

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 Developer*Connection* 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.

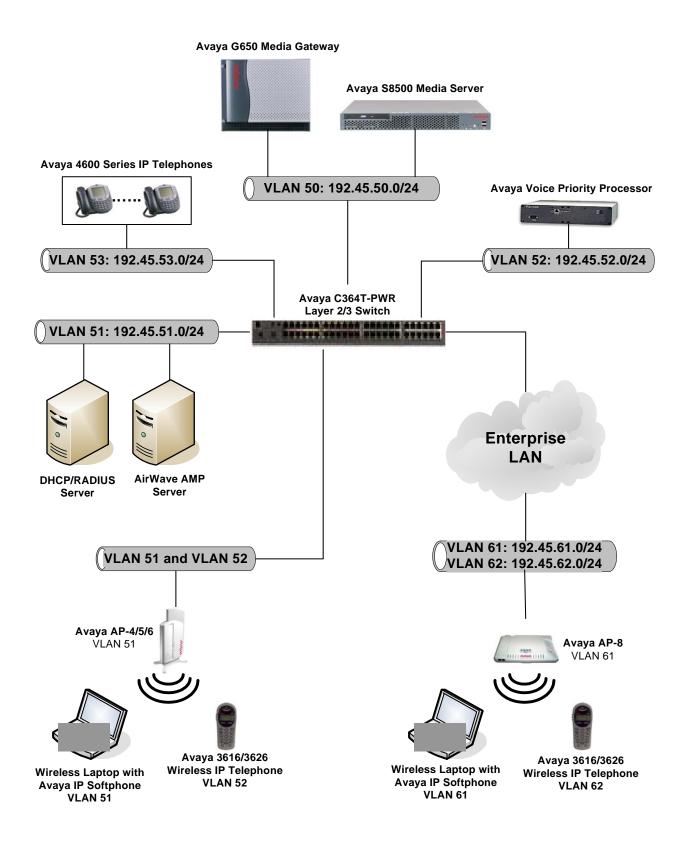


Figure 1: Sample configuration.

Solution & Interoperability Test Lab Application Notes ©2005 Avaya Inc. All Rights Reserved.

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	4.3.12
Switch	
AirWave Wireless AirWave Management	3.3.1
Platform (AMP)	
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		De	escription		
1.	Open a web browse credentials.	er and enter the AP's IP a	ddress in the URL.	Log in with the appropria	ite
2.				e the SNMP Read Comm ccessary, and click on "Ol	
	Password Configuration - Micros File Edit View Favorites Tools				
	← Back - → - 🙆 🙆 🚮 🔕	Search 🔝 Favorites 🛞 Media 🎯 🖏 🎝			
	Address 🙆 http://192.45.61.132/cfg/			÷ ا	Go Links ≫
	AVAYA				-
		Alarms Bridge System Network	QoS RADIUS Pro	ofiles SSID/VLAN/Security	
		oyotenn Hetwont	Management	ritering	
	Status	Passwords IP Access Table	Services AutoConfig	CHRD	
	Configure	This tab is used to configure SNMPv1/v2c ((CLI), and HTTP (web) passwords.	community, SNMPv3 authentication, Sl	IMPv3 privacy, Telnet	
	Monitor	Change the default passwords to a value k manage the access point and modify its co		ien users may be able to	
	Commands	Note: Changes to Password must be betwee	en 6 and 32 characters		
	Help	SNMP Read Community Password	Confirm	*****	
	Exit	SNMP Read/Write Community Password	Confirm	******	
		SNMPv3 Authentication Password	Confirm	*****	
		SNMPv3 Privacy Password	Confirm	*****	
		Telnet (CLI) Password	Confirm	******	
		HTTP (web) Password	Confirm	ХХЛАХАХ	
		ок	Cancel		
					<u> </u>
	iavascript:transmit()			Internet	h.

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.	Click on the "Groups" tab and then the "Create" tab. Specify a Name for the Group and click
	on "Create Group".
	🗿 Avaya DevConnect AMP - Microsoft Internet Explorer
	Elle Edit View Favorites Iools Help
	↓→ Back ▼ → ▼ ③ ② ③ △ ◎ ② △ ◎ ③ Favorites ③ Media ③ ◎ □ ▼ ④ □ □ □ Address ④ https://192.45.51.111/ap_group_create?
	Control (Control (Contro) (Contro) (Contro) (Control (Contro) (Contro) (Contro) (Contro)
	List Create
	Help Help
	Create Group
	Name: Test Group
	Create Group
	🙆 Done

Step		Γ	Description		
3.	The Basic tab for the newly cr	eated Group i	s invoked. The defaul	It settings may be used.	
	Optional: To have AMP auton	natically assig	n static IP addresses to	o Avava APs that obtained	IP
	addresses via DHCP, set Assig			•	
	address pool as depicted below	-		o ites and configure an in	-
	address poor as depicted below	v. Chek on a	Save.		
	🗿 Avaya DevConnect AMP - Microsoft Internet Explorer				- 8 ×
	Eile Edit View Favorites Tools Help				
	← Back → → → ③ ② ③ ④ ③ Search Favorites	🛞 Media 🎯 🖏 🎒			
	Address https://192.45.51.111/ap_group_basic?id=6			▼ @Go	Links »
		🕈 <u>Up: 2</u> 🔸 <u>Down: 0</u> 📢	🛛 Rogue: 0 🕴 Users: 0 🕨 Alerts: 0		
	Home Groups APs/Devices Users	Reports System		RAPIDS Site Plan Master Console	
	List Monitor Basic Radio Security SSI	DAVLAN RADIUS IOS	S Advanced MAC ACL Firmware	Actions Create	Help
	Group: Test Group				
	Basic		Note	s	
	Name: Te	est Group		<u> </u>	
	SNMP Polling Interval:	5 minutes 💌			
	Cisco IOS CLI Communication:	⊙ Telnet C SSH		Y	
	Cisco IOS File Communication: Allow One-to-One NAT:	TFTP C SCP	Automatic Static	(P Assignment	
	Track usernames on Cisco Aironet VxWorks APs:	C Yes ⊙ No C Yes ⊙ No	Assign Static IP addresses to Devices:	● Yes ○ No	
	Track usernames on Enterasys RoamAbout R2 APs:	C Yes ⊙ No	Start IP Address:	192.45.61.130	
	Requires <u>Radius Accounting Client</u> to be configured Intel/Symbol Client Inactivity Timeout (3-600 min):	3	Number of Addresses:	10	
	HTTP Server Port: (Proxim only)	80	Subnet Mask:	255,255,255.0	
		00	Gateway:	192.45.61.1	
			Next IP address:		
	Save and Apply Revert				
	(A) Data				
	Cone Cone Cone Cone Cone Cone Cone Cone			🗎 😫 👹 Internet	

