


# AirWave

## Version 7.4.0



User Guide

## Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include  **AirWave**, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](http://www.arubanetworks.com/open_source)

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.



[www.arubanetworks.com](http://www.arubanetworks.com)

1344 Crossman Avenue  
Sunnyvale, California 94089

Phone: 408.227.4500  
Fax 408.227.4550

<b>Preface .....</b>	<b>11</b>
Document Organization.....	11
Note, Caution, and Warning Icons .....	12
Contacting Support .....	12
<b>Chapter 1   Introduction.....</b>	<b>13</b>
AirWave—A Unified Wireless Network Command Center .....	13
AirWave Management Platform .....	13
Aruba Configuration .....	14
VisualRF .....	14
RAPIDS.....	14
Master Console and Failover.....	14
Integrating AMP into the Network and Organizational Hierarchy.....	15
<b>Chapter 2   Installing and Getting Started in AirWave .....</b>	<b>17</b>
AirWave Hardware Requirements and Installation Media .....	17
Supported Browsers .....	17
Installing Linux CentOS 5 (Phase 1) .....	18
Installing AirWave Software (Phase 2).....	18
Getting Started .....	18
Step 1: Configuring Date and Time, Checking for Prior Installations.....	18
Date and Time.....	18
Previous AirWave Installations.....	19
Step 2: Installing AMP Software.....	19
Step 3: Checking the AirWave Installation .....	19
Step 4: Assigning an IP Address to the AirWave System .....	19
Step 5: Naming the AirWave Network Administration System .....	20
Step 6: Assigning a Host Name to AirWave.....	20
Step 7: Changing the Default Root Password .....	20
Completing the Installation.....	21
Configuring and Mapping Port Usage for AMP .....	21
AirWave Navigation Basics.....	22
Status Section .....	22
Navigation Section .....	24
Activity Section.....	25
Help Links in the UI .....	26
Common List Settings.....	26
Buttons and Icons .....	26
Getting Started with AirWave .....	28
<b>Chapter 3   Configuring AMP .....</b>	<b>29</b>
Before You Begin .....	29
Formatting the Top Header .....	29
Customizing Columns in Lists .....	30
Resetting Pagination Records.....	31
Using the Pagination Widget.....	31

Using Export CSV for Lists and Reports .....	31
Defining Graph Display Preferences .....	32
Customizing the Dashboard .....	32
Customized Search .....	34
Setting Severe Alert Warning Behavior .....	34
Defining General AirWave Server Settings .....	35
Defining AirWave Network Settings .....	43
Creating AirWave Users .....	44
Creating AirWave User Roles .....	46
Configuring Login Message, TACACS+ and RADIUS Authentication.....	49
Setting Up Login Configuration Options .....	49
Setting up Single Sign-On.....	49
Configuring TACACS+ Authentication .....	50
Configuring RADIUS Authentication and Authorization .....	51
Integrating a RADIUS Accounting Server.....	52
Enabling AirWave to Manage Your Devices .....	53
Configuring Communication Settings for Discovered Devices .....	54
Loading Device Firmware Onto AirWave (optional).....	56
Overview of the Device Setup > Upload Firmware & Files Page.....	56
Loading Firmware Files to AirWave .....	57
Using Web Auth Bundles in AirWave.....	58
Setting Up Device Types.....	59
Configuring Cisco WLSE and WLSE Rogue Scanning.....	59
Introduction to Cisco WLSE .....	60
Configuring WLSE Initially in AirWave .....	60
Adding an ACS Server for WLSE.....	60
Enabling Rogue Alerts for Cisco WLSE .....	60
Configuring WLSE to Communicate with APs.....	60
Discovering Devices .....	61
Managing Devices .....	61
Inventory Reporting .....	61
Defining Access .....	61
Grouping .....	61
Configuring IOS APs for WDS Participation.....	62
WDS Participation.....	62
Primary or Secondary WDS .....	62
Configuring ACS for WDS Authentication .....	62
Configuring Cisco WLSE Rogue Scanning .....	63
Configuring ACS Servers.....	64
Integrating AirWave with an Existing Network Management Solution (NMS) .....	65
Auditing PCI Compliance on the Network.....	66
Introduction to PCI Requirements.....	66
PCI Auditing in the AirWave Interface .....	67
Enabling or Disabling PCI Auditing .....	68
Deploying WMS Offload .....	69
Overview of WMS Offload in AirWave.....	69
General Configuration Tasks Supporting WMS Offload in AirWave .....	69
Additional Information Supporting WMS Offload.....	70
<b>Chapter 4   Configuring and Using Device Groups in AMP.....</b>	<b>71</b>
AMP Groups Overview .....	72
Viewing All Defined Device Groups.....	72
Configuring Basic Group Settings.....	74
Adding and Configuring Group AAA Servers .....	81



Configuring Group Security Settings.....	82
Configuring Group SSIDs and VLANs .....	84
Configuring Radio Settings for Device Groups .....	88
Cisco WLC Group Configuration.....	92
Accessing Cisco WLC Configuration .....	92
Navigating Cisco WLC Configuration.....	92
Configuring WLANs for Cisco WLC Devices.....	93
Defining and Configuring LWAPP AP Groups for Cisco Devices .....	95
Viewing and Creating Cisco AP Groups.....	95
Configuring Cisco Controller Settings.....	95
Configuring Wireless Parameters for Cisco Controllers.....	96
Configuring Cisco WLC Security Parameters and Functions .....	96
Configuring Management Settings for Cisco WLC Controllers.....	96
Configuring Group PTMP Settings.....	97
Configuring Proxim Mesh Radio Settings .....	98
Configuring Group MAC Access Control Lists.....	99
Specifying Minimum Firmware Versions for APs in a Group.....	99
Comparing Device Groups .....	100
Deleting a Group .....	101
Changing Multiple Group Configurations .....	102
Modifying Multiple Devices .....	103
Using Global Groups for Group Configuration .....	105
<b>Chapter 5    Discovering, Adding, and Managing Devices .....</b>	<b>107</b>
Device Discovery Overview .....	107
Discovering and Adding Devices.....	107
SNMP/HTTP Scanning.....	108
Adding Networks for SNMP/HTTP Scanning .....	108
Adding Credentials for Scanning .....	108
Defining a Scan Set .....	109
Running a Scan Set .....	110
Enabling Cisco Discovery Protocol (CDP).....	111
Authorizing Devices to AMP from APs/Devices > New Page .....	111
Manually Adding Individual Devices.....	112
Adding Devices with the Device Setup > Add Page.....	112
Adding Multiple Devices from a CSV File .....	114
Adding Universal Devices .....	115
Assigning Devices to the Ignored Page .....	116
Monitoring Devices.....	116
Viewing Device Monitoring Statistics .....	117
Understanding the APs/Devices > Monitor Pages for All Device Types.....	118
Monitoring Data Specific to Wireless Devices .....	118
Evaluating Radio Statistics for an AP.....	124
Overview of the Radio Statistics Page .....	124
Viewing Real-Time ARM Statistics .....	124
Issues Summary section.....	125
802.11 Radio Counters Summary .....	125
Radio Statistics Interactive Graphs .....	125
Recent ARM Events Log.....	127
Detected Interfering Devices Table.....	128
Active BSSIDs Table .....	128
Monitoring Data for Mesh Devices .....	128
Monitoring Data for Wired Devices (Routers and Switches) .....	130
Understanding the APs/Devices > Interfaces Page .....	132
Auditing Device Configuration.....	133

	Using Device Folders (Optional) .....	134
	<b>Configuring and Managing Devices .....</b>	<b>134</b>
	Moving a Device from Monitor Only to Manage Read/Write Mode .....	135
	Configuring AP Settings .....	136
	Setting a Maintenance Window for a Device .....	141
	Configuring Device Interfaces for Switches .....	142
	Individual Device Support and Firmware Upgrades.....	144
	<b>Troubleshooting a Newly Discovered Down Device .....</b>	<b>146</b>
	<b>Setting up Aruba Spectrum Analysis in AMP .....</b>	<b>147</b>
	Spectrum Configurations and Prerequisites .....	147
	Setting up a Permanent Spectrum Aruba AP Group .....	148
	Configuring an Individual AP to run in Spectrum Mode.....	148
	Configuring a Controller to use the Spectrum Profile .....	149
<b>Chapter 6</b>	<b>Creating and Using Templates.....</b>	<b>151</b>
	<b>Group Templates .....</b>	<b>151</b>
	Supported Device Templates.....	151
	Template Variables.....	151
	<b>Viewing and Adding Templates .....</b>	<b>152</b>
	<b>Configuring General Template Files and Variables .....</b>	<b>155</b>
	Configuring General Templates.....	156
	IOS Configuration File Template.....	157
	Device Configuration File on APs/Devices > Audit Configuration Page.....	157
	Using Template Syntax .....	157
	Using Directives to Eliminate Reporting of Configuration Mismatches .....	157
	Ignore_and_do_not_push Command .....	158
	Push_and_exclude Command.....	158
	Using Conditional Variables in Templates.....	158
	Using Substitution Variables in Templates.....	159
	Using AP-Specific Variables.....	160
	<b>Configuring Cisco IOS Templates .....</b>	<b>160</b>
	Applying Startup-config Files .....	161
	WDS Settings in Templates.....	161
	SCP Required Settings in Templates.....	161
	Supporting Multiple Radio Types via a Single IOS Template .....	162
	Configuring Single and Dual-Radio APs via a Single IOS Template .....	162
	<b>Configuring Cisco Catalyst Switch Templates .....</b>	<b>162</b>
	<b>Configuring Symbol Controller / HP WESM Templates .....</b>	<b>163</b>
	<b>Configuring a Global Template.....</b>	<b>165</b>
<b>Chapter 7</b>	<b>Using RAPIDS and Rogue Classification .....</b>	<b>167</b>
	<b>Introduction to RAPIDS .....</b>	<b>167</b>
	<b>Viewing Overall Network Health on RAPIDS &gt; Overview .....</b>	<b>168</b>
	<b>Setting Up RAPIDS.....</b>	<b>169</b>
	Basic Configuration .....	169
	Rogue Containment Options.....	171
	Additional Settings .....	172
	<b>Defining RAPIDS Rules.....</b>	<b>172</b>
	Controller Classification with WMS Offload .....	172
	Device OUI Score.....	173
	Rogue Device Threat Level .....	173
	Viewing and Configuring RAPIDS Rules .....	174
	Deleting or Editing a Rule .....	176
	Recommended RAPIDS Rules.....	176
	Using RAPIDS Rules with Additional AirWave Functions .....	176

Viewing Rogues on the RAPIDS > List Page.....	176
Overview of the RAPIDS > Detail Page .....	179
Viewing Ignored Rogue Devices .....	180
Using RAPIDS Workflow to Process Rogue Devices.....	180
Score Override.....	180
Using the Audit Log .....	181
Additional Resources .....	182

## **Chapter 8 Performing Daily Administration in AirWave..... 183**

Monitoring and Supporting AMP with the System Pages.....	183
Using the System > Status Page .....	184
Viewing Device Events in System > Syslog & Traps .....	185
Using the System > Event Log Page.....	186
Viewing, Delivering and Responding to Triggers and Alerts .....	186
Viewing Triggers.....	187
Creating New Triggers.....	187
Setting Triggers for Devices .....	190
Setting Triggers for Interfaces and Radios .....	191
Setting Triggers for Discovery .....	191
Setting Triggers for Clients .....	192
Setting Triggers for RADIUS Authentication Issues.....	193
Setting Triggers for IDS Events.....	193
Setting Triggers for AMP Health .....	194
Delivering Triggered Alerts .....	194
Viewing Alerts.....	194
Responding to Alerts.....	195
Monitoring and Supporting WLAN Clients .....	196
Overview of the Clients Pages .....	196
Monitoring WLAN Users in the Clients > Connected and Clients > All Pages.....	196
Supporting Guest WLAN Users With the Clients > Guest Users Page.....	199
Supporting VPN Users with the Clients > VPN Sessions Page .....	201
Supporting RFID Tags With the Clients > Tags Page .....	202
Evaluating and Diagnosing User Status and Issues.....	203
Evaluating User Status with the Clients > Client Detail Page .....	203
Mobile Device Access Control in Clients > Client Detail and Clients > Connected ..	204
Classifying Aruba Devices in Client Detail .....	205
Quick Links for Clients on Aruba Devices .....	206
Using the Deauthenticate Client Feature.....	206
Viewing a Client's Association History .....	206
Viewing the Rogue Association History for a Client .....	206
Evaluating Client Status with the Clients > Diagnostics Page .....	207
Managing Mobile Devices with SOTI MobiControl and AirWave .....	207
Overview of SOTI MobiControl .....	207
Prerequisites for Using MobiControl with AirWave .....	207
Adding a Mobile Device Management Server for MobiControl.....	208
Accessing MobiControl from the Clients > Client Detail Page.....	208
Monitoring and Supporting AMP with the Home Pages .....	209
Monitoring AMP with the Home > Overview Page.....	209
Viewing and Updating License Information.....	211
Searching AMP with the Home > Search Page .....	211
Accessing AirWave Documentation .....	213
Configuring Your Own User Information with the Home > User Info Page.....	213
Using the System > Configuration Change Jobs Page.....	215
Using the System > Firmware Upgrade Jobs Page .....	215
Using the System > Performance Page .....	216
Supporting AMP Servers with the Master Console.....	220

	Using the Public Portal on Master Console .....	220
	Adding a Managed AMP with the Master Console .....	221
	Using Global Groups with Master Console .....	222
	<b>Upgrading AirWave .....</b>	<b>222</b>
	Upgrade Instructions .....	222
	Upgrading Without Internet Access .....	223
	<b>Backing Up AMP .....</b>	<b>223</b>
	Viewing and Downloading Backups .....	223
	Running Backup on Demand .....	223
	Restoring from a Backup .....	223
	<b>Using AirWave Failover for Backup .....</b>	<b>224</b>
	Navigation Section of AMP Failover .....	224
	Adding Watched AMP Stations .....	224
	<b>Logging out of AirWave .....</b>	<b>225</b>
<b>Chapter 9</b>	<b>Creating, Running, and Emailing Reports .....</b>	<b>227</b>
	<b>Overview of AMP Reports .....</b>	<b>227</b>
	Reports > Definitions Page Overview .....	227
	Reports > Generated Page Overview .....	229
	<b>Using Daily Reports .....</b>	<b>230</b>
	Viewing Generated Reports .....	230
	Using Custom Reports .....	230
	Using the Aruba License Report .....	232
	Using the Capacity Planning Report .....	232
	Using the Configuration Audit Report .....	234
	Using the Device Summary Report .....	235
	Using the Device Uptime Report .....	237
	Using the IDS Events Report .....	239
	Using the Inventory Report .....	239
	Using the Memory and CPU Utilization Report .....	241
	Using the Network Usage Report .....	241
	Using the New Rogue Devices Report .....	242
	Using the New Users Report .....	245
	Using the PCI Compliance Report .....	245
	Using the Port Usage Report .....	246
	Using the RADIUS Authentication Issues Report .....	246
	Using the RF Health Report .....	247
	Using the Rogue Clients Report .....	249
	Using the Rogue Containment Audit Report .....	250
	Using the Client Session Report .....	250
	<b>Defining Reports .....</b>	<b>252</b>
	<b>Emailing and Exporting Reports .....</b>	<b>255</b>
	Emailing Reports in General Email Applications .....	255
	Emailing Reports to Smarthost .....	255
	Exporting Reports to XML or CSV .....	256
	Transferring Reports Using FTP .....	256
<b>Chapter 10</b>	<b>Using VisualRF .....</b>	<b>257</b>
	<b>Features .....</b>	<b>258</b>
	<b>Useful Terms .....</b>	<b>258</b>
	<b>Starting VisualRF .....</b>	<b>259</b>
	<b>Basic QuickView Navigation .....</b>	<b>259</b>
	Network View Navigation .....	260
	Overlays .....	260
	Display Menu .....	261

Edit Menu.....	262
Mesh View Navigation.....	263
Using the Settings in the VisualRF > Setup Page .....	264
VisualRF Resource Utilization .....	267
Configuring QuickView Personal Preferences.....	268
Increasing Location Accuracy .....	269
Adding Exterior Walls.....	270
Location Training for Stationary Devices .....	270
Adding Client Surveys.....	271
Adding Location Probability Regions.....	272
Adding an IDF.....	273
Viewing Port Status on Deployed Switches.....	274
Fine-Tuning Location Service in VisualRF > Setup .....	274
Configuring Infrastructure.....	275
Deploying APs for Client Location Accuracy.....	276
Using QuickView to Assess RF Environments .....	276
Viewing a Wireless User's RF Environment .....	276
Tracking Location History.....	277
Checking Signal Strength to Client Location.....	278
Viewing an AP's Wireless RF Environment .....	278
Viewing a Floor Plan's RF Environment .....	279
Viewing a Network, Campus, Building's RF Environment .....	280
Viewing Campuses, Buildings, or Floors from a Tree View.....	280
Planning and Provisioning .....	281
Creating a New Campus .....	281
Creating a New Building in a Campus .....	282
Importing a Floor Plan .....	284
Editing a Floor Plan Image .....	284
Cropping the Floor Plan Image.....	284
Sizing a Non-CAD Floor Plan.....	285
Removing Color from a Floor Plan Image.....	285
Assigning Campus, Building and Floor Numbers.....	286
Assigning Optional Planner, Owner, or Installer Information for the Floor Plan .....	286
Controlling the Layers in the Uploaded Floor Plan (CAD only) .....	286
Error Checking of CAD Images.....	286
Last Steps in Editing an Uploaded Image .....	287
Provisioning Existing Access Points onto the Floor Plan.....	287
Automatically Provisioning APs onto a Floor Plan .....	288
Tweaking a Planning Region.....	289
Auto-Matching Planned Devices.....	290
Printing a Bill of Materials Report.....	290
Importing and Exporting in VisualRF .....	291
Exporting a campus .....	291
Importing from CAD .....	291
Batch Importing CAD Files.....	292
Requirements.....	292
Pre Processing Steps .....	292
Upload Processing Steps .....	292
Post Processing Steps .....	293
Sample Upload Instruction XML File .....	293
Common Importation Problems .....	293
Importing from an Aruba Controller .....	293
Pre-Conversion Checklist.....	293
Process on Controller .....	293
Process on AMP .....	294
VisualRF Location APIs .....	294
Sample Device Location Response .....	294

Sample Site Inventory Response .....	294
About VisualRF Plan .....	295
Overview .....	295
Minimum requirements.....	295
Installation .....	296
Differences between VisualRF Plan and VisualRF online.....	296
<b>Appendix A Setting Up Aruba Instant in AirWave .....</b>	<b>297</b>
Overview of Aruba Instant .....	297
Using Aruba Instant with AMP .....	297
Workflow of the Aruba Instant and AMP Integration Process.....	298
Setting up Aruba Instant Hardware.....	298
Required Personnel .....	298
Creating your Organization String .....	298
The Shared Secret Key .....	299
Entering the Organization String and AirWave Information into the IAP .....	299
Receiving the Aruba Instant Virtual Controller as a New Device in AMP .....	300
Verifying the Shared Secret and Adding the Device .....	300
Remaining Manual Admin Tasks in AMP .....	301
AMP Pages with Instant-Specific Features .....	301
Other Available Features .....	302
Firmware Image Management.....	302
Intrusion Detection System .....	302
Known Issues of the Aruba Instant integration with AirWave.....	302
<b>Index.....</b>	<b>303</b>

This preface provides an overview of this user guide and contact information for AirWave Wireless in the following sections:

- “Document Organization” on page 11
- “Note, Caution, and Warning Icons” on page 12
- “Contacting Support” on page 12

## Document Organization

This user guide includes instructions and examples of the graphical user interface (GUI) for installation, configuration, and daily operation of AirWave. This includes wide deployment of wired and wireless devices, rogue detection and classification, security, reports, and additional features.

**Table 1** *Document Organization and Purposes*

Chapter	Description
Chapter 1, “Introduction”	Introduces and presents AirWave, its components, and general network functions.
Chapter 2, “Installing and Getting Started in AirWave”	Describes system and network requirements, Linux OS installation, and AirWave installation.
Chapter 3, “Configuring AMP”	Describes the primary and required configurations for startup and launch of AMP, with frequently used optional configurations.
Chapter 4, “Configuring and Using Device Groups in AMP”	Describes configuration and deployment for group device profiles.
Chapter 5, “Discovering, Adding, and Managing Devices”	Describes how to discover and manage devices on the network.
Chapter 6, “Creating and Using Templates”	Describes and illustrates the use of templates in group and global device configuration.
Chapter 7, “Using RAPIDS and Rogue Classification”	Describes RAPIDS module of AMP, and enhanced rogue classification supported in AMP.
Chapter 8, “Performing Daily Administration in AirWave”	Describes common daily operations and tools in AirWave, to include general user administration, the use of triggers and alerts, network monitoring, and backups.
Chapter 9, “Creating, Running, and Emailing Reports”	Describes AMP reports, scheduling and generation options, and distribution of reports from AMP.
Chapter 10, “Using VisualRF”	Describes how to use VisualRF.
Appendix A, “Setting Up Aruba Instant in AirWave” on page 297	Describes how to set up and use Aruba Instant in AirWave.
Index	Provides extensive citation of and links to document topics, with emphasis on the AMP GUI and tasks relating to AirWave installation and operation.

## Note, Caution, and Warning Icons

This document uses the following note, caution, and warning icons to emphasize advisories for certain actions, configurations, or concepts:



---

Indicates helpful suggestions, pertinent information, and important things to remember.

---



---

Indicates a risk of damage to your hardware or loss of data.

---



---

Indicates a risk of personal injury or death.

---

## Contacting Support

**Table 2** *Support Contact Information*

Main Site	<a href="http://arubanetworks.com">arubanetworks.com</a>
Support Site	<a href="http://support.arubanetworks.com">support.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	<a href="http://arubanetworks.com/support-services/aruba-support-program/contact-support/">arubanetworks.com/support-services/aruba-support-program/contact-support/</a>
Software Licensing Site	<a href="http://licensing.arubanetworks.com/login.php">licensing.arubanetworks.com/login.php</a>
Wireless Security Incident Response Team (WSIRT)	<a href="http://arubanetworks.com/support/wsirt.php">arubanetworks.com/support/wsirt.php</a>
<b>Support Emails</b>	
Americas and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
EMEA	<a href="mailto:emea_support@arubanetworks.com">emea_support@arubanetworks.com</a>
WSIRT Email	<a href="mailto:wsirt@arubanetworks.com">wsirt@arubanetworks.com</a>
Please email details of any security problem found in an Aruba product.	



Thank you for choosing AirWave. AirWave makes it easy and efficient to manage your wireless network by combining industry-leading functionality with an intuitive user interface, enabling network administrators and helpdesk staff to support and control even the largest wireless networks in the world.

This User Guide provides instructions for the installation, configuration, and operation of AirWave. This chapter includes the following topics:

- “AirWave—A Unified Wireless Network Command Center” on page 13
- “Integrating AMP into the Network and Organizational Hierarchy” on page 15

If you have any questions or comments, please contact AirWave support.

### AirWave—A Unified Wireless Network Command Center

AirWave is the only network management software that offers you a single intelligent console from which to monitor, analyze, and configure wireless networks in automatic fashion. Whether your wireless network is simple or a large, complex, multi-vendor installation, AirWave manages it all.

AirWave supports hardware from leading wireless vendors including Alcatel-Lucent, Aruba Networks, Avaya, Cisco (Aironet and WLC), Dell PowerConnect W-Series, Enterasys, Juniper Networks, LANCOM Systems, Meru, Nortel, ProCurve by HP, Proxim, Symbol, Trapeze, Tropos, and many others.

The components of the AirWave are detailed below:

### AirWave Management Platform

The AirWave Management Platform (AMP) is the centerpiece of AirWave, offering the following functions and benefits:

- Core network management functionality:
  - Network discovery
  - Configuration of APs & controllers
  - Automated compliance audits
  - Firmware distribution
  - Monitoring of every device and user connected to the network
  - Real-time and historical trend reports
- Granular administrative access
  - Role-based (for example, Administrator contrasted with Help Desk)
  - Network segment (for example, “Retail Store” network contrasted with “Corporate HQ” network)
- Flexible device support
  - Thin, thick, mesh network architecture
  - Multi-vendor support
  - Current and legacy hardware support

## Aruba Configuration

AirWave supports global and group-level configuration of ArubaOS (AOS), the operating system, software suite, and application engine that operates Aruba mobility and centralizes control over the entire mobile environment. For a complete description of *ArubaOS*, refer to the *ArubaOS User Guide*.

AirWave consolidates and pushes global Aruba configurations from within AMP.

Two pages in AirWave support Aruba Configuration:

- **Device Setup > Aruba Configuration** for global Aruba Configuration
- **Groups > Aruba Config** for group-level Aruba Configuration

For additional information that includes a comprehensive inventory of all pages and settings that support Aruba Configuration, refer to the *Aruba Configuration Guide*.

## VisualRF

VisualRF is a powerful tool for monitoring and managing radio frequency (RF) dynamics within your wireless network, to include the following functions and benefits:

- Accurate location information for all wireless users and devices
- Up-to-date heat maps and channel maps for RF diagnostics
  - Adjusts for building materials.
  - Supports multiple antenna types.
- Floor plan, building, and campus views
- Visual display of errors and alerts
- Easy import of existing floor plans and building maps
- Planning of new floor plans and AP placement recommendations

## RAPIDS

RAPIDS is a powerful and easy-to-use tool for monitoring and managing security on your wireless network, to include the following features and benefits:

- Automatic detection of unauthorized wireless devices
- Rogue device classification that supports multiple methods of rogue detection
- Wireless detection:
  - Uses authorized wireless APs to report other devices within range.
  - Calculates and displays rogue location on VisualRF map.
- Wired network detection:
  - Discovers rogue APs located beyond the range of authorized APs/sensors.
  - Queries routers and switches.
  - Ranks devices according to the likelihood they are rogues.
  - Multiple tests to eliminate false positive results.
  - Provides rogue discovery that identifies the switch and port to which a rogue device is connected.

## Master Console and Failover

The AirWave **Master Console** and **Failover** tools enable network-wide information in easy-to-understand presentation, to entail operational information and high-availability for failover scenarios. The benefits of these tools include the following:

- Provides network-wide visibility, even when the WLAN grows to 50,000+ devices
- Executive Portal allows executives to view high-level usage and performance data
- Aggregated alerts

- Failover
  - Many-to-one failover
  - One-to-one failover

The Master Console and Failover servers can be configured with a **Device Down** trigger that generates an alert if communication is lost. In addition to generating an alert, the Master Console or Failover server can also send email or NMS notifications about the event.

## Integrating AMP into the Network and Organizational Hierarchy

AirWave generally resides in the NOC and communicates with various components of your WLAN infrastructure. In basic deployments, AirWave communicates solely with indoor wireless access points (and WLAN controllers over the wired network. In more complex deployments, AirWave seamlessly integrates and communicates with authentication servers, accounting servers, TACACS+ servers, routers, switches, network management servers, wireless IDS solutions, helpdesk systems, indoor wireless access points, mesh devices. AirWave has the flexibility to manage devices on local networks, remote networks, and networks using Network Address Translation (NAT). AirWave communicates over-the-air or over-the-wire using a variety of protocols.

The power, performance, and usability of AirWave become more apparent when considering the diverse components within a WLAN. [Table 3](#) itemizes some example network components.

**Table 3** *Components of a WLAN*

Component	Description
Autonomous AP	Standalone device which performs radio and authentication functions
Thin AP	Radio-only device coupled with WLAN controller to perform authentication
WLAN controller	Used in conjunction with thin APs to coordinate authentication and roaming
NMS	Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth)
RADIUS Authentication	RADIUS authentication servers (Funk, FreeRADIUS, ACS, or IAS)
RADIUS Accounting	AMP itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+	Used to authenticate AMP administrative users
Routers/Switches	Provide AMP with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR
Rogue APs	Unauthorized APs not registered in the AMP database of managed APs

The flexibility of AirWave enables it to integrate seamlessly into your business hierarchy as well as your network topology. AirWave facilitates various administrative roles to match each individual user's role and responsibility:

- A Help Desk user may be given read-only access to monitoring data without being permitted to make configuration changes.
- A U.S.-based network engineer may be given read-write access to manage device configurations in North America, but not to control devices in the rest of the world.
- A security auditor may be given read-write access to configure security policies across the entire WLAN.
- NOC personnel may be given read-only access to monitoring all devices from the Master Console.



This chapter contains information and procedures for installing and launching AirWave, and includes the following topics:

- “AirWave Hardware Requirements and Installation Media” on page 17
- “Supported Browsers” on page 17
- “Installing Linux CentOS 5 (Phase 1)” on page 18
- “Installing AirWave Software (Phase 2)” on page 18
- “Configuring and Mapping Port Usage for AMP” on page 21
- “AirWave Navigation Basics” on page 22
- “Getting Started with AirWave” on page 28



---

AMP does not support downgrading to older versions. Significant data could be lost or compromised in such a downgrade. In unusual circumstances requiring that you return to an earlier version of AMP, we recommend you perform a fresh installation of the earlier AMP version, and then restore data from a pre-upgrade backup.

---

### AirWave Hardware Requirements and Installation Media

The AirWave installation CD includes all software (including the Linux OS) required to complete the installation of AirWave. AirWave supports any hardware that is Red Hat Enterprise Linux 5 certified. By default, all installs are based on a 64-bit operating system.

AirWave hardware requirements vary by version. As additional features are added to AirWave, increased hardware resources become necessary. For the most recent hardware requirements, refer to the *AirWave Server Sizing Guide*, which you can find in **Home > Documentation**.

AirWave is intended to operate as a soft appliance. Other applications should not run on the same installation. Additionally, local shell users can access data on AirWave, so it is important to restrict access to the shell only to authorized users.

You can create sudo users in place of root for companies that don't allow root logins. For more information, see <http://kb.airwave.com/?sid=50140000000Merd> or contact Aruba support.

### Supported Browsers

Windows (XP, Vista, Windows 7)

- Internet Explorer 7/8/9
- Firefox 3.x
- Google Chrome 9.x (stable)

Mac (OS X, 10.5, 10.6)

- Safari 4.x and higher,
- Firefox 3.x
- Google Chrome 9.x

## Installing Linux CentOS 5 (Phase 1)

Perform the following steps to install the Linux CentOS 5 operating system. The Linux installation is a prerequisite to installing AirWave on the network management system.



---

**Caution:** This procedure erases the hard drive(s) on the server.

---

1. Insert the AirWave installation CD-ROM into the drive and boot the server.
2. If this is a new installation of the AirWave software, type **install** and press **Enter**.  
To configure the partitions manually, type **expert** and press **Enter**.  
The following message appears on the screen:  

```
Welcome to AMP Installer Phase I
- To install a new AMP, type install <ENTER>.
  WARNING: This will ERASE all data on your hard drive.

- To install AMP and manually configure hard drive settings, type expert <ENTER>.

boot:
```
3. Allow the installation process to continue. Installing the CentOS software (Phase I) takes 10 to 20 minutes to complete. This process formats the hard drive and launches Anaconda to install all necessary packages. Anaconda gauges the progress of the installation.  
Upon completion, the system will prompt you to eject the installation CD and reboot the system.
4. Remove the CD from the drive and store in a safe location.

## Installing AirWave Software (Phase 2)

### Getting Started

After the reboot, the GRUB screen appears.

1. Press **Enter** or wait six seconds, and the system automatically loads the kernel.
2. When the kernel is loaded, log into the server using the following credentials:
  - login = **root**
  - password = **admin**
3. Start the AirWave software installation script by executing the **./amp-install** command.  
Type **./amp-install** at the command prompt and press **Enter** to execute the script.

### Step 1: Configuring Date and Time, Checking for Prior Installations

#### Date and Time

The following message appears, and this step ensures the proper date and time are set on the server.

```
----- Date and Time Configuration -----
Current Time: Fri Nov 21 09:18:12 PST 2008
1) Change Date and Time
2) Change Time Zone

0) Finish
```

Ensure that you enter the accurate date and time during this process. *Errors will arise later in the installation if the specified date varies significantly from the actual date, **especially** if the specified*

*date is in the future and it is fixed later.* It is recommended to configure ntpd to gradually adjust your clock to the correct time.

1. Select **1** to set the date and select **2** to set the time zone. Press **Enter** after each configuration to return to the message menu above.



---

**Caution:** Changing these settings after the installation can cause data loss, especially for time-series data such as Client and Usage graphs. Avoid delayed configuration.

---

2. Press **0** to complete the configuration of date and time information, and to continue to the next step.

## Previous AirWave Installations

The following message appears after date and time are set:

```
Welcome to AMP Installer Phase 2
STEP 1:  Checking for previous AMP installations
```

If a previous version of AirWave software is not discovered, the installation program automatically proceeds to [“Step 2: Installing AMP Software” on page 19](#). If a previous version of the software is discovered, the following message appears on the screen.

```
The installation program discovered a previous version of the software. Would you
like to reinstall AMP? This will erase AMP's database. Reinstall (y/n)?
```

Type **y** and press **Enter** to proceed.



---

**Caution:** This action erases the current database, including all historical information. To ensure that the AMP database is backed up prior to reinstallation, answer **n** at the prompt above and contact your Value Added Reseller or directly contact AirWave support.

---

## Step 2: Installing AMP Software

The following message appears while AirWave software is transferred and compiled.

```
STEP 2:  Installing AMP software
This will take a few minutes.
Press Alt-F9 to see detailed messages.
Press Alt-F1 return to this screen.
```

This step requires no user input, but you can follow the instructions to monitor its progress and switch back to the installation screen.

## Step 3: Checking the AirWave Installation

After the AirWave software installation is complete, the following message appears:

```
STEP 3:  Checking AMP installation
Database is up.
AMP is running version: (version number)
```

This step requires no user input. Proceed to the next step as prompted to do so.

## Step 4: Assigning an IP Address to the AirWave System

While the AirWave primary network interface accepts a DHCP address initially during installation, *AirWave does not function when launched unless a static IP is assigned.* Complete these tasks to assign the static IP address. The following message appears:

```
STEP 4: Assigning AMP's address
AMP must be configured with a static IP.

----- Primary Network Interface Configuration -----
1)  IP Address      : xxx.xxx.xxx.xxx
```

```

2) Netmask      : xxx.xxx.xxx.xxx
3) Gateway      : xxx.xxx.xxx.xxx
4) Primary DNS  : xxx.xxx.xxx.xxx
5) Secondary DNS: xxx.xxx.xxx.xxx

9) Commit Changes
0) Exit (discard changes)

```

If you want to configure a second network interface, please use AMP's web interface, AMP Setup --> Network Tab

1. Enter the network information.




---

The Secondary DNS setting is an optional field.

---

2. Commit the changes by typing **9** and pressing **Enter**.  
To discard the changes, type **0** and press **Enter**.

## Step 5: Naming the AirWave Network Administration System

Upon completion of the previous step, the following message appears.

```

STEP 5: Naming AMP
AMP name is currently set to: New AMP
Please enter a name for your AMP:

```

At the prompt, enter a name for your AirWave server and press **Enter**.

## Step 6: Assigning a Host Name to AirWave

Upon completion of the previous step, the following message appears on the screen.

```

STEP 6: Assigning AMP's hostname
Does AMP have a valid DNS name on your network (y/n)?

```

1. If AirWave does not have a valid host name on the network, enter **n** at the prompt. The following appears:

```

Generating SSL certificate for < IP Address >

```

2. If AirWave does have a valid host name on the network, enter **y** at the prompt. The following appears:

```

Enter AMP's DNS name:

```

3. Type the AirWave DNS name and press **Enter**. The following message appears:

```

Generating SSL certificate for < IP Address >

```

Proceed to the next step as the system prompts you.

## Step 7: Changing the Default Root Password

Upon completion of the prior step, the following message appears.

```

STEP 7: Changing default root password.
You will now change the password for the 'root' shell user.

```

```

Changing password for user root.
New Password:

```

Enter the new root password and press **Enter**. The Linux root password is similar to a Windows administrator password. The root user is a super user who has full access to all commands and directories on the computer.



This password should be kept as secure as possible because it allows full access to the machine. This password is not often needed on a day-to-day basis, but is required to perform AirWave upgrades and advanced troubleshooting. If you lose this password, contact AirWave support for resetting instructions.

## Completing the Installation

Upon completion of all previous steps, the following message appears.

```
CONGRATULATIONS! AMP is configured properly.  
To access AMP web console, browse to https://<IP Address>  
Login with the following credentials:  
Username: admin  
Password: admin
```

- To view the Phase 1 installation log file, type **cat /root/install.log**.
- To view the Phase 2 installation log file, type **cat /tmp/amp-install.log**.
- To access the AirWave GUI, enter the AirWave IP address in the address bar of any browser. The AirWave GUI then prompts for your license key. If you are entering a dedicated **Master Console** or AirWave **Failover** license, refer to [“Supporting AMP Servers with the Master Console” on page 220](#) for additional information.

## Configuring and Mapping Port Usage for AMP

The following diagram itemizes the communication protocols and ports necessary for AirWave to communicate with wireless LAN infrastructure devices, including access points (APs), controllers, routers, switches, and RADIUS servers. Assign or adjust port usage on the network administration system as required to support these components.

**Table 4** AirWave Protocol and Port Chart

Port	Type	Protocol	Description	Direction	Device Type
21	TCP	FTP	Firmware distribution	>	APs or controllers
22	TCP	SSH	Configure devices	>	APs or controllers
22	TCP	SSH	Configure AMP from CLI	<	Laptop or workstation
22	TCP	VTUN	Support connection (optional)	>	AirWave support home office
22	TCP	SCP	Transfer configuration files or FW	<	APs or controllers
23	TCP	Telnet	Configure devices	>	APs or controllers
23	TCP	VTUN	Support connection (Optional)	>	AirWave support home office
25	TCP	SMTP	Support email (optional)	>	AirWave support email server
49	UDP	TACACS	AMP Administrative Authentication	>	Cisco TACACS+
53	UDP	DNS	DNS lookup from AMP	>	DNS Server
69	UDP	TFTP	Transfer configuration files or FW	<	APs or controllers
80	TCP	HTTP	Configure devices	>	Legacy APs
80	TCP	VTUN	Support connection (optional)	>	AirWave support home office
161	UDP	SNMP	Get and Set operations	>	APs or controllers
162	UDP	SNMP	Traps from devices	<	APs or controllers
162	UDP	SNMP	Traps from AMP	>	NMS
443	TCP	HTTPS	Web management	<	Laptop or workstation
443	TCP	HTTPS	WLSE polling	>	WLSE

**Table 4** AirWave Protocol and Port Chart (Continued)

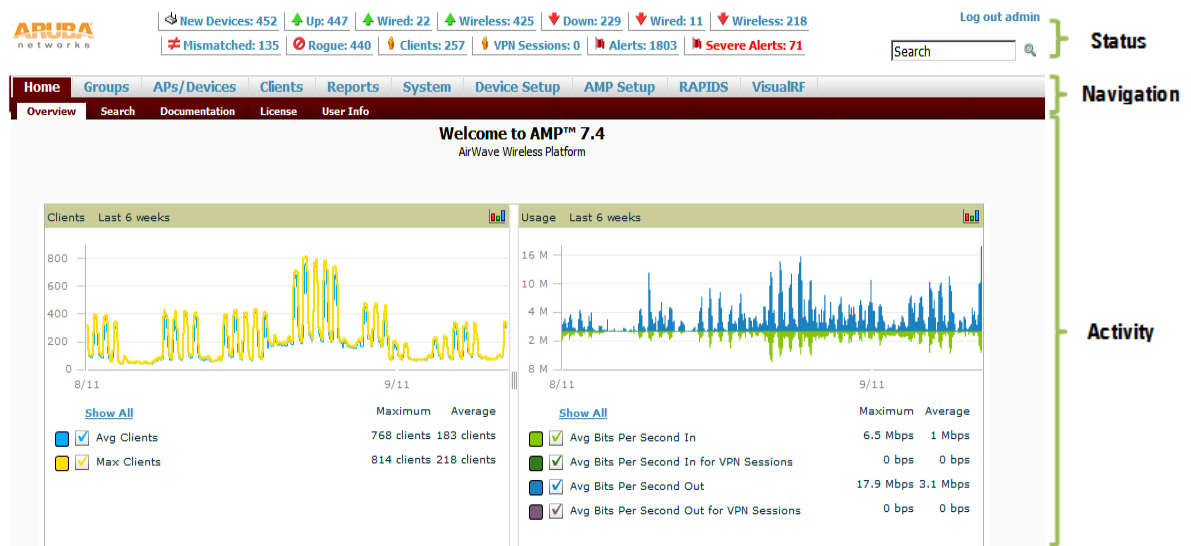
Port	Type	Protocol	Description	Direction	Device Type
443	TCP	VTUN	Support connection (optional)	>	AirWave support home office
1701	TCP	HTTPS	AP and rogue discovery	>	WLSE
1741	TCP	HTTP	WLSE polling	>	WLSE
1812	UDP	RADIUS Auth	Authenticate & authorize AMP administrative users on a RADIUS server.	>	RADIUS auth server
1813	UDP	RADIUS accounting	Retrieve usernames for authenticated WLAN clients from NAS (captive portal, controller, autonomous AP). Only used when usernames are not available in the SNMP MIB of a controller or autonomous AP.	<	RADIUS accounting client
2002	TCP	HTTPS	Retrieve client authentication info	>	ACS
5050	UDP	RTLS	Real Time Location Feed	<	Aruba thin APs
8211	UDP	PAPI	Real Time Feed	< >	WLAN switches
		ICMP	Ping Probe	>	APs or controllers

## AirWave Navigation Basics

Every AirWave page contains three basic sections, as illustrated in [Figure 1](#):

- Status Section
- Navigation Section
- Activity Section

The AirWave pages also contain **Help** links with GUI-specific help information and certain standard buttons.

**Figure 1** Home > Overview Page Illustration

### Status Section

The **Status** section is a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components. AirWave includes the ability to customize the contents of the Status section from the **Home > User Info** page, to include support for both wireless and wired network

components. Refer to [“Configuring Your Own User Information with the Home > User Info Page”](#) on page 213.

The table below describes these elements in further detail.

