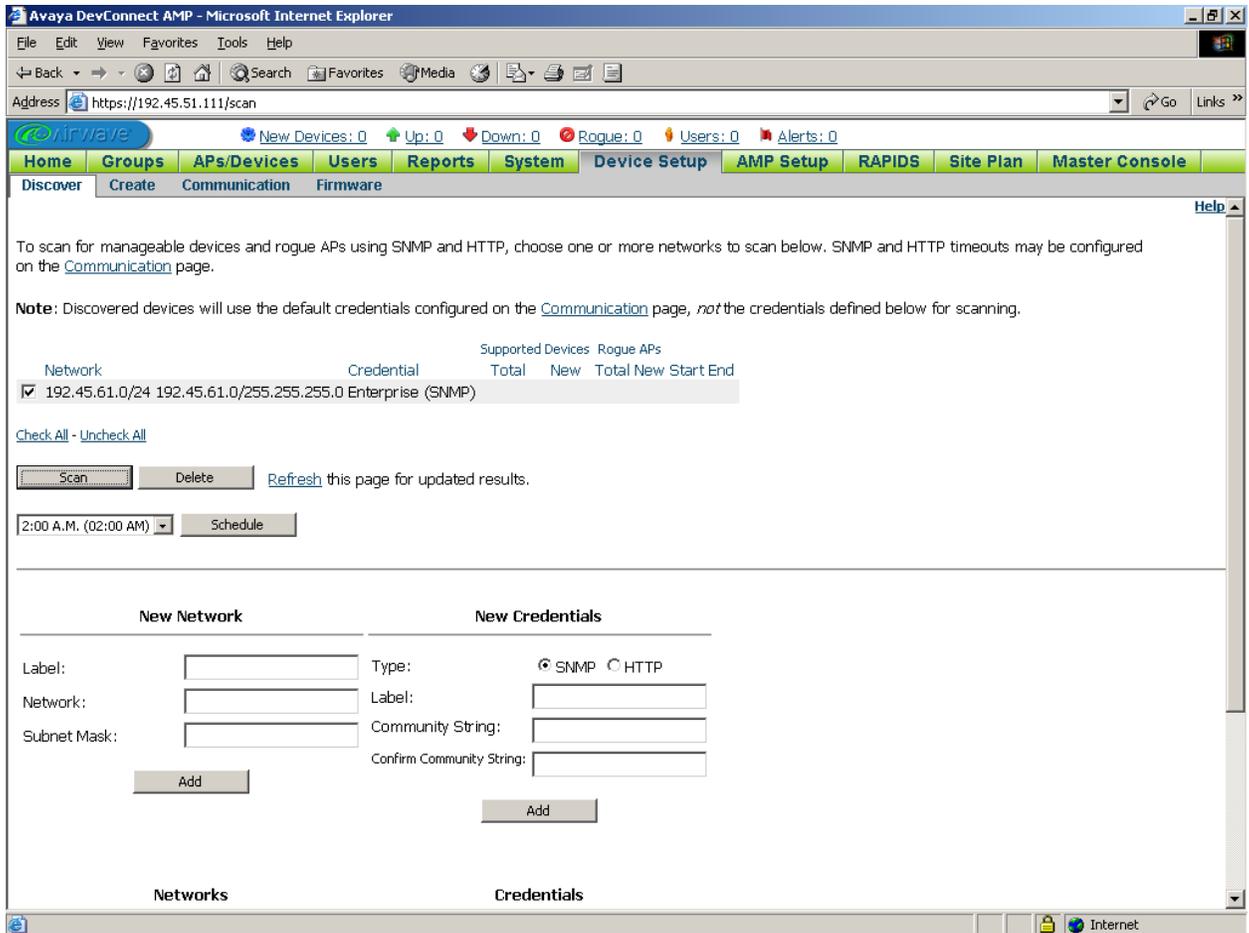
Step	Description
1.	<p>In the AMP web interface, click on the “AMP Setup” tab and then the “General” tab. Check the Proxim/OriNOCO checkbox and click on “Save”. This allows AMP to automatically discover Avaya APs on its local subnet.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows 'https://192.45.51.111/pref_general?'. The page title is 'Avaya DevConnect AMP - Microsoft Internet Explorer'. The navigation menu includes 'Home', 'Groups', 'APs/Devices', 'Users', 'Reports', 'System', 'Device Setup', 'AMP Setup', 'RAPIDS', 'Site Plan', and 'Master Console'. The 'AMP Setup' tab is selected, and the 'General' sub-tab is active. The configuration page is divided into several sections: 'General', 'Alert and Report Email', 'Historical Data', 'Auto Discovery', and 'Advanced Group Configuration'. In the 'Auto Discovery' section, the 'Proxim/ORINOCO' checkbox is checked, while 'CDP (via SNMP)' and 'Intel and Symbol (WNMP)' are unchecked. The 'Save' button is highlighted in red, and the 'Revert' button is also visible. The status bar at the bottom shows 'Done' and 'Internet'.</p>

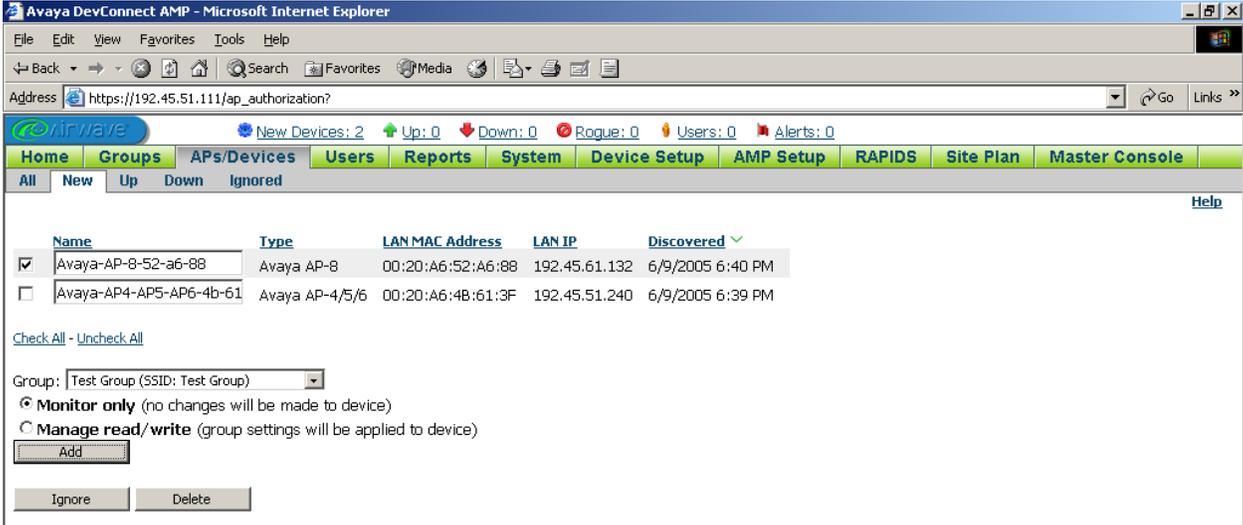
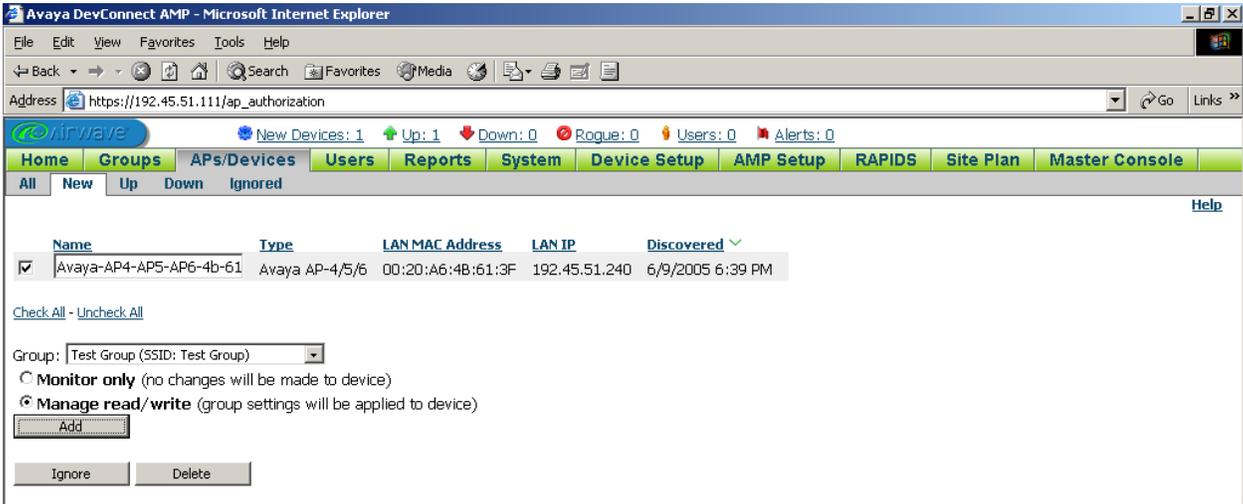
Step	Description								
2.	<p>Click on the “Device Setup” tab and then the “Discover” tab. In the New Network section, for each subnet that contains one or more Avaya APs, enter its Network address and Subnet Mask, assign a Label, and click on “Add”.</p> <div data-bbox="727 380 1073 569" style="text-align: center;"> <p>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><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="727 764 1073 982" style="text-align: center;"> <p>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><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="548 1234 1247 1472" style="text-align: center;"> <table border="0"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Networks</th> <th style="text-align: left; 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="vertical-align: bottom;"> Check All - Uncheck All </td> <td style="vertical-align: bottom;"> Check All - Uncheck All </td> </tr> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="Define Scan"/> <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