)			Description	
	Click on the "Radio'	' tab. Specify Radio	Settings and Avaya AP	settings according to custom
		1 i	down to the bottom of th	6
	requirements, and en	ek on bave (scion	down to the bottom of h	ie window).
	Note: Some AMP de	fault settings, such as	Allow Automatic Cha	nnel Selection, DTIM Perio
	Load Balancing, Int	erference Robustne	ss, Rogue Scanning, an	d Rogue Scan Interval may
	be different from the	equivalent default se	ttings in the Avava AP.	The AMP default settings w
		1	e .	mode (see Section 4.2 Step
	or Section 4.3 Step 2	.	s that are in Managed	mode (see Section 1.2 Step
	of Section 4.5 Step 2).		
	🍯 Avaya DevConnect AMP - Microsoft	Tatavaat Euglavav		5
		Internet Explorer		
		rch 📓 Favorites 🛞 Media 🍏 🖏 🗸	4 d B	
	Address Address https://192.45.51.111/ap_grou			▼ ∂Go Lini
		ew Devices: 0 🕈 Up: 0 🔸 Down: 0 ces Users Reports Syst		RAPIDS Site Plan Master Console
	· · · · · · · · · · · · · · · · · · ·	Security SSID/VLAN RADIUS		Actions Create
	Radio S	-	Proprietary Se	
	Allow Automatic Channel Selection:	C Yes 🖲 No	HP ProCurve 420:	
	802.11b Data Rates (Mb/sec):	1,0 Required 2,0 Required	Slot Time:	Auto 🔽
		5.5 Optional 11.0 Optional	HP ProCurve 420 Operational Mode:	802.11b + 802.11g 💌
	802.11a Data Rates (Mb/sec):	6.0 Required 9.0 Optional	Max Station Data Rate:	54 Mbps 💌
		12.0 Optional 💌 18.0 Optional 💌	Multicast Data Rate:	5.5 Mbps 💌
		24.0 Optional 💌 36.0 Optional 💌	Cisco Aironet:	
		48.0 Optional 🔽 54.0 Optional 🔽	Use Aironet Extensions:	⊙ Yes O No
	802.11g Data Rates (Mb/sec):	1.0 Required 2.0 Required 5.5 Required 6.0 Ontinent	Radio Fallback Action: IOS only	No Action (Radio Island)
		5.5 Required 6.0 Optional 9.0 Optional 11.0 Required	Lost Ethernet Action: VxWorks	Repeater Mode 💌
		12.0 Optional 💌 18.0 Optional 💌	Lost Ethernet Timeout (1-10000 sec):	2
		24.0 Optional - 36.0 Optional -	Short Slot-Time:	 Enabled Disabled
		48.0 Optional 💌 54.0 Optional 💌	Upgrade radio firmware when AP firmwan Radio Firmware x.xx):	e is upgraded (<i>Require Use of</i>
	Frag Threshold Enabled:	C Enabled O Disabled		⊙ Yes O No
	Threshold Value (256-2347 bytes):	2337	Proxim AP-600, AP-700, AP-2000, AP	-4000: Augus AB-2: Augus
	RTS/CTS Threshold Enabled:	C Enabled 💿 Disabled	AP-7, AP-4/5/6, AP-8; ProCurve5200	
	Threshold Value (0-2347 bytes):	2338	Load Balancing:	C Yes ⊙ No
	RTS/CTS Maximum Retries (1-255):	32	Interference Robustness:	C Yes ⊙ No
	Maximum Data Retries (1-255):	32	Distance between APs: 802.11q Operational Mode:	
	Beacon Period (19-5000 Kµsec):	100	802.11g Operational Mode: 802.11abg Operational Mode:	802.11b + 802.11g - 802.11b + 802.11g -
	DTIM Period (1-255):	2	802.11b Transmit Rate:	Auto Fallback V
	Ethernet Encapsulation:	C 802.1H @ RFC1042	802.11g Transmit Rate:	Auto Fallback 💌
	Radio Preamble:	⊙ Long ⊂ Short	802.11a Transmit Rate:	Auto Fallback 👻
	Spanning Tree Protocol:	Enabled O Disabled	Rogue Scanning:	
	1		Roque Scan Interval (15-1440 min):	15
			- · · · · · · · · · · · · · · · · · · ·	15