**Table 5** *Status Section Components of the AMP GUI*

Field	Description
<b>New Devices</b>	The number of wireless APs or wireless LAN controllers that have been discovered by AMP but not yet managed by network administrators. When selected, AMP directs you to a page that displays a detailed list of devices awaiting authorization.
<b>Up</b>	The number of managed authorized devices that are currently responding to AMP requests. When selected, AMP shows a detailed list of all Up devices.
<b>Down</b>	The number of managed, authorized devices that are not currently responding to AMP SNMP requests. When selected, AMP shows a detailed list of all Down devices.
<b>Mismatched</b>	The total number of Mismatched devices. A device is considered mismatched when the desired configuration in AMP does not match the actual device configuration read from the device.
<b>Rogue</b>	The number of devices that have been classified by the RAPIDS rules engine above the threshold defined on the <b>Home &gt; User Info</b> page.
<b>Clients</b>	The number of wireless users currently associated to the wireless network via all the APs managed by AMP. When selected, AMP shows a list of users that are associated. Prior to AMP 7.4, this was called “Users”.
<b>Alerts</b>	Displays the number of non-acknowledged AMP alerts generated by user-configured triggers. When selected, AMP shows a detailed list of active alerts.
<b>Severe Alerts</b> (conditional)	When triggers are given a severity of <b>Critical</b> , they generate <b>Severe Alerts</b> . When a Severe Alert exists, a new component appears at the right of the <b>Status</b> field in bold red font. Only users configured on the <b>Home &gt; User Info</b> page to be enabled to view critical alerts can see Severe Alerts. The functionality of Severe Alerts is the same as that described above for Alerts. Unlike Alerts, the <b>Severe Alerts</b> section is hidden if there are no Severe Alerts.
<b>Device Types to Include in Header Stats</b>	<p>You can support statistics for any combination of the following device types:</p> <ul style="list-style-type: none"> <li>• Autonomous APs</li> <li>• Controllers</li> <li>• Routers/Switches</li> <li>• Thin APs</li> <li>• Others</li> </ul> <p>Refer to <a href="#">“Configuring Your Own User Information with the Home &gt; User Info Page”</a> on page 213.</p>
<b>Search</b>	<p>In the <b>Search</b> field, you can perform partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP of all the APs as well as the client MAC, VPN user, LAN IP, VPN IP fields. Entering a search string displays search in two phases:</p> <ul style="list-style-type: none"> <li>• “Fast” search results - display quickly and divide the results into Clients, APs, Controllers, and Switches, and shows only basic columns relevant to each search category</li> <li>• “Full” search results - accessed by selecting the <b>“Click here to perform a Full Search to expand the results”</b> link at the top of the Fast search results. This action sends the earlier search term to a much deeper search of AMP, expanding the results to include all types of devices, clients (connected and historical), folders, groups, tags, rogue devices, VPN sessions (connected and historical), and rogue clients. You can customize search categories displayed in the Full search in <b>Home &gt; User Info</b>.</li> </ul>

## Navigation Section

The **Navigation** Section displays tabs for all main GUI pages within AirWave. The top bar is a static navigation bar containing tabs for the main components of AirWave, while the lower bar is context-sensitive and displays the subtabs for the highlighted tab.

**Table 6** *Components and Subtabs of the AMP Navigation*

Main Tab	Description	Subtabs
<b>Home</b>	<p>The <b>Home</b> tab provides basic AirWave information including system name, host name, IP address, current time, running time, and software version.</p> <p>The <b>Home</b> page also provides a central point for network status information and monitoring tools, giving graphical display of network activity, and links to many of the most frequent tools in AirWave. For additional information, refer to <a href="#">“Monitoring and Supporting AMP with the Home Pages”</a> on page 209.</p>	<ul style="list-style-type: none"> <li>● Overview</li> <li>● Search</li> <li>● Documentation</li> <li>● License</li> <li>● User Info</li> </ul>
<b>Groups</b>	<p>The <b>Groups</b> pages provide information on the logical “groups” of devices that have been established for efficient monitoring and configuration. For additional information, see <a href="#">Chapter 4, “Configuring and Using Device Groups in AMP”</a> on page 71.</p> <p><b>NOTE:</b> Some of the focused subtabs will not appear for all groups. Focused subtabs are visible based on the device type field on the <b>Groups &gt; Basic</b> page. This subtab is the first page to appear when adding or editing groups.</p> <p><b>NOTE:</b> When individual device configurations are specified, device-level settings override the Group-level settings to which a device belongs.</p>	<ul style="list-style-type: none"> <li>● List</li> <li>● Focused Subtabs <ul style="list-style-type: none"> <li>■ Monitor</li> <li>■ Basic</li> <li>■ Templates</li> <li>■ Security</li> <li>■ SSIDs</li> <li>■ AAA Servers</li> <li>■ Radio</li> <li>■ Aruba Config</li> <li>■ Cisco WLC Config</li> <li>■ PTMP</li> <li>■ Proxim Mesh</li> <li>■ MAC ACL</li> <li>■ Firmware</li> <li>■ Compare</li> </ul> </li> </ul>
<b>APs/Devices</b>	<p>The <b>APs/Devices</b> pages provide detailed information about all authorized APs and wireless LAN switches or controllers on the network, including all configuration and current monitoring data.</p> <p>These pages interact with several additional pages in AirWave. Refer to <a href="#">Chapter 5, “Discovering, Adding, and Managing Devices”</a> on page 107.</p> <p><b>NOTE:</b> When specified, device-level settings override the default Group-level settings.</p>	<ul style="list-style-type: none"> <li>● List</li> <li>● New</li> <li>● Up</li> <li>● Down</li> <li>● Mismatched</li> <li>● Ignored</li> <li>● Focused Subtabs <ul style="list-style-type: none"> <li>■ Monitor</li> <li>■ Manage</li> <li>■ Interfaces</li> <li>■ Audit</li> <li>■ Compliance</li> <li>■ Rogues Contained</li> </ul> </li> </ul>
<b>Clients</b>	<p>The <b>Clients</b> pages provide detailed information about all client devices and users currently and historically associated to the WLAN, including VPN users. Prior to 7.4, this tab was called “Users”. For additional information, refer to <a href="#">“Monitoring and Supporting WLAN Clients”</a> on page 196.</p>	<ul style="list-style-type: none"> <li>● Connected</li> <li>● All</li> <li>● Rogue Clients</li> <li>● Guest Users <ul style="list-style-type: none"> <li>■ Client Detail</li> <li>■ Diagnostics</li> </ul> </li> <li>● VPN Sessions</li> <li>● VPN Users <ul style="list-style-type: none"> <li>■ VPN Client Detail</li> </ul> </li> <li>● Tags</li> </ul>

**Table 6** Components and Subtabs of the AMP Navigation (Continued)

Main Tab	Description	Subtabs
<b>Reports</b>	The <b>Reports</b> pages list all the standard and custom reports generated by AMP. For additional information, refer to <a href="#">Chapter 9, “Creating, Running, and Emailing Reports”</a> on page 227.	<ul style="list-style-type: none"> <li>Generated</li> <li>Definition</li> <li>■Detail</li> </ul>
<b>System</b>	The <b>System</b> page provides information about AirWave operation and administration, including overall system status, the job scheduler, trigger/alert administration, and so forth. For additional information, refer to <a href="#">“Monitoring and Supporting AMP with the System Pages”</a> on page 183.	<ul style="list-style-type: none"> <li>Status</li> <li>Syslog &amp; Traps</li> <li>Event Log</li> <li>Triggers</li> <li>Alerts</li> <li>Backups</li> <li>Configuration Change Jobs</li> <li>Firmware Upgrade Jobs</li> <li>Performance</li> </ul>
<b>Device Setup</b>	The <b>Device Setup</b> pages provide the ability to add, configure, and monitor devices, to include setting AP discovery parameters, performing firmware management, defining VLANs, and so forth. For additional information, refer to <a href="#">“Enabling AirWave to Manage Your Devices”</a> on page 53.	<ul style="list-style-type: none"> <li>Discover</li> <li>Add</li> <li>Communication</li> <li>Aruba Configuration (if global Aruba Configuration is enabled)</li> <li>Upload Firmware &amp; Files</li> </ul>
<b>AMP Setup</b>	The <b>AMP Setup</b> pages provide all information relating to the configuration of AirWave itself and its connection to your network. This page entails several processes, configurations, or tools in AMP. For additional information, start with <a href="#">Chapter 3, “Configuring AMP”</a> on page 29.  <b>NOTE:</b> Some <b>AMP Setup</b> pages may not be visible depending on the role of the logged-in user set in AMP.	<ul style="list-style-type: none"> <li>General</li> <li>Network</li> <li>Users</li> <li>Roles</li> <li>Guest Users</li> <li>Authentication</li> <li>MDM Server</li> <li>Device Type Setup</li> <li>WLSE</li> <li>ACS</li> <li>NMS</li> <li>RADIUS Accounting</li> <li>PCI Compliance</li> </ul>
<b>RAPIDS</b>	The <b>RAPIDS</b> pages provide all information relating to rogue access points, including methods of discovery and lists of discovered and possible rogues. For additional information, refer to <a href="#">Chapter 7, “Using RAPIDS and Rogue Classification”</a> on page 167.  <b>NOTE:</b> The RAPIDS pages may not be visible to the logged-in user, depending on their role set in AMP.	<ul style="list-style-type: none"> <li>Overview</li> <li>List</li> <li>IDS Events</li> <li>Setup</li> <li>Rules</li> <li>Score Override</li> <li>Audit Log</li> </ul>
<b>VisualRF</b>	<b>VisualRF</b> pages provide graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network. Refer to <a href="#">Chapter 10, “Using VisualRF”</a> on page 257.	<ul style="list-style-type: none"> <li>Floor Plans</li> <li>Setup</li> <li>Import</li> <li>Audit Log</li> </ul>



The **AMP Setup** tab varies with user role. The RAPIDS and VisualRF tabs appear based on the license entered on the **Home > License** page, and might not be visible on your AMP view.

## Activity Section

The **Activity** section displays all detailed configuration and monitoring information, and is where you implement changes.

## Help Links in the UI

The **Help** link is available on every page within AirWave. When selected, this launches the *AirWave User Guide* PDF with information describing the AirWave page that is currently displayed.



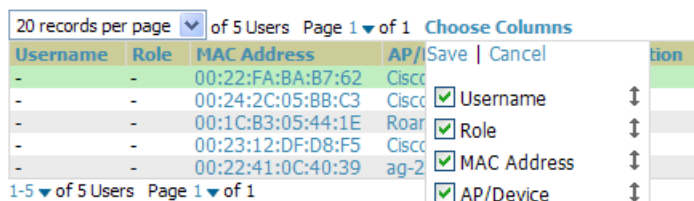
Adobe Reader must be installed to view the settings and default values in the PDF help file.

## Common List Settings

All of the lists in AirWave have some common options. All lists are paginated with a configurable number of items per page. Selecting the **Records Per Page** dropdown menu (which usually looks like a range such as 1-20 on the upper left hand side of a list table) enables you select or enter the number of rows that appear at a time in the list. The next down arrow displays a dropdown menu that allows you to select the exact page you would like to view, as shown in [Figure 2](#).

The **Choose Columns** option, illustrated on [Figure 2](#), allows you to configure the columns that are presented in the list and the order in which they are presented. To disable a column, clear its checkbox. To reorder the columns, drag a row to the appropriate new position. When you are satisfied with the enabled columns and their order, select **Save** at the top of the columns list.

**Figure 2** Common List Settings **Choose Columns** Illustration



These settings are user specific. To reset them, select **Reset List Preferences** on **Home > User Info**.



















## Buttons and Icons

Standard buttons and icons are used throughout AirWave as follows:

**Table 7** Standard Buttons and Icons of the AMP User Page




Function	Image <sup>a</sup>	Description
<b>Acknowledge</b>		Acknowledges and clears an AMP alert.
<b>Add</b>		Adds the object to both AMP's database and the onscreen display list.
<b>Add Folder</b>		Adds a new folder to hierarchically organize APs.
<b>Alert</b>		Indicates an alert.
<b>Apply</b>		Applies all "saved" configuration changes to devices on the WLAN.
<b>Audit</b>		Reads device configuration, compare to desired, and update status.
<b>Choose</b>		Chooses a new Helpdesk incident to be the Current Incident.
<b>Clients</b>		Indicates WLAN users. Select this number to see a list of connected clients.
<b>Create</b>		Creates a new Helpdesk incident.
<b>Customize</b>		Ignores selected settings when calculating the configuration status.
<b>Delete</b>		Deletes an object from AMP's database.
<b>Down</b>		Indicates Down devices and radios.

**Table 7** Standard Buttons and Icons of the AMP User Page (Continued)

Function	Image <sup>a</sup>	Description
<b>Drag and Drop</b>		Dragging and dropping objects with this icon changes the sequence of items in relation to each other. Refer to <a href="#">“Using RAPIDS and Rogue Classification” on page 167</a> as one example of drag-and-drop.
<b>Duplicate</b>		Duplicates or makes a copy of the configuration of an AMP object.
<b>Edit</b>		Edits the object properties.
<b>Email</b>		Links to email reports.
<b>Filter</b> (Funnel icon)		Filters list by values of the selected column. To reset all filters in all columns, click <b>Reset filters</b> link at the bottom of the table.
<b>Google Earth</b>		Views device's location in Google Earth (requires plug-in).
<b>Ignore</b>		Ignores specific device(s) - devices selected with check boxes.
<b>Import</b>		Updates a Group's desired settings to match current settings.
<b>Manage</b>		Manages the object properties.
<b>Mismatched</b>		Indicates mismatched device configuration, in which the most recent configuration in AMP and the current configuration on a device are mismatched.
<b>Monitor</b>		Indicates an access point is in “monitor only” mode.
<b>New Devices</b>		Indicates new access points and devices.
<b>Poll Now</b>		Polls device (or controller) immediately, override group polling settings.
<b>Preview</b>		Displays a preview of changes applicable to multiple groups.
<b>Print</b>		Prints the report.
<b>Reboot</b>		Reboots devices or AMP.
<b>Refresh</b>		Refreshes the display of interactive graphs when settings have changed.
<b>Relate</b>		Relates an AP, Group or Client to a Helpdesk incident.
<b>Replace Hardware</b>		Confers configuration and history of one AP to a replacement device.
<b>Revert</b>		Returns all configurable data on the screen to its original status.
<b>Rogue</b>		Indicates a rogue AP, and links to RAPIDS.
<b>Run</b>		Runs a new user-defined report.
<b>Save</b>		Saves the information on the page in the AMP database.
<b>Save &amp; Apply</b>		Saves changes to AMP's database and apply all changes to devices.
<b>Scan</b>		Scans for devices and rogues using selected networks.
<b>Schedule</b>		Schedules a window for reports, device changes, or maintenance.
<b>Search</b>		Searches AMP for the specified client, device, rogue, group, folder, tag, or session.
<b>Set Time Range</b>		Sets the time range for interactive graphs to the range specified.
<b>Up</b>		Indicates devices which are in the Up status.
<b>Update Firmware</b>		Applies a new firmware image to an AP/device.
<b>Usage</b>		Displays current bandwidth.



**Table 7** Standard Buttons and Icons of the AMP User Page (Continued)

Function	Image <sup>a</sup>	Description
<b>View Historical Graph in New Window</b>		Displays all data series for the selected graph over the last two hours, last day, last week, last month, and last year in one new pop-up window.
<b>VisualIRF</b>		Links to VisualIRF - real time visualization.
<b>XML</b>		Links to export XHTML versions of reports.

a. Not all AMP GUI components are itemized in graphic format in this table.

## Getting Started with AirWave

This topic describes how to perform an initial launch of the AirWave network management solution on the session-based authentication scheme introduced in AirWave 7.3.0.

When an AirWave URL is accessed either interactively using a browser or programmatically using an API, a sent cookie may match a session stored in the database, granting authentication (but not necessarily access, depending on how the user's role matches the required role for the URL). If the cookie is not present or the session in the database has expired, the request is denied.

For browser requests, this results in a login form being displayed. When you submit the login form, the supplied credentials are checked against the AMP's user database, an external RADIUS server, or external TACACS+ server per the AMP's configuration. If the credentials are valid, the user's browser is sent a session cookie to use in subsequent requests.

Use your browser to navigate to the static IP address assigned to the internal page of the AMP, as shown in [Figure 3](#). Enter the User Name and Password as **admin/admin** for your initial login, and then select **Log In**.

**Figure 3** AirWave Login Form

The image shows the AirWave login form. At the top, it says "Welcome to AirWave Management Platform". Below that is the Aruba Networks logo and the "AirWave" text. There are two input fields: "Username" and "Password". Below the "Password" field is a "Log In" button. At the bottom, there are language options: "English", "日本語", and "中文".

If desired, you can set one of the available languages for your login: English and Japanese (Chinese is planned, but not yet complete as of 7.4.0). AirWave will remember your selected language until you log out and select another.

After successful authentication, your browser launches the AirWave **Home > Overview** page.



AirWave pages are protected via SSL. Some browsers will display a confirmation dialog for your self-signed certificate. Signing your certificate will prevent this dialog from displaying. Changing the default login and password on the **AMP Setup > Users** page is recommended. Refer to the procedure [“Creating AirWave User Roles”](#) on [page 46](#) for additional information.



This chapter contains the following procedures to deploy initial AMP configuration:

- “Formatting the Top Header” on page 29
- “Customizing Columns in Lists” on page 30
- “Resetting Pagination Records” on page 31
- “Using the Pagination Widget” on page 31
- “Using Export CSV for Lists and Reports” on page 31
- “Defining Graph Display Preferences” on page 32
- “Customizing the Dashboard” on page 32
- “Setting Severe Alert Warning Behavior” on page 34
- “Defining General AirWave Server Settings” on page 35
- “Defining AirWave Network Settings” on page 43
- “Creating AirWave Users” on page 44
- “Creating AirWave User Roles” on page 46
- “Configuring Login Message, TACACS+ and RADIUS Authentication” on page 49
- “Enabling AirWave to Manage Your Devices” on page 53
- “Setting Up Device Types” on page 59
- “Configuring Cisco WLSE and WLSE Rogue Scanning” on page 59
- “Configuring ACS Servers” on page 64
- “Integrating AirWave with an Existing Network Management Solution (NMS)” on page 65
- “Auditing PCI Compliance on the Network” on page 66
- “Deploying WMS Offload” on page 69




---

Additional configurations of multiple types are available after basic configuration is complete.

---

## Before You Begin

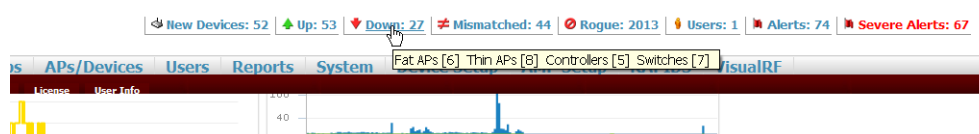
*Remember to complete the required configurations in this chapter before proceeding. AirWave support remains available to you for any phase of AirWave installation.*

## Formatting the Top Header

The AirWave interface centers around a horizontal row of tabs with nested subtabs.

A row of statistics hyperlinks called Top Header Stats above the tabs represents commonly used subtabs. These hyperlinks provide the ability to view certain key statistics by mousing over, such as number and type of **Down** devices, and serve as shortcuts to frequently viewed subtabs. [Figure 4](#) illustrates the navigation bar. For more details on hyperlinks, tabs and subtabs, see “[AirWave Navigation Basics](#)” on page 22.

**Figure 4** Navigation Bar Displaying Down Device Statistics



You can control which **Top Header Stats** links appear from the **AMP Setup > General** page, as described in “[Defining General AirWave Server Settings](#)” on page 35. Top Header Stats can also be customized for individual user on the **Home > User Info** page. There you can select the statistics to display for certain device types, and override the **AMP Setup** page.

All possible display options for users are shown in [Figure 5](#), and these fields are described in detail in “[Configuring Your Own User Information with the Home > User Info Page](#)” on page 213.

**Figure 5** *Home > User Info Top Header Stats Display Options*

You can also set the severity level of critical alerts displayed for a user role. For details including a description of what constitutes a severe alert, see “[Setting Severe Alert Warning Behavior](#)” on page 34.

## Customizing Columns in Lists

Customize the columns for any list table selecting **Choose Columns** as shown in [Figure 6](#). Use the up/down arrows to change the order in which the column heads appear.

**Figure 6** *Choose Columns Dropdown List*

For more information on the universal list elements, see “[Common List Settings](#)” on page 26.

You can also control which column heads appear for each user role by selecting **Yes** in the **Customize Header Columns** field in **Home > User Info**, as also appears in [Figure 5](#). This exposes the **Choose Columns for Roles** dropdown menu in all tables shown in [Figure 7](#).

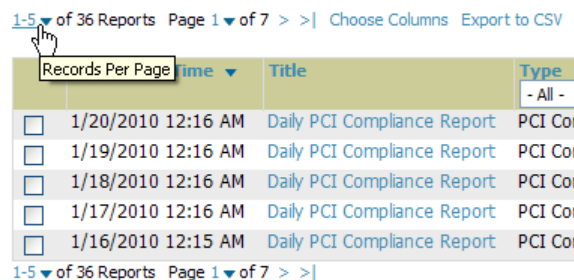
The first column shows the user roles that were customized, if any. The second column allows you to establish left to right columns and order them using the arrows.

**Figure 7** *Table With Choose Columns for Roles Menu Selected*

## Resetting Pagination Records

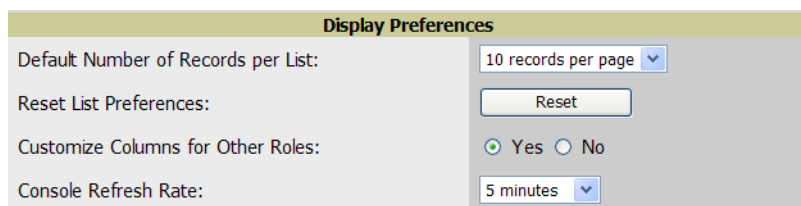
To control the number of records in any individual list, select the link with **Records Per Page** mouseover text at the top left of the table, as shown in [Figure 8](#). AirWave remembers each list table's pagination preferences.

**Figure 8** *Records Per Page* Drop Down Menu



To reset all Records Per Page preferences, select **Reset** in the **Display Preferences** section of the **Home > User Info** page, as shown in [Figure 9](#).

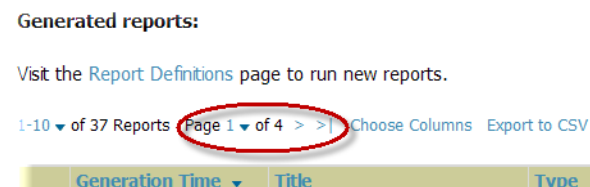
**Figure 9** *Home > User Info Display Preferences* section



## Using the Pagination Widget

The pagination widget is located at the top and bottom of every list table, as shown in [Figure 10](#).

**Figure 10** *Pagination Widget*

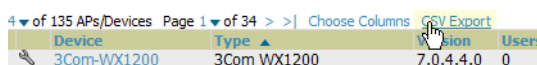


Use the down arrow next to **Page 1** to see all the page numbers for that table in a dropdown menu. From here, you can jump to any portion of the table. Select the **>** symbol to jump to the next page, and **>|** to jump to the last page.

## Using Export CSV for Lists and Reports

Some tables have a **Export CSV** setting you can use export the data as a spreadsheet. See [Figure 11](#) for an example of a list with the **Export CSV** option selected.

**Figure 11** *List with CSV Export Selected*

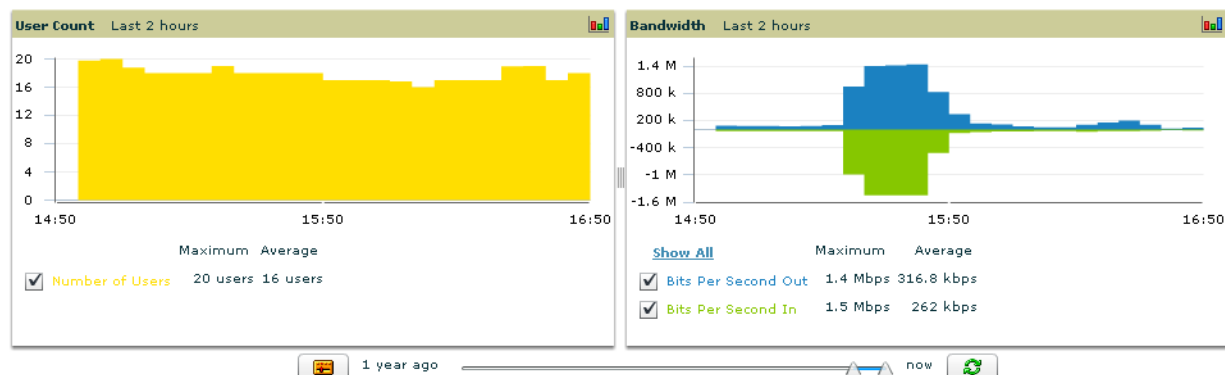


AirWave also enables CSV exporting of all report types. For more information, see “[Exporting Reports to XML or CSV](#)” on page 256.

## Defining Graph Display Preferences

Many of the graphs in AirWave are Flash-based which allows you adjust the graph settings attributes, as shown in [Figure 12](#).

**Figure 12** Interactive Graphs on the **Home > Overview** Page



This Flash-enabled GUI allows for custom settings and adjustments, as follows:

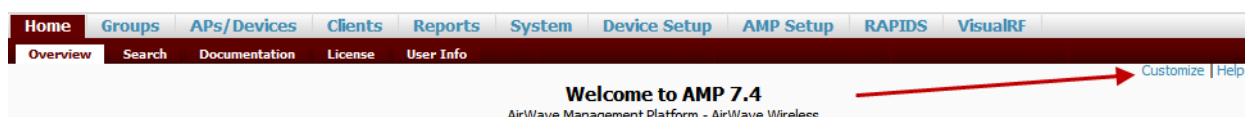
- Drag the slider at the bottom of the screen to move the scope of the graph between one year ago and the current time.
- Drag the slider between graphs to change the relative sizes of each.
- Deselect checkboxes to change the data displayed on each graph. The button with green arrows refreshes data on the graph.
- The **Show All** link displays all of the available checkboxes supporting the Flash graphs.
- Once a change to the slider bars or to the display boxes has been made, the same change can be applied to all other Flash graphs with an **apply** button (appears on mouse-over only).
- For non-Flash graphs, select the graph to open a popup window that shows historical data.

A non-Flash version of the AirWave user page is available if desired; instead of Flash it uses the RRD graphs that were used in earlier versions of AMP. Contact AirWave support for more information on activating this feature in the AirWave database.

## Customizing the Dashboard

You can rearrange or remove widgets appearing on the **Home > Overview** dashboard by selecting the **Customize** link to the right of this window, as shown in [Figure 13](#).


**Figure 13** **Customize** Button on the **Home > Overview** Page

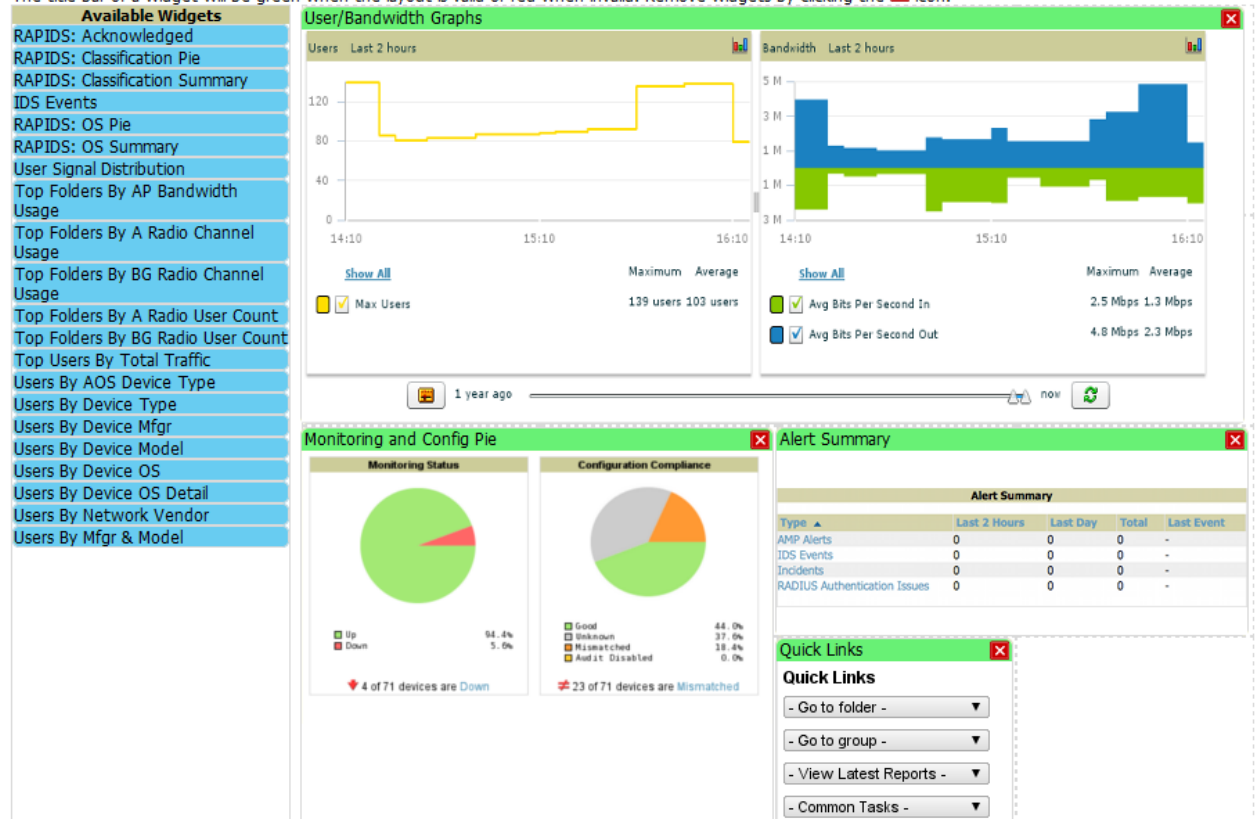


The **Customize** workspace that appears is shown in [Figure 14](#).

**Figure 14 Customize Overview Page**

Drag widgets from the Available Widgets list to the canvas on the right.

The title bar of a widget will be green when the layout is valid or red when invalid. Remove widgets by clicking the  icon.



The **Available Widgets** section on the left with no gridlines holds all possible (available) graphical elements (widgets). Select any blue widget tile with a verbal description enclosed, and it immediately turns into a graphical element with a description.

Drag the widgets you want to appear on the **Overview** dashboard across to the gridlines and arrange them in the right section, within the gridlines. A widget snaps back to the nearest available gridline if you drop it across two or more lines, and turns red if you attempt to place it over gridlines already occupied by widgets.

Green widgets are properly placed and set to appear when you select **Save**. Widgets that remain in the left section will not appear (although they can be reinstated by selecting **Restore Defaults**).

## Customized Search

You can customize the Full search results to display only desired categories of matches on the **Home > User Info** page. Go to the **Search Preferences** section and select **Yes** in the **Customize Search** field, then select or unselect categories of results and save your changes. Customized search is turned off by default, and all boxes are selected.

**Figure 15** *Home > User Info Customized Search Preferences*

**Search Preferences**

Customize Search: ☒ Yes ☐ No

Search Preferences:

- ☒ APs/Devices
- ☒ Clients (Connected)
- ☒ Clients (Historical)
- ☒ VPN Sessions (Connected)
- ☒ VPN Sessions (Historical)
- ☒ Rogue Clients
- ☒ Folders
- ☒ Groups
- ☒ Tags
- ☒ Rogues

[Select All](#) - [Unselect All](#)

## Setting Severe Alert Warning Behavior

You can control the alert levels you can see on the **Alerts** top header stats link from the **Home > User Info** page. When a trigger is assigned a severity of **Critical**, it generates a severe alert. When a severe alert exists, a new component named **Severe Alerts** appears at the right of the **Status** field in bold red font.

Only users who are enabled for viewing critical alerts on the **Home > User Info** page can see severe alerts. The **Severe Alert Threshold** dropdown menu, located in the **Top Header Stats** section of the **Home > User Info** page is shown in [Figure 16](#).

**Figure 16** *Home > User Info > Severe Alert Threshold Dropdown Menu*

**Top Header Stats**

Filter Level For Rogue Count:

Customize Header Columns: ☒ Yes ☐ No

Stats:

- ☒ New Devices
- ☒ Up (Wired & Wireless)
- ☒ Up (Wired)
- ☒ Up (Wireless)
- ☒ Down (Wired & Wireless)
- ☒ Down (Wired)
- ☒ Down (Wireless)
- ☒ Mismatched
- ☒ Rogues
- ☒ Users
- ☒ Alerts
- ☒ Severe Alerts

[Select All](#) - [Unselect All](#)

Severe Alert Threshold:

Include Device Types:

## Defining General AirWave Server Settings

This section describes all pages accessed from the **AMP Setup** tab and describes two pages in the **Device Setup** tab—the **Communication** and **Upload Files** pages. Once required and optional configurations in this chapter are complete, continue to later chapters in this document to create and deploy device groups and device configuration and discovery on the network.

The first step in configuring AirWave is to specify the general settings for the AirWave server. [Figure 17](#) illustrates the **AMP Setup > General** page:

**Figure 17** *AMP Setup > General Page Illustration (Partial View)*

General	
System Name:	AirWave Management Platform
Default Group:	Access Points
Device Configuration Audit Interval:	Daily
Automatically repair misconfigured devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send debugging messages to Aruba Networks:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Nightly Maintenance Time (00:00 - 23:59):	04:15
Check for software updates from Aruba Networks: Periodically check the Aruba Networks website for notices of new software versions or critical security notifications. News will be displayed for admins on the Home Overview page. Software will never be updated automatically.	
<input checked="" type="radio"/> Yes <input type="radio"/> No	

Automatic Authorization	
Add New Controllers and Autonomous Devices Location:	New Device List
Add New Thin APs Location:	New Device List

Top Header	
Stats:	<input checked="" type="checkbox"/> New Devices <input checked="" type="checkbox"/> Up (Wired & Wireless) <input type="checkbox"/> Up (Wired) <input type="checkbox"/> Up (Wireless) <input checked="" type="checkbox"/> Down (Wired & Wireless) <input type="checkbox"/> Down (Wired) <input type="checkbox"/> Down (Wireless) <input checked="" type="checkbox"/> Mismatched <input checked="" type="checkbox"/> Rogues <input checked="" type="checkbox"/> Clients <input type="checkbox"/> VPN Sessions <input checked="" type="checkbox"/> Alerts  <a href="#">Select All - Unselect All</a>
Include device types:	<input checked="" type="checkbox"/> Fat APs <input checked="" type="checkbox"/> Thin APs <input checked="" type="checkbox"/> Controllers <input checked="" type="checkbox"/> Switches <input checked="" type="checkbox"/> Others  <a href="#">Select All - Unselect All</a>

Search Preferences	
Search Preferences:	<input checked="" type="checkbox"/> APs/Devices <input checked="" type="checkbox"/> Clients (Connected) <input checked="" type="checkbox"/> Clients (Historical) <input checked="" type="checkbox"/> VPN Sessions (Connected) <input checked="" type="checkbox"/> VPN Sessions (Historical) <input checked="" type="checkbox"/> Rogue Clients <input checked="" type="checkbox"/> Folders <input checked="" type="checkbox"/> Groups <input checked="" type="checkbox"/> Tags <input checked="" type="checkbox"/> Rogues  <a href="#">Select All - Unselect All</a>

Home Overview Preferences	
Configure Channel Busy Threshold:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Historical Data Retention	
Inactive Client and VPN User Data (0-1500 days, zero disables):	60
Client Association and VPN Session History (0-550 days, zero disables):	14
Tag History (0-550 days, zero disables):	14
Rogue AP Discovery Events (2-550 days, zero disables): <small>Unless this value is 0, it cannot be smaller than the 'Delete Rogues not detected for' window (0) configured on the RAPIDS Setup page.</small>	14
Reports (0-550 days, zero disables):	60
Automatically acknowledge alerts (0-550 days, zero disables):	14
Acknowledged Alerts (0-550 days, zero disables):	60
Radius/ARM/IDS Events (0-550 days, zero disables):	14
Archived Device Configurations (0-100, zero disables):	10
Archive device configs even if they only have rogue classifications:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Guest Users (0-550 days, zero disables):	30
Inactive SSIDs (0-550 days, zero disables):	425
Inactive Interfaces (0-550 days, zero disables):	425
Interface Status History (0-550 days, zero disables):	425
Interfering Devices (0-550 days, zero disables):	14
Device Events (Syslog, Traps) (1-31 days):	2
Device Uptime (0-120 months, zero disables):	60

Firmware Upgrade Defaults	
Allow firmware upgrades in monitor-only mode:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Simultaneous Jobs (1-20):	20
Simultaneous Devices Per Job (1-1000):	20
Failures before stopping (0-20, zero disables):	1

Additional AMP Services	
Enable FTP server: required to manage Aruba AirMesh & Cisco WLC APs; optional for FTP upgrades on supported devices.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable RTLS collector: Aruba only	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use embedded mail server:	<input checked="" type="radio"/> Yes <input type="radio"/> No <a href="#">Send Test Email</a>
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AMON Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Performance	
Monitoring Processes (1-2):	2
Maximum number of configuration processes (1-10):	5
Maximum number of audit processes (1-10):	3
SNMP Fetcher Count (2-6):	2
Verbose logging of SNMP configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No



Perform the following steps to configure AirWave server settings globally across the product (for all users).

1. Browse to the **AMP Setup > General** page, locate the **General** section, and enter the information described in [Table 8](#):

**Table 8 AMP Setup > General > General Section Fields and Default Values**

Setting	Default	Description
<b>System Name</b>		Defines your name for the AirWave server, with a maximum limit of 20 alphanumeric characters.
<b>Automatically monitor/manage new devices</b>	No	<p>Launches a drop-down menu that specifies the behavior AirWave should follow when it discovers a new device. Devices are placed in the default group which is defined in the next field. Choose one of these options:</p> <ul style="list-style-type: none"> <li>● <b>Monitor Only:</b> AirWave compares the current configuration with the policy, and displays any discrepancies on the <b>APs/Devices &gt; Audit</b> page, but does not change the configuration of the device.</li> <li>● <b>Manage Read/Write:</b> AirWave compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy. Automatically placing devices in <b>Managed Read/Write</b> mode will overwrite the configuration with the desired configuration in AirWave, and should only be used when you are certain AirWave has the correct configuration. This can be risky, and generally, devices should be placed in <b>Monitor Only</b> mode as the default.</li> <li>● <b>Thin APs Only:</b> Only thin APs will be automatically authorized in <b>Monitor Only</b> mode. This setting is ideal for mixed environments of thin and autonomous APs, or for very large subnets in which you don't want to auto-monitor all switches.</li> </ul>
<b>Default Group</b>	Access Points	Sets the device group that this AirWave server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the <b>Groups &gt; List</b> page to appear in this drop-down menu. For additional information, refer to <a href="#">Chapter 4, "Configuring and Using Device Groups in AMP"</a> on page 71.
<b>Device Configuration Audit Interval</b>	Daily	<p>If enabled, this setting defines the interval of queries which compares actual device settings to the Group configuration policies stored in the AirWave database. If the settings do not match, the AP is flagged as mismatched and AirWave sends an alert via email, log, or SNMP.</p> <p><b>NOTE:</b> Enabling this feature with a frequency of Daily or more frequently is recommended to ensure that your AP configurations comply with your established policies.</p>
<b>Automatically repair misconfigured devices</b>	Disabled	If enabled, this setting automatically reconfigures the settings on the device when the device is in <b>Manage</b> mode and AirWave detects a variance between actual device settings and the Group configuration policy in the AirWave database.
<b>Send debugging messages</b>	Enabled	If enabled, AirWave automatically emails any system errors to AirWave Support to assist in debugging.
<b>Nightly Maintenance Time (00:00 - 23:59)</b>	04:15	Specifies the local time of day AirWave should perform daily maintenance. During maintenance, AirWave cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
<b>Check for software updates</b>	Yes	Enables AirWave to check automatically for multiple update types. Check daily for AirWave updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct internet connection via AirWave.

2. On the **AMP Setup > General** page, locate the **Automatic Authorization** section. These settings allow you to control the conditions by which devices are automatically authorized into AP groups and



folders. AMP validates the Folder and Group to ensure that both settings have been set to valid dropdown options. [Table 9](#) describes the settings and default values in this section.

**Table 9** *AMP Setup > General > Automatic Authorization Fields and Default Values*

Setting	Default	Description
<b>Add New Controllers and Autonomous Devices Location</b>	New Device List	<p>Globally add new controllers and autonomous devices to:</p> <ul style="list-style-type: none"> <li>The <b>New Devices</b> list (located in <b>APs/Devices &gt; New</b>).</li> <li>The same folder and group as the discovering device.</li> <li>The same group and folder of their closest IP neighbor on the same subnet.</li> <li>Choose a group and folder. If you select this option, enter the folder/group in the <b>Auto Authorization Group</b> and <b>Auto Authorization Folder</b> fields that display.</li> </ul> <p><b>NOTE:</b> This setting can be overridden in <b>Groups &gt; Basic</b>.</p>
<b>Add New Thin APs Location</b>	New Device List	<p>Globally add new thin APs to:</p> <ul style="list-style-type: none"> <li>The <b>New Devices</b> list.</li> <li>The same folder and group as the discovering device.</li> <li>The same group and folder of their closest IP neighbor on the same subnet.</li> <li>Choose a group and folder. If you select this option, enter the folder/group in the <b>Auto Authorization Group</b> and <b>Auto Authorization Folder</b> fields that display.</li> </ul> <p><b>NOTE:</b> This setting can be overridden in <b>Groups &gt; Basic</b>.</p>

- On the **AMP Setup > General** page, locate the **Top Header** section to select the Top Header Stats to be displayed at the top of the interface. For more detailed information about each option, refer to [Table 5 on page 23](#).
- On the **AMP Setup > General** page, locate the **Search Preferences** section. Select the search categories to include in a “Full” search of AMP such APs/devices, clients (connected and/or historical), VPN sessions (connected and/or historical), rogues, rogue clients, tags, folders, and groups. All are selected by default. Per-user search preferences can be set in the **Home > User Info** page; refer to [“Customized Search” on page 34](#).
- On the **AMP Setup > General** page, locate the **Home Overview Preferences** section. [Table 11](#) describes the settings and default values in this section.