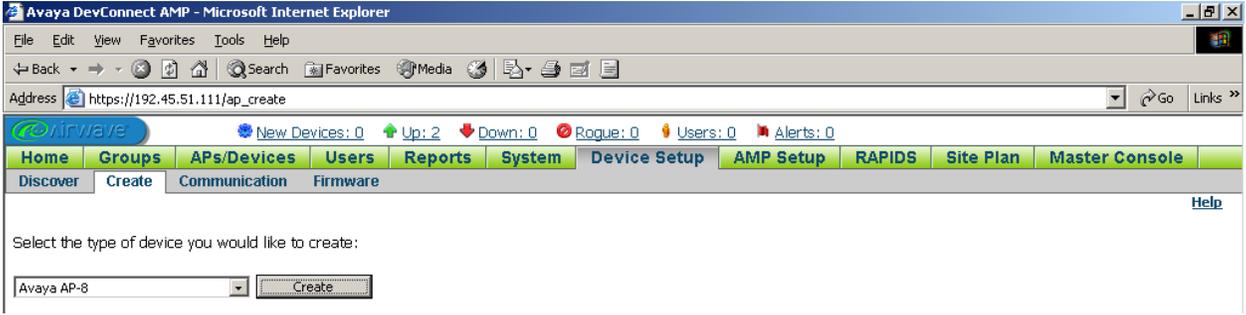
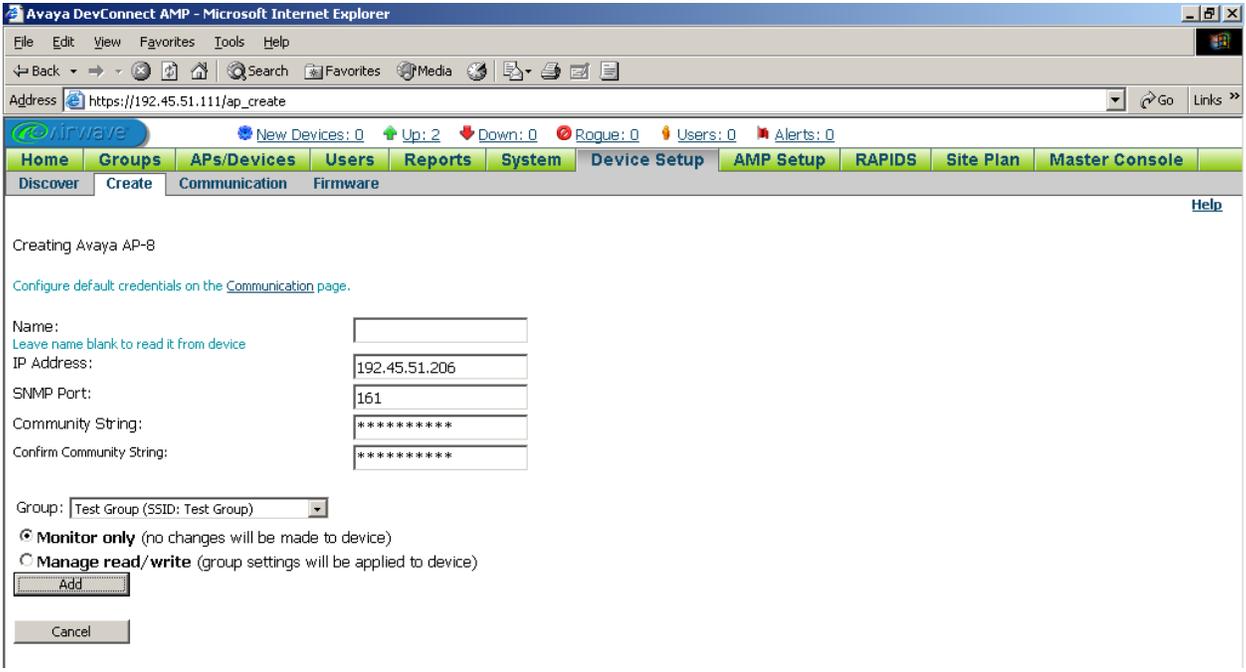
- 5. Scroll up to the top of the window. Check the checkboxes of the Network/Credential combinations to scan and click on “Scan”. The scan may take several seconds; click on “Refresh” to show the scan’s progress until completion.



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>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows https://192.45.51.111/ap_authorization?. The navigation menu includes Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The 'APs/Devices' section is active, showing a table of discovered devices:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>LAN MAC Address</th> <th>LAN IP</th> <th>Discovered</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Avaya-AP-8-52-a6-88</td> <td>Avaya AP-8</td> <td>00:20:A6:52:A6:88</td> <td>192.45.61.132</td> <td>6/9/2005 6:40 PM</td> </tr> <tr> <td><input type="checkbox"/> Avaya-AP4-AP5-AP6-4b-61</td> <td>Avaya AP-4/5/6</td> <td>00:20:A6:4B:61:3F</td> <td>192.45.51.240</td> <td>6/9/2005 6:39 PM</td> </tr> </tbody> </table> <p>Below the table, there are controls for selecting a group (Test Group (SSID: Test Group)), radio buttons for 'Monitor only' (selected) and 'Manage read/write', and an 'Add' button. There are also 'Ignore' and 'Delete' buttons.</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>  <p>The second screenshot shows the same Avaya DevConnect AMP web interface. In this view, the 'Manage read/write' radio button is selected, indicating that group settings will be applied to the devices. The 'Add' button is visible, and the 'Monitor only' option is now unselected.</p>	Name	Type	LAN MAC Address	LAN IP	Discovered	<input checked="" type="checkbox"/> Avaya-AP-8-52-a6-88	Avaya AP-8	00:20:A6:52:A6:88	192.45.61.132	6/9/2005 6:40 PM	<input type="checkbox"/> Avaya-AP4-AP5-AP6-4b-61	Avaya AP-4/5/6	00:20:A6:4B:61:3F	192.45.51.240	6/9/2005 6:39 PM
Name	Type	LAN MAC Address	LAN IP	Discovered												
<input checked="" type="checkbox"/> Avaya-AP-8-52-a6-88	Avaya AP-8	00:20:A6:52:A6:88	192.45.61.132	6/9/2005 6:40 PM												
<input type="checkbox"/> Avaya-AP4-AP5-AP6-4b-61	Avaya AP-4/5/6	00:20:A6:4B:61:3F	192.45.51.240	6/9/2005 6:39 PM												

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**.