ep		Description				
	v 1 y	SSID and other settings according to customer authentication settings and RADIUS servers, see				
	Section 4.5). Click on "Save and Apply", and confirm the changes when prompted.					
	Got g					
	Address Addres	▼ ∂Go Links »				
	Home Groups APs/Devices Users Reports Syste					
	List Monitor Basic Radio Security SSID/VLAN RADIUS	IOS Advanced MAC ACL Firmware Actions Create				
	Crown Test Prown					
	Group: Test Group					
	VLAN Tagging: C Enabled 💿 Disabled					
	General	EAP Options				
	Create Closed Network: O Yes O No.					
	Block All Inter-Client Communication: O Yes © No	WEP Key Rotation Interval (0-10000000 sec.): 300 Session Key Refresh Rate (0-1440 min.): HP ProCurve 420 only				
	SSID: Avaya1	Session Timeout (0-65535 sec.): HP ProCurve 420 only				
	Encryption	Cisco TKIP: O Enabled				
		Cisco MIC: C MMH © Disabled				
	Encryption Mode: No Encryption	RADIUS Servers				
		Radius Server #1: Select V				
		Radius Server #2:				
		Radius Server #3: Select Radius Server #4: Select				
		MAC Address Authentication: O Enabled O Disabled MAC Address Format: * Single Dash				
		* Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-				
		4/5/6, AP-8; ProCurve520WL only v2.1.0 and higher only				
		Authorization Lifetime (900-43200 sec.): 1800				
		Primary Server Reattempt Period (0-120 min.):				
	[manualing]					
	Save Save and Apply Revert	•				
	Done	📕 🕒 💆				

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.	In the AMP web interface, click on the "A			5		
	the Proxim/OriNOCO checkbox and click on "Save". This allows AMP to automatically					
	discover Avaya APs on its local subnet.	discover Avaya APs on its local subnet.				
	-					
	Avaya DevConnect AMP - Microsoft Internet Explorer File Edit View Favorites Tools Help		<u> </u>			
	Generation (and the second seco	4 ei E				
	Address Addres		▼ ∂ Go L	Links »		
	(@/\int/ave)	🖉 Rogue: 0 🕴 Users: 0 🔰 Alerts: 0				
	Home Groups APs/Devices Users Reports Syst General Network Users Routers and Switches WLSE ACS	em Device Setup AMP Setup RA NMS RADIUS Accounting	PIDS Site Plan Master Console			
			Ľ	<u>Help</u>		
	General	Alert and Report En	nail			
	System Name: Avaya DevConnect AMP	Provide the sender (return) address for alert and repor separated recipient email addresses can be entered for				
	Console Refresh Rate: 30 seconds 💌	Sender Address:	autosupport+dev@autosi			
	Automatically Monitor/Manage New Devices: No	Alert Recipient Addresses:	autosupport@autosuppoi			
	Device Configuration Audit Interval: Never Automatically Repair Misconfigured Devices:					
	Email Debugging Messages to AirWave Wireless, Inc.	Historical Data				
	Regulatory Domain: United States	Keep User Session Records (2-550 days):	14			
	Auto Discovery	Keep Discovery Events (2-550 days):	14			
	· · · · · · · · · · · · · · · · · · ·	Advanced Group Configu	ration			
	Devices can also be discovered through SNMP and HTTP scans on the <u>Device Discovery</u> page.					
	CDP (<u>via SNMP</u>): □ Proxim/OR/NOCO: □	Cisco IOS: Colubris:	Enabled ○ Disabled C = block ○ Di			
	Intel and Symbol (WNMP):	Coldons.	C Enabled 💿 Disabled			
	Save Revert					
	Done		🔒 🔮 Internet			

Step		Description				
2.	Click on the " Device Setup " tab and then	Click on the "Device Setup" tab and then the "Discover" tab. In the New Network section, for				
		ya APs, enter its Network address and Subnet Mask,				
	assign a Label, and click on "Add".					
		New Network				
	Label:	192.45.61.0/24				
	Network:	192.45.61.0				
	Subnet Mask	: 255.255.255.0				
		Add				
3.		re Avaya APs with community strings that are neither				
		y string and click on " Add ". Recall that community				
	strings were configured on the Avaya APs	in Section 3.				
		New Credentials				
	Type:					
		Label: Enterprise Community String: *****				
		unity String: *****				
		bha				
		<u> </u>				
4.		Networks and Credentials for each pertinent				
		ng. In the example below, a scan for Avaya APs on nity string specified for the "Enterprise" credential				
	will be defined.	inity sumg specified for the Enterprise credential				
	will be defined.					
	Networks	Credentials				
	☑ 192.45.61.0/24: 192.45.61.0/255.	255.255.0				
		□ default (HTTP) □ private (SNMP)				
		public (SNMP)				
	Check All - Uncheck All	Check All - Uncheck All				
		ine <u>Scan</u> Delete				

tep	Description	Ī			
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.				
	🖉 Avaya DevConnect AMP - Microsoft Internet Explorer				
	Elle Edit View Favorites Iools Help				
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console				
	Discover Create Communication Firmware				
	To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the <u>Communication</u> page.				
	Note: Discovered devices will use the default credentials configured on the <u>Communication</u> page, not the credentials defined below for scanning.				
	Supported Devices Rogue APs Network Credential Total New Total New Start End				
	☑ 192.45.61.0/24 192.45.61.0/255.255.255.0 Enterprise (SNMP)				
	Check All - Uncheck All				
	Scan Delete Refresh this page for updated results.				
	Scan Delete Refresh this page for updated results.				
	2:00 A.M. (02:00 AM) 👻 Schedule				
	New Victoria de Carden Victoria				
	New Network New Credentials				
	Label: Type: © SNMP © HTTP				
	Network:				
	Subnet Mask:				
	Confirm Community String:				
	Add				
	Add				
	Networks Credentials				
	e Internet				