**Table 10** *AMP Setup > General > Home Overview Preferences Fields and Default Values*

Setting	Default	Description
<b>Configure Channel Busy Threshold</b>	Yes	Whether you want to configure the threshold at which a channel is considered to be busy at the <b>Top Folders By Radio Channel Usage</b> Overview widget.
<b>Channel Busy Threshold (%)</b>	10	The threshold percent at which the radio channel is considered busier than normal.

- On the **AMP Setup > General** page, locate the **Display** section and select the **Group** tabs and options to appear by default in new device groups.



Changes to this section apply across all of AirWave. These changes affect all users and all new device groups.

Table 11 describes the settings and default values in this section.

**Table 11** *AMP Setup > General > Display Fields and Default Values*

Setting	Default	Description
<b>Use fully qualified domain names</b>	No	Sets AirWave to use fully qualified domain names for APs instead of the AP name. For example, "testap.yourdomain.com" would be used instead of "testap."  This option is supported only for Cisco IOS, Dell PowerConnect W, Aruba Networks, and Alcatel-Lucent devices.
<b>Show vendor-specific device settings for</b>	All Devices	Displays a drop-down menu that determines which <b>Group</b> tabs and options are viewable by default in new groups, and selects the device types that use fully qualified domain names. This field has three options, as follows: <ul style="list-style-type: none"> <li>• <b>All devices</b>—When selected, AirWave displays all Group tabs and setting options.</li> <li>• <b>Only devices on this AMP</b>—When selected, AirWave hides all options and tabs that do not apply to the APs and devices currently on AirWave.</li> <li>• <b>Selected device type</b>—When selected, a new field appears listing many device types. This option allows you to specify the device types for which AirWave displays group settings. You can override this setting.</li> </ul>
<b>Look up wireless user hostnames</b>	Yes	Enables AirWave to look up the DNS for new user hostnames. This setting can be turned off to troubleshoot performance issues.
<b>DNS Hostname Lifetime</b>	24 hours	Defines the length of time, in hours, for which a DNS server hostname remains valid on AirWave, after which AirWave refreshes DNS lookup: <ul style="list-style-type: none"> <li>• 1 hour</li> <li>• 2 hours</li> <li>• 4 hours</li> <li>• 12 hours</li> <li>• 24 hours</li> </ul>
<b>Device Troubleshooting Hint</b>	N/A	The message included in this field is displayed along with the Down if a device's upstream device is up. This applies to all APs and controllers but not to routers and switches.

7. Locate the **Device Configuration** section and adjust the settings. Table 12 describes the settings and default values of this section.

**Table 12** *AMP Setup > General > Device Configuration Section Fields and Default Values*

Setting	Default	Description
<b>Guest User Configuration</b>	Disabled	Enables or prevents guest users to/from pushing configurations to devices. Options are <b>Disabled</b> (default), <b>Enabled for Devices in Manage (Read/Write)</b> , <b>Enabled for all Devices</b> .
<b>Allow WMS Offload configuration in monitor-only mode</b>	No	When <b>Yes</b> is selected, you can enable the ArubaOS WMS offload feature on the <b>Groups &gt; Basic</b> page for WLAN switches in <b>Monitor Only</b> mode. Enabling WMS offload does not cause a controller to reboot. This option is supported only for Aruba and Dell PowerConnect W-Series devices.
<b>Allow disconnecting users while in monitor-only mode</b>	No	Sets whether you can deauthenticate a user for a device in monitor-only mode. If set to <b>No</b> , the <b>Deauthenticate Client</b> button for in a <b>Clients &gt; Client Detail</b> page is enabled only for Managed devices.
<b>Allow non-UTF8 characters</b>	No	Whether AMP can use character sets other than UTF-8 for configuration settings.

**Table 12 AMP Setup > General > Device Configuration Section Fields and Default Values (Continued)**

Setting	Default	Description
<b>Use Global Aruba Configuration</b>	Yes	<p>Enables Aruba configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within <b>Groups &gt; Aruba Config</b> instead of globally.</p> <p><b>NOTE:</b> Changing this setting may require importing configuration on your devices. When an existing Aruba configuration setup is to be converted from global to group, follow these steps:</p> <ol style="list-style-type: none"> <li>1. Set all the devices to Monitor Only mode before setting the flag.</li> <li>2. Each device Group will need to have an import performed from the <b>Audit</b> page of a controller in the AMP group.</li> <li>3. All of the thin APs need to have their settings imported after the device group settings have finished importing.</li> <li>4. If the devices were set to Monitor Only mode, set them back to Managed mode.</li> </ol>

5. Locate the **AMP Features** section and adjust settings to enable or disable VisualRF and RAPIDS. [Table 13](#) describes these settings and default values.

**Table 13 AMP Setup > General > AMP Features Fields and Default Values**

Setting	Default	Description
<b>Display VisualRF</b>	No	Enable or disable the <b>VisualRF</b> navigation tab.
<b>Display RAPIDS</b>	No	Enable or disable the <b>RAPIDS</b> navigation tab.
<b>Hide setup pages from non-admin users</b>	Yes	<p>Restrict access to following pages to users with the <b>AMP Administration</b> role only:</p> <ul style="list-style-type: none"> <li>• <b>VisualRF &gt; Setup</b></li> <li>• <b>AMP Setup &gt; NMS</b></li> <li>• <b>RAPIDS &gt; Score Override</b></li> <li>• <b>RAPIDS &gt; Rules</b></li> <li>• <b>RAPIDS &gt; Setup</b></li> <li>• <b>System &gt; Triggers</b></li> </ul>
<b>Allow role based report visibility</b>	Yes	Enable or disable role-based reporting in AMP. When disabled, reports can only be generated with by-subject visibility.

6. Locate the **External Logging** section and adjust settings to send audit and system events to an external syslog server. [Table 14](#) describes these settings and default values. You can send a test message using the Send Test Message button once any of the logging options are enabled.

**Table 14 AMP Setup > General > External Logging Section Fields and Default Values**

Setting	Default	Description
<b>Include event log messages</b>	No	Select <b>Yes</b> to send event log messages to an external syslog server.
<b>Syslog Server</b>	N/A	Enter the IP address of the syslog server.
<b>Syslog Port</b>	514	Enter the port of the syslog server.
<b>Event log facility</b>	local1	Select the facility for the event log from the drop-down menu.
<b>Include audit log messages</b>	No	Select <b>Yes</b> to send audit log messages to an external syslog server.
<b>Audit log facility</b>	local1	Select the facility for the audit log from the drop-down menu.

7. Locate the **Historical Data Retention** section and specify the number of days you wish to keep client session records and rogue discovery events. [Table 15](#) describes the settings and default values of this section. Many settings can be set to have no expiration date.

**Table 15 AMP Setup > General > Historical Data Retention Fields and Default Values**

Setting	Default	Description
<b>Inactive Client and VPN User Data</b> (0-1500 days, zero disables)	60	Defines the number of days AirWave stores basic information about inactive clients and VPN users. A shorter setting of 60 days is recommended for customers with high user turnover such as hotels. The longer you store inactive user data, the more hard disk space you require.
<b>Client Association and VPN Session History</b> (2-550 days)	14	Defines the number of days AirWave stores client and VPN session records. The longer you store client session records, the more hard disk space you require.
<b>Tag History</b> (2-550 days)	14	Sets the number of days AirWave retains location history for Wi-Fi tags.
<b>Rogue AP Discovery Events</b> (2-550 days)	14	Defines the number of days AirWave stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.
<b>Reports</b> (2-550 days)	60	Defines the number of days AirWave stores Reports. Large numbers of reports, over 1000, can cause the <b>Reports &gt; Generated</b> page to be slow to respond.
<b>Automatically Acknowledge Alerts</b> (0-550 days, zero disables)	14	Defines automatically acknowledged alerts as the number of days AirWave retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function, and alerts will never expire or be deleted from the database.
<b>Acknowledged Alerts</b> (2-550 days)	60	Defines the number of days AirWave retains information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the <b>System &gt; Alerts</b> page to be slow to respond.
<b>Radius/ARM/IDS Events</b> (0-550 days, zero disables)	14	Defines the number of days AirWave retains information about RADIUS, ARM, and IDS events. Setting this value to <b>0</b> disables this function, and the information will never expire or be deleted from the database.
<b>Archive device configs even if they only have rogue classifications</b> (1-100)	No	Sets whether to archive device configurations even if the device only has rogue classifications.
<b>Guest Users</b> (0-550 days, zero disables)	30	Sets the number of days that AirWave is to support any guest user. A value of <b>0</b> disables this function, and guest users will never expire or be deleted from the AirWave database.
<b>Inactive SSIDs</b> (0-550 days, zero disables)	425	Sets the number of days AirWave retains historical information after AirWave last saw a client on a specific SSID. Setting this value to <b>0</b> disables this function, and inactive SSIDs will never expire or be deleted from the database.
<b>Inactive Interfaces</b> (0-550 days, zero disables)	425	Sets the number of days AirWave retains inactive interface information after the interface has been removed or deleted from the device. Setting this value to <b>0</b> disables this function, and inactive interface information will never expire or be deleted from the database.
<b>Interface Status History</b> (0-550 days, zero disables)	425	Sets the number of days AirWave retains historical information on interface status. Setting this value to <b>0</b> disables this function.
<b>Interfering Devices</b> (0-550 days, zero disables)	14	Sets the number of days AirWave retains historical information on interfering devices. Setting this value to <b>0</b> disables this function.
<b>Device Events (Syslog, Traps)</b>	2	Sets the number of days AirWave retains historical information on device events such as syslog entries and SNMP traps. Setting this value to <b>0</b> disables this function. Refer to <a href="#">“Viewing Device Events in System &gt; Syslog &amp; Traps” on page 185</a> .

**Table 15 AMP Setup > General > Historical Data Retention Fields and Default Values (Continued)**

Setting	Default	Description
<b>Device Uptime</b> (0-120 months, zero disables)	60	Sets the number of months AirWave retains historical information on device uptime. Setting this value to <b>0</b> disables this function.

8. Locate the **Firmware Upgrade Defaults** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for AirWave. [Table 16](#) describes the settings and default values of this section.

**Table 16 AMP Setup > General > Firmware Upgrade Defaults Fields and Default Values**

Setting	Default	Description
<b>Allow firmware upgrades in monitor-only mode</b>	No	If <b>Yes</b> is selected, AirWave upgrades the firmware for APs in <b>Monitor Only</b> mode. When AirWave upgrades the firmware in this mode, the desired configuration are not be pushed to AirWave. Only the firmware is applied. The firmware upgrade may result in configuration changes. AirWave does not correct those changes when the AP is in <b>Monitor Only</b> mode.
<b>Simultaneous Jobs</b> (1-20)	20	Defines the number of jobs AirWave runs at the same time. A job can include multiple APs.
<b>Simultaneous Devices Per Job</b> (1-1000)	20	Defines the number of devices that can be in the process of upgrading at the same time. AirWave only runs one TFTP transfer at a time. As soon as the transfer to a device has completed, the next transfer begins, even if the first device is still in the process of rebooting or verifying configuration.
<b>Failures before stopping</b> (0-20)	1	Sets the default number of upgrade failures before AirWave pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to <b>0</b> disables this function.

9. Locate the **Additional AMP Services** section, and adjust settings as required. [Table 17](#) describes the settings and default values of this section.

**Table 17 AMP Setup > General > Additional AMP Services Fields and Default Values**

Setting	Default	Description
<b>Enable FTP Server</b>	No	Enables or disables the FTP server on AMP. The FTP server is only used to manage Cisco Aironet 4800 APs. Aruba recommends disabling the FTP server if you do not have any Cisco Aironet 4800 APs in the network.
<b>Enable RTLS Collector</b>	No	Enables or disables the RTLS Collector, which is used to allow ArubaOS controllers to send signed and encrypted RTLS (real time locating system) packets to VisualRF-- in other words, AirWave becomes the acting RTLS server. The RTLS server IP address must be configured on each controller. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Dell PowerConnect W, Alcatel-Lucent and Aruba Networks devices.  With selection of <b>Yes</b> , the following additional fields appear, which you should populate to match the settings configured on the controller: <ul style="list-style-type: none"> <li>• <b>RTLS Port</b>—Specify the port for the AirWave RTLS server.</li> <li>• <b>RTLS Username</b>—Enter the user name used by the controller to decode RTLS messages.</li> <li>• <b>RTLS Password</b>—Enter the RTLS server password that matches the controllers' value.</li> </ul>
<b>Use embedded mail server</b>	Yes	Enables or disables the embedded mail server that is included with AirWave. This field supports a <b>Send Test Email</b> button for testing server functionality. This button prompts you with a <b>To</b> and <b>From</b> field in which you must enter valid email addresses, and a button to send a test email.
<b>Process user roaming traps from Cisco WLC</b>	Yes	Whether AMP should parse client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.

**Table 17 AMP Setup > General > Additional AMP Services Fields and Default Values (Continued)**

Setting	Default	Description
<b>Enable AMON data collection</b>	Yes	Allows AMP to collect enhanced data from Aruba devices on certain firmware versions; see the <i>Best Practices Guide</i> in <b>Home &gt; Documentation</b> for more details.

10. Locate the **Performance** section. Performance tuning is unlikely to be necessary for many AirWave implementations, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact AirWave support if you think you might need to change any of these settings. [Table 18](#) describes the settings and default values of this section.

**Table 18 AMP Setup > General > Performance Fields and Default Values**

Setting	Default	Description
<b>Monitoring Processes</b>	Based on the number of cores for your server	Optional setting configures the throughput of monitoring data. Increasing this setting allows AirWave to process more data per second, but it can take resources away from other AirWave processes. Contact AirWave support if you think you might need to increase this setting for your network.
<b>Maximum number of configuration processes</b>	5	Increases the number of processes that are pushing configurations to your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact AirWave support if you think you might need to increase this setting for your network.
<b>Maximum number of audit processes</b>	3	Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact AirWave support if you are considering increasing this setting for your network.
<b>Verbose Logging of SNMP Configuration</b>	No	Enables or disables logging detailed records of SNMP configuration information.
<b>SNMP Rate Limiting for Monitored Devices</b>	No	When enabled, AirWave fetches SNMP data more slowly, potentially reducing device CPU load. Aruba recommends enabling this global setting when monitoring Aruba controllers only if your network contains a majority of legacy controllers (800, 2400, 5000, controllers that use Supervisor Module II). If your network mainly uses newer processors (3000 series, 600 series, the M3 module in the 6000 series), Aruba strongly recommends disabling this setting.
<b>RAPIDS Processing Priority</b>	Low	Defines the processing and system resource priority for RAPIDS in relation to AirWave as a whole. When AirWave is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth usage) is not adversely impacted. The default priority is <b>Low</b> . You can also tune your system performance by changing group poll periods.

11. Select **Save** when the **General Server** settings are complete and whenever making subsequent changes.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.



## Defining AirWave Network Settings

The next step in configuring AirWave is to confirm the AirWave network settings. Define these settings by navigating to the **AMP Setup > Network** page. Figure 18 illustrates the contents of this page.

Figure 18 AMP Setup > Network Page Illustration

The screenshot shows the 'AMP Setup > Network' configuration page. It is divided into several sections: 'Primary Network Interface' with fields for IP Address (192.2.2.1), Hostname (corp.server.com), Subnet Mask (255.255.255.0), Gateway (10.0.0.1), Primary DNS IP Address (10.1.1.0), and Secondary DNS IP Address (10.1.1.0); 'Secondary Network Interface' with an 'Enabled' checkbox (set to No); 'Network Time (NTP)' with 'Primary' and 'Secondary' server fields; and 'Static Routes' with a table showing three routes. At the bottom right are 'Save' and 'Revert' buttons.

Network	Subnet Mask	Gateway
0.0.0.0	0.0.0.0	10.2.32.254
192.2.2.1	255.255.255.0	0.0.0.0
192.2.2.20	255.255.0.0	0.0.0.0

Perform the following steps to define the AirWave network settings:

1. Locate the **Primary** and **Secondary Network Interface** sections. The information in these sections should match what you defined during initial network configuration and should not require changes. Table 19 describes the settings and default values.

Table 19 Primary and Secondary Network Interface Fields and Default Values

Setting	Default	Description
IP Address	None	Sets the IP address of the AirWave network interface. <b>NOTE:</b> This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the AirWave server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.
Gateway	None	Sets the default gateway for the network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the network interface.
Secondary Network Interface	No	Select <b>Yes</b> to enable a secondary network interface. You must also define the IP address and subnet mask.

2. On the **AMP Setup > Network** page, locate the **Network Time Protocol (NTP)** section. The Network Time Protocol is used to synchronize the time between AirWave and your network reference NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.



Specifying NTP servers is optional. NTP servers synchronize the time on the AirWave server, not on individual access points.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between AirWave and the NTP servers creates an entry in the event log. Table 20 describes the settings and default values in more detail. For more information on ensuring that AMP servers have the correct time, please see <http://support.ntp.org/bin/view/Servers/NTPPoolServers>.

Table 20 AMP Setup > Network > Secondary Network Fields and Default Values

Setting	Default	Description
Primary	ntp1.yourdomain.com	Sets the IP address or DNS name for the primary NTP server.
Secondary	ntp2.yourdomain.com	Sets the IP address or DNS name for the secondary NTP server.

3. On the **AMP Setup > Network** page, locate the **Static Routes** area. This section displays network, subnet mask, and gateway settings that you have defined elsewhere from a command-line interface.



---

This section does not enable you to configure new routes or remove existing routes.

---

4. Select **Save** when you have completed all changes on the **AMP Setup > Network** page, or select **Revert** to return to the last settings. **Save** restarts any affected services and may temporarily disrupt your network connection.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave configuration.

## Creating AirWave Users

AirWave installs with only one AMP user—the **admin**, who is authorized to:

- define additional users with varying levels of privilege, be it manage read/write or monitoring.
- limit the viewable devices as well as the level of access a user has to the devices.

Each general user that you add needs a **Username**, a **Password**, and a **Role**. Use unique and meaningful user names as they are recorded in the log files when you or other users make changes in AirWave.



---

Username and password are not required if you configure AirWave to use RADIUS or TACACS authentication. You do not need to add individual users to the AirWave server if you use RADIUS or TACACS authentication.

---

The user *role* defines the user type, access level, and the top folder for that user. User roles are defined on the **AMP Setup > Roles** page. Refer to the next procedure in this chapter for additional information, “[Creating AirWave User Roles](#)” on page 46.

The **admin** user can provide optional additional information about the user including the user's real name, email address, phone number, and so forth.

Perform the following steps to display, add, edit, or delete AirWave users of any privilege level. You must be an **admin** user to complete these steps.

1. Go to the **AMP Setup > Users** page. This page displays all users currently configured in AirWave. [Figure 19](#) illustrates the contents and layout of this page.

**Figure 19** *AMP Setup > Users Page Illustration*

The screenshot shows the 'AMP Setup > Users' page. At the top, there are two buttons: 'Add' and 'New User'. Below them is a table with the following columns: Username, Role, Enabled, Type, Access Level, Top Folder, Name, Email Address, Phone, and Notes. The table contains one row for the 'admin' user, with Role 'Administration', Enabled 'Yes', Type 'Administrator', Access Level '-', Top Folder 'Top', and empty fields for Name, Email Address, Phone, and Notes. Below the table, there is a link 'Select All - Unselect All' and a 'Delete' button.

	Username ▲	Role	Enabled	Type	Access Level	Top Folder	Name	Email Address	Phone	Notes
<input type="checkbox"/>	admin	Administration	Yes	Administrator	-	Top	-	-	-	-

Select All - Unselect All

Delete



2. Select **Add** to create a new user, select the pencil icon to edit an existing user, or select a user and select **Delete** to remove that user from AirWave. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 20.

**Figure 20** AMP Setup > Users > Add/Edit User Page Illustration

3. Enter or edit the settings on this page. Table 21 describes these settings in additional detail.

**Table 21** AMP Setup > Users > Add/Edit User Fields and Default Values

Setting	Default	Description
<b>Username</b>	None	Sets the username as an alphanumeric string. The Username is used when logging in to AirWave and appears in AirWave log files.
<b>Role</b>	None	Specifies the <b>User Role</b> that defines the Top viewable folder, type and access level of the user specified in the previous field. The <b>admin</b> user defines user roles on the <b>AMP Setup &gt; Roles</b> page, and each user in the system is assigned to a role.
<b>Password</b>	None	Sets the password for the user being created or edited. Enter an alphanumeric string without spaces, and enter the password again in the <b>Confirm Password</b> field. <b>NOTE:</b> Because the default user's password is identical to the name, it is <b>strongly recommended that you change this password</b> .
<b>Name</b>	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.
<b>Email Address</b>	None	Allows you to specify a specific email address that will propagate throughout many additional pages in AirWave for that user, including reports, triggers, and alerts.
<b>Phone</b>	None	Allows you to enter an optional phone number for the user.
<b>Notes</b>	None	Enables you to cite any additional notes about the user, including the reason they were granted access, the user's department, or job title.

4. Select **Add** to create the new user, **Save** to retain changes to an existing user, or **Cancel** to cancel out of this screen. The user information you have configured appears on the **AMP Setup > Users** page and the user propagates to all other AirWave pages and relevant functions.



AirWave enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support a subset of accounts or sites within a single AirWave deployment, such as help desk or IT staff.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Creating AirWave User Roles

The **AMP Setup > Roles** page defines the viewable devices, the operations that can be performed on devices, and general AirWave access. VisualRF uses the same user roles as defined for AirWave—users can see floor plans that contain an AP to which they have access in AirWave, although only visible APs appear on the floor plan.

Users can also see any building that contains a visible floor plan, and any campus that contains a visible building.



In **VisualRF > Setup > Server Settings**, a new flag added in AirWave 7.2 allows you to restrict the visibility of empty floor plans to the role of the user who created them. In previous versions, a floor plan without APs could be visible to all users. By default, this setting is set to No.

When a new role is added to AirWave, VisualRF must be restarted for the new user to be enabled. Refer to [Chapter 10, “Using VisualRF” on page 257](#) for additional information.

User **roles** can be created that have access to folders within multiple branches of the overall hierarchy. This feature assists non-administrative users, such as help desk or IT staff, who support a subset of accounts or sites within a single AirWave deployment. You can restrict user roles to multiple folders within the overall hierarchy even if they do not share the same top-level folder. Non-admin users are only able to see data and users for devices within their assigned subset of folders.

Perform the following steps to view, add, edit, or delete user **roles**:

1. Go to the **AMP Setup > Roles** page. This page displays all roles currently configured in AirWave. [Figure 21](#) illustrates the contents and layout of this page.

**Figure 21** *AMP Setup > Roles Page Illustration*

Add		New Role							
	Name ▲	Enabled	Type	Access Level	Top Folder	Visible Groups	RAPIDS	VisualRF	Helpdesk
<input type="checkbox"/>	My role	Yes	Guest Access Sponsor	-	Top	-	None	Read Only	No
<input type="checkbox"/>	Administration	Yes	Administrator		Top	All	Read/Write	Read/Write	Yes
<input type="checkbox"/>	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	All	None	Read Only	No

Select All - Unselect All

Delete

2. Select **Add** to create a new role, select the pencil icon to edit an existing role, or select a checkbox and select **Delete** to remove that role from AirWave. When you select **Add** or the edit icon, the **Add/Edit Role** page appears, illustrated in [Figure 22](#).

**Figure 22** *AMP Setup > Roles > Add/Edit Role Page Illustration*

**Role**

Name:

Enabled: ☒ Yes ☐ No

Type:

AP/Device Access Level:

Top Folder:

RAPIDS:

VisualRF:

Helpdesk: ☐ Yes ☒ No

**Guest User Preferences**

Allow creation of Guest Users: ☒ Yes ☐ No

Allow accounts with no expiration: ☒ Yes ☐ No

Allow sponsor to change sponsorship username: ☐ Yes ☒ No

Custom Message:

3. Enter or edit the settings on this page. [Table 22](#) describes these settings in additional detail.

As explained earlier in this section, **Roles** define the type of user-level access, the user-level privileges, and the view available to the user for device groups and devices in AirWave. [Table 22](#) describes the settings and default values of this section.

**Table 22** *AMP Setup > Roles > Add/Edit Roles Fields and Default Values*

Setting	Default	Description
<b>Name</b>	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
<b>Enabled</b>	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AirWave.
<b>Type</b>	AP/Device Manager	Defines the type of role. AirWave supports the following role types: <ul style="list-style-type: none"> <li>• <b>AMP Administrator</b>—The AMP Administrator has full access to AirWave and all of the devices. Only the AMP Administrator can create new users or access the <b>AMP Setup</b> page, the <b>VisualRF &gt; Setup</b> page, <b>VisualRF &gt; Audit Log</b> page, <b>System &gt; AMP Events</b>, and <b>System &gt; Performance</b>.</li> <li>• <b>AP/Device Manager</b>—AP/Device Managers have access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level.</li> <li>• <b>AirWave Management Client</b>—The AirWave Management Client (AMC) software allows WiFi-enabled devices to serve as additional sensors to gather data for RAPIDS. Use this role type to set up a client to be treated as a user with the AMC role. The user information defined in AMC must match the user with the Aruba Management Client type.</li> <li>• <b>Guest Access Sponsor</b>—Limited-functionality role to allow helpdesk or reception desk staff to grant wireless access to temporary personnel. This role only has access to the defined top folder of APs.</li> </ul>

**Table 22 AMP Setup > Roles > Add/Edit Roles Fields and Default Values (Continued)**

Setting	Default	Description
<b>AP/Device Access Level</b>	None	<p>Defines the privileges the role has over the viewable APs. AirWave supports three privilege levels, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Manage (Read/Write)</b>—Manage users can view and modify devices and Groups. Selecting this option causes a new field, <b>Allow authorization of APs/Devices</b>, to appear on the page, and is enabled by default.</li> <li>• <b>Audit (Read Only)</b>—Audit users have read only access to the viewable devices and Groups. Audit users have access to the <b>APs/Devices &gt; Audit</b> page, which may contain sensitive information including AP passwords.</li> <li>• <b>Monitor (Read Only)</b>—Monitor users have read-only access to devices and groups and VisualRF. Monitor users cannot view the <b>APs/Devices &gt; Audit</b> page which may contain sensitive information, including passwords.</li> </ul>
<b>Top Folder</b>	None	<p>Defines the Top viewable folder for the role. The role is able to view all devices and groups contained by the Top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view.</p> <p><b>NOTE:</b> AirWave enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support a <i>subset of accounts or sites</i> within a single AirWave deployment, such as help desk or IT staff.</p> <p>User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.</p>
<b>RAPIDS</b>	None	<p>Sets the RAPIDS privileges, which are set separately from the APs/Devices. This field specifies the RAPIDS privileges for the role, and options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>None</b>— Cannot view the RAPIDS tab or any Rogue APs.</li> <li>• <b>Read Only</b>— The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans.</li> <li>• <b>Read/Write</b>—The user may edit individual rogues, classification, threat levels and notes, and perform OS scans.</li> <li>• <b>Administrator</b>—Has the same privileges as the Read/Write user, but can also set up RAPIDS rules, override scores, and is the only user who can access the <b>RAPIDS &gt; Setup</b> page.</li> </ul>
<b>VisualRF</b>	None	<p>Sets the VisualRF privileges, which are set separately from the APs/Devices, for this role. Options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Read Only</b>— The user can view the VisualRF pages but cannot make any changes to floor plans.</li> <li>• <b>Read/Write</b>—The user may edit individual floor plans, buildings, and campuses.</li> </ul>
<b>Aruba Controller Role</b>	No	<p>Enables or disables <b>Single Sign-On</b> for the role. If enabled, allows the role to directly access Aruba controller UIs from the Quick Links or IP Address hypertext throughout AMP without having to enter credentials for the controller.</p>
<b>Display client diagnostics screens by default</b>	No	<p>Sets the role to support helpdesk users, with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network.</p>
<b>Enable Adobe Flash</b>	Yes	<p>Enables the Adobe Flash application for all users who are assigned this role. Adobe Flash supports interactive graphics on the <b>Home &gt; Overview</b> page, VisualRF, QuickView functions, the <b>Radio Statistics</b> page for thin AP radios, and additional AirWave pages.</p> <p><b>NOTE:</b> This field is only visible if a specific flag is set in the AirWave database. By default this option is hidden and Flash is enabled for all users.</p>
<b>Allow creation of Guest Users</b>	Yes	<p>If this option is enabled, users with an assigned role of Monitoring or Audit can be given access to guest user account creation along with the option to allow a sponsor to change its username. A custom message can also be included. The <b>Guest User Preferences</b> section does not appear if Guest User Configuration is disabled in <b>AMP Setup &gt; General</b>.</p>

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.

- Complete the required configurations in this chapter before proceeding. AirWave support remains available to you for any phase of AirWave configuration.

## Configuring Login Message, TACACS+ and RADIUS Authentication

As of 7.3, AMP uses session-based authentication with a configurable login message and idle timeout. As an option, you can set AirWave to use an external user database to simplify password management for AirWave administrators and users. This section contains the following procedures to be followed in **AMP Setup > Authentication**:

- [Setting Up Login Configuration Options](#)
- [Setting Up Login Configuration Options](#)
- [Configuring RADIUS Authentication and Authorization](#)
- [Integrating a RADIUS Accounting Server](#)

### Setting Up Login Configuration Options

Administrators can optionally configure AMP's user idle timeout or a message-of-the-day that appears when a user first logs in, as shown in [Figure 23](#):

**Figure 23** Login configuration field and results in AMP Login page



1. Go to **AMP Setup > Authentication**.
2. Complete the fields described on [Table 23](#):

**Table 23** Login Configuration section of **AMP Setup > Authentication**

Field	Default	Description
<b>Max AMP User Idle Timeout</b>	60	Number of minutes of idle time until AMP automatically ends the user session. Affects all users of this AMP. The range is 5-240 minutes.
<b>Login message</b>		A persistent message that will appear for all of this AMP's users after they log in.

3. Select Save if you are finished, or you can follow the next procedure to configure Single Sign-On, TACACS+ and RADIUS Authentication options.

### Setting up Single Sign-On

Administrators can set up single sign-on (SSO) for users that have access to Aruba controllers. This allows users to log in to an AMP and use the IP Address or Quick Links hypertext links across AMP to access the controller's UI, without having to enter credentials again. The links the user can select to access a controller can be found on the **APs/Devices > Monitor** page in the **Device Info** section, and on device list pages.

This feature must be enabled per role in **AMP Setup > Roles**.

To enable this feature for this AMP, locate the **Single Sign-On** section in **AMP Setup > Authentication**. In the **Enable Single Sign-On** field, select **Yes**. Then select **Save** if you are finished, or you can follow the next procedure to configure TACACS+ and RADIUS Authentication options.

## Configuring TACACS+ Authentication

For TACACS+ capability, you must configure the IP/Hostname of the TACACS+ server, the TCP port, and the server shared secret. This TACACS+ configuration is for AirWave users, and does not affect APs or users logging into APs.

1. Go to the **AMP Setup > Authentication** page. This page displays current status of TACACS+. [Figure 24](#) illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in AirWave.

**Figure 24** TACACS+ section **AMP Setup > Authentication**

2. Select **No** to disable or **Yes** to enable TACACS+ authentication. If you select **Yes**, several new fields appear. Complete the fields described in [Table 24](#).

**Table 24** **AMP Setup > Authentication** Fields and Default Values

Field	Default	Description
<b>Primary Server Hostname/IP Address</b>	N/A	Enter the IP address or the hostname of the primary TACACS+ server.
<b>Primary Server Port</b>	49	Enter the port for the primary TACACS+ server.
<b>Primary Server Secret</b>	N/A	Specify and confirm the primary shared secret for the primary TACACS+ server.
<b>Secondary Server Hostname/IP Address</b>	N/A	Enter the IP address or hostname of the secondary TACACS+ server.
<b>Secondary Server Port</b>	49	Enter the port for the secondary TACACS+ server.
<b>Secondary Server Secret</b>	N/A	Enter the shared secret for the secondary TACACS+ server.

3. Select **Save** and continue with additional steps.
4. To configure Cisco ACS to work with AirWave, you must define a new service named **AMP** that uses https on the ACS server.
  - The AMP https service is added to the **TACACS+** (Cisco) interface under the **Interface Configuration** tab.
  - Select a checkbox for a new service.
  - Enter **AMP** in the service column and **https** in the protocol column.
  - Select **Save**.
5. Edit the existing groups or users in TACACS to use the “AMP service” and define a role for the group or user.

- The role defined on the **Group Setup** page in ACS must match the exact name of the role defined on the **AMP Setup > Roles** page.
- The defined role should use the following format: **role=<name\_of\_AMP\_role>**. One example is as follows:

```
role=DormMonitoring
```

As with routers and switches, AirWave does not need to know usernames.

- AirWave also needs to be configured as an AAA client.
  - On the **Network Configuration** page, select **Add Entry**.
  - Enter the IP address of AirWave as the **AAA Client IP Address**.
  - The secret should be the same value that was entered on the **AMP Setup > TACACS+** page.
- Select **TACACS+** (Cisco IOS) in the **Authenticate Using** drop down menu and select **submit + restart**.



AirWave checks the local username and password store before checking with the TACACS+ server. If the user is found locally, the local password and local role apply. When using TACAS+, it is not necessary or recommended to define users on the AirWave server. The only recommended user is the backup administrator, in the event that the TACAS+ server goes down.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Configuring RADIUS Authentication and Authorization

For RADIUS capability, you must configure the IP/Hostname of the RADIUS server, the TCP port, and the server shared secret. Perform these steps to configuration RADIUS authentication:

- Go to the **AMP Setup > Authentication** page. This page displays current status of RADIUS. [Figure 25](#) illustrates this page.

**Figure 25** *AMP Setup > Authentication Page Illustration*

- Select **No** to disable or **Yes** to enable TACACS+ or RADIUS authentication. If you select **Yes**, several new fields appear. Complete the fields described in [Table 25](#).

**Table 25** *AMP Setup > Authentication Fields and Default Values*

Field	Default	Description
<b>Primary Server Hostname/IP Address</b>	N/A	Enter the IP address or the hostname of the primary RADIUS server.
<b>Primary Server Port</b>	1812	Enter the TCP port for the primary RADIUS server.
<b>Primary Server Secret</b>	N/A	Specify and confirm the primary shared secret for the primary RADIUS server.



**Table 25 AMP Setup > Authentication Fields and Default Values (Continued)**

Field	Default	Description
<b>Secondary Server Hostname/IP Address</b>	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
<b>Secondary Server Port</b>	1812	Enter the TCP port for the secondary RADIUS server.
<b>Secondary Server Secret</b>	N/A	Enter the shared secret for the secondary RADIUS server.

3. Select **Save** to retain these configurations, and continue with additional steps in the next procedure.



For instructions on setting up a RADIUS server, please see <http://www.airwave.com/support/knowledge-base/?sid=5014000000Mer6> in the AirWave knowledge base.

## Integrating a RADIUS Accounting Server



AirWave checks the local username and password before checking with the RADIUS server. If the user is found locally, the local password and role apply. When using RADIUS, it's not necessary or recommended to define users on the AirWave server. The only recommended user is the backup admin, in case the RADIUS server goes down.

Optionally, you can configure RADIUS server accounting on **AMP Setup > RADIUS Accounting**. This capability is not required for basic AirWave operation, but can increase the user-friendliness of AirWave administration in large networks. [Figure 26](#) illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable AirWave to receive accounting records from a separate RADIUS server. [Figure 26](#) illustrates the display of RADIUS accounting clients already configured, and [Figure 27](#) illustrates the **Add RADIUS Accounting Client** page.

**Figure 26 AMP Setup > RADIUS Accounting Page Illustration**

IP/Network	Nickname
<input type="checkbox"/> 10.0.0.0/8	test
<input type="checkbox"/> 10.11.0.0/16	off_site_network

[Check All - Uncheck All](#)

**Figure 27 AMP Setup > RADIUS > Add RADIUS Accounting Client Page Illustration**

**RADIUS Accounting Client**

IP/Network:  
Example Network entry: 10.0.0.0/8

Nickname:

Shared Secret:

Confirm Shared Secret:

1. To specify the RADIUS authentication server or network, browse to the **AMP Setup > RADIUS Accounting** page and select **Add**, illustrated in [Figure 27](#), and provide the information in [Table 26](#).



2. Select **Add**, then complete the following fields:

**Table 26 AMP Setup > Radius Accounting Fields and Default Values**

Setting	Default	Description
<b>Nickname</b>	None	Sets a user-defined name for the authentication server.
<b>IP/Network</b>	None	Cites the IP address or DNS Hostname for the authentication server if you only want to accept packets from one device. To accept packets from an entire network enter the IP/Netmask of the network (for example, 10.51.0.0/24).
<b>Shared Secret (Confirm)</b>	None	Sets the Shared Secret that is used to establish communication between AirWave and the RADIUS authentication server.

## What Next?

- Go to additional subtabs in **AMP Setup** to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Enabling AirWave to Manage Your Devices

Once AirWave is installed and active on the network, the next task is to define the basic settings that allow AirWave to communicate with and manage your devices. Device-specific firmware files are often required or are highly desirable. Furthermore, the use of Web Auth bundles is advantageous for deployment of Cisco WLC wireless LAN controllers when they are present on the network.

This section contains the following procedures:

- [Configuring Communication Settings for Discovered Devices](#)
- [Loading Device Firmware Onto AirWave \(optional\)](#)
  - [Overview of the Device Setup > Upload Firmware & Files Page](#)
  - [Loading Firmware Files to AirWave](#)

## Configuring Communication Settings for Discovered Devices

To configure AirWave to communicate with your devices, to define the default shared secrets, and to set SNMP polling information, navigate to the **Device Setup > Communication** page, illustrated in [Figure 28](#).

**Figure 28** *Device Setup > Communication Page Illustration*

**Default Credentials**

The credentials below are used to communicate with devices that are discovered by AMP (regardless of the credentials used for discovery). Changing these credentials does not affect APs that are already being managed or are already in the *New Devices* list.

Device Model	Edit	View
3Com		
3Com 8750		
APC		
Alcatel-Lucent		
Aruba		
Avaya		
BeAir		
Cisco Aironet 4800		
Cisco IOS AP		
Cisco Switch		
Cisco VxWorks		
Cisco WLC		
Columbus		
Custom Device		
D-Link		
Dell		
Enterasys		
Enterasys RoamAbout AP2000		
Enterasys RoamAbout AP3000/AP4102		
Enterasys RoamAbout R2		
Foundry		
HP ProCurve 420		
HP ProCurve 520WL		
HP ProCurve 530		

**SNMP Settings**

SNMP Timeout (3-60 sec):

SNMP Retries (1-20):

**SNMPv3 Informs**

[Add](#) [New SNMPv3 User](#)

1-1 of 1 SNMPv3 Users Page 1 of 1 [Choose Columns](#)

Username	Auth Protocol	Priv Protocol
v3informuser	SHA	DES

1-1 of 1 SNMPv3 Users Page 1 of 1

[Select All](#) [Unselect All](#)

[Delete](#)

**Telnet/SSH Settings**

Telnet/SSH Timeout (3-120 sec):

**HTTP Discovery Settings**

HTTP Timeout (3-120 sec):

**ICMP Settings**

Attempt to ping devices that were unreachable via SNMP: ☒ Yes ☐ No

**Cisco Aironet VxWorks User Creation Options**

☒ Do not modify security/SNMP settings

☐ Create and use a specified user

**Symbol 4131/Intel 2011B, Cisco Aironet IOS and Nomadix AG2000w SNMP Initialization**

Upon authorization into read-write manage mode, AMP can enable read-write SNMP on a device using telnet commands for Cisco IOS and Nomadix devices and using the web interface for Symbol 4131/Intel 2011B devices.

☒ Do not modify SNMP settings

☐ Enable read-write SNMP

[Save](#) [Revert](#)

Perform the following steps to define the default credentials and SNMP settings for the wireless network.

1. On the **Device Setup > Communication** page, locate the **Default Credentials** area. Enter the credentials for each device model on your network. The default credentials are assigned to all newly discovered APs.

The **Edit** button edits the default credentials for newly discovered devices. To modify the credentials for existing devices, use the **APs/Devices > Manage** page or the **Modify Devices** link on the **APs/Devices > List** page.



Community strings and shared secrets must have read-write access for AirWave to configure the devices. Without read-write access, AirWave may be able to monitor the devices but cannot apply any configuration changes.

2. Browse to the **Device Setup > Communication** page, locate the **SNMP Settings** section, and enter or revise the following information. [Table 27](#) lists the settings and default values.

**Table 27** *Device Setup > Communication > SNMP Settings Fields and Default Values*

Setting	Default	Description
<b>SNMP Timeout</b>	3	Sets the time, in seconds, that AirWave waits for a response from a device after sending an SNMP request.

**Table 27** *Device Setup > Communication > SNMP Settings Fields and Default Values (Continued)*

Setting	Default	Description
<b>SNMP Retries</b>	3	Sets the number of times AirWave tries to poll a device when it does not receive a response within the <b>SNMP Timeout Period</b> or the Group's <b>Missed SNMP Poll Threshold</b> setting (1-100). If AirWave does not receive an SNMP response from the device after the specified number of retries, AirWave classifies that device as <b>Down</b> .

3. Locate the **SNMP v3 Informs** section. Select **Add New SNMP v3 User** to reveal its configuration section. AMP users will need to configure all v3 users that are configured on the controller; the SNMP Inform receiver in the AMP will be restarted when users are changed or added to the controller.
  - **Username** - Username of the SNMP v3 user as configured on the controller.
  - **Auth Protocol** - Can be MD5 or SHA. The default setting is SHA.
  - **Auth and Priv Passphrases** - Enter the auth and priv passphrases for the user as configured on the controller.
  - **Priv Protocol** - Can be DES or AES. The default setting is DES.
4. Locate the **Telnet/SSH Settings** section, and complete or adjust the default value for the field. [Table 28](#) shows the setting and default value.

**Table 28** *Device Setup > Communication > Telnet/SSH Settings Fields and Default Values*

Setting	Default	Description
<b>Telnet/SSH Timeout</b> (3-120 sec)	10	Sets the timeout period in seconds used when performing Telnet and SSH commands.

5. Locate the **HTTP Discovery Settings** section and adjust the default value. [Table 29](#) shows the setting and default value.

**Table 29** *Device Setup > Communication > HTTP Discovery Settings Fields and Default Values*

Setting	Default	Description
<b>HTTP Timeout</b> (3-120 sec)	5	Sets the timeout period in seconds used when running an HTTP discovery scan.

6. Locate the **ICMP Settings** section and adjust the default value as required. [Table 30](#) shows the setting and default value.