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_manage?id=2`. The interface features a navigation menu with tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Below the navigation menu, there are sub-tabs for All, Monitor, Manage, Detail, New, Up, Down, and Ignored. The main content area is divided into three sections: General, Settings, and Device Communication.

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: Avaya-AP4-AP5-AP6-4b-61-3f
Location: System Location
Contact: Contact Name
Group: Test Group (SSID: Avaya1)
802.11abg ('bg' mode) Radio
Transmit Power: 100%
Channel: 11
Neighboring APs: No neighbors have been discovered yet.
DHCP: Yes No
LAN IP: 192.45.51.240
Subnet Mask: 255.255.255.0
Gateway: 192.45.51.1

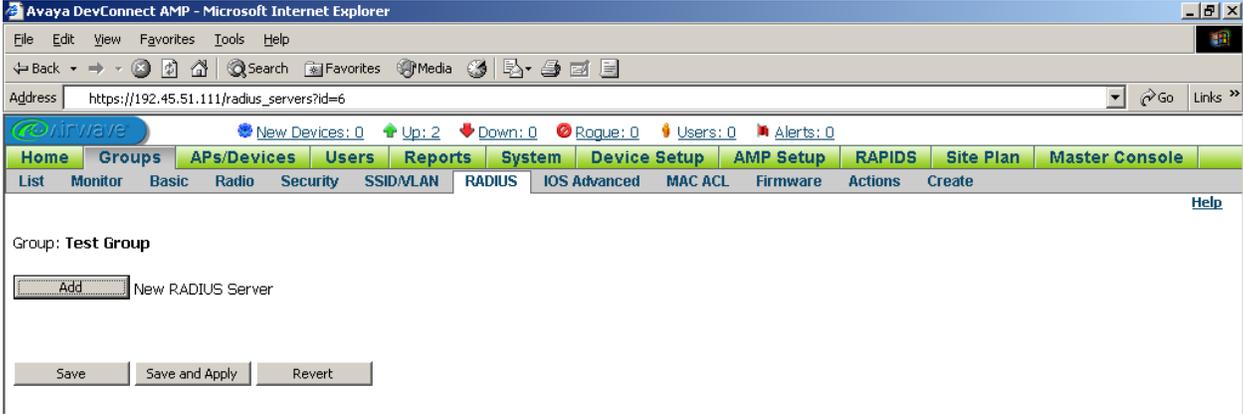
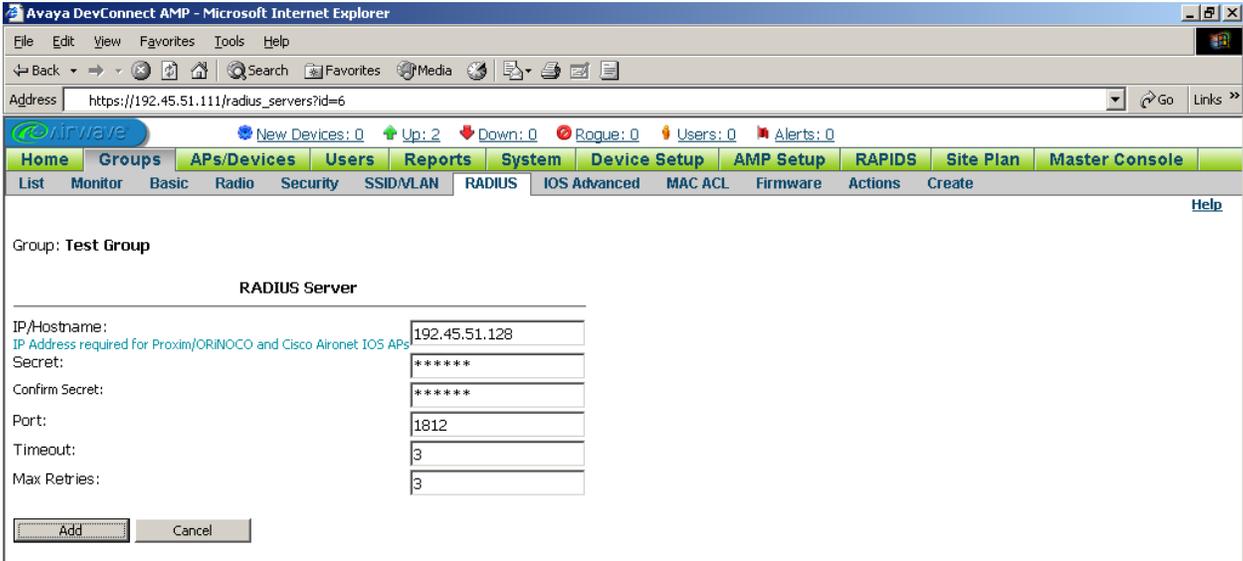
Device Communication