Step	Description
<u>6.</u>	The discovered Avaya APs are listed in the APs/Devices->New page.
0.	The discovered Tryaya Th 5 are listed in the Th Sibevices >110 w page.
	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".
	Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014
	Ele Edit View Favorites Iools Help → Back - → - ② ⑦ ⑦ ⑦ ③ Pavorites ③ Media ③ I ③ - ④ ☞ □
	Address @ https://192.45.51.111/ap_authorization?
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console
	All New Up Down Ignored
	Help
	Name Type LAN MAC Address LAN IP Discovered ✓ 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
	Avaya AP-0 52 00 00 Avaya AP-0 002/20.40.32/40.80 192/40.01132 0/9/2000 0.40 PM Avaya AP4-AP5-AP6-4b-61 Avaya AP-4/5/6 002/20.40.32/40.86 192/40.51.122 0/9/2005 6.39 PM
	Check All - Uncheck All
	Group: Test Group (SSID: Test Group)
	Monitor only (no changes will be made to device)
	C Manage read/write (group settings will be applied to device)
	Ignore Delete
	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.
	Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014 Image: Section 2014
	Lie Lot yow revealed in the second s
	Address in https://192.45.51.111/ap_authorization
	(@//ijr/Wzi/e)
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console
	All New Up Down Ignored
	Help
	Name Type LAN MAC Address LAN IP Discovered ✓ ✓ Avaya-AP4-AP5-AP6-4b-61 Avaya AP-4/5/6 00:20:A6:48:61:3F 192.45.51.240 6/9/2005 6:39 PM
	✓ Avaya-AP4-AP5-AP6-4b-61 Avaya AP-4/5/6 00:20:A6:48:61:3F 192.45.51.240 6/9/2005 6:39 PM
	Check All - Uncheck All
	Group: Test Group (SSID: Test Group)
	C Monitor only (no changes will be made to device)
	Manage read/write (group settings will be applied to device)
	Add
	Ignore Delete

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.	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".
	🗿 Avaya DevConnect AMP - Microsoft Internet Explorer
	Elle Edit View Favorites Iools Help
	↔ Back • → • ③ ④ ④ ④ GSearch ⓐ Favorites ④ Media ④ ⑤ • ④ · ④ ☑ □
	Address ∰ https://192.45.51.111/ap_create
	Image: Control Contro Control Control Contro Control Control Control Control Control Co
	Discover Create Communication Firmware
	Help Help
	Select the type of device you would like to create:
	Avaya AP-8 🔽 Create
2.	Enter the ID Address and Community String of the Avera AD select the Crown to assign the
4.	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".
	Note: The Community String should be set to the SNMP Read/Write Community String of the
	Avaya AP (see Section 3 Step 2).
	Avaya DevConnect AMP - Microsoft Internet Explorer
	Elle Edit View Favorites Iools Help ↓ Back → → → ② ② ② ③ ③ ③ ③ ● ■ Favorites ③ Media ③ ● ■ =
	Address 🙆 https://192.45.51.111/ap_create
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console
	Discover Create Communication Firmware Help
	Creating Avaya AP-8
	Configure default credentials on the <u>Communication</u> page.
	Name: Leave name blank to read it from device
	IP Address: 192.45.51.206
	SNMP Port: 161
	Community String: ******
	Confirm Community String: ********
	Group: Test Group (SSID: Test Group)
	Monitor only (no changes will be made to device)
	C Manage read/write (group settings will be applied to device) Add
	Cancel

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			_ 8 ×
<u>File E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			
$\Rightarrow Back \star \Rightarrow \star \textcircled{O} \textcircled{O} \textcircled{O} \texttt{Search} \textcircled{H} Favorites \textcircled{P}Media \textcircled{O} \textcircled{P} Media \textcircled{O} (\texttt{P} Media \texttt{O} \texttt{Media} $	4 ei 8		
Address https://192.45.51.111/ap_manage?id=2			▼ 🖉 Go Links »
Over the second secon	🖉 Rogue: 0 🕴 Users: 0 🔰 Ale	rts: 0	
Home Groups APs/Devices Users Reports Syste	em Device Setup AMP Se	tup RAPIDS Site Plan Ma	aster Console
All Monitor Manage Detail New Up Down Ignored			
			Help
General	Se	ttings	
Name: Avaya-AP4-AP5-AP6-4b-61-3f	Name:	Avaya-AP4-AP5-AP6-4b-61-3f	
Status: Up (OK)	Location:	System Location	
Configuration: Good Last Contacted: 6/9/2005 7:41 PM	Contact:	Contact Name	
Type: Avaya AP-4/5/6	Group:	Test Group (SSID: Avaya1)	
Firmware: 2.5.3 Current Group: Test Group	a oup i		
Management Mode: Manage Read/Write C Monitor Only	802.11abg ('bg' mode) Radio		
Notes (optional):	Transmit Power: Channel:	100% -	
	Channer;	11 💌	
×	Neighboring APs: N	No neighbors have been discovered yet.	
Device Communication	DHCP:	O Yes 💿 No	
	LAN IP:	192.45.51.240	
View Device Credentials If this device is down because its IP address or management ports have changed,	Subnet Mask:	255.255.255.0	
update the fields below with the correct information. IP Address:	Gateway:	192.45.51.1	
192,43,31,240	,	192.43.31.1	
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:			
Save and Apply Revert Delete Update Firmware			
Reboot			
Done			👌 Internet