**Table 30** *Device Setup > Communication > ICMP Settings Fields and Default Values*

Setting	Default	Description
<b>Attempt to ping devices that were unreachable via SNMP</b>	Yes	<ul style="list-style-type: none"> <li>• When <b>Yes</b> is selected, AirWave attempts to ping the AP device.</li> <li>• Select <b>No</b> if performance is affected in negative fashion by this function. If a large number of APs are unreachable by ICMP, likely to occur where there is in excess of 100 APs, the timeouts start to impede network performance.</li> </ul> <p><b>NOTE:</b> If ICMP is disabled on the network, select <b>No</b> to avoid the performance penalty caused by numerous ping requests.</p>

7. Locate the **Symbol 4131 and Cisco Aironet IOS SNMP Initialization** area. Select one of the options listed. [Table 31](#) describes the settings and default values:

**Table 31** *Device Setup > Communication > Symbol 4131 and Cisco Aironet IOS SNMP Initialization Fields and Default Values*

Setting	Default	Description
<b>Do Not Modify SNMP Settings</b>	Yes	When selected, specifies that AirWave not modify any SNMP settings. If SNMP is not already initialized on the Symbol, Nomadix, and Cisco IOS APs, AirWave is not able to manage them.
<b>Enable read-write SNMP</b>	No	When selected, and when on networks where the Symbol, Nomadix, and Cisco IOS APs do not have SNMP initialized, this setting enables SNMP so the devices can be managed by AirWave.

## Loading Device Firmware Onto AirWave (optional)

### Overview of the Device Setup > Upload Firmware & Files Page

AirWave enables automated firmware distribution to the devices on your network. Once you have downloaded the firmware files from the vendor, you can upload this firmware to AirWave for distribution to devices via the **Device Setup > Upload Firmware & Files** page.

This page lists all firmware files on AirWave with file information. This page also enables you to add new firmware files, to delete firmware files, and to add **New Web Auth Bundle** files.

The following additional pages support firmware file information:

- Firmware files uploaded to AirWave appear as options in the drop-down menus on the **Group > Firmware** page and on individual **APs/Devices > Manage** pages.
- Use the **AMP Setup** page to configure AirWave-wide default firmware options.

[Table 32](#) below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

**Table 32** *Device Setup > Upload Firmware & Files Fields and Default Values*

Setting	Default	Description
<b>Type</b>	ArubaCont roller (any model)	Displays a drop-down list of the primary AP makes and models that AirWave supports with automated firmware distribution.
<b>Owner Role</b>	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
<b>Description</b>	None	Displays a user-configurable text description of the firmware file.
<b>Server Protocol</b>	None	Displays the file transfer protocol by which the firmware file was obtained from the server.
<b>Use Group File Server</b>	None	Displays the name of the file server supporting the group.
<b>Firmware Filename</b>	None	Displays the name of the file that was uploaded to AirWave and to be transferred to an AP when the file is used in an upgrade.
<b>Firmware Version</b>	None	Displays the firmware version number. This is a user-configurable field.
<b>Firmware MD5 Checksum</b>	None	Displays the MD5 checksum of the file after it was uploaded to AirWave. The MD5 checksum is used to verify that the file was uploaded to AirWave without issue. The checksum should match the checksum of the file before it was uploaded.
<b>Firmware File Size</b>	None	Displays the size of the firmware file in bytes.
<b>HTML Filename</b>	None	Supporting HTML, displays the name of the file that was uploaded to AirWave and to be transferred to an AP when the file is used in an upgrade.

**Table 32 Device Setup > Upload Firmware & Files Fields and Default Values (Continued)**

Setting	Default	Description
<b>HTML Version</b>	None	Supporting HTML, displays the version of HTML used for file transfer.
<b>HTML MD5 Checksum</b>	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to AirWave. The MD5 checksum is used to verify that the file was uploaded to AirWave without issue. The checksum should match the checksum of the file before it was uploaded.
<b>HTML File Size</b>	None	Supporting HTML, displays the size of the file in bytes.
<b>Desired Firmware File for Specified Groups</b>	None	The firmware file is set as the desired firmware version on the <b>Groups &gt; Firmware Files</b> page of the specified groups. You cannot delete a firmware file that is set as the desired firmware version for a group.

## Loading Firmware Files to AirWave

Perform the following steps to load a device firmware file onto AirWave:

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Select **Add**. The **Add Firmware File** page appears. [Figure 29](#) illustrates this page.

**Figure 29 Device Setup > Upload Firmware and Files > Add Page Illustration**

3. Select **Supported Firmware Versions and Features** to view supported firmware versions.



Unsupported and untested firmware may cause device mismatches and other problems. Please contact AirWave support before installing non-certified firmware.

4. Enter the appropriate information and select **Add**. The file uploads to AirWave and once complete, this file appears on the **Device Setup > Upload Firmware & Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **APs/Devices > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. [Table 33](#) itemizes the settings of this page.

**Table 33 Supported Firmware Versions and Features Fields and Default Values**

Setting	Default	Description
<b>Type</b>	Aruba Controller	Indicates the firmware file is used with the specified type. If you select an IOS device from the <b>Type</b> drop-down menu, you have the option of choosing a server protocol of TFTP or FTP. If you choose FTP, you may later notice that the firmware files are pushed to the device more quickly. With selection of some types, particularly Cisco controllers, you can specify the boot software version.
<b>Firmware Version</b>	None	Provides a user-configurable field to specify the firmware version number. Appears if you did not select the default <b>Aruba Controller</b> type.

**Table 33 Supported Firmware Versions and Features Fields and Default Values (Continued)**

Setting	Default	Description
<b>Description</b>	None	Provides a user-configurable text description of the firmware file.
<b>Upload firmware files (and use built-in firmware)</b>	Built-in	Selects the TFTP server that access points use to download their firmware. The built-in TFTP server is recommended. If you choose to use an external TFTP server, enter the <b>File Server IP Address</b> and the <b>Firmware Filename</b> .
<b>Use an external firmware file server</b>	N/A	You can also choose to assign the external TFTP server on a per-group basis. If you select this option, you must enter the IP address on the <b>Groups &gt; Firmware</b> page. Complete the <b>Firmware File Server IP Address</b> field. <b>NOTE:</b> With selection of some Types, you are prompted with the Server Protocol field that lets you select which protocol to use, and this varies from device to device. If you select FTP, AirWave uses an anonymous user for file upload.
<b>Use Group File Server</b>	Disabled	If you opt to use an external firmware file server, this additional option appears. This setting instructs AirWave to use the server that is associated with the group instead of defining a server.
<b>Firmware File Server IP Address</b>	None	Provides the IP address of the External TFTP Server (like SolarWinds) used for the firmware upgrade. This option displays when the user selects the <b>Use an external firmware file</b> option.
<b>Firmware Filename</b>	None	Enter the name of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. If you are using a non-external server, you select <b>Choose File</b> to find your local copy of the file.



Additional fields may appear for multiple device types. AirWave prompts you for additional firmware information as required. For example, Intel and Symbol distribute their firmware in two separate files: an image file and an HTML file. Both files must be uploaded to AirWave for the firmware to be distributed successfully via AirWave.

6. Select **Add** to import the firmware file.

To delete a firmware file that has already been uploaded to AirWave, return to the **Device Setup > Upload Firmware & Files** page, select the checkbox for the firmware file and select **Delete**.



A firmware file may not be deleted if it is the desired version for a group. Use the **Group > Firmware** page to investigate this potential setting and status.

## Using Web Auth Bundles in AirWave

Web authentication bundles are configuration files that support Cisco WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco WLC devices.

Perform these steps to add or edit Web Auth bundles in AirWave.

1. Go to the **Device Setup > Upload Firmware & Files** page. This page displays any existing Web Auth bundles that are currently configured in AirWave, and allows you to add or delete Web Auth bundles.
2. Scroll to the bottom of the page. Select **Add New Web Auth Bundle** to create a new Web Auth bundle (see [Figure 30](#)), or select the pencil icon next to an existing bundle to edit. You may also delete Web Auth bundles by selecting that bundle with the checkbox, and selecting **Delete**.

**Figure 30 Add Web Auth Bundle Page Illustration**

3. Enter a descriptive label in the description field. This is the label used to identify and track Web Auth bundles on the page.
4. Enter the path and filename of the Web Auth configuration file in the **Web Auth Bundle** field or select **Choose File** to locate the file.
5. Select **Add** to complete the Web Auth bundle creation, or **Save** if replacing a previous Web Auth configuration file, or **Cancel** to abort the Web Auth integration.

For additional information and a case study that illustrates the use of Web Auth bundles with Cisco WLC controllers, refer to the following document on Cisco.com:

- Wireless LAN controller Web Authentication Configuration Example, Document ID: 69340  
[http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a008067489f.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008067489f.shtml)

## Setting Up Device Types

On **AMP Setup > Device Type Setup**, you can define how the Device Type displayed for users on your network is calculated from available data. The first matching property is used. These rules cannot be edited or deleted, but only reordered or enabled.

You can change the priority order of rules by dragging and dropping rows, as shown in [Figure 31](#).

Check or uncheck the checkbox under the **Enabled** column to turn device setup rules on or off.

Refer to “[Monitoring and Supporting WLAN Clients](#)” on page 196 for more information on the **Device Type** column that appears in **Clients** list tables.

**Figure 31** *AMP Setup > Device Type Setup Page Illustration*

**Device Type Rules**

Name	Enabled	
AOS Device Type	<input checked="" type="checkbox"/>	↑↓
Manufacturer+Model	<input checked="" type="checkbox"/>	↕
OS	<input checked="" type="checkbox"/>	↕
OS Detail	<input checked="" type="checkbox"/>	↕
Manufacturer	<input checked="" type="checkbox"/>	↕
Model	<input checked="" type="checkbox"/>	↕
Network Interface Vendor (from OUI)	<input checked="" type="checkbox"/>	↕

7 Device Type Setups

Save and Apply    Revert

## Configuring Cisco WLSE and WLSE Rogue Scanning

The Cisco Wireless LAN Solution Engine (WLSE) includes rogue scanning functions that AirWave supports. This section contains the following topics and procedures, and several of these sections have additional sub-procedures:

- [Introduction to Cisco WLSE](#)
- [Configuring WLSE Initially in AirWave](#)
- [Configuring IOS APs for WDS Participation](#)
- [Configuring ACS for WDS Authentication](#)
- [Configuring Cisco WLSE Rogue Scanning](#)

You must enter one or more CiscoWorks WLSE hosts to be polled for discovery of Cisco devices and rogue AP information.



## Introduction to Cisco WLSE

Cisco WLSE functions as an integral part of the Cisco Structured Wireless-Aware Network (SWAN) architecture, which includes IOS Access Points, a Wireless Domain Service, an Access Control Server, and a WLSE. In order for AirWave to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. [Table 34](#) describes these components.

**Table 34** Cisco SWAN Architecture Components

SWAN Component	Requirements
<b>WDS (Wireless Domain Services)</b>	<ul style="list-style-type: none"><li>WDS Name</li><li>Primary and backup IP address for WDS devices (IOS AP or WLSM)</li><li>WDS Credentials APs within WDS Group</li></ul> <p><b>NOTE:</b> WDS can be either a WLSM or an IOS AP. WLSM (WDS) can control up to 250 access points. AP (WDS) can control up to 30 access points.</p>
<b>WLSE (Wireless LAN Solution Engine)</b>	<ul style="list-style-type: none"><li>IP Address</li><li>Login</li></ul>
<b>ACS (Access Control Server)</b>	<ul style="list-style-type: none"><li>IP Address</li><li>Login</li></ul>
<b>APs</b>	<ul style="list-style-type: none"><li>APs within WDS Group</li></ul>

## Configuring WLSE Initially in AirWave

Use the following general procedures to configure and deploy a WLSE device in AirWave:

- [Adding an ACS Server for WLSE](#)
- [Enabling Rogue Alerts for Cisco WLSE](#)
- [Configuring WLSE to Communicate with APs](#)
- [Discovering Devices](#)
- [Managing Devices](#)
- [Inventory Reporting](#)
- [Defining Access](#)
- [Grouping](#)
- [WDS Participation](#)
- [Primary or Secondary WDS](#)

### Adding an ACS Server for WLSE

- Go to the **Devices > Discover > AAA Server** page.
- Select **New** from the drop-down list.
- Enter the **Server Name**, **Server Port** (default 2002), **Username**, **Password**, and **Secret**.
- Select **Save**.

### Enabling Rogue Alerts for Cisco WLSE

- Go to the **Faults > Network Wide Settings > Rogue AP Detection** page.
- Select the **Enable**.
- Select **Apply**.

Additional information about rogue device detection is available in “[Configuring Cisco WLSE Rogue Scanning](#)” on page 63.

### Configuring WLSE to Communicate with APs

- Go to the **Device Setup > Discover** page.



2. Configure SNMP Information.
3. Configure HTTP Information.
4. Configure Telnet/SSH Credentials.
5. Configure HTTP ports for IOS access points.
6. Configure WLCCP credentials.
7. Configure AAA information.

## Discovering Devices

There are three methods to discover access points within WLSE, as follows:

- Using Cisco Discovery Protocol (CDP)
- Importing from a file
- Importing from CiscoWorks

Perform these steps to discover access points.

1. Go to the **Device > Managed Devices > Discovery Wizard** page.
2. Import devices from a file.
3. Import devices from Cisco Works.
4. Import using CDP.

## Managing Devices

Prior to enabling radio resource management on IOS access points, the access points must be under WLSE management.



---

AirWave becomes the primary management/monitoring vehicle for IOS access points, but for AirWave to gather Rogue information, the WLSE must be an NMS manager to the APs.

---

Use these pages to make such configurations:

1. Go to **Device > Discover > Advanced Options**.
2. Select the method to bring APs into management **Auto**, or specify via filter.

## Inventory Reporting

When new devices are managed, the WLSE generates an inventory report detailing the new APs. AirWave accesses the inventory report via the SOAP API to auto-discover access points. This is an optional step to enable another form of AP discovery in addition to AirWave' CDP, SNMP scanning, and HTTP scanning discovery for Cisco IOS access points. Perform these steps for inventory reporting.

1. Go to **Devices > Inventory > Run Inventory**.
2. **Run Inventory** executes immediately between WLSE polling cycles.

## Defining Access

AirWave requires System Admin access to WLSE. Use these pages to make these configurations.

1. Go to **Administration > User Admin**.
2. Configure **Role** and **User**.

## Grouping

It's much easier to generate reports or faults if APs are grouped in WLSE. Use these pages to make such configurations.

1. Go to **Devices > Group Management**.

2. Configure **Role** and **User**.

## Configuring IOS APs for WDS Participation

IOS APs (1100, 1200) can function in three roles within SWAN:

- Primary WDS
- Backup WDS
- WDS Member

AMP monitors AP WDS role and displays this information on **AP Monitoring** page.



---

APs functioning as WDS Master or Primary WDS will no longer show up as Down if the radios are enabled.

---

### WDS Participation

Perform these steps to configure WDS participation.

1. Log in to the AP.
2. Go to the **Wireless Services > AP** page.
3. Select **Enable participation in SWAN Infrastructure**.
4. **Select Specified Discovery** and enter the IP address of the Primary WDS device (AP or WLSM).
5. Enter the **Username** and **Password** for the WLSE server.

### Primary or Secondary WDS

Perform these steps to configure primary or secondary functions for WDS.

1. Go to the **Wireless Services > WDS > General Setup** page.
2. If the AP is the Primary or Backup WDS, select **Use the AP as Wireless Domain Services**.
  - Select **Priority** (set **200** for Primary, **100** for Secondary).
  - Configure the **Wireless Network Manager** (configure the IP address of WLSE).
3. If the AP is Member Only, leave all options unchecked.
4. Go to the **Security > Server Manager** page.
5. Enter the **IP address** and **Shared Secret** for the ACS server and select **Apply**.
6. Go to the **Wireless Services > WDS > Server Group** page.
7. Enter the WDS Group of AP.
8. Select the **ACS server** in the **Priority 1** drop-down menu and select **Apply**.

## Configuring ACS for WDS Authentication

ACS authenticates all components of the WDS and must be configured first. Perform these steps to make this configuration.

1. Login to the ACS.
2. Go to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by selecting the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.
4. Select **User Setup** in the left frame.
5. Enter the **Username** that will be used to authenticate into the WDS and select **Add/Edit**.
6. Enter the **Password** that will be used to authenticate into the WDS and select **Submit**.
7. Go to the **Network Configuration > Add AAA Client** page.

8. Add **AP Hostname**, **AP IP Address**, and **Community String** (for the key).
9. Enter the **Password** that will be used to authenticate into the WDS and select **Submit**.

For additional and more general information about ACS, refer to “[Configuring ACS Servers](#)” on page 64.

## Configuring Cisco WLSE Rogue Scanning

The **AMP Setup > WLSE** page allows AirWave to integrate with the Cisco Wireless LAN Solution Engine (WLSE). AirWave can discover APs and gather rogue scanning data from the Cisco WLSE.

[Figure 32](#) illustrates and itemizes the AirWave settings for communication that is enabled between AirWave and WLSE.

**Figure 32** *AMP Setup > WLSE > Add WLSE Page Illustration*

Perform the following steps for optional configuration of AirWave for support of Cisco WLSE rogue scanning.

1. To add a Cisco WLSE server to AirWave, navigate to the **AMP Setup > WLSE** page and select **Add**. Complete the fields in this page. [Table 35](#) describes the settings and default values.

**Table 35** *AMP Setup > WLSE Fields and Default Values*

Setting	Default	Description
<b>Hostname/IP Address</b>	None	Designates the IP address or DNS Hostname for the WLSE server, which must already be configured on the Cisco WLSE server.
<b>Protocol</b>	HTTP	Specifies the protocol to be used when polling the WLSE.
<b>Port</b>	1741	Defines the port AirWave uses to communicate with the WLSE server.
<b>Username</b>	None	Defines the username AirWave uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on AirWave.  The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow AirWave to pull the necessary XML APIs.
<b>Password</b>	None	Defines the password AirWave uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on AirWave.  As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow AirWave to pull the necessary XML APIs.
<b>Poll for AP Discovery; Poll for Rogue Discovery</b>	Yes	Sets the method by which AirWave uses WLSE to poll for discovery of new APs and/or new rogue devices on the network.
<b>Last Contacted</b>	None	Displays the last time AirWave was able to contact the WLSE server.
<b>Polling Period</b>	10 minutes	Determines how frequently AirWave polls WLSE to gather rogue scanning data.

2. After you have completed all fields, select **Save**. AirWave is now configured to gather rogue information from WLSE rogue scans. As a result of this configuration, any rogues found by WLSE appear on the **RAPIDS > List** page.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Configuring ACS Servers

This is an optional configuration. The **AMP Setup > ACS** page allows AirWave to poll one or more Cisco ACS servers for wireless username information. When you specify an ACS server, AirWave gathers information about your wireless users. Refer to “[on page 59](#) if you want to use your ACS server to manage your AirWave users.

Perform these steps to configure ACS servers:

1. Go to the **AMP Setup > ACS** page. This page displays current ACS setup, as illustrated in [Figure 33](#).

**Figure 33** *AMP Setup > ACS Page Illustration*

2. Select **Add** to create a new ACS server, or select a pencil icon to edit an existing server. To delete an ACS server, select that server and select **Delete**. When selecting **Add** or edit, the **Details** page appears, as illustrated in [Figure 34](#).

**Figure 34** *AMP Setup > ACS > Add/Edit Details Page Illustration*

3. Complete the settings on **AMP Setup > ACS > Add/Edit Details**. [Table 36](#) describes these fields:

**Table 36** *AMP Setup > ACS > Add/Edit Details Fields and Default Values*

Field	Default	Description
<b>IP/Hostname</b>	None	Sets the DNS name or the IP address of the ACS Server.
<b>Protocol</b>	HTTP	Launches a drop-down menu specifying the protocol AirWave uses when it polls the ACS server.
<b>Port</b>	2002	Sets the port through which AirWave communicates with the ACS. AirWave generally communicates via SNMP traps on port 162.

**Table 36 AMP Setup > ACS > Add/Edit Details Fields and Default Values (Continued)**

Field	Default	Description
<b>Username</b>	None	Sets the Username of the account AirWave uses to poll the ACS server.
<b>Password</b>	None	Sets the password of the account AirWave uses to poll the ACS server.
<b>Polling Period</b>	10 min	Launches a drop-down menu that specifies how frequently AirWave polls the ACS server for username information.

4. Select **Add** to finish creating the new ACS server, or **Save** to finish editing an existing ACS server.
5. The ACS server must have logging enabled for passed authentications. Enable the **Log to CSV Passed Authentications report** option, as follows:
  - Log in to the ACS server, select **System Configuration**, then in the **Select** frame, select **Logging**.
  - Under **Enable Logging**, select **CSV Passed Authentications**. The default logging options function and support AirWave. These include the two columns AirWave requires: **User-Name** and **Caller-ID**.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Integrating AirWave with an Existing Network Management Solution (NMS)

This is an optional configuration. The **AMP Setup > NMS** configuration page allows AirWave to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

- AirWave can forward WLAN-related SNMP traps to the NMS, or AirWave can send SNMPv1 or SNMPv2 traps to the NMS.
- AirWave can be used in conjunction with Hewlett-Packard's ProCurve Manager.
- The necessary files for either type of NMS interoperability are downloaded from the **AMP Setup > NMS** page as follows. For additional information, contact support.

Perform these steps to configure NMS support in AirWave:

1. Go to **AMP Setup > NMS**, illustrated in [Figure 35](#).

**Figure 35 AMP Setup > NMS Page Illustration**

**NMS Integration**

AMP can send SNMP traps to NMS servers. First, add one or more NMS servers below, then select *NMS* as a notification option for *triggers*.

The *Sync* action will send one trap for each device managed by AMP to inform an NMS of each one's up/down and configuration status.

[Download the AMP MIB files.](#)

**NMS servers:**

[Add](#) [New NMS Server](#)

	Hostname	Port	SNMP Version	Enabled	Send Configuration Traps
<input type="checkbox"/>	acceptance-test.corp.airwave.com	162	2c	Yes	Yes
<input type="checkbox"/>	gauss.corp.airwave.com	162	2c	Yes	Yes

2. Select **Add** to integrate a new NMS server, or select the pencil icon to edit an existing server. Provide the information described in [Table 37](#):

**Table 37** *AMP Setup > NMS Integration Add/Edit Fields and Default Values*

Setting	Default	Description
<b>Hostname</b>	None	Cites the DNS name or the IP address of the NMS.
<b>Port</b>	162	Sets the port AirWave uses to communicate with the NMS. <b>NOTE:</b> AirWave generally communicates via SNMP traps on port 162.
<b>Community String</b>	None	Sets the community string used to communicate with the NMS.
<b>SNMP Version</b>	v2C	Sets the SNMP version of the traps sent to the Host.
<b>Enabled</b>	Yes	Enables or disables trap logging to the specified NMS.
<b>Send Configuration Traps</b>	Yes	Enables NMS servers to transmit SNMP configuration traps.

3. The **NMS Integration Add/Edit** page includes the **Netcool/OMNIbus Integration** link to information and instructions. The IBM Tivoli Netcool/OMNIbus operations management software enables automated event correlation and additional features resulting in optimized network uptime.
4. The **NMS Integration Add/Edit** page includes the **HP ProCurve Manager Integration** link. Select this link for additional information, zip file download, and brief instructions for installation with AirWave. Select **Add** to finish creating the NMS server, or **Save** to configure an existing NMS server.

## What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you for any phase of AirWave installation.

## Auditing PCI Compliance on the Network

This section describes PCI requirements and auditing functions in AirWave, with the following topics:

- [Introduction to PCI Requirements](#)
- [PCI Auditing in the AirWave Interface](#)
- [Enabling or Disabling PCI Auditing](#)

### Introduction to PCI Requirements

AirWave supports wide security standards and functions in the wireless network. One component of network security is the optional deployment of Payment Card Industry (PCI) Auditing.

The Payment Card Industry (PCI) Data Security Standard (DSS) establishes multiple levels in which payment cardholder data is protected in a wireless network. AirWave supports PCI requirements according to the standards and specifications set forth by the following authority:

- Payment Card Industry (PCI) Data Security Standard (DSS)
  - PCI Security Standards Council Website  
<https://www.pcisecuritystandards.org>
  - *PCI Quick Reference Guide*, Version 1.2 (October 2008)  
[https://www.pcisecuritystandards.org/pdfs/pci\\_ssc\\_quick\\_guide.pdf](https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf)

## PCI Auditing in the AirWave Interface

PCI Auditing in AirWave allows you to monitor, audit, and demonstrate PCI compliance on the network. There are five primary pages in which you establish, monitor, and access PCI auditing, as follows:

- The **AMP Setup > PCI Compliance** page enables or disables PCI Compliance monitoring on the network, and displays the current compliance status on the network. See [“Enabling or Disabling PCI Auditing” on page 68](#).
- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See [“Reports > Definitions Page Overview” on page 227](#).
- The **Reports > Generated** page lists PCI Compliance reports currently available, and allows you to generate the latest daily version of the PCI Compliance Report with a single select. Refer to [“Reports > Generated Page Overview” on page 229](#).
- The **APs/Devices > PCI Compliance** page enables you to analyze PCI Compliance for any specific device on the network. This page is accessible when you select a specific device from the **APs/Devices > Monitor** page. First, you must enable this function through **AMP Setup**. See [“Enabling or Disabling PCI Auditing” on page 68](#).
- The **PCI Compliance Report** offers additional information. Refer to [“Using the PCI Compliance Report” on page 245](#). This report not only contains **Pass** or **Fail** status for each PCI requirement, but cites the action required to resolve a **Fail** status when sufficient information is available.



When any PCI requirement is enabled on AirWave, then AirWave grades the network as pass or fail for the respective PCI requirement. Whenever a PCI requirement is not enabled in AirWave, then AirWave does not monitor the network's status in relation to that requirement, and cannot designate Pass or Fail network status. AMP users without RAPIDS visibility enabled will not see the 11.1 PCI requirements in the PCI Compliance Report.

**Table 38** *PCI Requirements and Support in AirWave*

Requirement	Description
<b>1.1</b>	Monitoring configuration standards for network firewall devices When Enabled: PCI Requirement 1.1 establishes firewall and router configuration standards. A device fails Requirement 1.1 if there are mismatches between the desired configuration and the configuration on the device. When Disabled: firewall router and device configurations are not checked for PCI compliance, and Pass or Fail status is not reported or monitored.
<b>1.2.3</b>	Monitoring firewall installation between any wireless networks and the cardholder data environment When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall. When Disabled: firewall router and device installation are not checked for PCI compliance.
<b>2.1</b>	Monitoring the presence of vendor-supplied default security settings When Enabled: PCI Requirement 2 establishes the standard in which all vendor-supplied default passwords are changed prior to a device's presence and operation in the network. A device fails requirement 2.1 if the username, passwords or SNMP credentials being used by AirWave to communicate with the device are on a list of forbidden default credentials. The list includes common vendor default passwords, for example. When Disabled: device passwords and other vendor default settings are not checked for PCI compliance.
<b>2.1.1</b>	Changing vendor-supplied defaults for wireless environments When Enabled: A device fails requirement 2.1.1 if the passphrases, SSIDs, or other security-related settings are on a list of forbidden values that AirWave establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance. When Disabled: network devices are not checked for forbidden information and PCI Compliance is not established.



**Table 38** *PCI Requirements and Support in AirWave (Continued)*







Requirement	Description
<b>4.1.1</b>	<p>Using strong encryption in wireless networks</p> <p>When Enabled: PCI Requirement 4 establishes the standard by which payment cardholder data is encrypted prior to transmission across open public networks. PCI disallows WEP encryption as an approved encryption method after June 20, 2010. A device fails requirement 4.1.1 if the desired or actual configuration reflect that WEP is enabled on the network, or if associated users can connect with WEP.</p> <p>When Disabled: AirWave cannot establish a pass or fail status with regard to PCI encryption requirements on the network.</p>
<b>11.4</b>	<p>Using intrusion-detection or intrusion-prevention systems to monitor all traffic</p> <p>When Enabled: AirWave reports pass or fail status when monitoring devices capable of reporting IDS events. Recent IDS events are summarized in the PCI Compliance report or the IDS Report.</p> <p>When Disabled: AirWave does not monitor the presence of PCI-compliant intrusion detection or prevention systems, nor can it report <b>Pass</b> or <b>Fail</b> status with regard to IDS events.</p>

## Enabling or Disabling PCI Auditing

Perform these steps to verify status and to enable or disable AirWave support for PCI 1.2 requirements. enabling one or all PCI standards on AirWave enables real-time information and generated reports that advise on Pass or Fail status. The PCI auditing supported in AirWave is reported in [Table 38](#).

1. To determine what PCI Compliance standards are enabled or disabled on AirWave, navigate to the **AMP Setup > PCI Compliance** page, illustrated in [Figure 36](#).

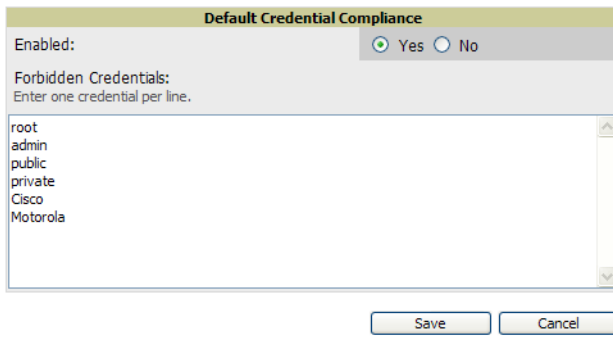
**Figure 36** *AMP Setup > PCI Compliance Page Illustration*

PCI Requirement ▲	Description	Enabled
 1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Yes
 1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Yes
 2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by OV3600 to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Yes
 2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Yes
 4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated users can connect with WEP.	Yes
 11.4	Use intrusion-detection systems and/or intrusion-prevention systems to monitor all traffic. A report will indicate a "pass" for the requirement if OV3600 is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Yes

2. To enable, disable, or edit any category of PCI Compliance monitoring in AirWave, select the pencil icon next to the category. The **Default Credential Compliance** page displays for the respective PCI standard.
3. Create changes as required. Specific credentials can be cited in the **Forbidden Credentials** section of any **Edit** page to enforce PCI requirements in AirWave. [Figure 37](#) shows one example.



**Figure 37 Default Credential Compliance for PCI Requirements**



4. Select **Save**.
5. To view and monitor PCI auditing on the network, use generated or daily reports. See [Chapter 9, “Creating, Running, and Emailing Reports”](#). In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
  - a. Go to the **APs/Devices > List** page, select a specific device, and the **Monitor** page for that device displays. The **Monitor** page displays a **PCI Compliance** subtab in the menu bar.
  - b. Select **PCI Compliance** to view complete PCI compliance auditing for that specific device.

## What Next?

- Go to other tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter before proceeding.* AirWave support remains available to you in any phase of AirWave installation.

## Deploying WMS Offload

### Overview of WMS Offload in AirWave

This section describes the Wireless LAN Management Server (WMS) offload infrastructure. WMS Offload is supported with the following two requirements:

- ArubaOS Version 2.5.4 or later
- AMP Version 6.0 or later

The WMS feature is an enterprise-level hardware device and server architecture with managing software for security and network policy. There are three primary components of the WMS deployment:

- Air Monitor AP devices establish and monitor RF activity on the network.
- The WMS server manages devices and network activity, to include rogue AP detection and enforcement of network policy.
- The AirWave graphical user interface (GUI) allows users to access and use the WMS functionality.

WMS Offload is the ability to place the burden of the WMS server data and GUI functions on AirWave. WMS master controllers provide this data so that AirWave can support rigorous network monitoring capabilities.

### General Configuration Tasks Supporting WMS Offload in AirWave

WMS Offload must be enabled with a six-fold process and related configuration tasks, as follows:

1. Configure WLAN switches for optimal AirWave monitoring.
  - Disable debugging.
  - Ensure AirWave server is a trap receiver host.

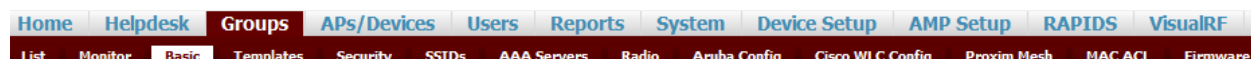
- Ensure proper traps are enabled.
- 2. Configure AirWave to optimally monitor the AirWave infrastructure.
  - Enable WMS offload.
  - Configure SNMP communication.
  - Create a proper policy for monitoring AirWave infrastructure.
  - Discover the infrastructure.
- 3. Configure device classification.
  - Set up rogue classification.
  - Set up rogue classification override.
  - Establish user classification override devices.
- 4. Deploy ArubaOS-specific monitoring features.
  - Enable remote AP and wired network monitoring.
  - View controller license information.
- 5. Convert existing floor plans to VisualRF, to include the following elements:
  - AOS
  - RF Plan
- 6. Use RTLS for increasing location accuracy (optional).
  - Enable RTLS service on the AirWave server.
  - Enable RTLS on ArubaOS Infrastructure.

### **Additional Information Supporting WMS Offload**

For additional information, including detailed concepts, configuration procedures, restrictions, ArubaOS infrastructure, and AirWave version differences in support of WMS Offload, refer to the *AirWave Best Practices Guide*.

This chapter describes the deployment of device groups within AMP. The section below describes the pages or focused subtabs available on the Groups tab. Note that the available subtabs can vary significantly from one device group to another—one or more subtabs may not appear, depending on the **Default Group** display option selected on the **AMP Setup > General** page and the types of devices you add to AMP.

**Figure 38** Subtabs under the **Group** tab



- **List**—This page is the default page in the **Groups** section of AMP. It lists all groups currently configured in AMP and provides the foundation for all group-level configurations. See [“Viewing All Defined Device Groups” on page 72](#).
- **Monitor**—This page displays client and bandwidth usage information, lists devices in a given group, provides an **Alert Summary** table for monitoring alerts for the group, and provides a detailed **Audit Log** for group-level activity.
- **Basic**—This page appears when you create a new group on the **Groups > List** page. Once you define a group name, AMP displays the **Basic** page from which you configure many group-level settings. This page remains available for any device group configured in AMP. Refer to [“Configuring Basic Group Settings” on page 74](#).
- **Templates**—This page manages templates for any device group. Templates allow you to manage the configuration of Dell PowerConnect W, 3Com, Alcatel-Lucent, Aruba Networks, Cisco Aironet IOS, Cisco Catalyst switches, Enterasys, HP, Nortel, Symbol and Trapeze devices in a given group using a configuration file. Variables in such templates configure device-specific properties, such as name, IP address and channel. Variables also define group-level properties. For additional information about using the **Templates** page, refer to [Chapter 6, “Creating and Using Templates” on page 151](#).
- **Security**—This page defines general security settings for device groups, to include RADIUS, encryption, and additional security settings on devices. Refer to [“Configuring Group Security Settings” on page 82](#).
- **SSIDs**—This page sets SSIDs, VLANs, and related parameters in device groups. Refer to [“Configuring Group SSIDs and VLANs” on page 84](#).
- **AAA Servers**—This page configures authentication, authorization, and accounting settings in support of RADIUS servers for device groups. Refer to [“Adding and Configuring Group AAA Servers” on page 81](#).
- **Radio**—This page defines general 802.11 radio settings for device groups. Refer to [“Configuring Radio Settings for Device Groups” on page 88](#).
- **Aruba Config**—This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Aruba devices on the network. Use this page as an alternative to the **Device Setup > Aruba Configuration** page. The appearance of this page varies depending on whether AMP is configured for global configuration or group configuration. For additional information, refer to the *ArubaOS Configuration Guide*.
- **Cisco WLC Config**—This page consolidates controller-level settings from the Group Radio, Security, SSIDs, Cisco WLC Radio and AAA Server pages into one navigation tree that is easier to navigate, and has familiar layout and terminology. Bulk configuration for per-thin AP settings, previously configured on the Group LWAPP APs tab, can now be performed from **Modify Devices** on the **APs/Devices > List** page. Refer to [“Cisco WLC Group Configuration” on page 92](#).
- **PTMP**—This page defines settings specific to Proxim MP devices when present. Refer to [“Configuring Group PTMP Settings” on page 97](#).

- **Proxim Mesh**—This page defines mesh AP settings specific to Proxim devices when present. Refer to [“Configuring Proxim Mesh Radio Settings” on page 98](#).
- **MAC ACL**—This page defines MAC-specific settings that apply to Proxim, Symbol, and ProCurve 520 devices when present. Refer to [“Configuring Group MAC Access Control Lists” on page 99](#).
- **Firmware**—This page manages firmware files for many devices. [“Specifying Minimum Firmware Versions for APs in a Group” on page 99](#).
- **Compare**—This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, select **Compare Two Groups**, select the two groups from the drop-down menus, then select **Compare**. [“Comparing Device Groups” on page 100](#).

This chapter also provides the following additional procedures for group-level configurations:

- [“Deleting a Group” on page 101](#)
- [“Changing Multiple Group Configurations” on page 102](#)
- [“Modifying Multiple Devices” on page 103](#)
- [“Using Global Groups for Group Configuration” on page 105](#)

## AMP Groups Overview

Enterprise APs, controllers, routers, and switches have hundreds of variable settings that must be configured precisely to achieve optimal performance and network security. Configuring all settings on each device individually is time consuming and error prone. AMP addresses this challenge by automating the processes of device configuration and compliance auditing. At the core of this approach is the concept of Device **Groups**, with the following functions and benefits:

- AMP allows certain settings to be managed efficiently at Group-level while others are managed at an individual device level.
- AMP defines a Group as a subset of the devices on the wireless LAN, ranging in size from one device to hundreds of devices that share certain common configuration settings.
- Groups may be defined based on geography (such as “5th Floor APs”), usage or security policies (such as “Guest Access APs”), function (such as “Manufacturing APs”), or any other appropriate variable.
- Devices within a group may be from different vendors or hardware models. All devices within a Group share certain basic configuration settings.

Typical group configuration variables include basic settings (SSID, SNMP polling interval, and so forth), security settings (VLANs, WEP, 802.1x, ACLs, and so forth), and some radio settings (data rates, fragmentation threshold, RTS threshold, DTIM, preamble, and so forth). When configuration changes are applied at a *group level*, they are assigned automatically to every device within that group. Such changes must be applied with every device in **Managed** mode. **Monitor** mode is the more common mode.



CAUTION

---

Always review the **Audit** page before pushing configuration to a device or group.

---

Individual device settings—such as device name, RF channel selection, RF transmission power, antenna settings, and so forth—typically should not be managed at a group level and must be individually configured for optimal performance. Individual AP settings are configured on the **APs/Devices > Manage** page.

You can create as many different groups as required. Administrators usually establish groups that range in size from five to 100 wireless devices.

Group configuration can be enhanced with the AMP **Global Groups** feature, which lets you create Global Groups with configurations that are pushed to individual Subscriber Groups.

## Viewing All Defined Device Groups

To display a list of all defined groups, browse to the **Groups > List** page, illustrated in [Figure 39](#).

**Figure 39 Groups > List Page Illustration**

Add

New Group

Compare two groups

1-41 of 41 Groups

Page 1 of 1

Choose Columns

CSV Export

Table 39 describes the columns in the **Groups > List** page.

**Table 39 Groups > List Columns**

Column	Description
<b>Add New Group</b>	Launches a page that enables you to add a new group by name and to define group parameters for devices in that group. For additional information, refer to <a href="#">“Configuring Basic Group Settings” on page 74</a> .
<b>Changes</b>	Whether the group has unapplied changes.
<b>Manage</b> (wrench icon)	Goes to the <b>Groups &gt; Basic</b> configuration page for that group. Hover your mouse over the icon to see a list of shortcuts to group-specific subtabs that would appear across the navigation section if this group is selected.
<b>Name</b>	Uniquely identifies the group by location, vendor, department or any other identifier (such as ‘Accounting APs,’ ‘Floor 1 APs,’ ‘Cisco devices,’ ‘802.1x APs,’ and so forth).
<b>Is Global Group</b>	If a group is designated as global, it may not contain APs but it may be used as a template for other groups. This column may also indicate <b>Yes</b> if this group has been pushed to the AMP from a Master Console.
<b>Global Group</b>	Specifies which group this Subscriber Group is using as its template.
<b>SSID</b>	The SSID assigned to supported device types within the group.
<b>Total Devices</b>	Total number of devices contained in the group including APs, controllers, routers, or switches.
<b>Down</b>	The number of access points within the group that are not reachable via SNMP or are no longer associated to a controller. Note that thin APs are not directly polled with SNMP, but are polled through the controller. That controller may report that the thin AP is down or is no longer on the controller. At this point, AMP classifies the device as down.
<b>Mismatched</b>	The number of devices within the group that are in a mismatched state.
<b>Ignored</b>	The number of ignored devices in that group.
<b>Clients</b>	The number of mobile users associated with all access points within the group. To avoid double counting of clients, clients are only listed in the group of the AP with which they are associated. Note that device groups with only controllers in them report no clients.
<b>Usage</b>	A running average of the sum of bytes in and bytes out for the managed radio page.
<b>VPN Sessions</b>	Number of active (connected) VPN sessions under this group.
<b>Duplicate</b>	Creates a new group with the name <b>Copy of &lt;Group Name&gt;</b> with configuration settings. (Aruba configuration settings will have to be manually added back.)
<b>Up/Down Status Polling Period</b>	The time between Up/Down SNMP polling periods for each device in the group. Detailed SNMP polling period information is available on the <b>Groups &gt; Basic</b> configuration page. Note that by default, most polling intervals do not match the up/down period.



When you first configure AMP, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to [“Configuring Basic Group Settings” on page 74](#).

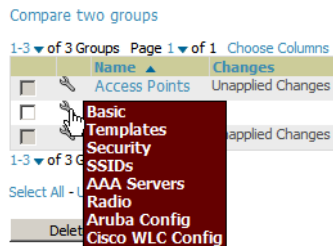
## Configuring Basic Group Settings

The first default device group that AMP sets up is the **Access Points** group, but you can use this procedure to add and configure any device group. Perform these steps to configure basic group settings, then continue to additional procedures to define additional settings as required.

1. Go to the **Groups > List** page. Existing device groups appear on this page.
2. To create a new group, select **Add**. Enter a group name and select **Add**. The **Groups > Basic** page appears.

To edit an existing device group, select the **manage** (wrench) icon next to the group. The **Groups > Basic** page appears. If you mouse over an existing group's wrench, a popup menu allows you to select **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, **Radio**, **Aruba Config** or **Cisco WLC Config** to edit those pages as desired, as illustrated in [Figure 40](#).