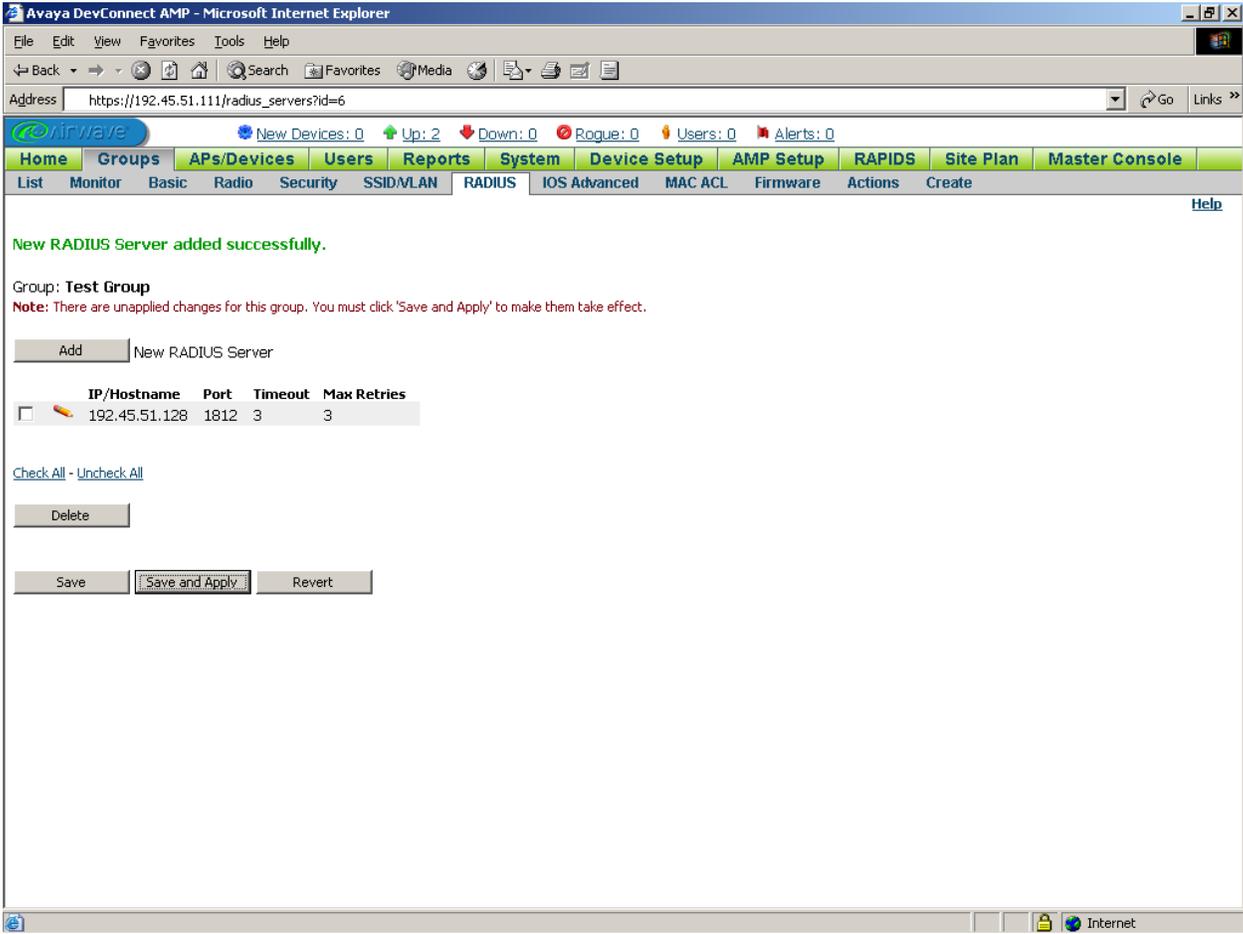
[View Device Credentials](#)
If this device is down because its IP address or management ports have changed, update the fields below with the correct information.
IP Address: 192.45.51.240
SNMP Port: 161
If this device is down because the credentials on the device have changed, update the fields below with the correct information.
Community String: *****
Confirm Community String: *****

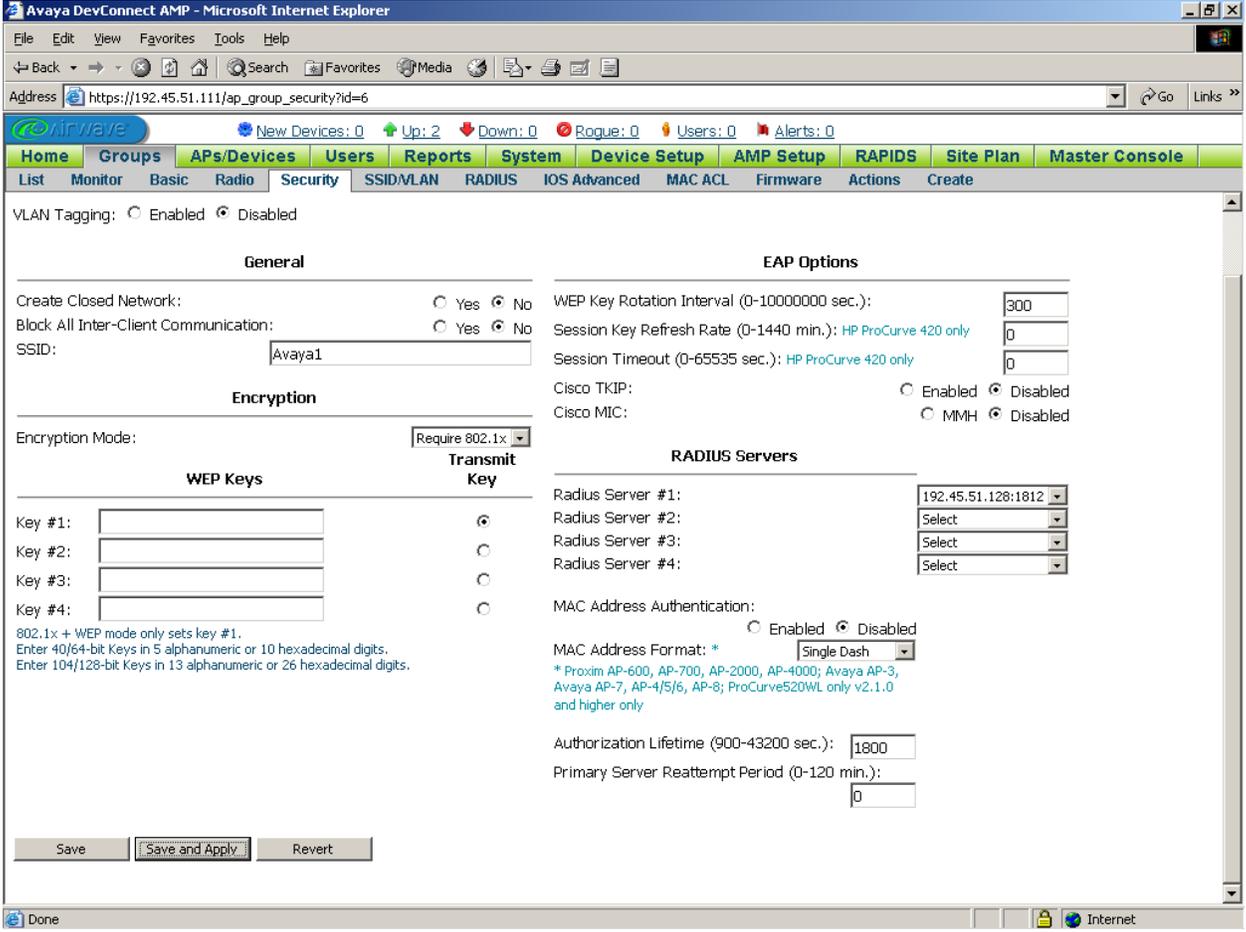
Buttons: Save and Apply, Revert, Delete, Update Firmware, Reboot

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
<p>1.</p>	<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 navigation menu includes Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The RADIUS tab is selected. The page title is 'Group: Test Group'. Below the title, there is an 'Add' button and the text 'New RADIUS Server'. At the bottom, there are buttons for 'Save', 'Save and Apply', and 'Revert'.</p>
<p>2.</p>	<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 navigation menu includes Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The RADIUS tab is selected. The page title is 'Group: Test Group'. Below the title, there is a 'RADIUS Server' section with a form. The form fields are: IP/Hostname: 192.45.51.128, Secret: ***** (with a note: IP Address required for Proxim/ORINOCO and Cisco Aironet IOS APs), Confirm Secret: *****, Port: 1812, Timeout: 3, and Max Retries: 3. At the bottom, there are buttons for 'Add' and 'Cancel'.</p>
<p>3.</p>	<p>Repeat steps 1-2 to enter information about additional RADIUS servers to be used by Avaya APs in the Group.</p>