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.	In the AMP web interface, select a Group and click on its RADIUS tab. Click on "Add".
	Avaya DevConnect AMP - Microsoft Internet Explorer
	Lie Luk new regionices Loops Lep → Back - → - ③ ② ③ △ ③ ③ Gearch ③ Favorites ④ Media ③ ⑤ · ④ · ⑤ ◎ ☑ ⑤
	Address https://192.45.51.111/radius_servers?id=6
	Image: Contraction of the second s
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console List Monitor Basic Radio Security SSID/MAN RADIUS IOS Advanced MAC ACL Firmware Actions Create
	Group: Test Group
	Add New RADIUS Server
	Save and Apply Revert
2.	Enter the information for a RADIUS server and click on "Add".
	Enter the information for a feribitory server and enter on Trade .
	🗿 Avaya DevConnect AMP - Microsoft Internet Explorer
	Ele Edit View Favorites Tools Help
	Contraction Contraction <thcontraction< th=""> <thcontraction< th=""></thcontraction<></thcontraction<>
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console
	List Monitor Basic Radio Security SSID/VLAN RADIUS IOS Advanced MAC ACL Firmware Actions Create Help
	Group: Test Group
	RADIUS Server
	TD Å lashes was
	IP/Hostname: IP Address required for Proxim/ORINOCO and Cisco Aironet IOS APs Secret:
	Confirm Secret: *****
	Port: 1812
	Timeout: 3
	Max Retries: 3
	Add Cancel
3.	Repeat steps 1-2 to enter information about additional RADIUS servers to be used by Avaya APs
з.	in the Group.

Step	Description		
4.	Click on "Save and Apply" when finished, and confirm the changes when prompted.		
	🚰 Avaya DevConnect AMP - Microsoft Internet Explorer	Ĩ	
	Ele Edit View Favorites Tools Help	<u> </u>	
	⇔Back + → - ③ ፼ ∰ @Search Maran @Media ③ By ⊕ = ■		
	Address https://192.45.51.111/radius_servers?id=6	▼ ∂Go	Links »
	(Ø/\ifr \//a/Ve)		
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master List Monitor Basic Radio Security SSID/VLAN RADIUS IOS Advanced MAC ACL Firmware Actions Create	er Console	
			<u>Help</u>
	New RADIUS Server added successfully.		
	Group: Test Group		
	Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.		
	Add New RADIUS Server		
	IP/Hostname Port Timeout Max Retries		
	□ [▶] 192.45.51.128 1812 3 3		
	Check All - Uncheck All		
	Delete		
	Save Save and Apply Revert		
		nternet	

		Description	
Slick on the Security tab, and a		eryption Mode to one of the	encryption/authenticat
ptions from the pull-down list			
- · · · · ·			1 1 .
For encryption/authentication of	-		•
Fransmit Key . In the example	e below, ho	wever, WEP Keys are not re	quired for 802.1x
encryption/authentication.			
For WPA encryption/authentica	ation speci	if v the WPA Cipher (AES or	TKIP) and in the case
WPA/PSK also the WPA Presh	· •	ity the wirk cipher (rills of	Tixit) and in the case
	lureu key.		
For RADIUS-based authenticat	tion options	s, select a RADIUS server fo	r Radius Server #1 , a
ptionally Radius Server #2 .	1	, ,	,
Click on " Save and Apply ", an	nd confirm	the changes when prompted.	
Avaya DevConnect AMP - Microsoft Internet Explorer File Edit View Favorites Iools Help			
⇔Back • → - 🙆 😰 🐴 🛛 🐼 Search 💽 Favorites 🔅	🝘 Media 🏼 🎯 🛛 🛃 🕶	5 e B	
Address Address https://192.45.51.111/ap_group_security?id=6			<u>▼</u> ∂°60
	Up: 2 Down: 0 Reports Syst		S Site Plan Master Console
	ALAN RADIUS	IOS Advanced MAC ACL Firmware Actions	Create
VLAN Tagging: O Enabled O Disabled			
General			
		EAP Options	
Create Closed Network: Block All Inter-Client Communication:	O Yes ⊙ No O Yes ⊙ No	LAP Uptions WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur	300
		WEP Key Rotation Interval (0-10000000 sec.):	ve 420 only
Block All Inter-Client Communication:		WEP Key Rotation Interval (0-1000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP:	ve 420 only 0
Block All Inter-Client Communication: SSID: Avaya1		WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP:	ve 420 only 0
Block All Inter-Client Communication: SSID: Avaya1 Encryption	C Yes O No	WEP Key Rotation Interval (0-1000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers	ve 420 only 0 0 Denabled I Isabled I MMH I Disabled
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys	C Yes C No Require 802.1x - Transmit Key	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP:	ve 420 only 0 Denabled O Disabled O MMH Disabled 192.45.51.128:1812
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode:	C Yes • No	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #2: Radius Server #3:	ve 420 only 0 v 0 Enabled © Disabled © MMH © Disabled 192.45.51.128:1812 • Select • Select •
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1:	C Yes C No Require 802.1x Transmit Key	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #2:	ve 420 only 0 v 0 Enabled © Disabled © MMH © Disabled 192.45.51.128:1812 v Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Key #4:	C Yes C No Require 802.1x Transmit Key	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #4: MAC Address Authentication:	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Rey #4: 802.1x + WEP mode only sets key #1. Enter 40/64-bit Keys in S alphanumeric or 10 hexadecimal digits.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: © Enabled © Disable MAC Address Format: *	ve 420 only 0 Denabled Disabled MMH Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #3: Key #4: 802.1x + WEP mode only sets key #1.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: (Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled O Disable MAC Address Format: * Single Dash * Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4(56, AP-8; ProCurve520WL only v2.1.0	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Rey #4: 802.1x + WEP mode only sets key #1. Enter 40/64-bit Keys in S alphanumeric or 10 hexadecimal digits.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled © Disable MAC Address Format: * Single Dash * Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4(5/6, AP-8; ProCurve520WL only v2.1.0 and higher only	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Rey #4: 802.1x + WEP mode only sets key #1. Enter 40/64-bit Keys in S alphanumeric or 10 hexadecimal digits.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #1: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled C Disable MAC Address Format: * Single Dash MAC Address Format: * Single Dash * * Proxim AP-600, AP-700, AP-2000, AP-400; Avaya AP-3,	ve 420 only 0 Denabled Disabled MMH Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Rey #4: 802.1x + WEP mode only sets key #1. Enter 40/64-bit Keys in S alphanumeric or 10 hexadecimal digits.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-10000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled © Disable MAC Address Format: * Single Dash * Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4(5/6, AP-8; ProCurve520WL only v2.1.0 and higher only	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Key #4: Block All Inter-Offent Subpartment or 10 hexadecimal digits. Enter 40/64-bit Keys in 13 alphanumeric or 26 hexadecimal digits	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-1000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled O Disable MAC Address Format: * Single Dash * Proxim AP-60, AP-700, AP-200, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only v2.1.0 and higher only Authorization Lifetime (900-43200 sec.): 1800 Primary Server Reattempt Period (0-120 min.):	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Rey #4: 802.1x + WEP mode only sets key #1. Enter 40/64-bit Keys in S alphanumeric or 10 hexadecimal digits.	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-1000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled O Disable MAC Address Format: * Single Dash * Proxim AP-60, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only v2.1.0 and higher only Authorization Lifetime (900-43200 sec.): 1800 Primary Server Reattempt Period (0-120 min.):	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select
Block All Inter-Client Communication: SSID: Avaya1 Encryption Encryption Mode: WEP Keys Key #1: Key #2: Key #3: Key #4: Block All Inter-Offent Subpartment or 10 hexadecimal digits. Enter 40/64-bit Keys in 13 alphanumeric or 26 hexadecimal digits	C Yes C No Require 802.1x V Transmit Key C C C	WEP Key Rotation Interval (0-1000000 sec.): Session Key Refresh Rate (0-1440 min.): HP ProCur Session Timeout (0-65535 sec.): HP ProCurve 420 on Cisco TKIP: Cisco MIC: RADIUS Servers Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled O Disable MAC Address Format: * Single Dash * Proxim AP-60, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only v2.1.0 and higher only Authorization Lifetime (900-43200 sec.): 1800 Primary Server Reattempt Period (0-120 min.):	ve 420 only 0 Denabled Disabled Ommon Min Disabled 192.45.51.128:1812 Select Select Select