**Figure 40** Pop-up When Hovering over Wrench Icon in Groups > List



[Figure 41](#) illustrates an example **Groups > Basic** page.

**Figure 41 Groups > Basic Page Illustration**

Basic	
Name:	aruba corp
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Audit Configuration on Devices: Toggling this will set all devices in this group to 'Monitor Only'	<input type="radio"/> Yes <input checked="" type="radio"/> No

Global Groups	
Use Global Group:	<input type="radio"/> Yes <input checked="" type="radio"/> No

SNMP Polling Periods	
Up/Down Status Polling Period:	5 minutes
Override Polling Period for Other Services:	<input checked="" type="radio"/> Yes <input type="radio"/> No
AP Interface Polling Period:	10 minutes
Client Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	5 minutes
802.11 Counters Polling Period:	15 minutes
Rogue AP and Device Location Data Polling Period:	Disabled
CDP Neighbor Data Polling Period:	30 minutes

Routers and Switches	
Read ARP Table:	4 hours
Read CDP Table for Device Discovery:	4 hours
Read Bridge Forwarding Table:	4 hours
Interface Up/Down Polling Period:	10 minutes
Interface Bandwidth Polling Period:	15 minutes
Interface Error Counter Polling Period:	30 minutes
Poll 802.3 error counters:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Poll Cisco interface error counters:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Notes	
Notes:	

Group Display Options	
Show device settings for:	All devices

Automatic Static IP Assignment	
Assign Static IP Addresses to Devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Spanning Tree Protocol	
Spanning Tree Protocol: Proxim only	<input type="radio"/> Yes <input checked="" type="radio"/> No

NTP	
NTP Server #1:	
NTP Server #2:	
NTP Server #3:	
UTC Time Zone:	0
Daylight Saving Time:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Cisco IOS/Catalyst	
SNMP Version:	2c
Cisco IOS CLI Communication:	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Cisco IOS Config File Communication:	<input checked="" type="radio"/> TFTP <input type="radio"/> SCP

Cisco WLC	
SNMP Version:	2c
CLI Communication:	<input type="radio"/> Telnet <input checked="" type="radio"/> SSH

Proxim/Avaya	
SNMP Version:	1
Enable DNS Client:	<input type="radio"/> Yes <input checked="" type="radio"/> No
HTTP Server Port (1-65535):	80
Country Code:	United States

HP ProCurve	
SNMP Version:	2c
ProCurve XL/ZLWeSM CLI Communication:	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Controller SNMP Version:	2c

Symbol	
SNMP Version:	2c
Client Inactivity Timeout (3-600 min):	3
Symbol Controller CLI Communication: WS5100, RF54000, RF56000, and RF57000 controllers only	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
SSH Version: WS2000 controllers only	<input checked="" type="radio"/> v1 <input type="radio"/> v2
Web Config Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Aruba	
SNMP Version:	2c
Offload WMS Database:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Aruba GUI Config:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Ignore Rogues Discovered by Remote APs:	<input type="radio"/> Yes <input checked="" type="radio"/> No

3Com/Enterasys/Nortel/Trapeze	
SNMP Version:	2c

Universal Devices, Routers and Switches	
SNMP Version:	1

Automatic Authorization	
Add New Controllers and Autonomous Devices Location:	Use Global Setting
Current Global Setting for Controllers:	New Device List
Add New Thin APs Location:	Use Global Setting
Current Global Setting for Thin APs:	New Device List

Maintenance Windows	
Add	New AP Group Maintenance Window

Save
Save and Apply
Revert

- Define the settings in the **Basic** and **Global Group** sections. [Table 40](#) describes several typical settings and default values of this **Basic** section.



**Table 40 Basic and Global Groups Fields and Default Values**

Setting	Default	Description
<b>Name</b>	Defined when first adding the group	Displays or changes the group name. As desired, use this field to set the name to uniquely identify the group by location, vendor, department, or any other identifier (such as “Accounting APs,” “Cisco devices,” “802.1x APs,” and so forth).
<b>Missed SNMP Poll Threshold</b>	1	Sets the number of Up/Down SNMP polls that must be missed before AMP considers a device to be down. The number of SNMP retries and the SNMP timeout of a poll can be set on the <b>Device Setup &gt; Communication</b> page.
<b>Regulatory Domain</b>	United States	Sets the regulatory domain in AMP, limiting the selectable channels for APs in the group.
<b>Timezone</b>	AMP System Time	Allows group configuration changes to be scheduled relative to the time zone in which the devices are located. This setting is used for scheduling group-level configuration changes.
<b>Allow One-to-One NAT</b>	No	Allows AMP to talk to the devices on a different IP address than the one configured on the device. <b>NOTE:</b> If enabled, the LAN IP Address listed on the <b>AP/Devices &gt; Manage</b> configuration page under the <b>Settings</b> area is different than the IP Address under the <b>Device Communication</b> area.
<b>Audit Configuration on Devices</b>	Yes	Auditing and pushing of configuration to devices can be disabled on all the devices in the group. Once disabled, all the devices in the groups will not be counted towards mismatched devices.
<b>Use Global Group</b>	No	When enabled, this field allows you to define the device group to be a Global Group. Refer to <a href="#">“Using Global Groups for Group Configuration” on page 105</a> .

- Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. [Table 41](#) describes the SNMP polling settings.

**Table 41 SNMP Polling Periods Fields and Default Values**

Setting	Default	Description
<b>Up/Down Status Polling Period</b>	5 minutes	Sets time between Up/Down SNMP polling for each device in the group. The Group SNMP Polling Interval overrides the global parameter configured on the <b>Device Setup &gt; Communication</b> page. An initial polling interval of <b>5</b> minutes is best for most networks.
<b>Override Polling Period for Other Services</b>	No	Enables or disables overriding the base SNMP Polling Period. If you select <b>Yes</b> , the other settings in the SNMP Polling Periods section are activated, and you can override default values.
<b>AP Interface Polling Period</b>	5 minutes	Sets the interval at which AMP polls for radio monitoring and bandwidth being used by a device.
<b>Client Data Polling Period</b>	5 minutes	Sets time between SNMP polls for client data for devices in the group.
<b>Thin AP Discovery Polling Period</b>	5 minutes	Sets time between SNMP polls for Thin AP Device Discovery. Controllers are the only devices affected by this polling interval.
<b>Device-to-Device link Polling Period</b>	5 minutes	Sets time between SNMP polls for Device-to-Device link polling. Mesh APs are the only devices affected by this polling interval.
<b>802.11 Counters Polling Period</b>	5 minutes	Sets time between SNMP polls for 802.11 Counter information.
<b>Rogue AP and Device Location Data Polling Period</b>	5 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.
<b>CDP Neighbor Data Polling Period</b>	30 minutes	Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors.

- Record additional information and comments about the group in the **Notes** section.



6. To configure which options and tabs are visible for the group, complete the settings in the **Group Display Options** section. [Table 42](#) describes the settings and default values.

**Table 42** *Group Display Options Fields and Default Values*

Setting	Default	Description
<b>Show device settings for:</b>	Only devices on this AMP	Drop-down menu determines which Group tabs and options are to be viewable by default in new groups. Settings include the following: <ul style="list-style-type: none"><li>• <b>All Devices</b>—AMP displays all Group tabs and setting options.</li><li>• <b>Only devices in this group</b>—AMP hides all options and tabs that do not apply to the devices in the group. If you use this setting, then to get the group list to display the correct SSIDs for the group, you must <b>Save and Apply</b> on the group.</li><li>• <b>Only devices on this AMP</b>— hides all options and tabs that do not apply to the APs and devices currently on AMP.</li><li>• <b>Use system defaults</b>—Use the default settings on <b>AMP Setup &gt; General</b></li><li>• <b>Selected device types</b>—Allows you to specify the device types for which AMP displays Group settings.</li></ul>
<b>Selected Device Types</b>	N/A	This option appears if you chose to display selected device types, allowing you to select the device types to display group settings. Use <b>Select devices in this group</b> to display only devices in the group being configured.

7. To assign dynamically a range of static IP addresses to new devices as they are added into the group, locate the **Automatic Static IP Assignment** section on the **Groups > Basic** configuration page. If you select **Yes** in this section, additional fields appear. Complete these fields as required. [Table 43](#) describes the settings and default values. This section is only relevant for a small number of device types, and will appear when they are present.

**Table 43** *Automatic Static IP Assignment Fields and Default Values*

Setting	Default	Description
<b>Assign Static IP Addresses to Devices</b>	No	Enables AMP to statically assign IP addresses from a specified range to all devices in the Group.
<b>Start IP Address</b>	Blank	Sets the first address AMP assigns to the devices in the Group.
<b>Number of Addresses</b>	Blank	Sets the number of addresses in the pool from which AMP can assign IP addresses.
<b>Subnet Mask</b>	Blank	Sets the subnet mask to be assigned to the devices in the Group.
<b>Subnet Gateway</b>	Blank	Sets the gateway to be assigned to the devices in the Group.
<b>Next IP Address</b>	Blank	Defines the next IP address queued for assignment. This field is disabled for the initial Access Points group.

8. To configure Spanning Tree Protocol on WLC devices and Proxim APs, locate the Spanning Tree Protocol section on the **Groups > Basic** configuration page. Adjust these settings as required. [Table 44](#) describes the settings and default values.

**Table 44** *Spanning Tree Protocol Fields and Default Values*

Setting	Default	Description
<b>Spanning Tree Protocol</b>	No	Enables or disables Spanning Tree Protocol on Proxim APs.
<b>Bridge Priority</b>	32768	Sets the priority for the AP. Values range from 0 to 65535. Lower values have higher priority. The lowest value is the root of the spanning tree. If all devices are at default the device with the lowest MAC address will become the root.
<b>Bridge Maximum Age</b>	20	Sets the maximum time, in seconds, that the device stores protocol information. The supported range is from 6 to 40.

**Table 44 Spanning Tree Protocol Fields and Default Values (Continued)**

Setting	Default	Description
<b>Bridge Hello Time</b>	2	Sets the time, in seconds, between Hello message broadcasts.
<b>Bridge Forward Delay</b>	15	Sets the time, in seconds, that the port spends in listening and learning mode if the spanning tree has changed.

9. To configure NTP settings locate the **NTP** section and adjust these settings as required. [Table 45](#) describes the settings and default values.

**Table 45 NTP Fields and Default Values**

Setting	Default	Description
<b>NTP Server #1,2,3</b>	None	Sets the IP address of the NTP server to be configured on the AP.
<b>UTC Time Zone</b>	0	Sets the hour offset from UTC time to local time for the AP. Times displayed in AMP graphs and logs use the time set on the AMP server.
<b>Daylight Saving Time</b>	No	Enables or disables the advanced daylight saving time settings in the Proxim section of the <b>Groups &gt; Basic</b> configuration page.

10. To configure settings specific to Cisco IOS/Catalyst, locate the **Cisco IOS/Catalyst** section and adjust these settings as required. [Table 46](#) describes the settings and default values.

**Table 46 Cisco IOS/Catalyst Fields and Default Values**

Setting	Default	Description
<b>SNMP Version</b>	2c	The version of SNMP used by AMP to communicate to the AP.
<b>Cisco IOS CLI Communication</b>	Telnet	The protocol AMP uses to communicate with Cisco IOS devices. Selecting <b>SSH</b> uses the secure shell for command line page (CLI) communication. Selecting <b>Telnet</b> sends the data in clear text via Telnet.
<b>Cisco IOS Config File Communication</b>	TFTP	The protocol AMP uses to communicate with Cisco IOS devices. Selecting <b>SCP</b> uses the secure copy protocol for file transfers and displays the <b>SCP Version</b> option. Selecting <b>TFTP</b> will use the insecure trivial file transfer protocol. The SCP login and password should be entered in the Telnet username and password fields.

11. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section and adjust these settings as required. [Table 47](#) describes the settings and default values.

**Table 47 Cisco WLC Fields and Default Values**

Setting	Default	Description
<b>SNMP Version</b>	2c	Sets the version of SNMP used by AirWave to communicate to WLC controllers.
<b>CLI Communication</b>	Telnet	Sets the protocol AMP uses to communicate with Cisco IOS devices. Selecting <b>SSH</b> uses the secure shell for command line page (CLI) communication. Selecting <b>Telnet</b> sends the data in clear text via Telnet.



When configuring Cisco WLC controllers, refer to “[Configuring Wireless Parameters for Cisco Controllers](#)” on [page 96](#).

12. To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section and adjust these settings as required. [Table 48](#) describes the settings and default values.

**Table 48** *Proxim/Avaya Fields and Default Values*

Setting	Default	Description
<b>SNMP Version</b>	1	Sets the version of SNMP used by AMP to communicate to the AP.
<b>Enable DNS Client</b>	No	Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select <b>Yes</b> for this setting, additional DNS fields display.
<b>Primary DNS server</b>	Blank	Sets the IP address of the Primary DNS server.
<b>Secondary DNS server</b>	Blank	Sets the IP address of the Secondary DNS server.
<b>Default DNS domains</b>	Blank	Sets the default DNS domain used by the AP.
<b>HTTP Server Port</b>	80	Sets this port as the HTTP server port on all Proxim APs in the group.
<b>Country Code</b>	United States	Configures AMP to derive its time settings based on the country of location, as specified in this field.

13. To configure HP ProCurve specific settings, locate the **HP ProCurve** section and adjust these settings as required. [Table 49](#) describes the settings and default values.

**Table 49** *HP ProCurve Fields and Default Values*

Setting	Default	Description
<b>SNMP Version</b>	2c	Sets the version of SNMP used by AMP to communicate to the AP.
<b>ProCurve XL/ZWeSM CLI Communication</b>	Telnet	Sets the protocol AMP uses to communicate with ProCurve XLWeSM devices. Selecting <b>SSH</b> will use the secure shell for command line (CLI) communication. Selecting <b>Telnet</b> will send the data in clear text via telnet.
<b>Controller SNMP Version</b>	2c	Specifies the version of SNMP used by AMP to communicate to the controller.



DST Start Month, Start Day, End Month, End Day, and DST Offset are only visible if Daylight Saving Time is enabled in the NTP section of the **Groups > Basic** configuration page.

14. To configure Symbol/Motorola settings, locate the **Symbol** section and adjust these settings as required. [Table 50](#) describes the settings and default values of this section.

**Table 50** *Symbol Fields and Default Values*

Setting	Default	Description
<b>SNMP Version</b>	2c	Specifies the version of SNMP used by AMP to communicate to the device.
<b>Client Inactivity Timeout (3-600 min)</b>	3	Sets the minutes of inactivity after which a client associated to a Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. <b>NOTE:</b> For other APs, AMP has more precise methods to determine when inactive clients are no longer associated to an AP.
<b>Symbol Controller CLI Communication</b>	Telnet	The connection type to support the command-line interface (CLI) connection. The options are <b>Telnet</b> and secure shell ( <b>SSH</b> ). This is supported for WS5100, RFS4000, RFS6000 and RFS7000 devices only.
<b>Web Config Interface</b>	Yes	Enables or disables the <b>http/https</b> configuration page for the Symbol 4131 devices.

15. To configure settings specific to ArubaOS, locate the **Aruba** section and adjust these settings as required. Table 51 describes the settings and default values of this section.

**Table 51** *Aruba Fields and Default Values*

Setting	Default	Description
<b>SNMP Version</b>	2c	The version of SNMP used by AMP to communicate to the AP.
<b>Offload WMS Database</b>	No	Configures commands previously documented in the <i>AirWave Best Practices Guide</i> . When enabled, this feature allows AMP to display historical information for WLAN switches.  Changing the setting to <b>Yes</b> pushes commands via SSH to all WLAN switches in Monitor Only mode without rebooting the controller. The command can be pushed to controllers in manage mode (also without rebooting the controller) if the <b>Allow WMS Offload</b> setting on <b>AMP Setup &gt; General</b> is changed to <b>Yes</b> .
<b>Aruba GUI Config</b>	Yes	This setting selects whether you'd like to configure your Aruba devices using the <b>Groups &gt; Aruba Config</b> method (either global or group) or using Templates.
<b>Ignore Rogues Discovered by Remote APs</b>	No	Configures whether to turn off RAPIDS rogue classification and rogue reporting for RAPs in this group.

16. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/Trapeze** section and define the version of SNMP to be supported.
17. To configure support for routers and switches in the group, locate the **Routers and Switches** section and adjust these settings as required. This section defines the frequency in which all devices in the group polled. These settings can be disabled entirely as desired. Table 52 describes the settings and default values of this section.

**Table 52** *Routers and Switches Fields and Default Values*

Setting	Default	Description
<b>Read ARP Table</b>	4 hours	Sets the frequency in which devices poll routers and switches for Address Resolution Protocol (ARP) table information. This setting can be disabled, or set to poll for ARP information in a range from every 15 seconds to 12 hours.
<b>Read CDP Table for Device Discovery</b>	4 hours	For Cisco devices, sets the frequency in which devices poll routers and switches for Cisco Discovery Protocol (CDP) information. This setting can be disabled, or set to poll for CDP neighbor information in a range from every 15 seconds to 12 hours.
<b>Read Bridge Forwarding Table</b>	4 hours	Sets the frequency in which devices poll the network for bridge forwarding information. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours.
<b>Interface Up/Down Polling Period</b>	5 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll from switches in a range from every 15 seconds to 30 minutes.
<b>Interface Bandwidth Polling Period</b>	15 minutes	Sets the frequency in which network interfaces are polled for bandwidth usage. This setting can be disabled, or set to poll from switches in a range from every 5 minutes to 30 minutes.
<b>Interface Error Counter Polling Period</b>	30 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 5 minutes to 30 minutes.
<b>Poll 802.3 error counters</b>	No	Sets whether 802.3 error counters should be polled.
<b>Poll Cisco interface error counters</b>	No	Sets whether the interface error counters for Cisco devices should be polled.

18. To configure settings for universal devices on the network, including routers and switches that support both wired and wireless networks, locate the **Universal Devices, Routers and Switches** section of the **Groups > Basic** page and define the version of SNMP to be supported.
19. To control the conditions by which devices are automatically authorized into this group, locate the **Automatic Authorization** settings section and adjust these settings as required. [Table 53](#) describes the settings and default values.

**Table 53 Automatic Authorization Fields and Default Values**

Setting	Default	Description
<b>Add New Controllers and Autonomous Devices Location</b>	Use Global Setting	Whether to auto authorize new controllers to the <b>New Devices</b> List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder. The Current Global Setting set in <b>AMP Setup &gt; General</b> is shown below this field. Selecting a different option overrides the global setting.
<b>Add New Thin APs Location</b>	Use Global Setting	Whether to auto authorize new thin APs to the <b>New Devices</b> List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder. The Current Global Setting set in <b>AMP Setup &gt; General</b> is shown below. Selecting a different option overrides the global setting for this group.

20. To automate putting multiple devices in this group into Manage mode at once so that changes can be applied and have the devices revert to Monitor-Only mode after the maintenance period is over, locate the **Maintenance Windows** option and define a new AP Group Maintenance Window.
21. Select **Save** when the configurations of the **Groups > Basic** configuration page are complete to retain these settings, but without pushing these settings to all devices in the group. **Save** is a good option if you intend to make additional device changes in the group, and wish to wait until all configurations are complete before you push all configurations at one time.  
  
Select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

## What Next?

Continue to additional sections in this chapter to create new groups or to edit existing groups.

Once general group-level configurations are complete, continue to later chapters in this document to add or edit additional device-level configurations and to use several additional AMP functions.

## Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Groups > AAA Servers** page.

Once defined on this page, RADIUS servers are selectable in the drop-down menus on the **Groups > Security and Groups > SSIDs** configuration pages. Perform these steps to create RADIUS servers.



TACACS+ servers are configurable only for Cisco WLC devices. Refer to [“Configuring Cisco WLC Security Parameters and Functions” on page 96](#).

1. Go to the **Groups > List** page and select the group for which to define AAA servers by selecting the group name. The **Monitor** page appears.
2. Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. [Figure 42](#) illustrate this page for AAA RADIUS Servers:

**Figure 42 Groups > AAA Servers Page Illustration**

WLANs on a Cisco WLC can be configured on the [Cisco WLC Config](#) page.

New RADIUS Server

	Hostname/IP Address ▲	Authentication	Authentication Port	Accounting	Accounting Port	Timeout	Max Retries
	10.180.180.180	Yes	1812	No	-	3	0
	10.181.181.181	Yes	1812	No	-	4	0
<input type="checkbox"/>	10.183.183.183	Yes	1812	No	-	2	0
<input type="checkbox"/>	10.182.182.182	Yes	1812	No	-	2	0

4 RADIUS Servers

[Select All](#) - [Unselect All](#)

- To add a RADIUS server or edit an existing server, select **Add New RADIUS Server** or the corresponding pencil icon to edit an existing server. [Table 54](#) describes the settings and default values of the **Add/Edit** page.

**Table 54 Adding a RADIUS Server Fields and Default Values**

Setting	Default	Description
<b>Hostname/IP Address</b>	None	Sets the IP Address or DNS name for RADIUS Server. <b>NOTE:</b> IP Address is required for Proxim/ORiNOCO and Cisco Aironet IOS APs.
<b>Secret and Confirm Secret</b>	None	Sets the shared secret that is used to establish communication between AMP and the RADIUS server. <b>NOTE:</b> The shared secret entered in AMP must match the shared secret on the server.
<b>Authentication</b>	No	Sets the RADIUS server to perform authentication when this setting is enabled with <b>Yes</b> .
<b>Authorization Port</b>	1812	Appears when <b>Authentication</b> is enabled. Sets the port used for communication between the AP and the RADIUS server.
<b>Accounting</b>	No	Sets the RADIUS server to perform accounting functions when enabled with <b>Yes</b> .
<b>Accounting Port</b>	No	Appears when <b>Accounting</b> is enabled. Sets the port used for communication between the AP and the RADIUS server.
<b>Timeout (0-86400)</b>	None	Sets the time (in seconds) that the access point waits for a response from the RADIUS server.
<b>Max Retries (0-20)</b>	None	Sets the number of times a RADIUS request is resent to a RADIUS server before failing. <b>NOTE:</b> If a RADIUS server is not responding or appears to be responding slowly, consider increasing the number of retries.

- Select **Add** to complete the creation of the RADIUS server, or select **Save** if editing an existing RADIUS server. The **Groups > AAA Servers** page displays this new or edited server. You can now reference this server on the **Groups > Security** page.

AMP supports reports for subsequent RADIUS Authentication. These are viewable by selecting **Reports > Generated**, scrolling to the bottom of the page, and selecting **Latest RADIUS Authentication Issues Report**.

- To make additional RADIUS configurations for device groups, use the **Groups > Security** page and continue to the next topic.

## Configuring Group Security Settings

The **Groups > Security** page allows you to set security policies for APs in a device group:

- Select the device group for which to define security settings from the **Groups > List** page.



2. Go to **Groups > Security**. Some controls on this page interact with additional AMP pages. [Figure 43](#) illustrates this page and [Table 55](#) explains the fields and default values.

**Figure 43** *Groups > Security Page Illustration*

**VLANs**

VLAN Tagging and Multiple SSIDs: ☒ Enabled ☐ Disabled

Create and edit VLANs and SSIDs on this group's [SSIDs](#) page.

Management VLAN ID (0-4094, Untagged):

Permit RADIUS-Assigned Dynamic VLANs: ☐ Yes ☒ No

VLAN ID Format: HP ProCurve 420 only ☐ ASCII ☒ Hex

Ethernet Untagged VLAN ID (1-4094):

**General**

Create Closed Network: ☐ Yes ☒ No

Block All Inter-Client Communication: ☐ Yes ☒ No

**EAP Options**

WEP Key Rotation Interval (0-10000000 sec):

Session Key Refresh Rate (0-1440 min):

Session Timeout (0-65535 sec):

Cisco TKIP: ☐ Yes ☒ No

Cisco MIC: ☐ MMH ☒ Disabled

**RADIUS Authentication Servers**

RADIUS Authentication Server #1:

RADIUS Authentication Server #2:

RADIUS Authentication Server #3:

RADIUS Authentication Server #4:

Authentication Profile Name: Proxim Only

Authentication Profile Index: Proxim Only

**RADIUS Accounting Servers**

RADIUS Accounting Server #1:

RADIUS Accounting Server #2:

RADIUS Accounting Server #3:

RADIUS Accounting Server #4:

Accounting Profile Name: Proxim Only

Accounting Profile Index: Proxim Only

**MAC Address Authentication**

MAC Address Authentication: ☐ Yes ☒ No

MAC Address Format: Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL v2.1.0 and higher only

Authorization Lifetime (900-43200 sec):

Primary RADIUS Server Reattempt Period (0-120 min):

**Table 55** *Groups > Security Page Fields and Default Values*

Setting	Default	Description
<b>VLANs Section</b>		
<b>VLAN Tagging and Multiple SSIDs</b>	Enabled	This field enables support for VLANs and multiple SSIDs on the wireless network. If this setting is enabled, define additional VLANs and SSIDs on the <b>Groups &gt; SSIDs</b> page. Refer to “ <a href="#">Configuring Group SSIDs and VLANs</a> ” on page 84.
<b>Management VLAN ID</b>	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in AMP. This setting is supported only for the following devices: <ul style="list-style-type: none"> <li>Proxim AP-600, AP-700, AP-2000, AP-4000</li> <li>Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8</li> <li>ProCurve520WL</li> </ul>
<b>General Section</b>		
<b>Create Closed Network</b>	No	If enabled, the APs in the Group do not broadcast their SSIDs. <b>NOTE:</b> Creating a closed network will make it more difficult for intruders to detect your wireless network.
<b>Block All Inter-client Communication</b>	No	If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. <b>NOTE:</b> This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks.
<b>EAP Options Section</b>		
<b>WEP Key Rotation Interval</b>	300	Sets the frequency at which the Wired Equivalent Privacy (WEP) keys are rotated in the device group being configured. The supported range is from 0 to 10,000,000 seconds.
<b>RADIUS Authentication Servers Section</b>		
<b>RADIUS Authentication Server #1 - #4</b>	Not selected	Defines one or more RADIUS Authentication servers to be supported in this device group. Select up to four RADIUS authentication servers from the four drop-down menus.

**Table 55 Groups > Security Page Fields and Default Values (Continued)**

Setting	Default	Description
<b>Authentication Profile Name</b>	AMP-Defined Server #1	For Proxim devices only, this field sets the name of the authentication profile to be supported in this device group.
<b>Authentication Profile Index</b>	1	For Proxim devices only, this field sets the name of the authentication profile index to be supported in this device group.
<b>RADIUS Accounting Servers Section</b>		
<b>RADIUS Accounting Server #1 - #4</b>	Not selected	Defines one or more RADIUS Accounting servers to be supported in this device group. Select up to four RADIUS accounting servers from the four drop-down menus.
<b>Authentication Profile Name</b>		For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group.
<b>Authentication Profile Index</b>	3	For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group.
<b>MAC Address Authentication Section</b>		
<b>MAC Address Authentication</b>	No	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
<b>MAC Address Format</b>	Single Dash	<p>Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests:</p> <ul style="list-style-type: none"> <li>• Dash Delimited: xx-xx-xx-xx-xx-xx (default)</li> <li>• Colon Delimited: xx:xx:xx:xx:xx:xx</li> <li>• Single-Dash: xxxxxx-xxxxxx</li> <li>• No Delimiter: xxxxxxxxxxxx</li> </ul> <p>This option is supported only for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, HP ProCurve 520WL</p>
<b>Authorization Lifetime</b>	1800	Sets the amount of time a user can be connected before reauthorization is required. The supported range is from 900 to 43,200 seconds.
<b>Primary RADIUS Server Reattempt Period</b>	0	Specifies the time (in minutes) that the AP awaits responses from the primary RADIUS server before communicating with the secondary RADIUS server, and so forth

3. Select **Save** to retain these security configurations for the group, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.
4. Continue with additional security-related procedures in this document for additional RADIUS and SSID settings for device groups, as required.

## Configuring Group SSIDs and VLANs

The **Groups > SSIDs** configuration page allows you to create and edit SSIDs and VLANs that apply to a device group. Perform these steps to create or edit VLANs and to set SSIDs.



WLANs that are supported from one or more Cisco WLC controllers can be configured on the **Groups > Cisco WLC Config** page.



Figure 44 illustrates an example of the **Groups > SSIDs** page.

**Figure 44** *Groups > SSIDs Page Illustration*

Group: **Aruba HQ**

Configure VLANs for a Cisco WLC on the [Cisco WLC Config](#) page.

	SSID ▲	VLAN ID	Name	Encryption Mode	1st Radio		2nd Radio		Native VLAN
					Enabled	Primary	Enabled	Primary	
<input type="checkbox"/>	wpa	51	wpa	No Encryption	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>

[Select All - Unselect All](#)



AMP reports users by radio and by SSID. Graphs on the AP and controller monitoring pages display bandwidth in and out based on SSID. AMP reports can also be run and filtered by SSID. An option on the **AMP Setup > General** page can age out SSIDs and their associated graphical data; by default, this is set to 365 days.

1. Go to **Groups > List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups > SSIDs** configuration page. [Table 56](#) describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

**Table 56** *Groups > SSIDs Fields and Descriptions*

Field	Description
<b>SSID</b>	Displays the SSID associated with the VLAN.
<b>VLAN ID</b>	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.
<b>Name</b>	Displays the name of the VLAN.
<b>Encryption Mode</b>	Displays the encryption on the VLAN.
<b>First or Second Radio Enabled</b>	Enables the VLAN, SSID and Encryption Mode on the radio control.
<b>First or Second Radio Primary</b>	Specifies which VLAN to be used as the primary VLAN. A primary VLAN is required. <b>NOTE:</b> If you create an open network (see the <b>Create Closed Network</b> setting below) in which the APs broadcast an SSID, the primary SSID is broadcast.
<b>Native VLAN</b>	Sets this VLAN to be the native VLAN. Native VLANs are untagged and typically used for management traffic only. AMP requires a Native VLAN to be set. For AP types do not require a native VLAN, create a dummy VLAN, disable it on both radio controls, and ensure that it has the highest VLAN ID.

3. Select **Add** to create a new SSID or VLAN, or select the pencil icon next to an existing SSID/VLAN to edit that existing SSID or VLAN. The **Add SSID/VLAN** configuration page appears as illustrated in [Figure 45](#) and explained in [Table 57](#).

**Figure 45** *Groups > SSIDs > Add SSID/VLAN Page Illustration*

The screenshot shows the 'Add SSID/VLAN' configuration page. It includes sections for SSID/VLAN settings, Encryption, EAP Options, RADIUS Authentication Servers, and RADIUS Accounting Servers. The SSID/VLAN section has fields for Specify Interface Name, Interface, SSID, Name, Maximum Allowed Associations, Broadcast SSID, Partial Closed System, Unique Beacon, and Block All Inter-Client Communication. The Encryption section has an Encryption Mode dropdown. The EAP Options section has a WEP Key Rotation Interval field. The RADIUS Authentication Servers and RADIUS Accounting Servers sections each have three server entries with dropdown menus for server selection and text fields for profile name and index. At the bottom right are 'Add' and 'Cancel' buttons.

4. Locate the **SSID/VLAN** section on the **Groups > SSIDs** configuration page and adjust these settings as required. This section encompasses the basic VLAN configuration. [Table 57](#) describes the settings and default values. Note that the displayed settings can vary.

**Table 57** *Groups > SSIDs > SSID/VLAN Section Fields and Default Values*

Setting	Default	Description
<b>Specify Interface Name</b>	Yes	Enables or disables an interface name for the VLAN interface. Selecting <b>No</b> for this option displays the <b>Enable VLAN Tagging</b> and <b>VLAN ID</b> options.
<b>Interface</b>	None	Sets the interface to support the SSID/VLAN combination.
<b>SSID</b>	None	Sets the Service Set Identifier (SSID), which is a 32-character user-defined identifier attached to the header of packets sent over a WLAN. It acts as a password when a mobile device tries to connect to the network through the AP, and a device is not permitted to join the network unless it can provide the unique SSID.
<b>Name</b>	None	Sets a user-definable name associated with SSID/VLAN combination.
<b>VLAN ID (1-4094)</b>	None	Indicates the number of the VLAN designated as the Native VLAN, typically for management purposes. Displays if <b>Specify Interface Name</b> is set to <b>No</b> .
<b>Maximum Allowed Associations (0-2007)</b>	255	Indicates the maximum number of mobile users which can associate with the specified VLAN/SSID. <b>NOTE:</b> 0 means unlimited for Cisco.
<b>Broadcast SSID</b> (Cisco WLC, Proxim and Symbol 4131 only)	No	For specific devices as cited, this setting enables the AP to broadcast the SSID for the specified VLAN/SSID. This setting works in conjunction with the <b>Create Closed Network</b> setting on the <b>Groups &gt; Security</b> configuration page. Proxim devices support a maximum of four SSIDs. <b>NOTE:</b> This option should be enabled to ensure support of legacy users.
<b>Partial Closed System</b> (Proxim only)	No	For Proxim only, this setting enables to AP to send its SSID in every beacon, but it does not respond to any probe requests.
<b>Unique Beacon</b> (Proxim only)	No	For Proxim only, if more than one SSID is enabled, this option enables them to be sent in separate beacons.
<b>Block All Inter-Client Communication</b>	Yes	This setting blocks communication between client devices based on SSID.

5. Locate the **Encryption** area on the **Groups > SSIDs** page and adjust these settings as required. [Table 58](#) describes the settings and default values.

**Table 58** *Groups > SSIDs > Encryption Section Field and Default Values*

Setting	Default	Description
<b>Encryption Mode</b>	No Encryption	Drop-down menu determines the level of encryption required for devices to associate to the APs. The drop-down menu options are as follows. Each option displays additional encryption settings that must be defined. Complete the associated settings for any encryption type chosen: <ul style="list-style-type: none"> <li>• <b>No Encryption</b></li> <li>• <b>Optional WEP</b>—Wired Equivalent Privacy, not PCI compliant as of 2010</li> <li>• <b>Require WEP</b>—Wired Equivalent Privacy, not PCI compliant as of 2010</li> <li>• <b>Require 802.1x</b>—Based on the WEP algorithm</li> <li>• <b>Require Leap</b>—Lightweight Extensible Authentication Protocol</li> <li>• <b>802.1x+WEP</b>—Combines the two encryption types shown</li> <li>• <b>802.1x+LEAP</b>—Combines the two encryption types shown</li> <li>• <b>LEAP+WEP</b>—Combines the two encryption types shown</li> <li>• <b>Static CKIP</b>—Cisco Key Integrity Protocol</li> <li>• <b>WPA</b>—Wi-Fi Protected Access protocol</li> <li>• <b>WPA/PSK</b>—Combines WPA with Pre-Shared Key encryption</li> <li>• <b>WPA2</b>—Wi-Fi Protected Access 2 encryption</li> <li>• <b>WPA2/PSK</b>—Combines the two encryption methods shown</li> <li>• <b>xSec</b>—FIPS-compliant encryption including Layer 2 header info</li> </ul>

6. Locate the **EAP Options** area on the **Groups > SSIDs** page, and complete the settings. [Table 59](#) describes the settings and default values.

**Table 59** *Groups > SSIDs > EAP Options Section Field and Default Value*

Setting	Default	Description
<b>WEP Key Rotation Interval</b>	120	Time (in seconds) between WEP key rotation on the AP.

7. Locate the **RADIUS Authentication Servers** area on the **Groups > SSIDs** configuration page and define the settings. [Table 60](#) describes the settings and default values.

**Table 60** *Groups > SSIDs > RADIUS Authentication Servers Fields and Default Values*

Setting	Default	Description
<b>RADIUS Authentication Server 1-3</b> (Cisco WLC, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the <b>Groups &gt; RADIUS</b> configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network.
<b>Authentication Profile Name</b> (Proxim Only)	None	Sets the Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000.
<b>Authentication Profile Index</b> (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

8. Select **Save** when the security settings and configurations in this procedure are complete.



You may need to return to the **Groups > Security** configuration page to configure or reconfigure RADIUS servers.

9. Locate the **RADIUS Accounting Servers** area on the **Groups > SSIDs** configuration page and define the settings. [Table 61](#) describes the settings and default values.

**Table 61** *Groups > SSIDs > Radius Accounting Servers Fields and Default Values*

Setting	Default	Description
<b>RADIUS Accounting Server 1-3</b> (Cisco WLC, Proxim Only)	None	Pull-down menu selects RADIUS Accounting servers previously entered on the <b>Groups &gt; RADIUS</b> configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets for this SSID/VLAN.
<b>Accounting Profile Name</b> (Proxim Only)	None	Sets the Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000.
<b>Accounting Profile Index</b> (Proxim Only)	None	Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

10. Select **Save** to retain these **Security** configurations for the group, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.
11. Continue with additional security-related procedures in this document for additional RADIUS, and SSID settings for device groups, as required.

## Configuring Radio Settings for Device Groups

The **Groups > Radio** configuration page allows you to specify detailed RF-related settings for devices in a particular group.



---

If you have existing deployed devices, you may want to use the current RF settings on those devices as a guide for configuring the settings in your default Group.

---

Perform the following steps to define RF-related radio settings for groups.

1. Go to the **Groups > List** page and select the group for which to define radio settings by selecting the group name. Alternatively, select **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Go to the **Groups > Radio** page. [Figure 46](#) illustrates this page.

**Figure 46 Groups > Radio Page Illustration**

Group: Aruba HQ

Radio Settings	
Allow Automatic Channel Selection (2.4 GHz):	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow Automatic Channel Selection (5 GHz):	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow Automatic Channel Selection (4.9 GHz Public Safety):	<input type="radio"/> Yes <input checked="" type="radio"/> No
802.11b Data Rates (Mbps):	1.0: <input type="text" value="Optional"/> 2.0: <input type="text" value="Required"/> 5.5: <input type="text" value="Optional"/> 11.0: <input type="text" value="Optional"/>
Frag Threshold Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Threshold Value (256-2347 bytes):	<input type="text" value="2337"/>
RTS/CTS Threshold Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Threshold Value (0-2347 bytes):	<input type="text" value="1200"/>
RTS/CTS Maximum Retries (1-255):	<input type="text" value="32"/>
Maximum Data Retries (1-255):	<input type="text" value="32"/>
Beacon Period (19-5000 msec):	<input type="text" value="100"/>
DTIM Period (1-255):	<input type="text" value="1"/>
Ethernet Encapsulation:	<input type="radio"/> 802.1H <input checked="" type="radio"/> RFC1042
Radio Preamble:	<input type="radio"/> Long <input checked="" type="radio"/> Short

Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, ProCurve520WL	
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:	<input type="text" value="Large"/>
802.11g Operational Mode:	<input type="text" value="802.11b only"/>
802.11abg Operational Mode:	<input type="text" value="802.11b + 802.11g"/>
802.11b Transmit Rate:	<input type="text" value="Auto Fallback"/>
802.11g Transmit Rate:	<input type="text" value="Auto Fallback"/>
802.11a Transmit Rate:	<input type="text" value="Auto Fallback"/>
Rogue Scanning:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Rogue Scanning Interval (15-1440 min):	<input type="text" value="15"/>

Proxim 4900M	
4.9GHz Public Safety Channel Bandwidth:	<input type="text" value="20"/>
802.11a/4.9GHz Public Safety Operational Mode:	<input type="text" value="802.11a"/>

Symbol	
Rogue Scanning:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Rogue Scanning Interval (5-480 min):	<input type="text" value="240"/>

- Locate the **Radio Settings** area and adjust these settings as required. [Table 62](#) describes the settings and default values.

**Table 62 Groups > Radio > Radio Settings Fields and Default Values**

Setting	Default	Description
<b>Allow Automatic Channel Selection</b> (2.4, 5, and 4.9GHz Public Safety)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and select its optimal RF channel based on observed signal strength from other radios. <b>NOTE:</b> If you enable this feature, AMP automatically reboots the APs in the group when the change is implemented.
<b>802.11b Data Rates</b> (Mbps)	Required: <ul style="list-style-type: none"> <li>1.0</li> <li>2.0</li> </ul> Optional: <ul style="list-style-type: none"> <li>5.5</li> <li>11.0</li> </ul>	Displays pull-down menus for various data rates for transmitting data. <b>NOTE:</b> This setting does not apply to Cisco LWAPP devices. The three values in each of the pull-down menus are as follows: <ul style="list-style-type: none"> <li><b>Required</b>—The AP transmits only unicast packets at the specified data rate; multicast packets are sent at a higher data rate set to optional. (Corresponds to a setting of <b>yes</b> on Cisco devices.)</li> <li><b>Optional</b>—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of <b>basic</b> on Cisco devices.)</li> <li><b>Not Used</b>—The AP does not transmit data at the specified data rate. (Corresponds to a setting of <b>no</b> on Cisco devices.)</li> </ul>
<b>Frag Threshold Enabled</b>	No	If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, leave this option disabled.
<b>Threshold Value</b>	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower <b>Fragmentation Threshold</b> setting might be required if there is a great deal of radio interference.
<b>RTS/CTS Threshold Enabled</b>	No	If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, leave this option disabled.
<b>RTS/CTS Threshold Value</b>	2338	If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP sends the RTS before sending the packet.
<b>RTS/CTS Maximum Retries</b>	32	If RTS/CTS is enabled, this specifies the maximum number of times the AP issues an RTS before stopping the attempt to send the packet through the radio. Acceptable values range from <b>1</b> to <b>128</b> .

**Table 62 Groups > Radio > Radio Settings Fields and Default Values (Continued)**

Setting	Default	Description
<b>Maximum Data Retries</b>	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet. Acceptable values range from <b>1</b> to <b>255</b> .
<b>Beacon Period</b> (19-5000 msec)	100	Time between beacons (in microseconds).
<b>DTIM Period</b> (1-255)	2	DTIM alerts power-save devices that a packet is waiting for them. This setting configures DTIM packet frequency as a multiple of the number of beacon packets. The DTIM Interval indicates how many beacons equal one cycle.
<b>Ethernet Encapsulation</b>	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.
<b>Radio Preamble</b>	Long	This setting determines whether the APs uses a <b>short</b> or <b>long</b> preamble. The preamble is generated by the AP and attached to the packet prior to transmission. The short preamble is 50 percent shorter than the long preamble and thus may improve wireless network performance. <b>NOTE:</b> Because older WLAN hardware may not support the “short” preamble, the “long” preamble is recommended as a default setting in most environments.

- Certain wireless access points offer proprietary settings or advanced functionality that differ from prevailing industry standards. If you use these APs in the device group, you may wish to take advantage of this proprietary functionality.