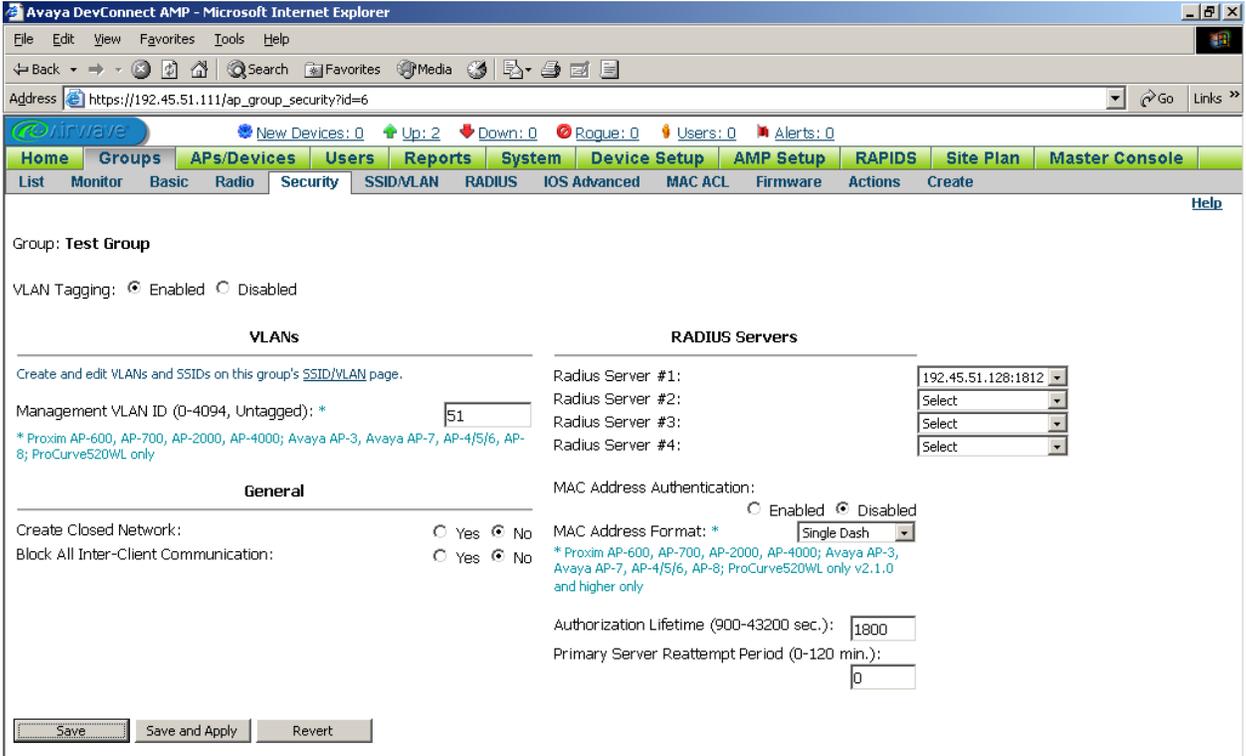
Step	Description								
4.	<p>Click on “Save and Apply” when finished, and confirm the changes when prompted.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar displays <code>https://192.45.51.111/radius_servers?id=6</code>. The navigation menu includes tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. A status bar at the top indicates: New Devices: 0, Up: 2, Down: 0, Rogue: 0, Users: 0, Alerts: 0. A green message states: "New RADIUS Server added successfully." Below this, the group is identified as "Test Group" with a note: "Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect." A table lists the added RADIUS server:</p> <table border="1"> <thead> <tr> <th>IP/Hostname</th> <th>Port</th> <th>Timeout</th> <th>Max Retries</th> </tr> </thead> <tbody> <tr> <td>192.45.51.128</td> <td>1812</td> <td>3</td> <td>3</td> </tr> </tbody> </table> <p>Buttons for "Save and Apply", "Save", and "Revert" are visible at the bottom of the interface.</p>	IP/Hostname	Port	Timeout	Max Retries	192.45.51.128	1812	3	3
IP/Hostname	Port	Timeout	Max Retries						
192.45.51.128	1812	3	3						

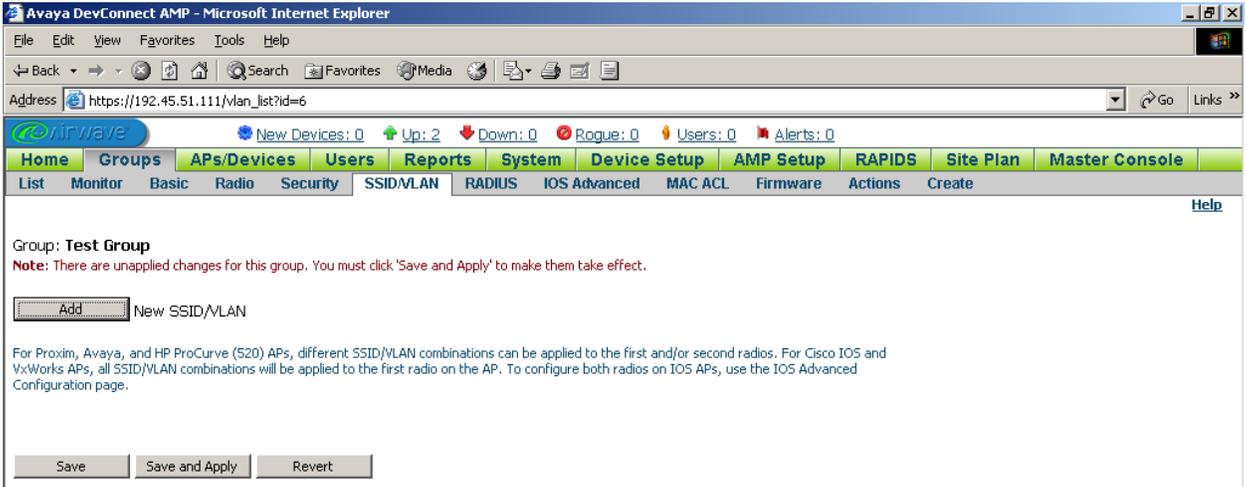
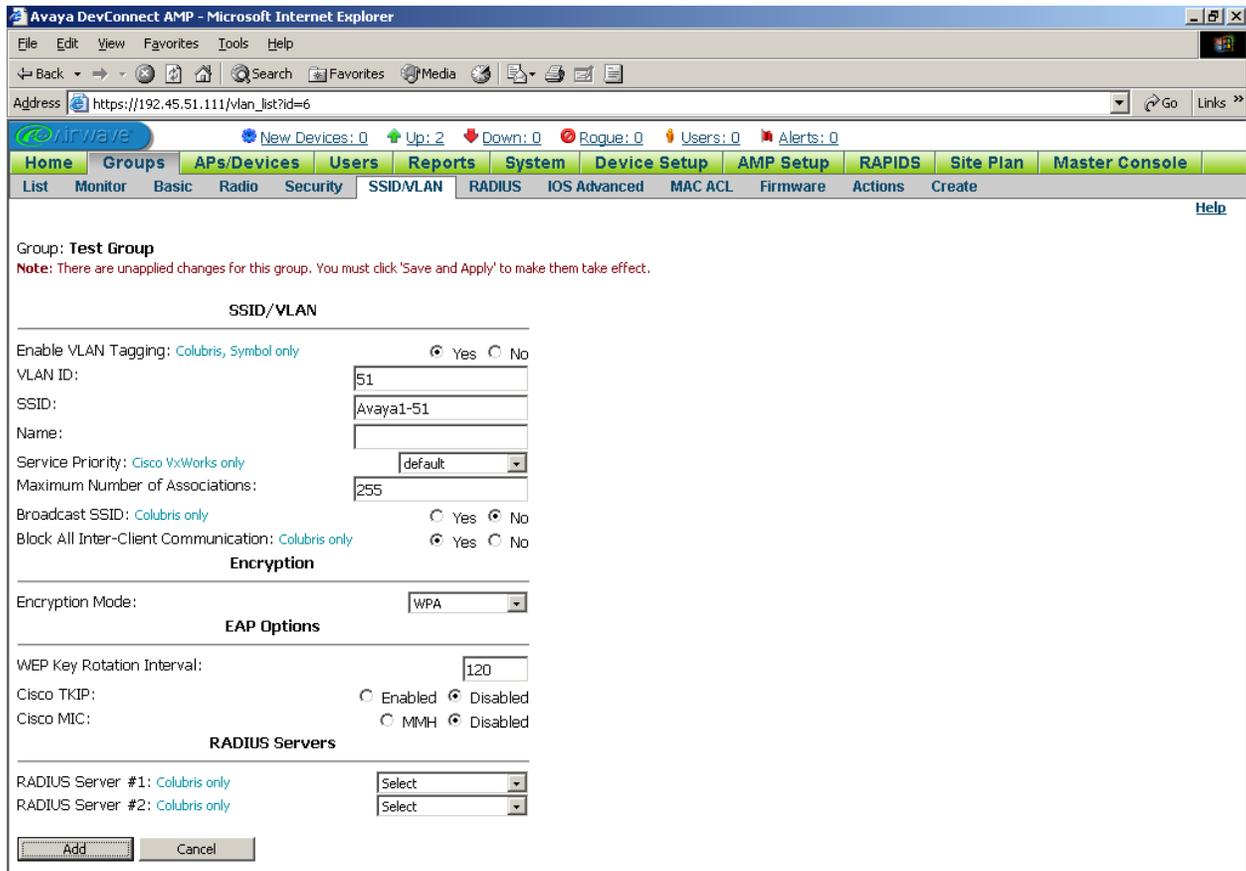
Step	Description
5.	<p>Click on the Security tab, and set the Encryption Mode to one of the encryption/authentication options from the pull-down list.</p> <p>For encryption/authentication options that use WEP, enter the WEP Keys and select one as a Transmit Key. In the example below, however, WEP Keys 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>
	 <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 navigation menu with tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. The 'Security' tab is selected, and the 'SSID/MLAN' sub-tab is active. The main content area is divided into several sections: <ul style="list-style-type: none"> General: Includes options for 'Create Closed Network' (Yes/No), 'Block All Inter-Client Communication' (Yes/No), and an 'SSID' field containing 'Avaya1'. Encryption: The 'Encryption Mode' is set to 'Require 802.1x'. Below this are 'WEP Keys' (Key #1-4) and a 'Transmit Key' selection (radio buttons). EAP Options: Includes 'WEP Key Rotation Interval' (300), 'Session Key Refresh Rate' (0), 'Session Timeout' (0), and radio buttons for 'Cisco TKIP' (Disabled) and 'Cisco MIC' (Disabled). RADIUS Servers: Lists 'Radius Server #1' through #4. 'Radius Server #1' is set to '192.45.51.128:1812', while others are set to 'Select'. It also includes 'MAC Address Authentication' (Disabled) and 'MAC Address Format' (Single Dash). At the bottom, there are 'Save', 'Save and Apply', and 'Revert' buttons. The status bar at the bottom of the browser shows 'Done' and 'Internet'.</p>