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.

ep		Description									
•	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" * 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 configur they are in different VLANs.	1									
	🚰 Avaya DevConnect AMP - Microsoft Internet Explorer		_ B ×								
	<u>Elle Edit View Favorites Tools H</u> elp		(B)								
	↔ Back • → • ② ② ② △ ③ Search Favorites ③ Media ③ 5	4 eí 8									
	Address https://192.45.51.111/ap_group_security?id=6		▼ 🖓 Go Links »								
	Image: Construction of the state o		S Site Plan Master Console Create								
			<u>Help</u>								
	Group: Test Group VLAN Tagging: ⓒ Enabled 〇 Disabled VLANs	PADIIIS Servers	i Liege								
	VLAN Tagging: Enabled Disabled VLANs	RADIUS Servers									
	VLAN Tagging: Enabled VLANs Create and edit VLANs and SSIDs on this group's <u>SSID/VLAN</u> page.	RADIUS Servers Radius Server #1: Radius Server #2:	192.45.51.128:1812 •								
	VLAN Tagging: Enabled VLANs Create and edit VLANs and SSIDs on this group's <u>SSID/VLAN</u> page. Management VLAN ID (0-4094, Untagged): * 51	Radius Server #1:									
	VLAN Tagging: Enabled Disabled VLANs Create and edit VLANs and SSIDs on this group's <u>SSID/VLAN</u> page.	Radius Server #1: Radius Server #2:	192.45.51.128:1812 • Select •								
	VLAN Tagging: Enabled Disabled VLANs Create and edit VLANs and SSIDs on this group's <u>SSID/VLAN</u> page. Management VLAN ID (D-4094, Untagged): * * Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-	Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #4: MAC Address Authentication:	192.45.51.128:1812 • Select • Select • Select •								
	VLAN Tagging: Enabled	Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #4:	192.45.51.128:1812 • Select • Select • Select •								
	VLAN Tagging:	Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #4: MAC Address Authentication: © Enabled © Disable MAC Address Format: * Single Dash * Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurveS20WL only v2:1.0 and higher only	192.45.51.128:1812 • Select • Select • Select •								
	VLAN Tagging:	Radius Server #1: Radius Server #2: Radius Server #3: Radius Server #4: MAC Address Authentication: C Enabled ● Disable MAC Address Format: * Single Dash * Proxim AP-600, AP-700, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5(6, AP-8; ProCurveS20WL only v2.1.0	192.45.51.128:1812 • Select • Select •								

Step	Description
2.	Click on the "SSID/VLAN" tab and then "Add".
	🚰 Avaya DevConnect AMP - Microsoft Internet Explorer
	Eile Edit View Favorites Iools Help
	↔ Back • → • ② ② ② △ ③ Search ⓐ Favorites ③ Media ③ ⑤ • ④ ☑ Address ④ https://192.45.51.111/Man list?d=6 • • @Go Links »
	Address ∰ https://192.45.51.111/vlan_list?id=6
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console
	List Monitor Basic Radio Security SSID//LAN RADIUS IOS Advanced MAC ACL Firmware Actions Create
	Group: Test Group Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.
	Add New SSID/VLAN
	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.
	Save and Apply Revert
3.	Enter a VLAN ID, SSID, and, if desired, the Encryption Mode. In the example below, VLAN
5.	51 is configured for the wireless laptop clients in Figure 1 . Click on " Add ".
	Avaya DevConnect AMP - Microsoft Internet Explorer
	Ele Edit View Favorites Iools Help IIII Construction (Construction Construction Constructico Construction Construction Construction Co
	Address @ https://192.45.51.111/vlan_ist?id=6
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console List Monitor Basic Radio Security SSID/VLAN RADIUS IOS Advanced MAC ACL Firmware Actions Create
	Group: Test Group
	Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.
	SSID/ VLAN
	Enable VLAN Tagging: Colubris, Symbol only O Yes C No
	VLAN ID: 51 SSID: Avaya1-51
	Name: Avaya1-51
	Service Priority: Cisco VxWorks only default
	Maximum Number of Associations: 255
	Broadcast SSID: Colubris only O Yes O No Block All Inter-Client Communication: Colubris only O Yes O No
	Encryption
	Encryption Mode:
	EAP Options
	WEP Key Rotation Interval: 120
	Cisco TKIP: O Enabled O Disabled Cisco MIC: O MMH O Disabled
	RADIUS Servers
	RADIUS Server #1: Colubris only Select
	RADIUS Server #2: Colubris only Select
	Add Cancel