To configure these settings, locate the proprietary settings areas on the **Groups > Radio** page and continue with the additional steps in this procedure.



Proprietary settings are only applied to devices in the group from the specific vendor and are not configured on devices from vendors that do not support the functionality.

- To configure settings specific to the Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3/4/5/6/7/8, and ProCurve 520WL, locate the appropriate section of **Groups > Radio** page and define the required fields. [Table 63](#) describes the settings and default values.

**Table 63 Groups > Radio > Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL Fields and Default Values**

Setting	Default	Description
<b>Load Balancing</b>	No	If enabled, this setting allows client devices associating to an AP with two radio cards to determine which card to associate with, based on the load (# of clients) on each card. <b>NOTE:</b> This feature is only available when two 802.11b wireless cards are used in an AP-2000.
<b>Interference Robustness</b>	No	If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput.
<b>Distance Between APs</b>	Large	This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point.
<b>802.11g Operational Mode</b>	802.11b +802.11g	This setting sets the operational mode of all g radios in the group to either b only, g only or b + g.
<b>802.11abg Operational Mode</b>	802.11b +802.11g	This setting sets the operational mode of all a/b/g radios in the group to either a only, b only, g only or b + g.
<b>802.11b Transmit Rate</b>	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.

**Table 63 Groups > Radio > Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL Fields and Default Values (Continued)**

Setting	Default	Description
<b>802.11g Transmit Rate</b>	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
<b>802.11a Transmit Rate</b>	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
<b>Rogue Scanning</b>	Yes	If enabled, any ORiNOCO or Avaya APs in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. <b>NOTE:</b> This feature can affect the data performance of the access point.
<b>Rogue Scanning Interval</b>	15 minutes	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

- To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. [Table 64](#) describes the settings and default values.

**Table 64 Groups > Radio > Proxim 4900M Fields and Default Values**

Setting	Default	Description
<b>4.9GHz Public Safety Channel Bandwidth</b>	20	This setting specifies the channel bandwidth for the 4.9 GHz radio. It is only applicable if you are running the 802.11a/4.9GHz radio in 4.9GHz mode.
<b>802.11a/4.9GHz Public Safety Operational Mode</b>	802.11a	This setting specifies if the AP will run the 802.11a/4.9GHz radio in 802.11a mode or in 4.9 GHz mode. Please note that 4.9 GHz is a licensed frequency used for public safety.

- To configure Symbol-only settings, locate the **Symbol** section and define the required fields. [Table 65](#) describes the settings and default values.

**Table 65 Groups > Radio > Symbol Fields and Default Values**

Setting	Default	Description
<b>Rogue Scanning</b>	Yes	If enabled, Symbol access points with 3.9.2 or later firmware in the group will passively scan for rogue access points at the specified interval. This rogue scan will not break a user's association to the network.
<b>Rogue Scanning Interval (5-480 min)</b>	240	If rogue scanning is enabled, this setting controls the frequency with which scans are conducted (in minutes). Frequent scans provide the greatest security, but AP performance and throughput available to user devices may be impacted modestly during a rogue scan.

- Select **Save** when radio configurations as described above are complete, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.



## Cisco WLC Group Configuration

The **Groups > Cisco WLC Config** page consolidates the settings for Cisco WLC devices from all group pages. The **Groups > SSIDs** subtab applies to all device types except for Cisco WLC, which have WLANs configured on the **Cisco WLC Config** page. It is not recommended to have Symbol 4131 and Proxim APs in the same group as Cisco devices. Also, it is recommended that users set device preferences to **Only devices in this group**. This topic describes how to access and navigate the **Groups > Cisco WLC Config** page.

### Accessing Cisco WLC Configuration

Go to the **Cisco WLC Config** page in one of these two ways:

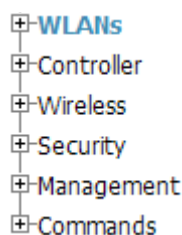
1. In **Groups > List**, select a group that has been defined to support Cisco devices and the **Cisco WLC Config** option appears in the subtabs.
2. In **Groups > List**, create a new group to support Cisco devices with these steps:
  - Select **Add** from the **Groups > List** page to create a new group, enter a group name, and select **Add**.
  - Once AMP prompts you with the **Groups > Basic** page, ensure that you enable device-specific settings for **Cisco WLC**.
  - Once you select **Save** or **Save and Apply**, then the **Groups > Cisco WLC Config** subtab appears in the navigation pane at the top in association with that group.

### Navigating Cisco WLC Configuration

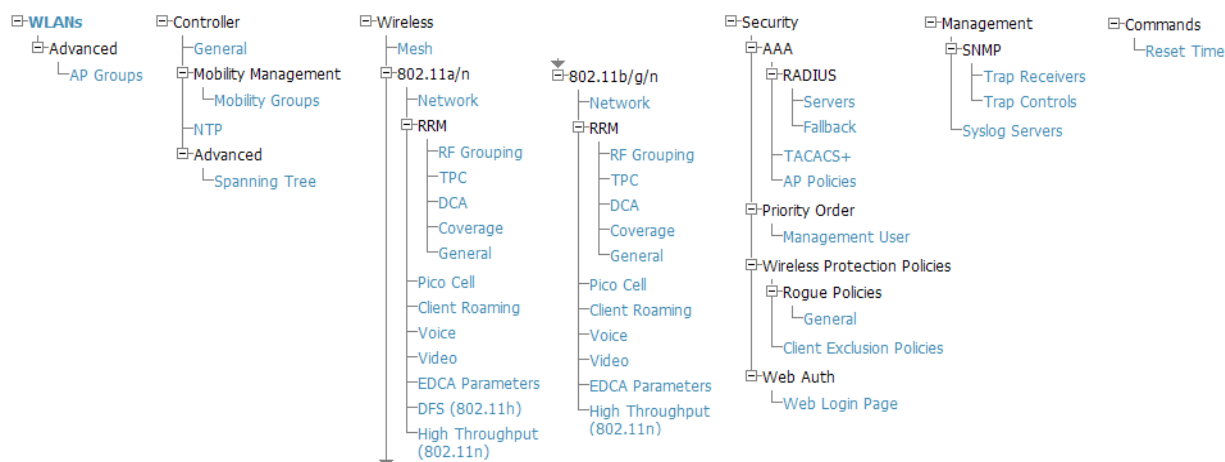
The navigation pane on the left side of the **Groups > Cisco WLC Config** page is expandable, and displays the Cisco configurations supported and deployed. [Figure 47](#) and [Figure 48](#) illustrate this navigation pane.

You can pre-populate the group WLC settings from a controller in the same group by performing an import on the controller's **Audit** page.

**Figure 47** *Groups > Cisco WLC Config Page Illustration, collapsed view*



**Figure 48** *Groups > Cisco WLC Config Page Illustration, expanded view*





## Configuring WLANs for Cisco WLC Devices

In **Cisco WLC Config**, WLANs are based on SSIDs or VLANs that are dedicated to Cisco WLC controllers. Perform the following steps to define and configure WLANs for Cisco WLC controllers.

1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs** in the navigation pane at left. This page displays the SSIDs or VLANs that are available for use with Cisco WLC devices, and enables you to define new SSIDs or VLANs. [Figure 49](#) illustrates this page.
2. To change the ID/position of a WLAN on the controller by dragging and dropping, set the toggle to **yes**. Note that the by setting this flag to **yes**, AMP will display a mismatch if the WLANs in the desired and device config differ only on the order.

**Figure 49** *Groups > Cisco WLC Config > WLANs* page illustration

WLANs

Group: Access Points

Enforce WLAN Order on Controllers: ☐ Yes ☒ No

Add New SSID/VLAN

Profile	SSID	Type	Admin Status	Encryption Mode	Radio Policy
5500 8021x	10.22.42.11	WLAN	Yes	Require 802.1X	All

Select All - Unselect All

Delete

Save and Apply Revert

3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either select the **Add New SSID/VLAN** button, or select the pencil icon for an existing SSID/VLAN. A new page appears comprised of four tabs, as follows:
  - **General**—Defines general administrative parameters for the Cisco WLC WLAN.
  - **Security**—Defines encryption and RADIUS servers.
  - **QoS**—Defines quality of service (QoS) parameters for the Cisco WLC WLAN.
  - **Advanced**—Defines advanced settings that are available only with Cisco WLC devices, for example, AAA override, coverage, DHCP and DTIM period.



Refer to Cisco documentation for additional information about Cisco WLC devices and related features.

**Figure 50** *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > General Tab* Illustration

General Security QoS Advanced

General

Profile:

SSID:

Guest LAN: ☐ Yes ☒ No

WLAN ID (1-512):

Admin Status: ☒ Yes ☐ No

Specify Interface Name: ☒ Yes ☐ No

Interface:

Radio Policy:

Broadcast SSID: ☐ Yes ☒ No

Add Cancel

**Figure 51** Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Security Tab Illustration

The screenshot shows the 'Security' tab of the 'Add New SSID/VLAN' configuration page. The 'General' tab is selected, and the 'Security' sub-tab is active. The 'Security' section contains the following fields:

- Encryption Mode: No Encryption (dropdown)
- Web Policy: Authentication (dropdown)
- Preauthentication ACL: (text input)
- Override Global Config: ☒ Yes ☐ No
- Web Authentication Type: External (dropdown)
- External Web Authentication URL: /cisco/auth/ (text input)

The 'AAA Servers' section contains the following fields:

- RADIUS Authentication Server #1: Select (dropdown)
- RADIUS Authentication Server #2: Select (dropdown)
- RADIUS Authentication Server #3: Select (dropdown)
- Enable AAA Accounting Servers: ☒ Yes ☐ No
- RADIUS Accounting Server #1: Select (dropdown)
- RADIUS Accounting Server #2: Select (dropdown)
- RADIUS Accounting Server #3: Select (dropdown)

**Figure 52** Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > QoS Tab Illustration

The screenshot shows the 'QoS' tab of the 'Add New SSID/VLAN' configuration page. The 'General' tab is selected, and the 'QoS' sub-tab is active. The 'QoS' section contains the following fields:

- Quality of Service: Platinum (voice) (dropdown)
- WMM Policy: Allowed (dropdown)

At the bottom of the page, there are 'Add' and 'Cancel' buttons.

**Figure 53** Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Advanced Tab Illustration

The screenshot shows the 'Advanced' tab of the 'Add New SSID/VLAN' configuration page. The 'General' tab is selected, and the 'Advanced' sub-tab is active. The 'Advanced' section contains the following fields:

- Allow AAA Override: ☐ Yes ☒ No
- Coverage Hole Detection: ☒ Yes ☐ No
- Session Timeout (0-86400): 0 (text input)
- Enable IPv6: ☐ Yes ☒ No
- P2P Blocking Action: Disabled (dropdown)
- Client Exclusion: ☐ Yes ☒ No
- Media Session Snooping: ☐ Yes ☒ No
- Requires Platinum QoS
- DHCP Server: (text input)
- Require DHCP: ☐ Yes ☒ No
- Aironet IE Support: ☒ Yes ☐ No
- MFP Signature Generation: ☐ Yes ☒ No
- H-REAP Local Switching: ☐ Yes ☒ No
- Mobility Anchor #1: Select (dropdown)
- Mobility Anchor #2: Select (dropdown)
- Mobility Anchor #3: Select (dropdown)
- Mobility Anchor #4: Select (dropdown)
- DTIM Period 802.11a/n (1-255 beacon periods): 1 (text input)
- DTIM Period 802.11bg/n (1-255 beacon periods): 1 (text input)
- Client Load Balancing: ☐ Yes ☒ No
- Client Band Select: ☒ Yes ☐ No
- Requires a Radio Policy of "All"

## Defining and Configuring LWAPP AP Groups for Cisco Devices

The **Groups > Cisco WLC Config > WLANs > Advanced > AP Groups** page allows you to add/edit/delete AP Groups on the Cisco WLC. LWAPP AP Groups are used to limit the WLANs available on each AP. Cisco thin APs are assigned to LWAPP AP Groups.

### Viewing and Creating Cisco AP Groups

1. Go to the **Groups > Cisco WLC Config** page, and select **WLANs > Advanced > AP Groups** in the navigation pane at left. This page displays the configured LWAPP APs. [Figure 54](#) illustrates this page.

**Figure 54** *Groups > Cisco WLC Config > WLANs > Advanced > AP Groups Page Illustration*

The screenshot shows the configuration page for AP Groups. On the left is a navigation pane with a tree structure: WLANs (expanded), 5500 8021x, Advanced (expanded), and AP Groups (selected). The main content area is titled 'Group: Access Points'. It contains three sections: 1. 'AP Groups' with a toggle 'LWAPP AP Groups VLAN Enabled:' set to 'Yes'. 2. 'LWAPP AP Group' with fields for 'Name:' (802) and 'Description:' (Limit to 5). 3. 'LWAPP AP Group Interface Mapping' with fields for 'SSID:' (10.22.42.11), 'Specify Interface Name:' (Yes), 'Interface:' (management), and 'NAC State:' (Disabled). At the bottom are buttons for 'Add' and 'Cancel' for each section, and a row of buttons: 'Save and Apply', 'Save', 'Revert', and 'Revert All'.

2. To add a new LWAPP AP group, select **Yes** in the **AP Groups** section. Additional controls appear.
3. Select **Add** to create a new LWAPP AP group. To edit an existing LWAPP AP group, select the pencil icon next to that group. Add one or more SSIDs and the interface/VLAN ID mapping on the **Add/Edit** page of the LWAPP AP Group.
4. Select **Save and Apply** to make these changes permanent, or select **Save** to retain these changes to be pushed to controllers at a later time.

### Configuring Cisco Controller Settings

The **Groups > Cisco WLC Config > Controller** page defines general Cisco WLC settings, Multicast settings, Cisco mobility groups to be supported on Cisco controllers, Network Transfer Protocol (NTP), and Spanning Tree Protocol settings.

Go to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in [Figure 55](#).

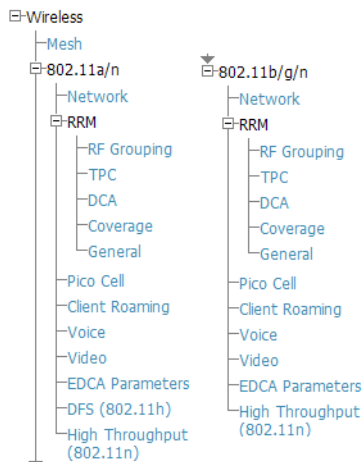
**Figure 55** *Groups > Cisco WLC Config > Controller Navigation*



## Configuring Wireless Parameters for Cisco Controllers

This section illustrates the configuration of **Wireless** settings in support of Cisco WLC controllers. The navigation for Wireless settings is illustrated in [Figure 56](#).

**Figure 56** *Groups > Cisco WLC Config > Wireless Navigation Illustration*



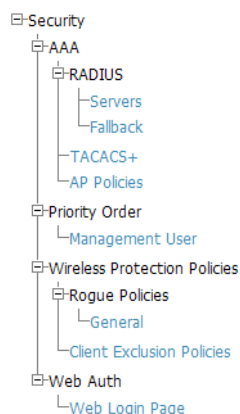
## Configuring Cisco WLC Security Parameters and Functions

AMP enables you to configure many security settings that are specific to Cisco WLC controllers. This section supports four overriding types of configuration, as follows:

- **AAA**, to cover both RADIUS and TACACS+ server configuration
- **Priority Order**
- **Wireless Protection Policies**
- **Web Auth**

[Figure 57](#) illustrates these components and this navigation:

**Figure 57** *Groups > Cisco WLC Config > Security Navigation Illustration*



## Configuring Management Settings for Cisco WLC Controllers

AMP allows you to configure of SNMP and Syslog Server settings for Cisco WLC controllers. You can configure up to four trap receivers on the Cisco WLC including the AMP IP that can be used in Global Groups. To define SNMP and server settings, go to the **Groups > Cisco WLC Config > Management** page, illustrated in [Figure 58](#).

**Figure 58** *Groups > Cisco WLC Config > Management Navigation Illustration*



## Configuring Group PTMP Settings

The **Groups > PTMP** configuration page configures Point-to-Multipoint (PTMP) for all subscriber and base stations in the device group. Subscriber stations must be in the same group as all base stations with which they might connect.

Perform the following steps to configure these functions.

1. Go to the **Groups > List** page and select the group for which to define PTMP settings by selecting the group name. Alternatively, select **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Select the PTMP tab in the AMP navigation menu. [Figure 59](#) illustrates this page.

**Figure 59** *Groups > PTMP Page Illustration*

The screenshot shows the PTMP configuration page for a device group named "Proxim MP.11". The page contains the following fields and controls:

- 802.11a Radio Channel:** Channel Range (30-215) with a text input field containing "58".
- 802.11g Radio Channel:** A dropdown menu with "10" selected.
- Channel Bandwidth:** A dropdown menu with "20" selected.
- Network Name:** A text input field containing "Wireless Network".
- Network Secret:** A text input field.
- Confirm Network Secret:** A text input field.

At the bottom of the page, there are three buttons: "Save", "Save and Apply", and "Revert".

3. Define the settings on this page. [Table 66](#) describes the settings and default values.

**Table 66** *Groups > PTMP Fields and Default Values*

Setting	Default	Description
<b>802.11a Radio Channel</b>	58	Selects the channel used for 802.11a radios by the devices in this group.
<b>802.11g Radio Channel</b>	10	Selects the channel used for 802.11g radios by the devices in this group.
<b>Channel Bandwidth</b>	20	Defines the channel bandwidth used by the devices in this group.
<b>Network Name</b>	Wireless Network	Sets the Network name, with a range of length supported from two to 32 alphanumeric characters.
<b>Network Secret</b>	None	Sets a shared password to authenticate clients to the network.

4. Select **Save and Apply** when configurations are complete to make them permanent, or select **Save** to retain these settings prior to pushing to controllers at a later time.

## Configuring Proxim Mesh Radio Settings

1. Go to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. [Figure 60](#) illustrates this page. [Table 67](#) and [Table 68](#) describe the settings and default values.

**Figure 60** *Groups > Proxim Mesh Page Illustration*

The screenshot shows the Proxim Mesh configuration page with three main sections: General, Security, and Mesh Cost Matrix. The General section includes fields for Mesh Radio (4.9/5 Ghz), Maximum Mesh Links (6), Neighbor RSSI Smoothing (16), Roaming Threshold (80), and Deauth Client When Uplink is Down (Yes). The Security section includes SSID (Wireless Mesh) and Enable AES (Yes). The Mesh Cost Matrix section includes fields for Hop Factor (2), Maximum Hops to Portal (4), RSSI Factor (5), RSSI Cut-Off (10), Medium Occupancy Factor (5), and Current Medium Occupancy Weight (7). At the bottom are Save, Save and Apply, and Revert buttons.

The **General** section contains settings for mesh radio, number of mesh links, RSSI smoothing, roaming threshold and de-auth client.

**Table 67** *Groups > Proxim Mesh > General Fields and Default Values*

Setting	Default	Description
<b>Mesh Radio</b>	4.9/5Ghz	Drop-down selects the radio that acts as the backhaul to the network.
<b>Maximum Mesh Links</b>	6	Sets the maximum number of mesh links allowed on an AP. This number includes the uplink to the portal as well as downlinks to other mesh APs.
<b>Neighbor RSSI Smoothing</b>	16	Specifies the number of beacons to wait before switching to a new link.
<b>Roaming Threshold</b>	80	Specifies the difference in cost between two paths that must be exceeded before the AP roams. To switch to a new path it must have a cost that is less by at least the roaming threshold. A high threshold results in fewer mesh roams.
<b>Deauth Client when Uplink is Down</b>	Yes	With <b>Yes</b> selected, clients have authentication removed (are deauthenticated) if the uplink is lost.

The **Security** section contains settings for SSID and enabling AES encryption.

**Table 68** *Groups > Proxim Mesh > Security Fields and Default Values*

Setting	Default	Description
<b>SSID</b>	None	Sets the SSID used by the Mesh Radio to connect to the mesh network.
<b>Enable AES</b>	No	Enable or disable AES encryption.

3. The **Mesh Cost Matrix** configuration section contains settings for hop factor and maximum hops to portal, RSSI factor and cut-off, medium occupancy factor and current medium occupancy weight. Adjust these settings as required for your network. [Table 69](#) describes these settings and default values.

**Table 69** *Groups > Proxim Mesh > Mesh Cost Matrix Fields and Default Values*

Setting	Default	Description
<b>Hop Factor</b>	5	Sets the factor associated with each hop when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
<b>Maximum Hops to Portal</b>	4	Set the maximum number of hops for the AP to reach the Portal AP.

**Table 69** *Groups > Proxim Mesh > Mesh Cost Matrix Fields and Default Values (Continued)*

Setting	Default	Description
<b>RSSI Factor</b>	5	Sets the factor associated with the RSSI values used when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
<b>RSSI Cutoff</b>	10	Specifies the minimum RSSI needed to become a mesh neighbor.
<b>Medium Occupancy Factor</b>	5	Sets the factor associated with Medium Occupancy when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
<b>Current Medium Occupancy Weight</b>	7	Specifies the importance given to the most recently observed Medium Occupancy against all of the previously viewed medium occupancies. Lower values place more importance on previously observed Medium Occupancies.

4. Select **Save** when configurations are complete to retain these settings. Select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

## Configuring Group MAC Access Control Lists

This configuration is optional. If you use Symbol, Proxim, or ProCurve 520WL wireless access points, AMP enables you to specify the MAC addresses of devices that are permitted to associate with APs in the Group. Other devices are not able to associate to APs in the Group, even if the users of those devices are authorized users on the network.

Perform the following steps to use the MAC ACL function.

1. Browse to the **Groups > MAC ACL** configuration page. [Figure 61](#) illustrates this page.

**Figure 61** *Groups > MAC ACL Page Illustration*

Group: **infrastructure**

These settings apply to Proxim, Cisco VxWorks, Symbol and ProCurve 520 devices.

MAC ACL

Use MAC ACL:

Authorized MAC Addresses:  
This list will not be set on Cisco VxWorks APs.

Yes

No

Yes

Use manual setting on each device

Save

Save and Apply

Revert

2. Select **Yes** on the **Use MAC ACL** drop-down menu. Enter all authorized MAC addresses, separated by white spaces.
3. Select **Save** when configurations are complete to retain these settings. Select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

## Specifying Minimum Firmware Versions for APs in a Group

This configuration is optional. AMP allows you the option of defining the minimum firmware version for each AP type in a group on the **Groups > Firmware** configuration page. At the time that you define the minimum version, AMP automatically upgrades all eligible APs.

When you add APs into the group in the future, you will be able to upgrade APs manually. The firmware for an AP is not upgraded automatically when it is added to a group. Perform the following steps to make this firmware configuration.

1. Browse to the **Groups > Firmware** configuration page. [Figure 62](#) illustrates this page.



**Figure 62** *Groups > Firmware Page Illustration*

Group: Access Points

**Firmware Upgrade Options**  
Configure the File Server IP Address to use when upgrading devices in this group. The firmware file definition must be configured to use the per-group setting.  
Firmware File Server IP Address:

**Desired Version**  
Choose the desired firmware version to be applied to the devices in this group. Upload firmware files on the Device Setup [Upload Firmware & Files](#) page.  

Aruba 200:	<input type="text" value="NONE"/>
Aruba 2400:	<input type="text" value="NONE"/>
Aruba 2400-E:	<input type="text" value="NONE"/>
Aruba 3xxx:	<input type="text" value="NONE"/>
Aruba 5000/6000:	<input type="text" value="NONE"/>
Aruba 6xx:	<input type="text" value="NONE"/>
Aruba 800:	<input type="text" value="NONE"/>
Aruba 800-4:	<input type="text" value="NONE"/>
Aruba 800-E:	<input type="text" value="NONE"/>
Azalea AP:	<input type="text" value="NONE"/>
Azalea MSR2000:	<input type="text" value="NONE"/>

Start or schedule firmware upgrade job:

Save desired version preferences without upgrading now:

2. For each device type in the group, specify the minimum acceptable firmware version. If no firmware versions are listed, go to the **Device Setup > Upload Firmware & Files** configuration page to upload the firmware files to AMP.
3. Select **Upgrade** to apply firmware preferences to devices in the group.
4. Select **Save** to save the firmware file as the desired version for the group.
5. If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup > Upload Firmware & Files** configuration page, you can enter the IP address in the **Firmware Upgrade Options** field on the top of this configuration page.
6. Once you have defined your first group, you can configure that group to be the **default** group on your network. When AMP discovers new devices that need to be assigned to a management group, the default group appears at the top of all drop-down menus and lists. Newly discovered devices are placed automatically in the default group if AMP is set to **Automatically Monitor/Manage New Devices** on the AMP configuration page.
7. Browse to the **Groups > List** configuration page.
8. From the list of groups, check the **Default** radio button next to the desired default group to make it the default.

## Comparing Device Groups

You can compare two existing device groups with a detailed line-item comparison. Group comparison allows several levels of analysis to include the following:

- compare performance, bandwidth consumption, or troubleshooting metrics between two groups
- debug one device group against the settings of a similar and better performing device group
- use one group as a model by which to fine-tune configurations for additional device groups

This topic presumes that at least two device groups are at least partly configured in AMP, each with saved configurations. Perform the following steps to compare two existing device groups:

1. From the **Groups > List** page, select **Compare two groups**. Two drop-down menus appear.
2. Select the two groups to compare to each other in the drop-down menus, and select **Compare**. The **Compare** page appears, displaying some or many configuration categories. [Figure 63](#) illustrates this page.

**Figure 63** Comparing Two Devices Groups on the **Groups > List > Compare** Page (Partial View)

Comparing group **HQ-RemoteAP** to group **Outdoor**:

Show Similar Fields

	HQ-RemoteAP (edit)	Basic	Outdoor (edit)
802.11 Counters Polling Period:	30 minutes	➡	15 minutes
Allow One-to-One NAT:	No	➡	Yes
Bridge Forward Delay:	15	➡	16
Bridge Hello Time:	2	➡	4
Bridge Maximum Age:	20	➡	22
Bridge Priority:	32768	➡	32760
Cisco IOS CLI Communication:	Telnet	➡	SSH
Cisco IOS Config File Communication:	TFTP	➡	SCP
Device Bandwidth Polling Period:	10 minutes	➡	5 minutes
Device-to-Device Link Polling Period:	15 minutes	➡	30 minutes
NTP Polling Interval:	86400	➡	3600
NTP Server #1:	(empty string)	➡	10.2.25.162
Override Polling Period for Other Services:	Yes	➡	No
Read ARP Table:	4 hours	➡	8 hours
Read Bridge Forwarding Table:	4 hours	➡	8 hours
Read CDP Table for Device Discovery:	4 hours	➡	8 hours

3. Note the following factors when using the **Compare** page:

- The **Compare** page can be very long or very abbreviated, depending on how many configurations the device groups share or do not share.
- When a configuration differs between two groups, the setting is flagged in red text for the group on the right.
- The default setting of the **Compare** page is to highlight settings that differ between two groups.
  - To display settings that are similar or identical between two device groups, select **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
  - Select **Hide Similar Fields** to return to the default display, emphasizing configuration settings that differ between two groups.
- You can change the configuration for either or both groups by selecting **Edit** in the corresponding column heading. The appropriate configuration page appears.
- If you make and save changes to either or both groups, go back to the **Groups > List** page and select **Compare two groups**. Select the same two groups again for updated information.
- Additional topics in this document describe the many fields that can appear on the **Groups > List > Compare** page.

## Deleting a Group

Perform the following steps to delete an existing Group from the AMP database:

1. Browse to the **Groups > List** configuration page.
2. Ensure that the Group you wish to delete is not marked as the **default** group. AMP does not permit you to delete the current default Group.
3. Ensure that there are no devices in the Group you wish to delete. AMP does not permit you to delete a Group that still contains managed devices. You must move all devices to other Groups before deleting a Group.
4. Ensure that the Group is not a Global Group which has Subscriber Groups, and is not a Group that was pushed from a Master Console. AMP will not delete a Group in which either of those is true.
5. Select the checkbox and select **Delete**.

## Changing Multiple Group Configurations

Perform the following steps to make any changes to an existing group's configuration:

1. Browse to the **Groups > List** configuration page.
2. Select the **Manage** link (the pencil icon) for the group you wish to edit. The **Groups > Basic** configuration page appears.
3. Select the fields to be edited on the **Basic** configuration page or go to **Radio**, **Security**, **VLANs**, or **MAC ACL** configuration page and edit the fields. Use the **Save** button to store the changes prior to applying them.
4. When all changes for the group are complete select the **Save and Apply** button to make the changes permanent. Figure 64 illustrates the confirmation message that appears.

**Figure 64** *Groups > Basic Configuration Change Confirmation Page Illustration*

Confirm changes:

Group "Access Points Not Managed by MC"		
CDP Neighbor Data Polling Period	5 minutes	10 minutes
Device-to-Device Link Polling Period	60 seconds	90 seconds
Interface Error Counter Polling Period	30 minutes	15 minutes
Rogue AP and Device Location Data Polling Period	5 minutes	10 minutes
Thin AP Discovery Polling Period	2 minutes	5 minutes
Up/Down Status Polling Period	60 seconds	90 seconds
Use MAC ACL	No	Use manual setting on each device

**Scheduling Options**

Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like **tomorrow at noon** or **next tuesday at 4am**). Other input formats may be accepted.

Current Local Time: January 17, 2011 3:39 pm PST

Desired Start Date/Time:

Select other groups to change:

Group	Current Local Time
<input type="checkbox"/> 1111	January 17, 2011 3:39 pm PST
<input type="checkbox"/> ws5100	January 17, 2011 3:39 pm PST

[Select All - Unselect All](#)

5. AMP displays a **Configuration Change** screen confirming the changes that will be applied to the group's settings.
6. There are several action possibilities from within this confirmation configuration page.
  - **Apply Changes Now** — Applies the changes immediately to access points within the group. If you wish to edit multiple groups, you must use the **Preview** button.



NOTE

You cannot apply Aruba Config changes to other groups. If the only changes on the configuration page are to Aruba devices, the list of groups and the preview button will not appear.

- **Schedule** — Schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time** field. AMP takes the time zone into account for the group if a time zone other than **AMP System Time** has been configured on the **Groups > Basic** configuration page.
- **Cancel** — Cancels the application of changes (immediately or scheduled).



NOTE

To completely nullify the change request, select **Revert** on one of the group configuration pages after you have selected **Cancel**.

7. Apply changes to multiple groups by selecting the appropriate group or groups and selecting **Preview**.

## Modifying Multiple Devices

AMP provides a very powerful utility that modifies all APs or a subset of access points unrelated to the typical AMP group construct. This utility provides the ability to delete simultaneously multiple devices, migrate multiple devices to another group and/or folder, update credentials and optimize channels. Perform these steps to modify multiple devices.

1. To modify multiple devices, go to one of the following pages with a device list:

- **APs/Devices > List**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**
- **Groups > Monitor** configuration pages

Each of these pages displays a list of devices. Controller monitoring pages also have lists of their thin APs which can be modified using **Modify Devices**.

2. Select **Modify Devices** to make the checkboxes at the left of all devices appear. In addition, a new section appears in this page location to display various settings that can be configured for multiple devices at one time (some operations cannot be performed on the selected devices). [Figure 65](#) illustrates this page.

**Figure 65** *Modify Multiple Devices Section Illustration*

[Modify Devices](#)

1-3 of 19 APs/Devices Page 1 of 6 > > | Choose Columns CSV Export

	Device	Status	Configuration	Type	Version	Controller	Group	APs	Use
<input type="checkbox"/>	cisco-catalyst-500	Down	Good	Cisco Catalyst Express 500	12.2(25)SEG6	-	infrastructure	-	0
<input type="checkbox"/>	Cisco-3750	Down	Error	Cisco Catalyst 3750-24TS	12.2(35)SE5	-	infrastructure	-	0
<input type="checkbox"/>	Cisco-3750-2	Down	Verifying	Cisco Catalyst 3750-24TS	12.2(35)SE5	-	infrastructure	-	0

1-3 of 19 APs/Devices Page 1 of 6 > > |

Select All - Unselect All

**Change properties of selected devices:**

AMP Group/Folder:  and/or

Aruba AP Group:

Management Level: ☐ Monitor Only + Firmware Upgrades ☐ Manage Read/Write

Desired Radio Status: ☐ Enable ☐ Disable

Cisco Thin AP Settings:

**Perform actions:**

Poll selected devices:

Audit selected devices:

Run report on selected devices:

Update the credentials AMP uses to communicate with these devices:

Import settings from selected devices (and discard current per-device desired settings):

Import unreferenced Aruba profiles from selected devices:

Reboot selected devices:

Reprovision selected Aruba devices:

**Firmware:**

Upgrade firmware for selected devices:

Cancel firmware upgrade for selected devices:

**Ignore/Delete:**

Ignore selected devices (that may be down for maintenance):

Delete selected devices from AMP:

3. Select one or more devices that are to share the configurations. Select the checkbox for each device to modify.
4. In the **Modify Multiple Devices** section, select any button or use any drop-down menu for the supported changes. Any action you take applies to all selected devices. Each action you take will direct you to a new configuration page, or prompt you with a confirmation page to confirm your changes.
5. You are taken to a confirmation configuration page that allows you to schedule the change for a time in the future. Enter a start date and time in the scheduling field and select when the change should occur from the drop-down menu (one time is the default, but you may select recurring options for many of the actions). Scheduled jobs can be viewed and edited in the **System > Configuration Change Jobs** tab.
6. Using the neighbor lists, AMP is able to optimize channel selection for APs. Select the APs to optimize and AMP minimizes the channel interference while giving channel priority to the most heavily used APs. [Table 70](#) describes these actions and controls.

**Table 70** *Modify Multiple Devices Section Fields and Default Values*

Action	Description
<b>AMP Group/Folder</b>	Move the selected devices to a new group or folder. If the AP is in managed mode when it is moved to a new group, it will be reconfigured.
<b>Aruba AP Group</b>	Moves the selected APs to a new group or folder. If the AP is in managed mode when it is moved to a new group it will be reconfigured.
<b>Management Level</b>	Move the selected devices into <b>Monitor Only</b> or <b>Manage Read/Write Mode</b> .
<b>Planned Maintenance Mode</b>	Puts the selected devices into Planned Maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up.
<b>Desired Radio Status</b>	Enables or disables the radios on the selected device. Does <i>not</i> apply Cisco IOS APs.
<b>Update Cisco Thin AP Settings</b>	Bulk configuration for per-thin AP settings, previously configured on the <b>Group LWAPP AP</b> tab, can be performed from <b>Modify Devices</b> on the <b>APs/Devices List</b> page. Make changes to LWAPP AP groups, including the option that was under Modify Devices.
<b>Poll now</b>	Polls selected devices for current user count and bandwidth data; overrides default poll settings for the group. Polling numerous devices may create a temporary performance load on your AirWave server.
<b>Audit selected devices</b>	Fetches the current configuration from the device and compares it to the desired AMP configuration. The audit action updates the Configuration Status. <b>NOTE:</b> In versions of AMP previous to 7.3, the <b>Audit</b> button appeared on <b>Groups &gt; List</b> for groups with audit disabled. Now, if a group has audit disabled for its devices, AMP doesn't show the <b>Audit</b> button in the <b>Modify devices</b> list.
<b>Run report on selected devices</b>	Takes you to the <b>Reports &gt; Definitions</b> page where you can define or run a custom report for selected devices. For more details and a procedure, see <a href="#">“Using Custom Reports” on page 230</a> .
<b>Update the credentials AMP uses to communicate with these devices</b>	<b>Update</b> changes the credentials AMP uses to communicate with the device. It does <i>not</i> change the credentials on the AP.
<b>Add Maintenance Window</b>	Automate the manual action of putting the selected devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode. Maintenance windows can be set as a one-time or recurring event.
<b>Delete all Maintenance Windows</b>	Deletes all maintenance windows set for these devices.

**Table 70** *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
<b>Import settings from selected devices (and discard current pre-device desired settings)</b>	Audit updates a number of the AP specific settings AMP initially read off of the AP including channel, power, antenna settings and SSL certifications. AMP recommends using this setting if APs have been updated outside of AMP. Most settings on the <b>APs/Devices Manage</b> configuration page are set to the values currently read off of the devices.
<b>Reboot selected devices</b>	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
<b>Reprovision selected Aruba devices</b>	Configures the controller to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning.
<b>Upgrade firmware for selected devices</b>	Upgrades firmware for the selected devices. Refer to the firmware upgrade help under <b>APs/Devices &gt; Manage</b> configuration page for detailed help on Firmware job options.
<b>Cancel firmware upgrade for selected devices</b>	Cancels any firmware upgrades that are scheduled or in progress for the selected APs.
<b>Rename devices</b>	Rename all the selected devices in bulk. Note that you can also rename the devices one at a time using the editable <b>Name</b> fields in each row.
<b>Delete selected devices from AMP</b>	Removes the selected APs from AMP. The deletes will be performed in the background and may take a minute to be removed from the list.

## Using Global Groups for Group Configuration

To apply group configurations using the AMP Global Groups feature, first go to the **Groups > List** configuration page. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group. Select the **Duplicate** icon (usually near the last column of the list) to create a new group with identical configuration to an existing group.

- To have Global Group status, a group must contain no devices; accordingly, access points can never be added to a Global Group. Global groups are visible to users of all roles, so they may not contain devices, which can be made visible only to certain roles. [Figure 66](#) illustrates the **Groups > List** page.

**Figure 66** *Groups > List Page Illustration*

Add

New Group

Compare two groups

1-41 of 41 GroupsPage 1 of 1

Choose Columns

CSV Export

	Name	Up/Down Status	Polling Period	Total Devices	Is Global Group	Global Group	Down	Mismatched	Ignored	Users	BW	Duplicate	SSID
<div><div><div></div><div></div></div></div>	ws5100	60 seconds		5	No	gauss three	4	4	0	0	0	<div><div></div></div>	-
<div><div><div></div><div></div></div></div>	infrastructure	60 seconds		31	No	gauss two	9	16	0	0	0	<div><div></div></div>	Guest, R
<div><div><div></div><div></div></div></div>	airespace	60 seconds		5	No	gauss one	4	2	0	0	0	<div><div></div></div>	4000 80

- To set a group as a Global Group, go to the **Groups > Basic** configuration page for an existing or a newly created group. Select **Yes** for the **Is Global Group** field under the Global Group section.
- When the change is saved and applied, the group will have a checkbox next to fields. [Figure 67](#) illustrates this configuration page.

**Figure 67 Groups > Basic Page for a Global Group (partial view)**

Group: **gauss one**

Selecting a checkbox allows subscriber groups to override the corresponding setting.

**Basic**

Name: gauss one

☒ Missed SNMP Poll Threshold (1-100): 1

☐ Regulatory Domain: United States

☐ Timezone: AMP system time  
For scheduling group configuration changes

☒ Allow One-to-One NAT: ☐ Yes ☐ No

☐ Audit Configuration on Devices: ☐ Yes ☐ No

- When a Global Group configuration is pushed to Subscriber Groups, all settings are static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration page, override options are available only on the **Add** configuration page (go to the **Groups > SSIDs** configuration page and select **Add**). Global templates are also configurable as part of Global Groups; for more information, see [“Creating and Using Templates” on page 151](#).
- Once Global Groups have been configured, groups may be created or configured to subscribe to a particular Global Group. Go to the **Groups > Basic** configuration page of a group and locate the **Use Global Groups** section. Select the **Yes** radio button and select the name of the Global Group from the drop-down menu. Then select **Save and Apply** to make the changes permanent. [Figure 68](#) illustrates this page.

**Figure 68 Groups > Basic > Managed Page Illustration**

Group: **Access Points**

**Basic**

Name: Access Points

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: AMP system time  
For scheduling group configuration changes

Allow One-to-One NAT: ☐ Yes ☒ No

**Global Groups**

Use Global Group: ☒ Yes ☐ No

Global Group: globalgrouponMC (SSID: -)

- Once the configuration is pushed, the unchecked fields from the Global Group appears on the Subscriber Group as static values and settings. Only fields that had the override checkbox selected in the Global Group appear as fields that can be set at the level of the Subscriber Group. Any changes to a static field must be made on the Global Group.
- If a Global Group has Subscriber Groups, it cannot be changed to a non-Global Group. A Global Group without Subscriber Groups can be changed to a regular Group by updating the setting on the **Groups > Basic** configuration interface. The Global Groups feature can also be used with the Master Console. For more information about this feature, refer to [“Supporting AMP Servers with the Master Console” on page 220](#).



This chapter describes how to add, configure, and monitor wired and wireless devices, and contains the following sections corresponding to features of the **Device Setup** and **APs/Devices** tabs:

- “Device Discovery Overview” on page 107
- “Discovering and Adding Devices” on page 107
- “Monitoring Devices” on page 116
- “Configuring and Managing Devices” on page 134
- “Troubleshooting a Newly Discovered Down Device” on page 146
- “Setting up Aruba Spectrum Analysis in AMP” on page 147

### Device Discovery Overview

Once you have deployed AMP on the network, the next step is to discover all existing devices connected to your network.

AMP allows device discovery in the following ways, all of which are described in this chapter:

- **SNMP/HTTP discovery scanning**—This is the primary method to discover devices on your network, configured in the **Device Setup > Discover** page. See “[SNMP/HTTP Scanning](#)” on page 108.
- **Cisco Discovery Protocol (CDP)**—AMP enhances support for CDP by discovering a Cisco device’s CDP neighbors. See “[Enabling Cisco Discovery Protocol \(CDP\)](#)” on page 111.
- **Manual device entry**—This admin-supported method of discovery applies when you know of devices that are already on your network. See the following sections for information and procedures:
  - “[Manually Adding Individual Devices](#)” on page 112
  - “[Adding Multiple Devices from a CSV File](#)” on page 114
  - “[Adding Universal Devices](#)” on page 115
- **Controller-driven device discovery**—Thin APs will automatically be discovered in the network and added to the **New Devices** list when you add their controller to AMP. To add the thin APs, refer to “[Authorizing Devices to AMP from APs/Devices > New Page](#)” on page 111.

### Discovering and Adding Devices

This section describes the following topics:

- [SNMP/HTTP Scanning](#)
- [Enabling Cisco Discovery Protocol \(CDP\)](#)
- [Authorizing Devices to AMP from APs/Devices > New Page](#)
- [Manually Adding Individual Devices](#)

## SNMP/HTTP Scanning

SNMP/HTTP discovery scanning is the primary method for discovering devices on your network, including rogue devices. Enable this scanning method from the **Device Setup > Discover** page.