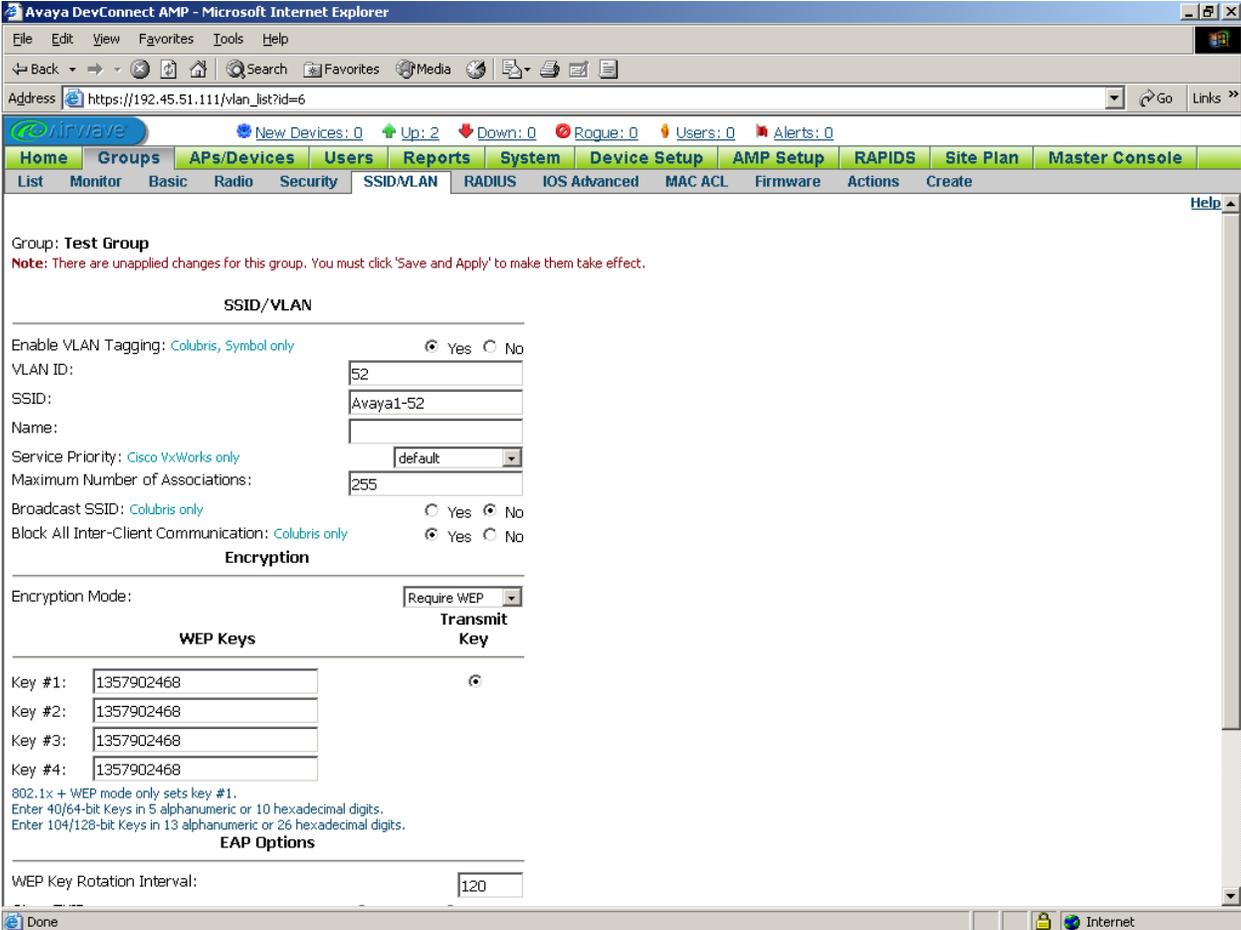
4.6. Multiple VLANs

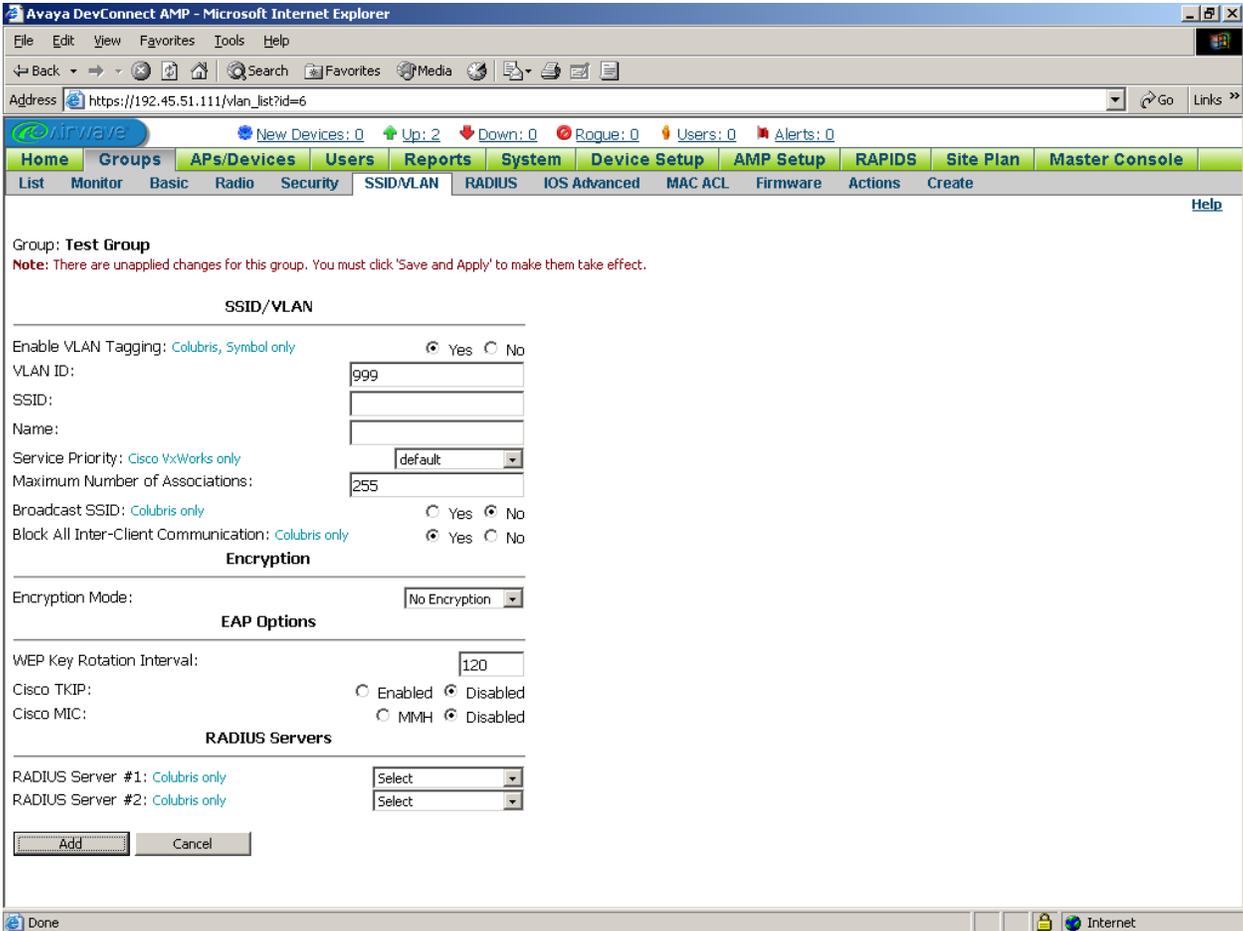
Avaya APs support multiple VLANs on each wireless interface with the following requirements:

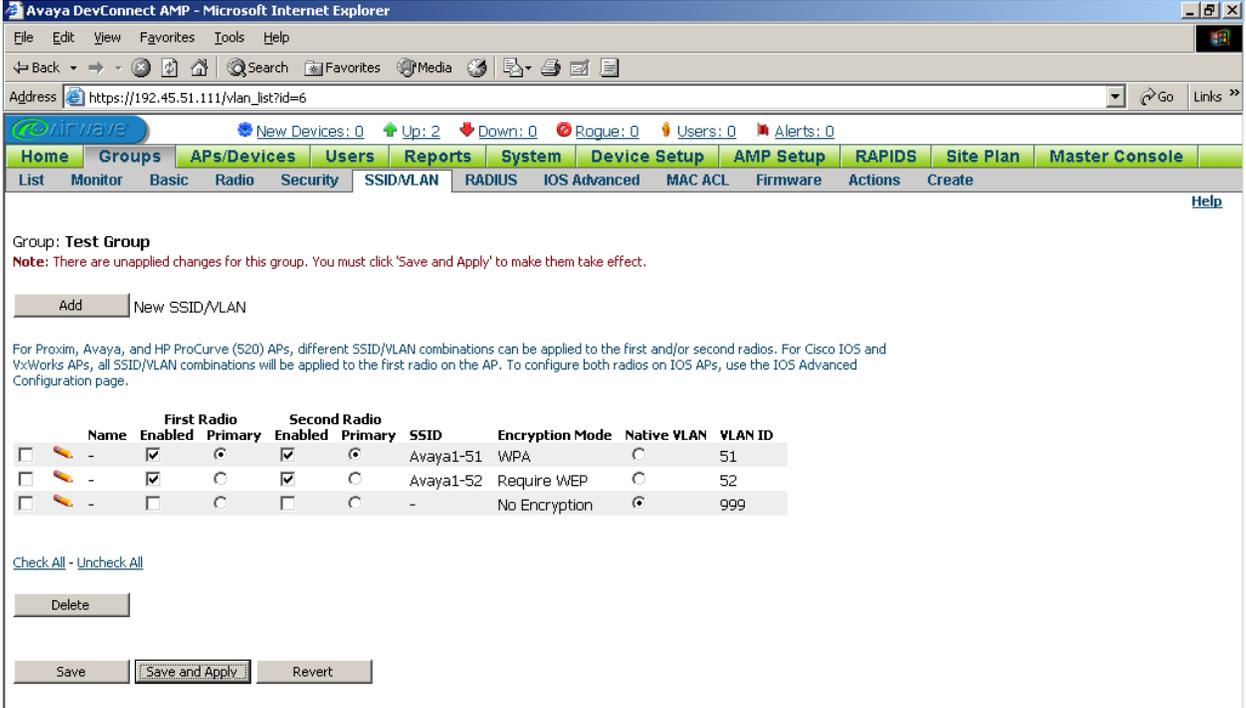
1. The Ethernet switch port to which the AP is connected must tag all VLANs. For example, on the Avaya C364T-PWR in **Figure 1**, the port trunking mode must be set to “dot1q”.
2. All VLANs on the wireless interfaces must be tagged.

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>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows https://192.45.51.111/vlan_list?id=6. The navigation menu includes 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, there is a 'Group: Test Group' section with a note: 'Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.' An 'Add' button is highlighted, followed by the text 'New SSID/VLAN'. Below this, there is explanatory text for Proxim, Avaya, and HP ProCurve (520) APs, and buttons for 'Save', 'Save and Apply', and 'Revert'.</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>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The address bar shows https://192.45.51.111/vlan_list?id=6. The navigation menu is the same as in the previous screenshot. The 'SSID/VLAN' tab is selected. Below the navigation, there is a 'Group: Test Group' section with 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 fields and options:</p> <ul style="list-style-type: none"> Enable VLAN Tagging: Colubris, Symbol only <input checked="" type="radio"/> Yes <input type="radio"/> No VLAN ID: <input type="text" value="51"/> SSID: <input type="text" value="Avaya1-51"/> Name: <input type="text"/> Service Priority: Cisco VxWorks only <input type="text" value="default"/> Maximum Number of Associations: <input type="text" value="255"/> Broadcast SSID: Colubris only <input type="radio"/> Yes <input checked="" type="radio"/> No Block All Inter-Client Communication: Colubris only <input checked="" type="radio"/> Yes <input type="radio"/> No Encryption Mode: <input type="text" value="WPA"/> EAP Options: <ul style="list-style-type: none"> WEP Key Rotation Interval: <input type="text" value="120"/> Cisco TKIP: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Cisco MIC: <input type="radio"/> MMH <input checked="" type="radio"/> Disabled RADIUS Servers: <ul style="list-style-type: none"> RADIUS Server #1: Colubris only <input type="text" value="Select"/> RADIUS Server #2: Colubris only <input type="text" value="Select"/> <p>At the bottom of the form, there are 'Add' and 'Cancel' buttons.</p>