Solution & Interoperability Test Lab Application Notes ©2005 Avaya Inc. All Rights Reserved.

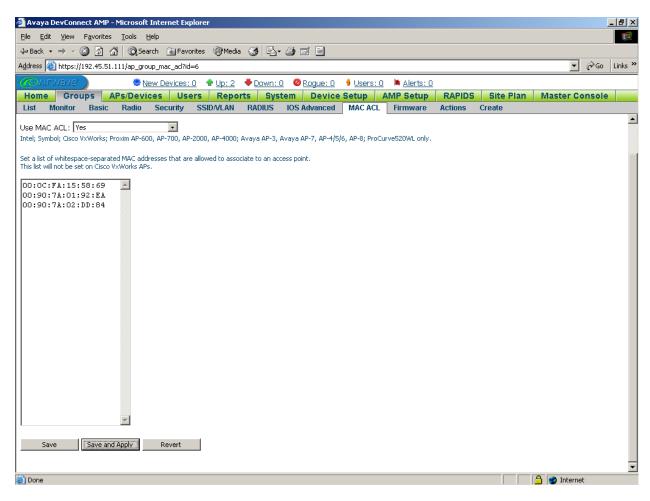
		Description								
R	epeat Step 3 as necessary	to add additional VLANs. The example below shows the	e							
С	onfiguration of VLAN 52	for the Avaya 3616 and 3626 Wireless IP Telephones in	Figure 1.							
	C	y 1	8							
ø	Avaya DevConnect AMP - Microsoft Internet E	xplorer	_ 5							
Ē	ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp									
↓ Back • → → ② ② ③ ④ ③ Favorites ③ Media ③ ■ • ④ □										
A	ddress 🕘 https://192.45.51.111/vlan_list?id=6		💌 🤗 Go Lir							
(Mew Devices									
	Home Groups APs/Devices Us List Monitor Basic Radio Security		aster Console							
E			He							
	Group: Test Group									
	lote : There are unapplied changes for this group. You m	must click 'Save and Apply' to make them take effect.								
	SSID/YLAN									
-	·									
	nable VLAN Tagging: Colubris, Symbol only /LAN ID:	© Yes O No								
	SID:	52								
	Jame:	Avaya1-52								
5	Service Priority : Cisco V×Works only	default								
1	Naximum Number of Associations:	255								
	roadcast SSID: Colubris only	O Yes 💿 No								
E	Slock All Inter-Client Communication: Colubris only	ly ⊙ Yes O No								
	Encruption									
-	Encryption									
E	Encryption	Require WEP								
E										
-	incryption Mode: WEP Keys	Require WEP T Transmit Key								
- k	encryption Mode: WEP Keys Eey #1: 1357902468									
- k	incryption Mode: WEP Keys	Require WEP T Transmit Key								
- k k	WEP Keys (ey #1: 1357902468 (ey #2: 1357902468	Require WEP T Transmit Key								
	WEP Keys iev #1: 1357902468 iev #2: 1357902468 iev #3: 1357902468 iev #4: 1357902468	Require WEP Transmit Key								
- K K K K K K K K K K K K K K K K K K K	WEP Keys (ey #1: 1357902468 (ey #2: 1357902468 (ey #3: 1357902468 (ey #4: 1357902468 (ey #4: 1357902468 (ey #4: 1357902468 (e) #4: 1357902468 (e) #4: 1357902468 (e) #4: 1357902468	Require WEP Transmit Key								
- 	WEP Keys iery #1: 1357902468 iey #2: 1357902468 iey #3: 1357902468 iey #4: 1357902468 i02.1x + WEP mode only sets key #1. neter 10/(126 kit Keys in 5 alphanumeric or 10 hexadecimal neter 10/(126 kit Keys in 5 alphanumeric or 26 hexadecimal neter 10/(126 kit Keys in 13 alphanumeric or 26 hexadecimal neter 10/(126 kit Keys in 13 alphanumeric or 26 hexadecimal neter 10/(126 kit Keys in 126	Require WEP Transmit Key								

Step	Description	
5.	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.	
	Ele Edit View Favorites Iools Help → Back - → - ② ② ⑦ ⚠ ③ @Q.Search ⓐ Favorites ③ Media ③ □ □ =	
		inks »
	Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS Site Plan Master Console	
	List Monitor Basic Radio Security SSID/VLAN RADIUS IOS Advanced MAC ACL Firmware Actions Create	lelp
	Group: Test Group	
	Note: There are unapplied changes for this group. You must click 'Save and Apply' to make them take effect.	
	SSID/VLAN	
	Enable VLAN Tagging: Colubris, Symbol only O Yes O No	
	VLAN ID: 9999	
	SSID:	
	Name:	
	Service Priority: Clsco VxWorks only default Maximum Number of Associations: 255	
	Broadcast SSID: Colubris only O Yes 💿 No	
	Block All Inter-Client Communication: Colubris only © Yes © No Encryption	
	Encryption Mode: No Encryption C	
	WEP Key Rotation Interval: 120	
	Cisco TKIP: O Enabled O Disabled	
	Cisco MIC: O MMH O Disabled	
	RADIUS Server #1: Colubris only Select RADIUS Server #2: Colubris only Select	
	Add Cancel	
	🙆 Done 🕒 🔒 🔮 Internet	