This page is only visible to users with the AMP Administrator role, or roles that have “**Allow authorization of APs/Devices**” enabled in **AMP Setup > Roles**.

SNMP/HTTP scanning information is provided in these sections:

- [Adding Networks for SNMP/HTTP Scanning](#)—explains how to enable networks that have been defined for scanning.
- [Adding Credentials for Scanning](#)—explains how to define network credentials for scanning. Credentials must be defined before using them in scan sets.
- [Defining a Scan Set](#)—explains how to create a scan set by combining networks and credentials when scanning for devices.
- [Running a Scan Set](#)—provides a procedure for running a scan set.

### Adding Networks for SNMP/HTTP Scanning

The first step when enabling SNMP/HTTP scanning for devices is to define the network segments to be scanned. Perform these steps.

1. Go to the **Device Setup > Discover** page, and locate the **Networks** section.
2. In the **Networks** section, select **Add New Scan Network**. The **Scan Network** page appears, as shown in [Figure 69](#). Alternatively, you can edit an existing scan network by selecting the corresponding pencil icon. The **New/Edit Networks** page also appears in this instance.

**Figure 69** *Device Setup > Discover > New Network Section Illustration*

Networks	
Scan Network	
Name:	<input type="text"/>
Network:	<input type="text"/>
Subnet Mask:	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

3. In the **Name** field, provide a name for the network to be scanned (for example, **Accounting Network**).
4. In the **Network** field, define the IP network range, or the first IP address on the network, to be scanned. One example would be 10.52.0.0.
5. Enter the **Subnet Mask** for the network to be scanned (for example, 255.255.252.0). The largest subnet AMP supports is 255.255.0.0.
6. Select **Add**.
7. Repeat these steps to add as many networks for which to enable device scanning. All network segments configured in this way appear in the **Network** section of the **Device Setup > Discover** page.
8. Complete the configuration of scan credentials, then combine scan networks and scan credentials to create scan sets. The next two procedures in this section describe these tasks.

### Adding Credentials for Scanning

The next step in SNMP/HTTP device discovery is to define the scan credentials that govern scanning of a given network. New APs inherit scan credentials from the System Credentials that you configure on the **Device Setup > Communications** page.

Perform these steps to define scan credentials for SNMP/HTTP scanning:

1. Locate the **Credentials** section on the **Device Setup > Discover** page. This page displays scan sets, networks, and credentials that have been configured so far, and allows you to define new elements for device scanning.
2. To create a new scan credential, select **Add New Scan Credential**. [Figure 70](#) illustrates this page.

**Figure 70** *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*

3. Enter a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters, both upper and lower case, blank spaces, hyphens, and underscore characters.
4. Choose the type of scan to be completed (**SNMPv1**, **SNMPv2**, or **HTTP**). In most cases, perform scans using SNMP for device discovery, but consider the following factors in your decision:
  - SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.
  - HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.
5. Define and confirm the **Community String** to be used during scanning. In this section, the community string used can be either **read-only** or **read/write**, as AMP only uses it for discovering APs. To bring APs under management, AMP uses the credentials supplied in the **Device Setup > Communication SNMP** section. Once the device is authorized, it will use the non-scanning credentials.




---

AMP automatically appends the type of scan (SNMP or HTTP) to the Label.

---

6. Select **Add**. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
7. Repeat these steps to add as many credentials as you require.
8. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure: [“Defining a Scan Set” on page 109](#).

## Defining a Scan Set

Once you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery. Perform these steps to create a scan set.

1. Locate the **Scan Set** area at the top of the **Device Setup > Discover** page.
2. Select **Add New Scan Set** to see all scan components configured so far. If you wish to create a new network, or new scanning credentials, you can select **Add** in either of these fields to create new components prior to creating a scan set.
3. Select the **Network(s)** to be scanned and the **Credential(s)** to be used. AMP defines a unique scan for each **Network-Credential** combination.
4. In the **Automatic Authorization** section, select whether to override the global setting in **AMP Setup > General** and have New Devices be automatically authorized into the New Device List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder.

5. Select **Add** to create the selected scans, which then appear in a list at the top of the **Device Setup > Discover** page.
6. To edit an existing scan, select the **pencil** icon next to the scan on the **Device Setup > Discover** page.
7. When ready, proceed to the next task, “[Running a Scan Set](#)” on page 110.



Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer APs, like most D-Link, Linksys, and NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper credentials are not required to discover these APs. Wireless scans and the AMC discover these rogues without any special changes.

## Running a Scan Set

Once a scan has been defined on the **Device Setup > Discover** page, AMP can now scan for devices. Perform these steps.

1. Browse to the **Device Setup > Discover** page and locate the list of all scan sets that have been defined so far. [Figure 71](#) illustrates this page.

**Figure 71** *Device Setup > Discover Executing a Scan Illustration*

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 [Communication](#) page, *not* the credentials defined below for scanning.

**Note:** Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

1-2 of 2 Scan Sets	Page 1 of 1	Choose Columns	CSV Export			
<input type="checkbox"/>	Network	Credentials	Total Devices Found	New Devices Found	Start	Stop
<input type="checkbox"/>	China	admin, default, private, public	0	0	5/24/2011 1:36 PM	5/24/2011 1:37 PM
<input type="checkbox"/>	Static IP Dev Net	AA, admin, default, e, pe, private, public	41	0	5/24/2011 7:03 PM	5/24/2011 7:07 PM

1-2 of 2 Scan Sets Page 1 of 1

Select All - Unselect All

Scan Delete Refresh this page for updated results.

Show Scheduling Options

2. Check the box next to the scan(s) that you would like to execute.
3. Select **Scan** to execute the selected scans, and the scan immediately begins. The **last** column indicates the scan is **In Progress**.
4. For future scans, select **Show Scheduling Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, refresh the browser page and view the results of the scan. When the **Start** and **Stop** columns display date and time information, the scan is available to display the results.
6. Select the **pencil** icon for the scan to display the results. [Table 71](#) describes the scan results and related information.

**Table 71** *Device Setup > Discover > Discovery Execution Fields*

Column	Description
<b>Network</b>	Displays the network to be scanned.
<b>Credentials</b>	Displays the credentials used in the scan.
<b>Total Devices Found</b>	Displays the total number of APs detected during the scan that AMP can configure and monitor. <b>Total</b> includes both APs that are currently being managed by AMP as well as newly discovered APs that are not yet being managed.
<b>New Devices Found</b>	Displays the number of discovered APs that are not yet managed, but are available.
<b>Total Rogues Found</b>	Displays the total number of APs detected during the scan that AMP could not configure or monitor. <b>Total</b> includes both APs that have been discovered in earlier scans as well as newly discovered APs from the most recent scan.
<b>New Rogues Found</b>	Displays the number of rogue APs discovered on the most recent scan.

**Table 71** *Device Setup > Discover > Discovery Execution Fields (Continued)*

Column	Description
<b>Start</b>	Displays the date and time the most recent scan was started.
<b>Stop</b>	Displays the date and time the scan most recently completed.
<b>Scheduled</b>	Displays the scheduled date and time for scans that are scheduled to be run.

- Go to the **APs/Devices > New** page to see a full list of the newly discovered devices that the scan detected. [Figure 72](#) illustrates this page.



This page is only visible to users with the AMP Administrator role, or roles that have “**Allow authorization of APs/Devices**” enabled in **AMP Setup > Roles**.

**Figure 72** *APs/Devices > New Page Illustration*

To discover more devices, visit the [Discover](#) page.

1-3 ▼ of 146 APs/Devices Page 1 ▼ of 49 > | Choose Columns CSV Export

Device ▲	Controller	Type	IP Address	LAN MAC Address	Discovered
<input type="checkbox"/> 00:0b:86:ce:e1:84	Aruba3200-RN	Aruba AP 70	10.51.6.222	00:0B:86:CE:E1:84	6/11/2010 1:26 PM
<input type="checkbox"/> 00:1a:1e:c0:6c:46	Aruba3600-Master	Aruba AP 125	10.51.81.175	00:1A:1E:C0:6C:46	12/23/2010 12:00 PM
<input type="checkbox"/> 00:1a:1e:c4:5a:10	Aruba3200-RN	Aruba AP 60	10.51.3.44	00:1A:1E:C4:5A:10	9/29/2010 3:03 PM

1-3 ▼ of 146 APs/Devices Page 1 ▼ of 49 > |

Select All - Unselect All

[View Ignored Devices](#)

Group:

Folder:

Aruba AP Group:

☒ Monitor Only + Firmware Upgrades  
☐ Manage Read/Write

## What Next?

- To authorize one or more devices to a group, see “[Authorizing Devices to AMP from APs/Devices > New Page](#)” on page 111.
- To delete a device altogether from AMP, select the corresponding check box for each device, and select **Delete**.
- Aruba thin APs can have Aruba AP Group specified, and Cisco thin APs can have LWAPP AP Group specified when they are authorized.

## Enabling Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual Cisco switch or router on the **Groups > List** page. AMP requires read-only access to a router or switch for all subnets that contain wired or wireless devices. The polling interval is specified on the **Group > Basic** page.

## Authorizing Devices to AMP from APs/Devices > New Page

Once you have discovered devices on your network, add these devices to a group and specify whether the device is to be placed in **Manage Read/Write** or **Monitor Only** mode. To configure a new group, refer to “[Configuring and Using Device Groups in AMP](#)” on page 71.

In **Manage Read/Write** mode, AMP compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy.

In **Monitor Only** mode, AMP updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **APs/Devices > Audit** page, but does not change the configuration of the device.



---

**Caution:** Put devices in **Monitor Only** mode when they are added to a newly established device group. This avoids overwriting any important existing configuration settings.

---

Once you have added several devices to the Group, and verified that no unexpected or undesired configuration changes will be made to the devices, you can begin to put the devices in **Manage Read/Write** mode using the **APs/Devices > Manage** or the **Modify these devices** link on any list page.

Perform the following steps to add a newly discovered device to a group:

1. Browse to the **APs/Devices > New** page. The **APs/Devices > New** page displays all newly discovered devices, the related controller (when known/applicable) and the device vendor, model, LAN MAC Address, IP Address, and the date/time of discovery.
2. Select the group and folder to which the device will be added from the drop-down menu (the default group appears at the top of the **Group** listing). Devices cannot be added to a Global Group; groups designated as Global Groups cannot contain access points.
3. Select either the **Monitor Only** or the **Manage Read/Write** radio button and select **Add**.  
At this point, you can go to the **APs/Devices > List** page and select the folder(s) to which you have assigned one or more devices to verify that your device has been properly assigned. If you wish to assign a device to the **Ignored** page, or delete it entirely from AMP, go to [step 4](#).



---

If you select **Manage Select Devices**, AMP automatically overwrites existing device settings with the specified Group settings. Placing newly discovered devices in Monitor mode is strongly recommended until you can confirm that all group configuration settings are appropriate for that device.

---

4. If you do not wish to manage or monitor a discovered device, you may select the device(s) from the list and select either **Ignore** or **Delete**. If you choose to **Ignore** the devices, they will not be displayed in the **APs/Devices > New** list, even if they are discovered in subsequent scans. You can view a list of all **Ignored** devices on the **APs/Devices > Ignored** page. If you choose to **Delete** the device, it will be listed on the **APs/Devices > New** list if discovered by AMP in a subsequent scan. Refer to “[Assigning Devices to the Ignored Page](#)” on page 116.

## Manually Adding Individual Devices

Some deployment situations may require that you manually add devices to AMP. You can add devices manually by uploading a CSV file, or from the **Device Setup > Add** page.

This section describes the following procedures:

- [Adding Devices with the Device Setup > Add Page](#)
- [Adding Multiple Devices from a CSV File](#)
- [Adding Universal Devices](#)

### Adding Devices with the Device Setup > Add Page

Manually adding devices from the **Device Setup > Add** page to AMP is an option for adding all device types. You only need to select device vendor information from a drop down menu for Cisco and Aruba devices, and AMP automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to AMP:

1. The first step to add a device manually is to select the vendor and model. Browse to the **Device Setup > Add** page and select the vendor and model of the device to add. [Figure 73](#) illustrates this page.

**Figure 73** *Device Setup > Add Page Illustration*

Select the type of device to add:

3Com 8750

3Com 8750  
3Com WX100  
3Com WX1200  
3Com WX2200  
3Com WX4400

Add

Import Devices via CSV

2. Select **Add**, and the **Device Communications** and **Location** sections appear, illustrated in [Figure 74](#).

**Figure 74** *Device Setup > Add > Device Communications and Location Sections*

Device Communications

Name:

Leave name blank to read it from device

IP Address:

SNMP Port:

161

Community String:

.....

Confirm Community String:

.....

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol:

MD5

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol:

DES

Telnet/SSH Username:

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

Location

Group:

San Francisco (SSID: -)

Folder:

Top

☒ Monitor Only (no changes will be made to device)

☐ Manage read/write (group settings will be applied to device)

Add

Cancel

3. Complete these **Device Communications** and **Location** settings for the new device. [Table 72](#) further describes the contents of this page. Settings may differ from device to device. In several cases, the default values from any given device derive from the **Device Setup > Communication** page.

**Table 72** *Device Communication and Location Fields and Default Values*

Setting	Default	Description
<b>Name</b>	None	User-configurable name for the AP (maximum of 20 characters).
<b>IP Address</b>	None	IP address of the device. This field is required.
<b>SNMP Port</b>	161	Port AMP uses to communicate with the AP using SNMP.
<b>Community String (Confirm)</b>	Taken from <b>Device Setup &gt; Communication</b>	Community string used to communicate with the AP. <b>NOTE:</b> The <b>Community String</b> should have RW (Read-Write) capability. New, out-of-the-box Cisco devices typically have SNMP disabled and a blank username and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
<b>SNMPv3 Username</b>	Taken from <b>Device Setup &gt; Communication</b>	If you are going to manage configuration for the device, this field provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. AMP initially uses this username and password combination to control the Cisco AP. AMP creates a user-specified account with which to manage the AP if the <b>User Creation Options</b> are set to <b>Create</b> and user Specified as User.
<b>Auth Password (Confirm)</b>		



**Table 72 Device Communication and Location Fields and Default Values (Continued)**

Setting	Default	Description
<b>Privacy Password (Confirm)</b>	Taken from <b>Device Setup &gt; Communication</b>	SNMPv3 privacy password.
<b>SNMPv3 Auth Protocol</b>	Taken from <b>Device Setup &gt; Communication</b>	Drop-down menu that allows you to enable the SNMPv3 authentication protocol to the device being added.
<b>SNMPv3 Privacy Protocol</b>	Taken from <b>Device Setup &gt; Communication</b>	Drop-down menu that allows you to enable SNMPv3 privacy protocol to the device being added.
<b>Telnet/SSH Username &amp; Password (Confirm)</b>	Taken from <b>Device Setup &gt; Communication</b>	Telnet username and password for existing Cisco IOS APs. AMP uses the Telnet username/password combination to manage the AP and to enable SNMP if desired. <b>NOTE:</b> New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet username of <b>Cisco</b> and default password of <b>Cisco</b> . This value is required for management of any existing Cisco IOS-based APs.
<b>“enable” Password (Confirm)</b>	Taken from <b>Device Setup &gt; Communication</b>	Password that allows AMP to enter <b>enable</b> mode on the device.
<b>HTTP Username &amp; Password</b>	Taken from <b>Device Setup &gt; Communication</b>	HTTP password used to manage the device initially, and to enable SNMP if desired.
<b>Auth Password</b>	Taken from <b>Device Setup &gt; Communication</b>	SNMPv3 authentication password. <b>NOTE:</b> SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AMP currently only supports authentication and encryption.
<b>Privacy Password</b>	Taken from <b>Device Setup &gt; Communication</b>	SNMPv3 privacy password. <b>NOTE:</b> SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AMP currently only supports authentication and encryption.

4. In the **Location** field, select the appropriate group and folder for the device.
5. At the bottom of the page, select either the **Monitor Only** or **Management read/write** radio button. The choice depends on whether or not you wish to overwrite the **Group** settings for the device being added. For more information and a detailed procedure, see [“Authorizing Devices to AMP from APs/Devices > New Page” on page 111](#).



If you select **Manage read/write**, AMP overwrites existing device settings with the **Group** settings. Place newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings.

6. Select **Add** to finish adding the devices to the network.

### Adding Multiple Devices from a CSV File

You can add devices in bulk from a CSV file to AMP. Here you also have the option of specifying vendor name only, and AMP will automatically determine the correct type while bringing up the device. If your CSV file includes make and model information, AMP will add the information provided in the CSV file as it did before. It will not override what you have specified in this file in any way.

The CSV list must contain the following columns:

- IP Address
- SNMP Community String

- Name
- Type
- Auth Password
- SNMPv3 Auth Protocol
- Privacy Password
- SNMPv3 Username
- Telnet Username
- Telnet Password
- Enable Password
- SNMP Port

You can download a CSV file and customize it as you like. A sample CSV file is illustrated in [Figure 75](#).

**Figure 75** Sample CSV File

```
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Telnet Username,Telnet Password,Enable Password,SNMP Port
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,aes,sv3user,telnetuser,telnetpwd,enable,161
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,des,user
10.70.36.172,public,Cisco-WLC-4012-3,Cisco 4000 WLC,
10.46.111.48,,
```

1. To import a CSV file, go to the **Device Setup > Add** page.
2. Select the **Import Devices via CSV** link. The **Upload a list of devices** page displays; see [Figure 76](#).

**Figure 76** Device Setup > Add > Import Devices via CSV Page Illustration

Upload a list of devices

Location

Group: Spectrum APs
Folder: Top

import\_devices.csv

The list must be in comma-separated values (CSV) format, containing the following columns:

1. IP Address
2. SNMP Community String
3. Name
4. Type
5. Auth Password
6. SNMPv3 Auth Protocol
7. Privacy Password
8. SNMPv3 Privacy Protocol
9. SNMPv3 Username
10. Telnet Username
11. Telnet Password
12. Enable Password
13. SNMP Port

**IP Address** is required, the others are optional.  
**Type** is a case-insensitive string; you can [view a list of device types](#).

[Download a sample file](#) or see the example below:

```
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Telnet Username,Telnet Password,Enable Password,SNMP Port
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,aes,sv3user,telnetuser,telnetpwd,enable,161
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,des,user
```

3. Select a group and folder into which to import the list of devices.
4. Select **Choose File** and select the CSV list file on your computer.
5. Select **Upload** to add the list of devices into AMP.

## Adding Universal Devices

AMP gets basic monitoring information from any device including switches, routers and APs whether or not they are supported devices. Entering SNMP credentials is optional. If no SNMP credentials are entered, AMP will provide ICMP monitoring of universal devices. This allows you to monitor key elements of the wired network infrastructure, including upstream switches, RADIUS servers and other devices. While AMP can manage most leading brands and models of wireless infrastructure, universal device support also enables basic monitoring of many of the less commonly used devices.

Perform the same steps to add universal devices to AMP that were detailed in “[Adding Devices with the Device Setup > Add Page](#)” on page 112.

AMP collects basic information about universal devices including name, contact, uptime and location. Once you have added a universal device, you can view a list of its interfaces on **APs/Devices > Manage**.

By selecting the **pencil** icon next to an interface, you can assign it to be non-monitored or monitored as Interface 1 or 2. AMP collects this information and displays it on the **APs/Devices > Monitor page in the Interface** section. AMP supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. AMP also monitors sysUptime.

## Assigning Devices to the Ignored Page

A device can be assigned to the **Ignored** page from the **APs/Devices > New** page. The advantage of having the device be designated in this way, as in the case of a device that is temporarily down for a known reason, is that when you take it off the ignored list, it returns immediately to the location in AMP where it had resided before it was marked **Ignored**.

- Ignored devices are *not* displayed in **APs/Devices > New** if discovered in subsequent scans.
- Deleted devices *will* be listed on the **APs/Devices > New** if discovered in subsequent scans.

Perform these steps to further process or return an ignored device to a managed status.

1. To view all devices that are ignored, go to the **APs/Devices > Ignored** page, illustrated in [Figure 77](#).

**Figure 77** *APs/Devices > Ignored Page Illustration*

4-6 ▼ of 17 Ignored APs/Devices |< < Page 2 ▼ of 6 > >| Choose Columns CSV Export

	Device	Controller	Type	IP Address	LAN MAC Address	Discovered ▼
<input type="checkbox"/>	Aruba6000	-	Aruba Controller	10.15.90.15	-	6/8/2010 4:14 AM
<input type="checkbox"/>	Cisco_2100_5B:60	-	Cisco 2100 WLC	10.50.100.2	-	3/29/2010 7:29 PM
<input type="checkbox"/>	hp-poe-switch	-	HP ProCurve 2626-PWR	10.51.0.22	00:13:21:AC:5E:40	10/26/2009 4:35 PM

4-6 ▼ of 17 Ignored APs/Devices |< < Page 2 ▼ of 6 > >|

Select All - Unselect All

View New Devices

Unignore Delete

This page provides the following information for any ignored device:

- device name or MAC address, when known
  - controller associated with that device
  - device type
  - device IP address
  - LAN MAC address for the LAN on which the device is located
  - date and time of device discovery
2. To change the device parameters for a given device, select its checkbox and adjust group, folder, monitor, and manage settings as desired.
  3. Select **Add** to add the device to AMP so that it appears on the **APs/Devices > New** list.
  4. The **Unignore** button will either return the device to its regular folder or group, or send it to the **APs/Devices > New** page.

## Monitoring Devices

This section discusses various device monitoring options and includes the following sections:

- [Viewing Device Monitoring Statistics](#)
- [Understanding the APs/Devices > Monitor Pages for All Device Types](#)
- [Evaluating Radio Statistics for an AP](#)
- [Monitoring Data for Mesh Devices](#)
- [Monitoring Data for Wired Devices \(Routers and Switches\)](#)

- [Understanding the APs/Devices > Interfaces Page](#)
- [Auditing Device Configuration](#)
- [Using Device Folders \(Optional\)](#)

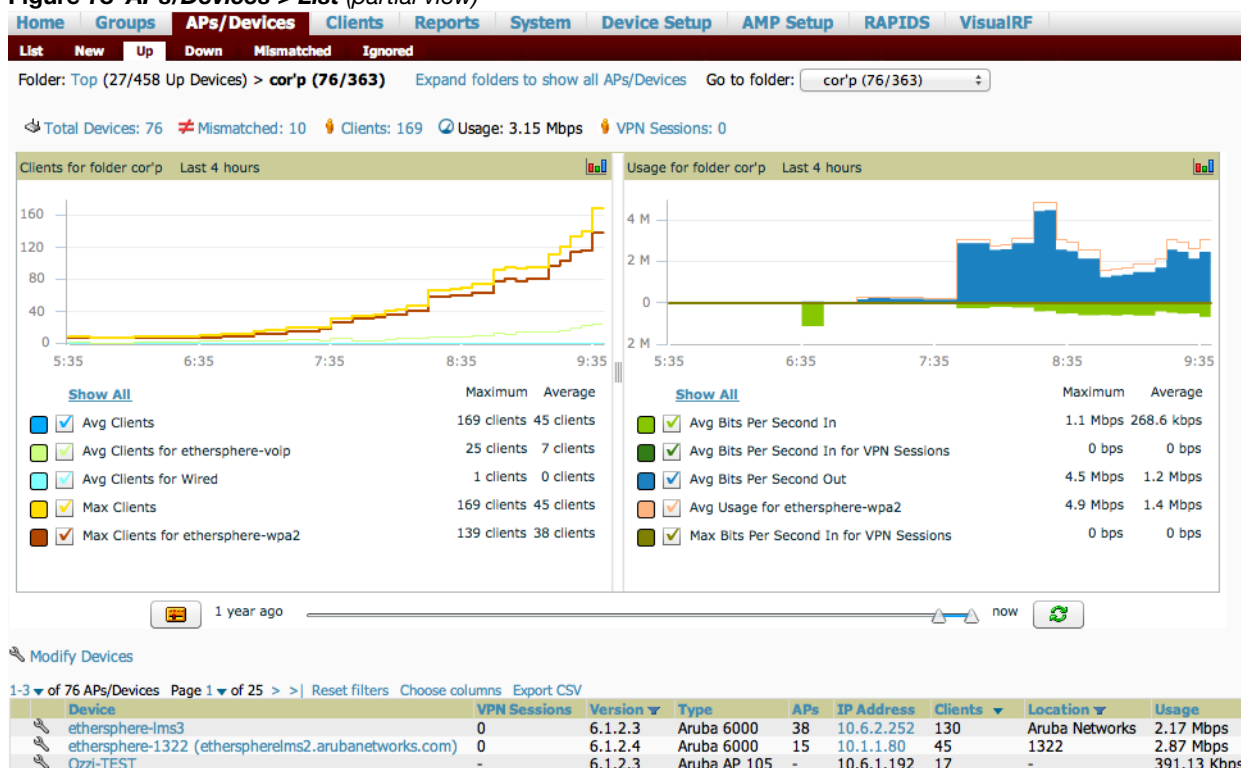
## Viewing Device Monitoring Statistics

You can view many useful device monitoring statistics in the **APs/Devices > List** page. The **APs/Devices > List** page displays Clients and Usage interactive graphs (formerly Users and Bandwidth prior to 7.4) and lists all devices that are managed or monitored by AMP.

To see only the Up devices, you can click the **Up** link in the Top Header Stats bar (next to the green arrow). This displays the **APs/Devices > Up** page with the same information, but only containing active devices. You can do the same with the **Down** and **Mismatched** top header stats links.

Use the **Go to folder** field to filter the list by folder, or click **Expand folders to show all APs/Devices** if you are looking at a filtered device list. A lock icon in the **Configuration** column indicates that the device in that row is in **Monitor only** mode. Figure 78 illustrates this page.

**Figure 78** *APs/Devices > List (partial view)*



Verify that the devices you added are now appearing in the devices list with a Status of **Up**.



Newly added devices will be status **Down** until they have been polled the first time. They will be configuration **Unknown** until they have finished verification. The **Up** status is not contingent on verification.

The same section also appears on the **Groups > Monitor** page, and is hyperlinked from a controller's monitoring interface.

The **Alert Summary** section of **APs/Devices > List** cites the number of events that have occurred in the last two hours, the last 24 hours, and total. There are four categories of alerts as listed below:

- AMP Alerts
- IDS Events



The **Alert Summary** table is also a feature of the **Home > Overview** page, and has the same links in that location.

For more information on the **Alert Summary** table, refer to “[Viewing Alerts](#)” on page 194.

## Understanding the APs/Devices > Monitor Pages for All Device Types

You can quickly go to any device’s monitoring page once you go to its specific folder or group on the **APs/Devices > List** page, by selecting its hyperlinked name in the **Device** column.

All **Monitor** pages include a section at the top displaying information such as monitoring/configuration status, serial number, total users, firmware version and so on, as shown in [Figure 79](#).

**Figure 79 Monitoring Page Top Level Data Common to All Device Types**

The alert summary, recent events, and audit log sections are also the same regardless of device type and these sections appear at the bottom of these pages, a portion of which is shown in [Figure 80](#).

**Figure 80 Monitoring Page Bottom Level Data Common to All Device Types**

**Alert Summary** at 2/3/2010 5:23 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
Alerts	0	0	0	-
IDS Events	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

### Recent Events ([view system event log](#))

Time	User	Event
Wed Feb 3 16:46:28 2010	System	Configuration verification succeeded; configuration is good ...omitted 19 duplicate messages...
Fri Jan 29 08:31:38 2010	System	Configuration verification succeeded; configuration is good
Fri Jan 29 08:30:08 2010	System	Status changed to 'OK'
Fri Jan 29 08:30:08 2010	System	Up

### Audit Log

Time	User	Event
Mon Jan 25 17:23:47 2010	admin	ap (id 15365): monitor_only: '0' => '1'
Mon Jan 25 13:04:35 2010	burton	ap (id 15365): monitor_only: '1' => '0'

Monitoring pages vary according to whether they are wired routers/switches or controllers/WLAN switches, or thin or fat APs, whether the device is a Mesh device, and whether Spectrum is enabled. These differences are discussed in the sections that follow.

## Monitoring Data Specific to Wireless Devices

The **APs/Devices > Monitor page** for controllers and APs include a graph for users and bandwidth. The controller graph lists the APs connected to it, while the APs include a list of users it has connected.

When available, lists of CDP and RF neighbors are also listed.

A sample monitoring page for wireless devices is shown in [Figure 81](#).

**Figure 81 APs/Devices > Monitor Page for Wireless Devices (partial view of an AP)**

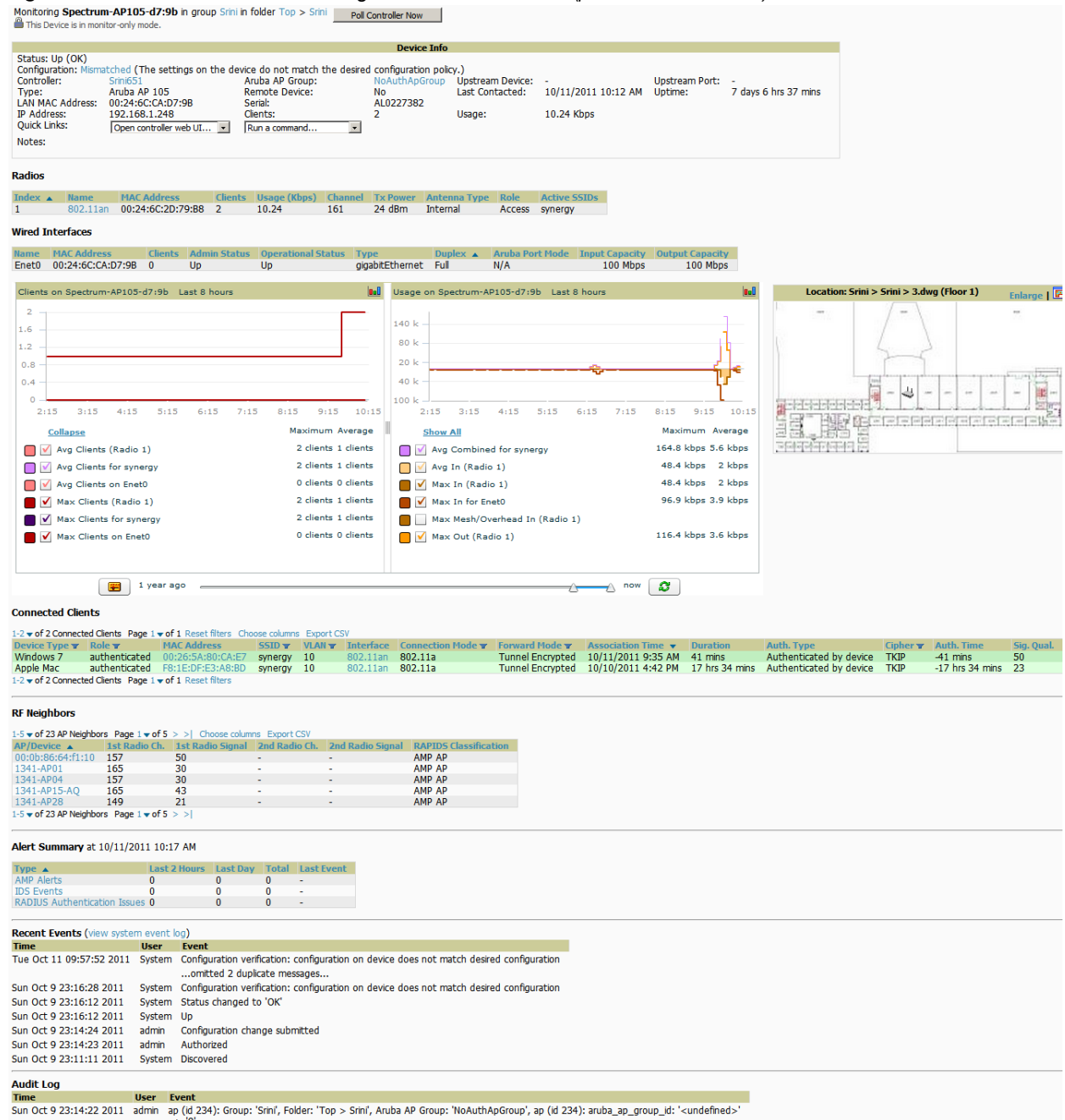


Table 73 describes the fields and information displayed in the **Device Info** section. The displayed fields vary from device to device.

**Table 73 APs/Devices > Monitor > Device Info Fields and Default Values**

Field	Description
<b>Poll Now</b>	Button above the <b>Device Info</b> section that, when pressed, immediately polls the individual AP or the controller for a thin AP; this overrides the group's preset polling intervals to force an immediate update of all data except for rogue information. Shows "attempt" status and last polling times.



**Table 73 APs/Devices > Monitor > Device Info Fields and Default Values (Continued)**

Field	Description
<b>Status</b>	Displays ability of AMP to connect to the AP. <b>Up</b> (no issue) means everything is working as it should. <b>Down</b> (SNMP “get” failed) means AMP can get to the device but not speak with it using SNMP. Check the SNMP credentials AMP is using the view secrets link on the <b>APs/Devices &gt; Manage</b> page and verify SNMP is enabled on the AP. Many APs ship with SNMP disabled. <b>Down</b> (ICMP ping failed after SNMP get failed) means AMP is unable to connect to the AP using SNMP and is unable to ping the AP. This usually means AMP is blocked from connecting to the AP or the AP needs to be rebooted or reset.
<b>Configuration</b>	<b>Good</b> means all the settings on the AP agree with the settings AMP wants them to have. <b>Mismatched</b> means there is a configuration mismatch between what is on the AP and what AMP wants to push to the AP. The <b>Mismatched</b> link directs you to this specific <b>APs/Devices &gt; Audit</b> page where each mismatch is highlighted. <b>Unknown</b> means the device configuration has not yet been fetched (possible issue with credentials). <b>Verifying</b> means it's fetching configuration to be compared to desired settings.
<b>Firmware</b>	Displays the firmware version running on the AP.
<b>Licenses</b> (Appears for Aruba controllers)	Selecting this link opens a pop-up window that lists the licenses installed for this controller, and whether they have expired.
<b>Controller</b> (Appears for APs)	Displays the controller for the associated AP device as a link. Select the link to display the <b>APs/Devices &gt; Monitor</b> page for that controller.
<b>Mesh Gateway *</b>	Specifies the mesh AP acting as the wired connection to the network.
<b>Mesh Mode*</b>	Specifies whether the AP is a portal device or a mesh node. The portal device is connected to the network over a wired connection. A node is a device downstream of the portal that uses wireless connections to reach the portal device.
<b>Mesh ID *</b>	The name of the mesh device.
<b>View in Google Earth*</b>	Selecting the Google Earth icon opens the mesh network view in Google Earth.
<b>Type</b>	Displays the make and model of the device.
<b>Last Contacted</b>	Displays the most recent time AMP has polled the AP for information. The polling interval can be set on the <b>Groups &gt; Basic</b> page.
<b>Uptime</b>	Displays the amount of time since the AP has been rebooted. This is the amount of time the AP reports and is not based on any connectivity with AMP.
<b>LAN MAC Address</b>	Displays the MAC address of the Ethernet interface on the device.
<b>Serial</b>	Displays the serial number of the device.
<b>Radio Serial</b>	Displays the serial number of the radios in the device. This field is not available for all APs.
<b>Location</b>	Displays the SNMP location of the device.
<b>Contact</b>	Displays the SNMP contact of the device.
<b>IP Address</b>	Displays the IP address that AMP uses to communicate to the device. This number is also a link to the AP web interface. When the link is moused over a pop-up menu will appear allowing you to http, https, telnet or SSH to the device. <b>NOTE:</b> For Aruba controllers, if Single Sign-On is enabled for your role in this AMP and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link.
<b>Outer IP</b>	Public IP address for a RAP device.
<b>Remote LAN IP</b>	LAN IP address for a RAP. This address is useful for troubleshooting from the local network.
<b>Quick Links</b>	<ul style="list-style-type: none"> <li>● <b>Open controller web UI:</b> A drop-down menu that allows you to jump to the controller’s UI in a new window.</li> </ul> <p><b>NOTE:</b> For Aruba controllers, if Single Sign-On is enabled for your role in this AMP and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link.</p> <ul style="list-style-type: none"> <li>● <b>Run a command:</b> A drop-down menu with a list of CLI commands you can run directly from the <b>APs/Devices &gt; Monitor</b> page.</li> </ul>



**Table 73 APs/Devices > Monitor > Device Info Fields and Default Values (Continued)**

Field	Description
<b>APs</b>	For controllers, displays the number of APs managed by this device at the time of the last polling.
<b>Clients</b>	Displays the total number of users associated to the device or its APs regardless of which radio they are associated to, at the time of the last polling.
<b>Usage</b>	Combined bandwidth through the device at time of polling.

\*This field is only available for mesh APs. To see an example of mesh monitoring, see [“Monitoring Data for Mesh Devices” on page 128](#).

[Table 74](#) describes the information in the **Radio** table for APs:

**Table 74 APs/Devices > Monitor > Radio Fields and Descriptions**

Field	Description
<b>Index</b>	The number of the radio, used to distinguish radios that may be of the same type on a device.
<b>Name</b>	The Radio type (802.11a/b/g/n) as a link to the <b>Radio Statistics</b> page for that radio.
<b>MAC Address</b>	The MAC address of the corresponding radio in the AP.
<b>Clients</b>	The number of users associated to the corresponding radio at the time of the last polling.
<b>Usage (Kbps)</b>	The amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.
<b>Channel</b>	The channel of the corresponding radio.
<b>Tx Power</b>	Some devices report transmit power reduction rather than transmit power; no value is reported for those devices.
<b>Antenna Type</b>	Indicates <b>Internal</b> or <b>External</b> radio. For devices where antenna type is defined per AP, the same antenna type will be listed for each radio.
<b>Channel Width*</b>	The bandwidth of the channel used by 802.11 stations. Legacy devices use <b>20 MHz</b> channels, and newer devices that support the 802.11n standard can use <b>40 MHz</b> channels to increase throughput.
<b>Mesh Links *</b>	The total number of mesh links to the device including uplinks and downlinks.
<b>Role</b>	Whether the radio acts as a Mesh Node or Access
<b>Active SSIDs</b>	The SSID(s) of the radio.

Devices with wired interfaces (except Aruba Instant IAPs) will display the **Wired Interfaces** table, which is described in [Table 75](#):

**Table 75 APs/Devices > Monitor > Wired Interfaces Fields and Descriptions**

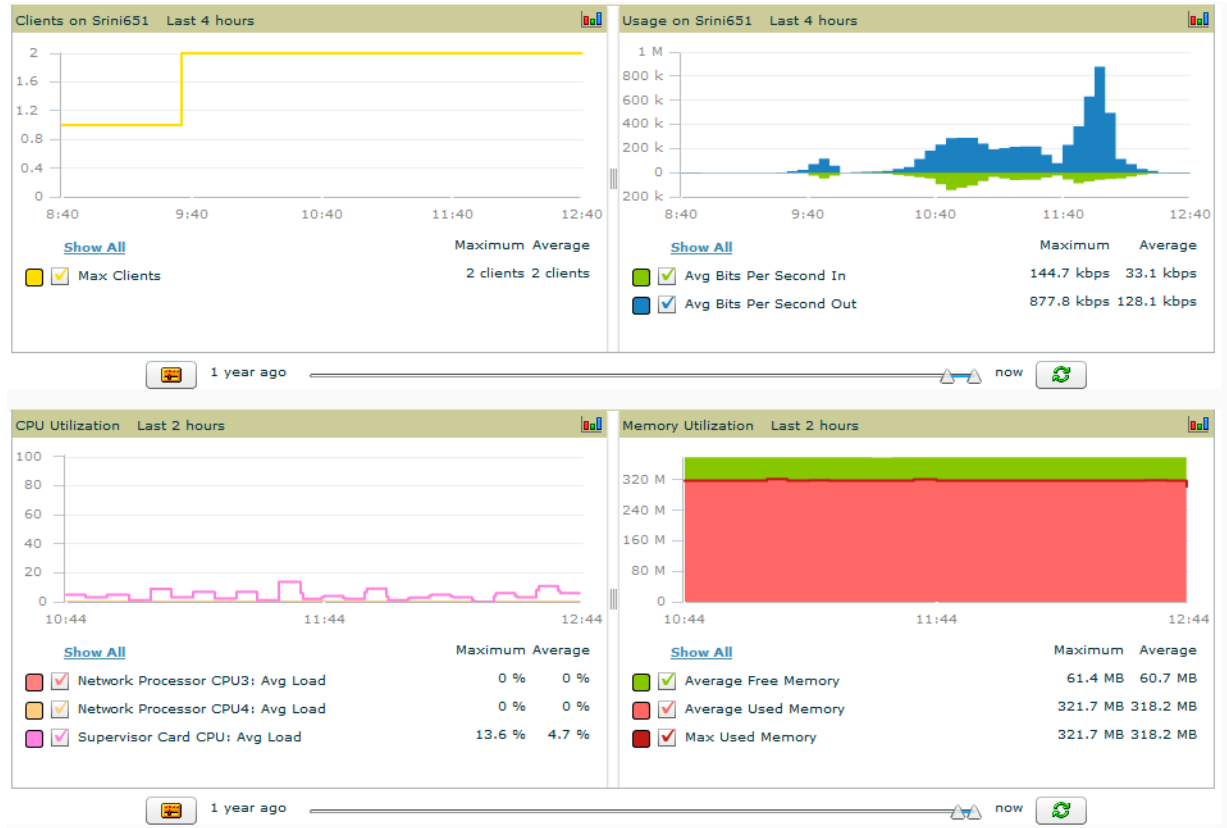
Field	Description
<b>Name</b>	Displays the name of the interface.
<b>MAC Address</b>	Displays the MAC address of the corresponding interface in the device.
<b>Clients</b>	Displays the number of users associated to the corresponding interface at the time of the last polling.
<b>Type</b>	Indicates the type of interface - gigabitEthernet or fastEther for wired interfaces.
<b>Admin Status</b>	The administrator setting that determined whether the port is on or off.
<b>Operational Status</b>	Displays the current status of the interface. If an interface is <b>Up</b> , then AMP is able to ping it and fetch SNMP information. If the AP is listed <b>Down</b> then AMP is either unable to ping the interface or unable to read the necessary SNMP information from the device.
<b>Duplex</b>	Duplex mode of the link, full or half.
<b>Aruba Port Mode</b>	Either Active Standby (which provides redundancy so that when an active interface fails, the user traffic can failover to the standby interface) or one of the forwarding modes (Split, Bridge).