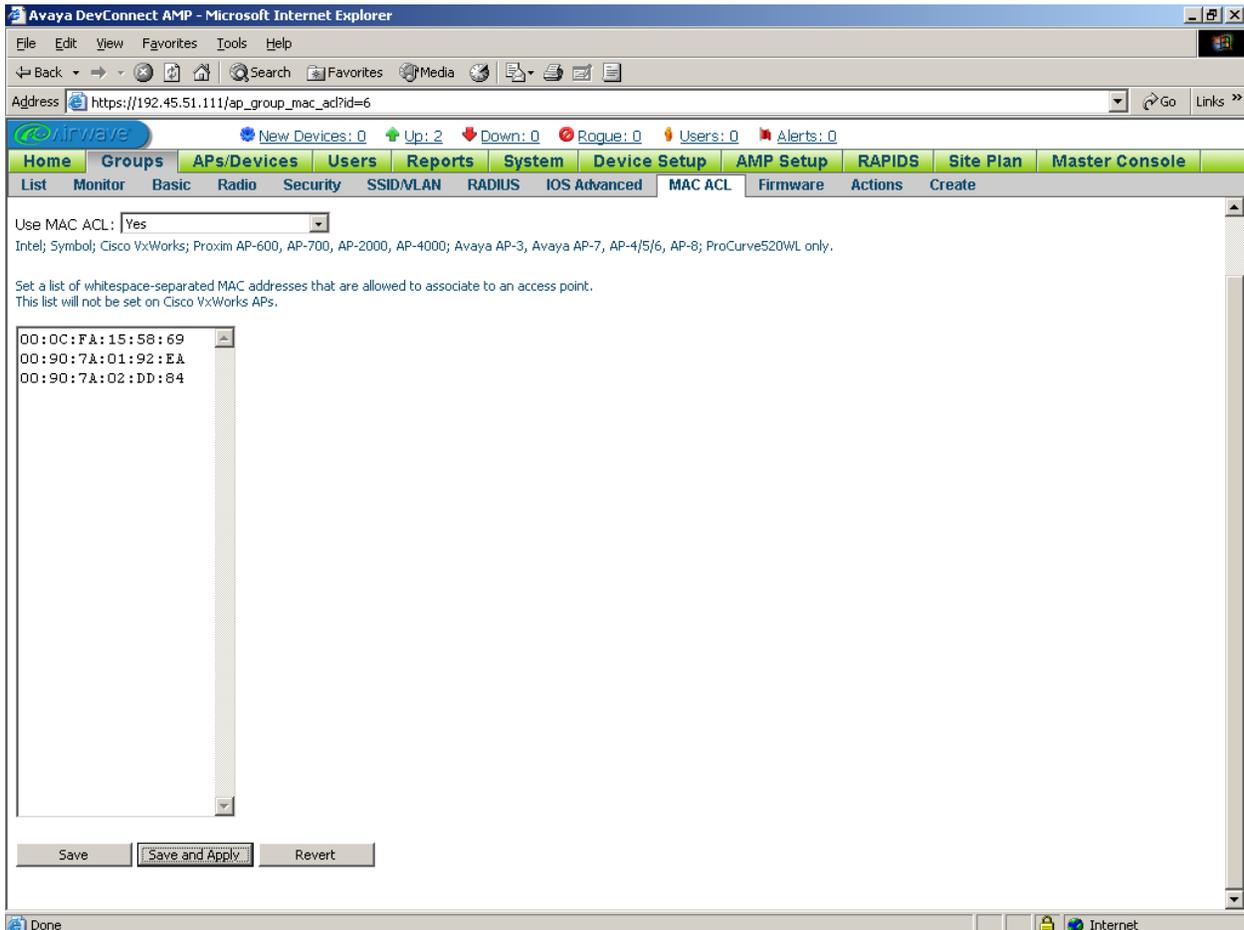
Step	Description
4.	<p>Repeat Step 3 as necessary to add additional VLANs. The example below shows the configuration of VLAN 52 for the Avaya 3616 and 3626 Wireless IP Telephones in Figure 1.</p>  <p>The screenshot shows the Avaya DevConnect AMP web interface in Microsoft Internet Explorer. The browser address bar shows <code>https://192.45.51.111/Vlan_list?id=6</code>. The interface has a navigation menu with tabs for Home, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, Site Plan, and Master Console. Under the APs/Devices tab, there are sub-tabs for 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 configuration is for the "SSID/VLAN" section. It includes fields for "Enable VLAN Tagging" (set to Yes), "VLAN ID" (52), "SSID" (Avaya1-52), "Name", "Service Priority" (default), "Maximum Number of Associations" (255), "Broadcast SSID" (No), and "Block All Inter-Client Communication" (Yes). The "Encryption" section is set to "Require WEP". The "WEP Keys" section shows four keys, all set to "1357902468". The "EAP Options" section shows "WEP Key Rotation Interval" set to "120".</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> 

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>Group: Test Group Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.</p> <p>Add <input type="button" value="New SSID/VLAN"/></p> <p>For Proxim, Avaya, and HP ProCurve (520) APs, different SSID/VLAN combinations can be applied to the first and/or second radios. For Cisco IOS and VxWorks APs, all SSID/VLAN combinations will be applied to the first radio on the AP. To configure both radios on IOS APs, use the IOS Advanced Configuration page.</p> <table border="1"> <thead> <tr> <th rowspan="2"></th> <th rowspan="2">Name</th> <th colspan="2">First Radio</th> <th colspan="2">Second Radio</th> <th rowspan="2">SSID</th> <th rowspan="2">Encryption Mode</th> <th rowspan="2">Native VLAN</th> <th rowspan="2">VLAN ID</th> </tr> <tr> <th>Enabled</th> <th>Primary</th> <th>Enabled</th> <th>Primary</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>-</td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td>Avaya1-51</td> <td>WPA</td> <td><input type="radio"/></td> <td>51</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> <td>Avaya1-52</td> <td>Require WEP</td> <td><input type="radio"/></td> <td>52</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> <td>-</td> <td>No Encryption</td> <td><input checked="" type="radio"/></td> <td>999</td> </tr> </tbody> </table> <p>Check All - Uncheck All</p> <p><input type="button" value="Delete"/></p> <p><input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Revert"/></p>		Name	First Radio		Second Radio		SSID	Encryption Mode	Native VLAN	VLAN ID	Enabled	Primary	Enabled	Primary	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	Avaya1-51	WPA	<input type="radio"/>	51	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	Avaya1-52	Require WEP	<input type="radio"/>	52	<input type="checkbox"/>	-	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="radio"/>	-	No Encryption	<input checked="" type="radio"/>	999
	Name			First Radio		Second Radio						SSID	Encryption Mode	Native VLAN	VLAN ID																														
		Enabled	Primary	Enabled	Primary																																								
<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	Avaya1-51	WPA	<input type="radio"/>	51																																				
<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	Avaya1-52	Require WEP	<input type="radio"/>	52																																				
<input type="checkbox"/>	-	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="radio"/>	-	No Encryption	<input checked="" type="radio"/>	999																																				

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**”.



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.