								Desc	ription										
Description 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																			
								MP require	,										
								-					•	~~				- ·	
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). Not												te							
that since the "stub" VLAN is not enabled on any radio (wireless interface), it will not be																			
							n the G		iy ruuro	(110	1000	meen	uee), 10	,, 11	i not			
com	ng	urce	i on t		aya A	1511		ioup.											
Clie	1	· · ·	Savo	and	Annly	", on	daanfi	rm tha ah	ngoa w	hon n	rom	atad							
Che	к	Ш	Save		Appiy	ano	a conn	rm the cha	inges w	nen p	orom	jieu.							
🥔 Ava	va De	vConn	ect AMP -	- Microsoft	Internet Ex	plorer												_ 8	
					<u>t</u> elp														1
Eile Edit View Favorites Iools Help ↓→ Back → → ~ ② ② ① ① ③ Barch ⓐ Favorites ③ Media ③ ⑤ → ④ ☑ ⑤																			
🕀 Bac	Address @ https://192.45.51.111/vlan_list?id=6																		
	_		192.45.51.	.111/vlan_lis	t?id=6												<u> </u>	Go Link	;
Addres:	s 🔊	https:// /aivei		🙁 <u>N</u> e	ew Devices:			own: 0 Ø Rogue			Alerts: 0								;
Address	s 🔊 Nirva ne	https:// /ave Grou	Jps A	🥮 <u>N</u> e APs/Devie	ew Devices: ces Us	ers	Reports	System De	vice Setup	AMP 9	Setup	RAPID: Actions		Site Pla	an	Maste	r Cons		; '
Addres:	s 🔊 Nirva ne	https:// /aivei		🙁 <u>N</u> e	ew Devices:		Reports		vice Setup	AMP 9		RAPID: Actions	S S Cre		an	Maste			
Addres: Hon List	s 🙋 Airv ne Ma	https:// /alve Grou onitor	ups A Basic	🥮 <u>N</u> e APs/Devie	ew Devices: ces Us	ers	Reports	System De	vice Setup	AMP 9	Setup				an	Maste		ole	
Addres: Mon List Group	s 🙆 Alirva Mo	https:// /3//2 Grou onitor	Jps A Basic	😻 <u>Ne</u> APs/Devid Radio	ew Devices: ces Us Security	ers SSIDA	Reports VLAN RAI	System De	vice Setup ced MAC A	AMP 9	Setup				an	Maste		ole	
Addres: Mon List Group	s 🙆 Alirva Mo	https:// Grou onitor are una	Jps A Basic	Ne N	ew Devices: ces Us Security	ers SSIDA	Reports VLAN RAI	System De DIUS IOS Advan	vice Setup ced MAC A	AMP 9	Setup				an	Maste		ole	
Address Hon List Group Note:	s air wanted a final and a fin	https:// Grou onitor are una waya, a s, all SSI	Jps A Basic	Radio	<u>ew Devices:</u> ces Us Security group. You mathematical APs, different	ers SSIDA	Reports VLAN RAI Save and Apply	System De DIUS IOS Advan	vice Setup ced MAC A fect.	CL Firm	Setup mware	Actions IOS and			an	Maste		ole	
Address Hon List Group Note: For Pro	s air wanted a final and a fin	https:// Grou onitor are una waya, a s, all SSI	JPS A Basic JP pplied char New SSII ond HP ProC D/VLAN cor	Ne N	ew Devices: Ces Us Security group. You ma APs, different ill be applied to	SSID/VLA	Reports VLAN RAI Save and Apply	System De DIUS IOS Advan	vice Setup ced MAC A fect.	CL Firm	Setup mware	Actions IOS and			an	Maste		ole	
Address Hon List Group Note:	s Alir // Mo Mo Controls Add Add	https:// Grotonitor st Groto are una avaya, a s, all SSI 1 page.	Jp 5 A Basic Jp pplied char New SSII and HP Pro(D/VLAN cor First Enabled	Ne N	ew Devices: ces Us Security group. You m APs, different ill be applied to Second R Enabled P	SSID/VLA sSID/VLA sSID/VLA so the first Sadio Primary	Reports VLAN RAI	System De DIUS IOS Advan ' to make them take el 's can be applied to the P. To configure both i Encryption Mode	vice Setup ced MAC A ffect. a first and/or sec adios on IOS AP Native VLAN	CL Firm	Setup mware	Actions IOS and			an	Maste		ole	
Address Hon List Group Note:	s Alir // Mo Mo Controls Add Add	https:// Grotonitor st Groto are una avaya, a s, all SSI 1 page.	Jps A Basic Jp pplied char New SSII D/VLAN cor First	Network Net	ew Devices: ces Us Security group. You m APs, different ill be applied to Second R Enabled P	ers SSIDA ust click 'S SSID/VLA so the first	Reports VLAN RAI Save and Apply AN combination : radio on the A SSID Avaya1-51	System De DIUS IOS Advan ' to make them take el 's can be applied to the P. To configure both i Encryption Mode	vice Setup ced MAC A fect. e first and/or sec adios on IOS AP	CL Firm	Setup mware	Actions IOS and			an	Maste		ole	

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:

- MP 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: <u>support@airwave.com</u>
- 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 <u>http://www.airwave.com/prodserv_products.html</u>.

©2005 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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.