**Table 75 APs/Devices > Monitor > Wired Interfaces Fields and Descriptions (Continued)**

Field	Description
<b>Input Capacity</b>	The input capacity of the interface.
<b>Output Capacity</b>	The output capacity of the interface.

Figure 82 illustrates the interactive graphs, and Table 76 describes the graphs on this page.

**Figure 82 Interactive Graphs for an Aruba Controller**



**Table 76 APs/Devices > Monitor Graphical Data**

Graph	Description
<b>Clients</b>	Formerly “Users”. Shows the max and average client count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Checkboxes below the graph can be used to limit the data displayed.
<b>Usage</b>	Formerly “Bandwidth”. Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Checkboxes below the graph can be used to limit the data displayed.
<b>CPU Utilization</b> (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only)	Reports overall CPU utilization (not on a per-CPU basis) of the device.
<b>Memory Utilization</b> (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only)	Reports average used and free memory and average max memory for the device.

Table 77 describes the fields and information displayed for the **Connected Clients** display.

**Table 77** *APs/Devices > Monitor > Connected Clients Fields and Default Values*

Field	Description
<b>Username</b>	Provides the name of the User associated to the AP. AMP gathers this data in a variety of ways. It can be taken from RADIUS accounting data or traps.
<b>Device Type</b>	The type of device the user is using as determined by the Device Type Rules set up by an administrator in <b>AMP Setup &gt; Device Type Setup</b> . For more information, refer to <a href="#">“Setting Up Device Types” on page 59</a> .
<b>Role</b>	The role of the connected client such as employee, perforce, or logon (captive portal).
<b>MAC Address</b>	Displays the Radio MAC address of the user associated to the AP. Also provides a link that redirects to the <b>Users &gt; Detail</b> page.
<b>Radio</b>	Displays the radio to which the user is associated.
<b>Association Time</b>	Displays the first time AMP recorded the MAC address as being associated.
<b>Duration</b>	Displays the length of time the MAC address has been associated.
<b>Auth. Type</b>	<p>Displays the type of authentication employed by the user. Supported auth types include:</p> <ul style="list-style-type: none"> <li>• <b>EAP</b>—Extensible Authentication Protocol.</li> <li>• <b>RADIUS accounting</b>—RADIUS accounting servers integrated with AMP provide the RADIUS Accounting Auth type.</li> <li>• <b>WPA2</b>—Wi-Fi Protected Access 2 encryption</li> <li>• <b>No Encryption</b></li> </ul> <p>AMP considers all other types as not authenticated.</p> <p>The information AMP displays in <b>Auth. Type</b> and <b>Cipher</b> columns depends on what information the server receives from the devices it is monitoring. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different <b>Auth. Type</b> or <b>Cipher</b> values may be reported to AMP.</p> <p>If all APs are the same model and all are set up the same way, then another reason for differing <b>Auth Types</b> might be the use of multiple VLANs or SSIDs. One client device might authenticate on one SSID using one <b>Auth. Type</b> and another client device might authenticate on a second SSID using a different <b>Auth. Type</b>.</p>
<b>Cipher</b>	Displays the encryption or decryption cipher supporting the user, when this information is available. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different <b>Auth. Type</b> or <b>Cipher</b> values may be reported to AMP.
<b>Auth. Time</b>	Shows how long the user has been authenticated, in minutes. A negative number (such as -17 min) indicates that the user has not authenticated for the duration displayed.
<b>Signal Quality</b>	Displays the average signal quality the user experienced.
<b>Usage</b>	Displays the average bandwidth consumed by the MAC address.
<b>Goodput</b>	The ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.
<b>Location</b>	Displays the QuickView box allows users to view features including heatmap for a device and location history for a user.
<b>LAN IP Addresses</b>	Displays the IP assigned to the user MAC. This information is not always available. AMP can gather it from the ARP cache of switches discovered by AMP. As of AMP 7.4, this column can accommodate multiple IP addresses for a client if it has both IPv4 and IPv6.
<b>LAN Hostnames</b>	The DNS hostname(s) broadcast by the client. As of 7.4, this column can accommodate multiple hostnames for a client if it has both IPv4 and IPv6.

If you are viewing an Aruba AirMesh device’s monitoring page, the **Mesh Links** table lists the mesh devices linked to this device, as shown in [Figure 83](#):

**Figure 83** Mesh Links Table on APs/Devices > Monitor Illustration

Mesh Links									
AP Name	Device Address	Link Time	Duration	Local Radio Index	Remote Radio Index	Link Speed	Signal	RSSI	Transmit Rate
MSR4000	00:17:78:11:70:56	10/11/2011 1:30 PM	0 mins	2		48 Mbps	-20 dBm	75	504 bps

The **Recent Events** area lists the most recent events specific to the device. This information also appears on the **System > Events Log** page (refer to “Using the System > Event Log Page” on page 186). Table 78 describes the fields in this page that display in the **Recent Events** table.

**Table 78** APs/Devices > Monitor > Recent Events Fields and Default Values

Field	Description
<b>Time</b>	Displays the day and time the event was recorded.
<b>User</b>	Displays the user that triggered the event. Configuration changes are logged as the AMP user that submitted them. Automated AMP events are logged as the <b>System</b> user.
<b>Event</b>	Displays a short text description of the event.

## Evaluating Radio Statistics for an AP

The **APs/Devices > Monitor > Radio Statistics** page contains useful data for pinpointing network issues at the AP radio level for Aruba APs and Cisco WLC thin APs (firmware 4.2 or greater).

To see radio statistics details, navigate to the **APs/Devices > Monitoring** page for a supported AP and select the linked radio under the **Name** column in the **Radios** list table, as illustrated in Figure 84.

**Figure 84** Links to the Radio Statistics page on APs/Devices > Monitoring for an AP

Radios							
Name	MAC Address	Users	BW (Kbps)	Channel	Tx Power	Antenna Type	Active SSIDs
802.11an	00:1A:1E:85:54:70	-	-	-	-	Internal	-
802.11bgn	00:1A:1E:85:54:60	-	-	-	-	Internal	-

## Overview of the Radio Statistics Page

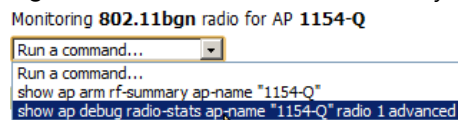
The Radio Statistics page displays transmit and receive statistics about the communication quality of individual radios. Depending on the AP, assigned group profiles, and recent activity on this radio, this data gives visibility into recent and historical changes in the network, fetches real-time statistics from the AP's controller, indicates actively interfering devices (requires Aruba APs set to Spectrum mode), and summarizes major issues.

## Viewing Real-Time ARM Statistics

Aruba AP Groups that have the **Adaptive Radio Management (ARM)** feature enabled continuously optimize each AP to use the best channel and transmission power settings available. An AP configured with ARM will automatically adjust to a better channel if it reaches a configured threshold for noise, MAC errors, or PHY errors; additionally, it can attenuate transmit power and switch between radio modes as needed. For more information, refer to the ARM chapter in the *ArubaOS User Guide*.

Complete ARM statistics from Aruba controllers can be retrieved from the Radio Statistics page by selecting the **Run a command** drop-down menu and choosing button, as illustrated in Figure 85.

**Figure 85** Fetch additional radio stats by running a show command



When this button is selected, a new browser window launches with the statistics in plain text. Other ARM-tracked metrics are visible in the **Radio Statistics** page for Aruba APs.

## Issues Summary section

The **Issues Summary** section only displays when noise, client count, non-802.11 interfering devices, channel utilization, usage, and MAC and PHY errors reach a certain threshold of concern, as described in [Table 79](#) and illustrated in [Figure 86](#):

**Table 79** *Issues Summary labels and thresholds*

Issue	Triggering Threshold
High Noise	> -80
High Number of Clients	> 15
High Channel Utilization	> 75%
High Usage	> 75% of max
Interfering Devices Detected	Detected within the last 5 minutes
High MAC/Phy Errors	> 1000 frames/sec

**Figure 86** *Issues Summary Section Illustration*

Monitoring 802.11bg radio for AP AP0018.19bd.b1d0

Issues Summary	
<b>Issue:</b>	<b>Description</b>
High Noise:	Noise > -80
High Channel Utilization:	Channel Utilization > 75%

These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the [Radio Statistics Interactive Graphs](#) section of this chapter for details.

## 802.11 Radio Counters Summary

This table appears for radios with 802.11 counters and summarizes the number of times an expected acknowledgement frame was not received, the number of duplicate frames, the number of frames containing Frame Check Sequence (FCS) errors, and the number of frame/packet transmission retries and failures. These aggregate error counts are broken down by Current, Last Hour, Last Day, and Last Week time frames, as illustrated in [Figure 87](#).

**Figure 87** *802.11 Radio Counters Summary table*

**802.11 Radio Counters Summary (frames/sec)**

	Current	Last Hour	Last Day	Last Week
Unacked	0	0	0	1
Retries	0	0	0	0
Failures	0	0	0	1
Dup Frames	0	0	0	0
FCS Errors	380	380	386	464

The frame- per-second rate of these and other 802.11 errors over time are tracked and compared in the **802.11 Counters** graph on the same page.

## Radio Statistics Interactive Graphs

Time-series graphs for the radio are displayed across a tabbed, dual-pane interface to show changes recorded at every polling interval over time. Clients and Usage data are polled based on the AP's group's **User Data Polling Period**. Channel, Noise, and Power are based on **AP Interface Polling Period**. 802.11 Counters data are based on the AP's group's **802.11 Counters Polling Period**.

You can adjust the attributes of these graphs as follows:

- Drag the horizontal slider under the graphs to move the scope of all graphs between one year ago and the current time.
- Drag the vertical slider between graphs to change the relative width of each.
- The **Show All** link displays all of the available data series.

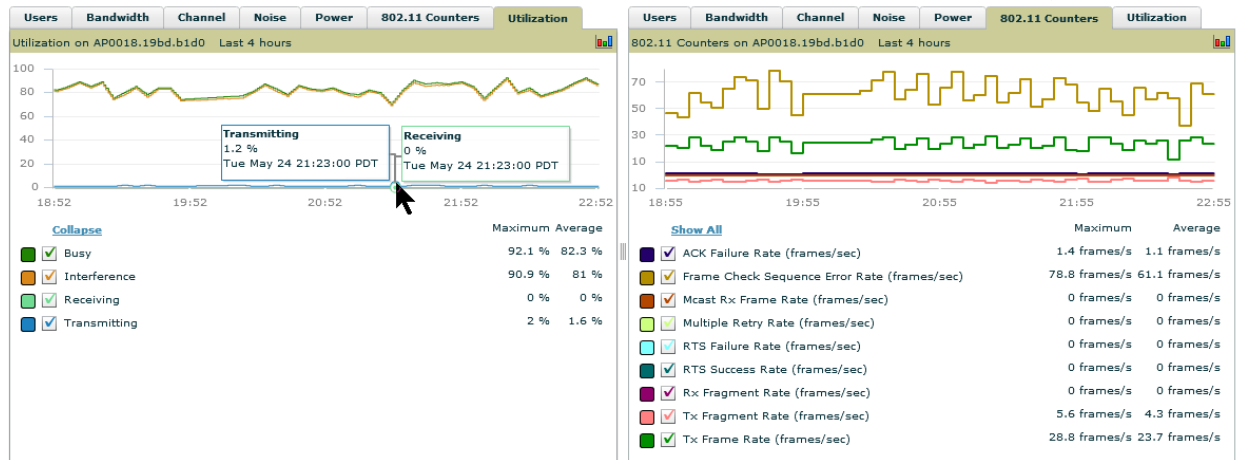
- The bar-graph icon on the upper right-hand corner of each graph opens a new window and displays all data series for the selected graph over the last two hours, last day, last week, last month, and last year in one page. The graphs that display depend on the AP and/or its controller.
- Select the checkbox next to any metric to remove its data from the graph. Select **Collapse** to remove unchecked metrics from the legend, and **Show All** to restore them.

The two graph panes enable simultaneous display of two different information sets, as detailed in :

**Table 80** *Radio Statistics Interactive Graphs Descriptions*

Graph Title	Description
<b>Clients</b>	A line graph that displays the maximum users associated to the corresponding radio at polling intervals over the time range set in the slider. Select <b>Show All</b> for other metrics such as average users and max users for various individual devices.
<b>Usage</b>	An area graph displaying the average bandwidth in each direction for the radio. Select <b>Show All</b> for other metrics such as max bandwidth in and out, average and max mesh/overhead or overhead bandwidth, and average/max Enet0.
<b>Channel</b>	An area graph that displays the channel changes (if any) of the radio over time. Frequent, regular channel changes on an Aruba or Cisco WLC AP radio usually indicate that the Adaptive Radio Management feature (ARM) in AOS is compensating for high noise levels from interfering devices.
<b>Noise</b>	An area graph that displays signal interference (noise floor) levels in units of dBm. Noise from interfering devices above your AP's noise threshold can result in dropped packets. For ARM-enabled Aruba APs, crossing the noise threshold triggers an automatic channel change.
<b>Power</b>	A line graph that displays the average and maximum radio transmit power, between 0 and 30 dBm, over the time range set in the slider. You can adjust the transmit power manually in the <b>APs/Devices &gt; Manage</b> page for this radio's AP, or enable ARM on Aruba APs to dynamically adjust the power toward your acceptable Coverage Index as needed. For more information, see the "Adaptive Radio Management" chapter of the <i>ArubaOS User Guide</i> .
<b>MAC/Phy Errors</b>	A line graph displaying the frame reception rate, physical layer error rate (resulting from poor signal reception or broken antennas), and the data link (MAC) layer (corrupt frames, driver decoding issues) for the radio.
<b>802.11 Counters</b>	A line graph that displays statistics such as frame rate, fragment rate, retry rate, duplicate frame rate, and other metrics tracked by 802.11 counters.
<b>Utilization</b> ( <i>Aruba and Cisco WLC thin APs on supported firmware versions only</i> )	Displays max and average percentages on this radio for busy, interfering receiving and transmitting signals. Special configuration on the controller is required to enable this data; consult the <i>Aruba and AirWave Best Practices Guide</i> in <b>Home &gt; Documentation</b> for details.

**Figure 88 Radio Statistics Interactive Graphs Illustration – Bandwidth and 802.11 Counters displayed**



## Recent ARM Events Log

If this radio references an active and enabled ARM profile, and if your AMP is enabled as a trap host (see *AirWave and Aruba Best Practices Guide* for instructions), ARM-initiated events such as automatic channel changes, power changes, and mode changes are displayed in the ARM Events table with the original and modified values; these values can be selected for filtering the results. You can export the table in CSV format. The columns and values are described in , and illustrated in Figure 89.

**Figure 89 ARM Events Table Illustration**

ARM Events

1-10 of 23 ARM Events Page 1 of 3 > > | Choose Columns CSV Export

Time	Trap Type	Previous Tx Power	Current Tx Power	Previous Radio Mode	Current Radio Mode	Previous Channel	Current Channel	Previous Secondary Channel	Current Secondary Channel
1/4/2011 10:55 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 10:51 AM	Power Change	6	3	-	-	-	-	-	-
1/4/2011 10:51 AM	Channel Change	-	-	-	-	7	1	Above	Above
1/4/2011 9:55 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 9:51 AM	Power Change	6	3	-	-	-	-	-	-
1/4/2011 9:50 AM	Channel Change	-	-	-	-	7	1	Above	Above
1/4/2011 4:38 AM	Channel Change	-	-	-	-	1	7	Above	Above
1/4/2011 4:34 AM	Power Change	6	3	-	-	-	-	-	-

**Table 81 ARM Events table Columns and Values**

Column	Description
<b>Time</b>	The time of the ARM event.
<b>Trap Type</b>	The type of trap that delivered the change information. Current ARM trap types that display in AirWave are: <ul style="list-style-type: none"> <li>Power Change</li> <li>Mode Change</li> <li>Channel Change</li> </ul> Values that display in the following columns depend on the Trap Type.
<b>Previous Tx Power</b>	Old value for transmit power before the Power Change event took place.
<b>Current Tx Power</b>	New transmit power value after the change.
<b>Previous Radio Mode</b>	Old value for radio mode before the Mode Change event took place.
<b>Current Radio Mode</b>	New radio mode value after the change.
<b>Previous Channel</b>	Old primary channel value before the Channel Change event took place.
<b>Current Channel</b>	New primary channel value after the change.
<b>Previous Secondary Channel</b>	Old secondary channel value (for 40Mhz channels on 802.11n devices) before the Channel Change event took place.



**Table 81** ARM Events table Columns and Values (Continued)

Column	Description
<b>Current Secondary Channel</b>	New secondary channel value after the change.
<b>Change Reason</b>	If the noise and interference cause for the change can be determined, they will be displayed here. Mode change reasons are not yet tracked.

## Detected Interfering Devices Table

For Aruba APs running in Spectrum mode, the same non-802.11 interfering devices identified in the **Issues Summary** section are classified in the **Detected Interfering Devices** table along with the timestamp of its last detection, the start and end channels of the interference, the signal to noise ratio, and the percentage of time the interference takes place, as illustrated in [Figure 90](#). This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

**Figure 90** Detected Interfering Devices Table Illustration

1-7 of 7 Interfering Devices Page 1 of 1 Choose Columns CSV Export

Device Type ▲	Last Seen	Start Channel	End Channel	SNR	Duty Cycle
Cordless Base Freq Hopper	1/14/2011 3:31 PM	1	14	69	5
XBox Freq Hopper	1/14/2011 3:17 PM	1	14	63	5
Cordless Phone Freq Hopper	1/14/2011 2:10 PM	1	14	80	5
Generic Freq Hopper	1/14/2011 3:52 PM	1	14	73	5
Video Device Fixed Freq	1/14/2011 9:25 AM	10	13	72	99

Possible device types for the Detected Interfering Devices table are:

- Wi-Fi
- Microwave
- Bluetooth
- Generic Fixed Freq
- Cordless Phone Fixed Freq
- Video Device Fixed Freq
- Audio Device Fixed Freq
- Generic Freq Hopper
- Cordless Phone Freq Hopper
- Xbox Freq Hopper
- Microwave Inverter
- Cordless Base Freq Hopper
- Unknown

## Active BSSIDs Table

The Active BSSIDs table maps the BSSIDs on a radio with the SSID it broadcasts to the network, as illustrated in [Figure 91](#). This table appears only for Aruba AP radios.

**Figure 91** Active BSSIDs Table Illustration

### Active BSSIDs

BSSID ▲	SSID
00:1A:1E:86:C4:60	aruba-ap
00:1A:1E:86:C4:61	3600_wpa2_psk

## Monitoring Data for Mesh Devices

The monitoring page for mesh devices includes basic device information at the top, two tables for Radios and Wired Interfaces, a Users interactive graph and a Bandwidth interactive graph. Under these graphs are a list of associated Users, Mesh Links, RF Neighbors, and other common event logs and information.

**Figure 92** *APs/Devices > Monitor* page for a Mesh Device

Monitoring **Mesh-Portal-124-2b:3e** in group **Access Points** in folder **Top** [Poll Controller Now](#)

This Device is in monitor-only mode.

**Device Info**  
Status: Up (OK)  
Configuration: Error (Too many errors fetching existing configuration)  
Controller: [Srin651](#)  
Mesh Portal: [Mesh-Portal-124-2b:3e](#)  
Type: Aruba AP 124  
LAN MAC Address: 00:1A:1E:C0:2B:3E  
View in Google Earth:   
IP Address: 192.168.1.253  
Quick Links: [Open controller web UI...](#) [Run a command...](#)  
Notes:

Aruba AP Group: -  
Mesh Mode: Portal AP  
Remote Device: No  
Serial: AD0006035  
Upstream Device: -  
Mesh ID: -  
Last Contacted: 5/23/2011 6:44 PM  
Upstream Port: -  
Hop Count: 0  
Uptime: 4 days 7 hrs 51 mins  
Total Users: 0  
Bandwidth: -

**Radios**

Name	MAC Address	Users	BW (Kbps)	Channel	Tx Power	Mesh Links	Radio Role	Active SSIDs
802.11an	00:1A:1E:82:B3:F0	0	0.00	149	12 dBm	1	Mesh Portal	-
802.11bgn	00:1A:1E:82:B3:F0	0	0.00	6	15 dBm	-	-	-

**Wired Interfaces**

Name	MAC Address	Users	Admin Status	Operational Status	Type	Duplex	Aruba Port Mode	Input Capacity	Output Capacity
Enet0	00:1A:1E:C0:2B:3E	0	Up	Up	gigabitEthernet	Full	N/A	100 Mbps	100 Mbps
Enet1	00:1A:1E:C0:2B:3F	0	Up	Down	gigabitEthernet	Half	Active Standby	10 Mbps	10 Mbps

**Users on Mesh-Portal-124-2b:3e** Last 10 weeks  
  
[Show All](#)  

☒ Max Users (Radio 1) 0 users 0 users  
☒ Max Users (Radio 2) 0 users 0 users

**Bandwidth on Mesh-Portal-124-2b:3e** Last 10 weeks  
  
[Show All](#)  

☐ Avg In (Radio 1) 0 bps 0 bps  
☐ Avg In (Radio 2) 0 bps 0 bps  
☐ Avg Out (Radio 1) 0 bps 0 bps

1 year ago now

No users associated to this device.

**Mesh Links**

AP Name	Device Address	Link Time	Duration	Link Type
Mesh-Point-35:a6	00:24:6C:C8:35:A6	5/19/2011 11:52 AM	4 days 6 hrs 54 mins	Downlink

These fields are described in detail in “[Viewing Device Monitoring Statistics](#)” on page 117.

## Monitoring Data for Wired Devices (Routers and Switches)

The monitoring page for routers and switches includes basic device information at the top, a bandwidth graph depicting the sum of all the physical interfaces, and beneath that, CPU/memory usage graphs as shown in Figure 93.

**Figure 93** *APs/Devices > Monitor Page for an Aruba Mobility Access Switch*



All managed wired devices also include an **Interfaces** subtab, as shown in Figure 94.

**Figure 94** *APs/Devices > Interfaces* Page for Wired Devices (partial view).

[Home](#)
[Helpdesk](#)
[Groups](#)
[APs/Devices](#)
[Users](#)
[Reports](#)
[System](#)
[Device Setup](#)

[List](#)
[Monitor](#)
[Interfaces](#)
[Manage](#)
[Audit](#)
[Compliance](#)
[New](#)
[Up](#)
[Down](#)
[Mismatched](#)
[Ignored](#)

Interface Summary for **ArubaS3500** in group [aruba gui no wms](#) in folder [Top > aruba > corvina](#)

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution	Up	Down
ArubaS3500	27	16	11	26	15	11	1	1	0

### Physical Interfaces

[Edit Interfaces](#)

1-10 ▼ of 24 Interfaces Page 1 ▼ of 3 > | [Reset filters](#) [Choose columns](#) [Export CSV](#)

Interface	Mode	Name	Operational Status ▼	Type ▼
gigabitethernet0/0/1	Distribution	corvina uplink	Up	ethernetCsmacd
gigabitethernet0/0/20	Access	GE0/0/20	Down	ethernetCsmacd
gigabitethernet0/0/21	Access	GE0/0/21	Down	ethernetCsmacd
gigabitethernet0/0/22	Access	GE0/0/22	Down	ethernetCsmacd
gigabitethernet0/0/3	Access	Locally Authed Port	Up	ethernetCsmacd
gigabitethernet0/0/5	Access	Locally Authed Port	Up	ethernetCsmacd
gigabitethernet0/0/7	Access	Locally Authed Port	Up	ethernetCsmacd
gigabitethernet0/0/14	Access	GE0/0/14	Down	ethernetCsmacd
gigabitethernet0/0/0	Access	a3200-1.dev.airwave.com uplink	Up	ethernetCsmacd
gigabitethernet0/0/2	Access	Locally Authed Port	Up	ethernetCsmacd

1-10 ▼ of 24 Interfaces Page 1 ▼ of 3 > | [Reset filters](#)

### Virtual Interfaces

[Edit Interfaces](#)

1-3 ▼ of 3 Interfaces Page 1 ▼ of 1 [Reset filters](#) [Choose columns](#) [Export CSV](#)

Interface	Name	Type ▼	MAC Address	Admin Status ▼	Operational Status ▼
mgmt	MGMT	rfc877x25	00:08:86:6A:62:01	Up	Down
tunnel0	Tunnel Interface	tunnel	00:08:86:6A:62:00	Up	Up
vlan51	802.1Q VLAN	l3ipvlan	00:08:86:6A:62:00	Up	Up

1-3 ▼ of 3 Interfaces Page 1 ▼ of 1 [Reset filters](#)

### VLANs

Name ▲	VLAN	Tagged Ports	Untagged Ports
VLAN0001	1	-	-
VLAN0051	51	gigabitethernet0/0/0-7,14-23	gigabitethernet0/0/0-7,14-23
VLAN4089	4089	gigabitethernet0/0/13	gigabitethernet0/0/13
VLAN4090	4090	gigabitethernet0/0/12	gigabitethernet0/0/12
VLAN4091	4091	gigabitethernet0/0/11	gigabitethernet0/0/11
VLAN4092	4092	gigabitethernet0/0/10	gigabitethernet0/0/10
VLAN4093	4093	gigabitethernet0/0/9	gigabitethernet0/0/9
VLAN4094	4094	gigabitethernet0/0/8	gigabitethernet0/0/8

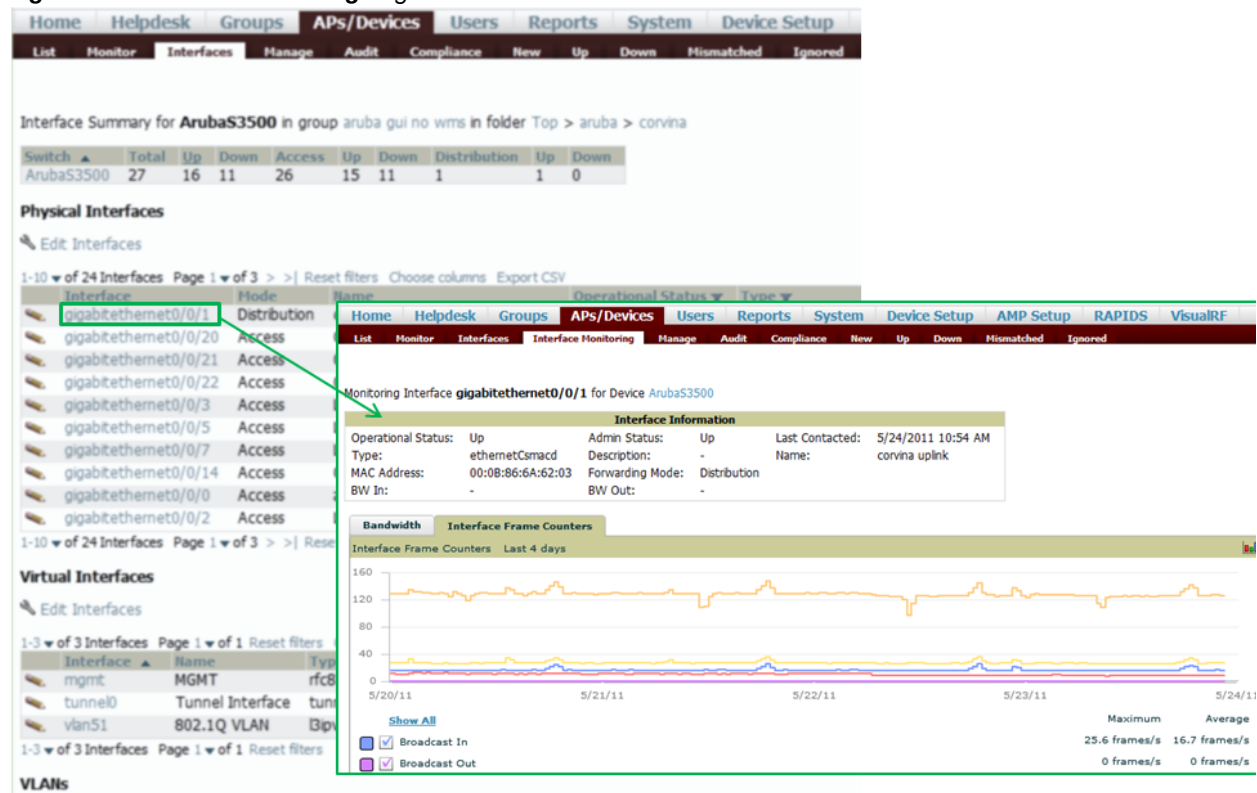
The **Interfaces** page includes a summary of all the interfaces at the top. In case of the stacked switches, the master includes the interfaces of all the members including its own. The physical and the virtual interfaces are displayed in separate tables, labeled **Physical Interfaces** and **Virtual Interfaces**. VLANs are listed below the interface.

AMP monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by selecting one of the two **Edit Interfaces** hyperlinks. Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers.

## Understanding the APs/Devices > Interfaces Page

“Monitoring Data for Wired Devices (Routers and Switches)” on page 130 showed you how to view high-level interface information for all physical and virtual interfaces on an entire router or switch. Select any interface hotlink in the **Interface** column of the Physical or Virtual Interfaces tables on the stacked switches to go to an **Interface Monitoring** page displaying data relevant to that specific interface, as shown Figure 95.

**Figure 95** *Interface Monitoring Page for a Wired Device*



An **Interface Monitoring** page is comprised of three sections: Interface Information, Usage and Interface Frame Counters graphs, and Connected Clients.

Specifics of the interface are in the Interface Information section, as depicted in Figure 96.

**Figure 96** *Individual Interface Information Section*

Interface Information					
Operational Status:	Down	Admin Status:	Up	Last Contacted:	1/26/2010 3:50 PM
Type:	ethernetCsmacd	Alias:	-	Description:	FastEthernet0/4
MAC Address:	00:18:18:8D:40:06				
BW In (kbps):	0	BW Out (kbps):	0		

Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower section in a tabbed graph, which are shown in Figure 95 above.

**Connected Clients**, if any, are listed in a table below the interactive graphs as shown in Figure 97.

**Figure 97** *Connected Clients list in APs/Devices > Interface Monitoring for a selected interface*

Connected Users							
1-1 of 1 Connected Users	Page 1 of 1	Reset filters	Choose columns	Export CSV			
Device Type	Role	MAC Address	VLAN	Interface	Connection Mode	Forward Mode	Tunneled Controller
Speed Dragon Multimedia Limited	logon	00:18:18:8D:40:06	51	gigabitethernet0/0/9	Wired	Tunnel Encrypted	Aruba3200
1-1 of 1 Connected Users	Page 1 of 1	Reset filters					

## What Next?

All device lists in AirWave act as portals to management pages if you have the proper read/write privileges. Selecting the wrench or pencil icon next to a device table entry, or selecting **Modify Devices** where appropriate above a device table, will take you to the appropriate Management page (**APs/Devices > Manage**). For more information, see “[Configuring and Managing Devices](#)” on page 134.

## Auditing Device Configuration

When you have added a newly discovered device successfully to a Group in **Monitor** mode, the next step is to verify device configuration status. Determine whether any changes will be applied to that device when you convert it to **Managed read/write** mode.

AMP uses SNMP or Telnet to read a device’s configuration. SNMP is used for Cisco controllers. Aruba devices and wired routers and switches use Telnet/SSH to read device configuration. See “[Individual Device Support and Firmware Upgrades](#)” on page 144 for more details.

Perform these steps to verify the device configuration status:

1. Browse to the **APs/Devices > List** page.
2. Locate the device in the list and check the information in the **Configuration** column.
3. If the device is in **Monitor** mode, the **lock** symbol appears in the **Configuration** column, indicating that the device is locked and will not be configured by AMP.
4. Verify the additional information in the **Configuration** column for that device.
  - A status of **Good** indicates that all of the device's current settings match the group policy settings, and that no changes will be applied when the device is shifted to **Manage** mode.
  - A status of **Mismatched** indicates that at least one of the device's current configuration settings do not match the group policy, and will be changed when the device is shifted to **Manage** mode.
5. If the device configuration is **Mismatched**, select the **Mismatched** link to go to the **APs/Devices > Audit** page. The **APs/Devices > Audit** page lists detailed information on all existing configuration parameters and settings for an individual device.

The group configuration settings are displayed on the right side of the page. If the device is moved from **Monitor** to **Manage** mode, the settings on the right side of the page overwrite the settings on the left.

[Figure 98](#) illustrates this page.

**Figure 98** *APs/Devices > Audit Page Illustration*

Device Configuration of **ArubaS3500** in group **aruba gui no wms** in folder **Top > aruba >**  
This Device is in monitor-only-with-firmware-upgrades mode.  
Configuration read from device at 5/24/2011 4:43 PM

Configuration: Good

**Audit** | Audit the device's current configuration.

[Show Archived Device Configuration](#)

[Show only mismatched settings](#)

[Refresh this page](#)

Device Settings	
Current Device Configuration	
Name	corvina-qa-1
Serial Number	AU0000180
Uptime	22 days 0 hrs 52 mins
System Properties	
Current Device Configuration	
Contact	Steve
Description	ArubaOS (MODEL: ArubaS3500-24T), Version 7.0.0.0 (28131)
Location	AW Server Room
ObjectID	.1.3.6.1.4.1.14823.1.1.25

6. Review the list of changes to be applied to the device to determine whether the changes are appropriate. If not, you need to change the Group settings or reassign the device to another Group.

## Using Device Folders (Optional)

The devices on the **APs/Devices List** pages include **List**, **Up**, **Down**, and **Mismatched** fields. These devices are arranged in groups called folders. Folders provide a logical organization of devices unrelated to the configuration groups of the devices. Using folders, you can quickly view basic statistics about devices. You *must* use folders if you want to limit the APs and devices AMP users can see.

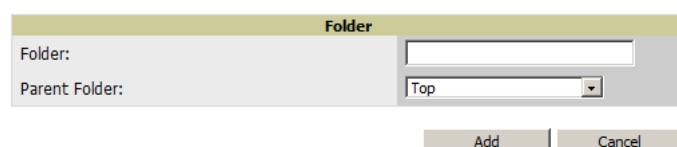
Folder views are persistent in AMP. If you select the **Top** folder and then select the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

If you want to see every **down** device, select the **Expand folders to show all devices** link. When the folders are expanded, you see all of the devices on AMP that satisfy the criteria of the page. You also see an additional column that lists the folder containing the AP.

Perform the following steps to add a device folder to AMP.

1. To add a folder, select the **Add New Folder** link at the bottom of **APs/Devices > List**, **> Up**, **> Down**, or **> Mismatched**. [Figure 99](#) illustrates the page.

**Figure 99** Folder Creation Page Illustration



2. Enter the name of the new folder.
3. Select the **Parent** folder.
4. Select **Add**.

Once a new folder has been created, devices can be moved into it using the **Modify Devices** link or when **New Devices** are added into AMP.

## Configuring and Managing Devices

This section contains the following topics describing individual device configuration within device groups:

- [Moving a Device from Monitor Only to Manage Read/Write Mode](#)
- [Configuring AP Settings](#)
- [Configuring Device Interfaces for Switches](#)
- [Individual Device Support and Firmware Upgrades](#)

While most device configuration settings can be efficiently managed by AMP at a Group level, certain settings must be managed at the individual device level. For example, because devices within a Group are often contiguous with one another, and have overlapping coverage areas, it makes sense to manage these devices individually to avoid RF interference.



---

Any changes made at an individual device level will automatically override Group level settings.

---

AMP automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **APs/Devices > Audit** page and identified by name. By default, configuration is tracked by the date and time it was created; device configurations are also archived by date.

It is not possible to push archived configurations to devices, but archived configurations can be compared to the current configuration, the desired configuration, or to other archived configurations using the drop-down menus on the **APs/Devices > Audit** page. This applies to startup or to running configuration files.



Compare two configurations to highlight the specific lines that are mismatched. The Audit page provides links to the AMP pages where any mismatched settings can be configured.



These procedures assume you are familiar with the function buttons available to save, apply, revert, and so on. For details on button functions, see [“Buttons and Icons” on page 26](#).

## Moving a Device from Monitor Only to Manage Read/Write Mode

Once the device configuration status is **Good** on the **APs/Devices > List** page, or once you have verified all changes that will be applied to the device on the **APs/Devices > Audit** page, you can safely shift the device from **Monitor Only** mode to **Manage Read/Write** mode.



Once a device is in Manage mode, AMP will push a new configuration to the device in the event that the actual device configuration does not match the AMP configuration for that device.

To move a device from **Monitor Only** to **Manage Read/Write** mode, perform the following steps.

1. Go to the **APs/Devices > List** page and select the **wrench** icon next to the name of the AP to be shifted from **Monitor Only** mode to **Manage Read/Write** mode. This directs you to the **APs/Devices > Manage** page.
2. Locate the **General** area as shown in [Figure 100](#).

**Figure 100** *APs/Devices > Manage > General Section Illustration*

General	
Name:	Cisco4400
Status:	Up (OK)
Configuration:	Mismatched ( <a href="#">More Details</a> )
Last Contacted:	10/19/2011 2:54 PM
Type:	Cisco 4400 WLC
Firmware:	4.2.209.0 (Bootloader: 4.0.217.0)
Group:	<a href="#">Access Points</a>
Folder:	<a href="#">Top</a>
Management Mode:	<input checked="" type="radio"/> Monitor Only + Firmware Upgrades <input type="radio"/> Manage Read/Write
Enable Planned Maintenance Mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No

3. Select **Manage Read/Write** on the **Management Mode** field.
4. Select **Save and Apply**, then **Confirm Edit** on the confirmation page to retain these settings and to push configuration to the device.
5. For device configuration changes that require the device to reboot, use the **Schedule** function to push the changes at a time when WLAN users will not be affected.
6. To move multiple devices into managed mode at once, use the **Modify Devices** link on an AP list page. For more information, refer to [“Modifying Multiple Devices” on page 103](#).



Use the **Enable Planned Maintenance Mode** field in **APs/Devices > Manage > General** to put this device into planned maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page.

## Configuring AP Settings

1. Browse to the **APs/Devices > List** page and select the wrench icon next to the device whose AP settings you want to edit. This directs you to the **Manage** page for that device. [Figure 101](#) illustrates this page.

**Figure 101** *APs/Devices > Manage Page Illustration*

General	
Name:	ap125-meshportal-karen
Status:	Up (OK)
Configuration:	Good
Last Contacted:	2/12/2010 10:29 AM
Type:	AP 125
Controller:	<a href="#">sphere-lms</a>
Group:	<a href="#">sphere-lms</a>
Folder:	<a href="#">Top &gt; HQ</a>
Management Mode:	<input type="radio"/> Monitor Only + Firmware Upgrades <input checked="" type="radio"/> Manage Read/Write

Settings	
Name:	ap125-meshportal-karen
Domain Name:	
Location:	
Contact:	
Latitude:	10.02450899096407
Longitude:	0.7395866645358211
Altitude (m):	0
Group:	sphere-lms3
Folder:	HQ
Auto Detect Upstream Device:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upstream device will automatically be updated when the device is poled.	
Automatically clear Down Status Message when device comes back up:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Down Status Message:	
Aruba AP Group:	default
Installation:	Default
Mesh Mode:	Portal AP

Authentication Method	
PPPoE Authentication:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote AP:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Master Discovery	
Master Discovery Type:	Host Controller (IP)
Host Controller IP Address:	16.2.250
Master Controller IP Address/DNS Name:	16.2.250

Link Priority Settings	
Link Priority Ethernet (0-255):	
Link Priority Cellular (0-255):	

USB Settings	
USB User Name:	
USB Password:	
Confirm USB Password:	
USB Device Type:	any
USB Device Identifier:	
USB Dial String:	
USB Initialization String:	
USB TTY Device Path:	

Network Settings	
Use DHCP:	<input type="radio"/> Yes <input checked="" type="radio"/> No
LAN IP Address:	
Subnet Mask:	
Gateway:	
DNS IP Address:	

Save and Apply  
Ignore

Revert  
Import Settings

Delete  
Replace Hardware

If any changes are scheduled for this AP, they appear in a **Scheduled Changes** section at the top of the page above the other fields. The linked name of the job takes you to its **System > Configuration Change Job Detail** page.

2. Locate the **General** section for information about the AP's current status. [Table 82](#) describes the fields, information, and settings.

**Table 82** *APs/Devices > Manage > General Fields and Descriptions*

Field	Description
<b>Name</b>	Displays the name currently set on the device.
<b>Status</b>	Displays the current status of an AP. If an AP is <b>Up</b> , then AMP is able to ping it and fetch SNMP information from the AP. If the AP is listed <b>Down</b> then AMP is either unable to ping the AP or unable to read the necessary SNMP information from the device.
<b>Configuration</b>	Displays the current configuration status of the AP. To update the status, select <b>Audit</b> on the <b>APs/Devices &gt; Audit</b> page.
<b>Last Contacted</b>	Displays the last time AMP successfully contacted the AP.
<b>Type</b>	Displays the type of AP.
<b>Firmware</b>	Displays the version of firmware running on the AP.
<b>Group</b>	Links to the <b>Group &gt; Monitoring</b> page for the AP.
<b>Template</b>	Displays the name of the group template currently configuring the AP. Also displays a link to the <b>Groups &gt; Template</b> page. This is only visible for APs that are managed by templates.
<b>Folder</b>	Displays the name of the folder containing the AP. Also displays a link to the <b>APs/Devices &gt; List</b> page for the folder.
<b>Management Mode</b>	Displays the current management mode of the AP. No changes are made to the AP when it is in <b>Monitor Only</b> mode. AMP pushes configurations and makes changes to an AP when it is in <b>Manage Read/Write</b> mode.
<b>Enable Planned Maintenance Mode</b>	Put this device into planned maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the <b>Modify Devices</b> link on an AP list page.
<b>Notes</b>	Provides a free-form text field to describe device information.

3. Review and provide the following information in the **Settings** area. Devices with dual radios display radio-specific settings in the Slot A and Slot B area. If a device is dual-radio capable but only has one device installed, AMP manages that device as if it were a single slot device.



Devices from different vendors have different RF settings and capabilities. The fields in the **Settings** section of the **APs/Devices > Manage** page are context-sensitive and only present the information relevant for the particular device vendor and model.

[Table 83](#) describes field settings, default values, and information for the **Settings** section of this page.

**Table 83** *APs/Devices > Manage > Settings Fields and Default Values*

Setting	Default	Device Type	Description
<b>Name</b>	None	All	User-configurable name for the device (max. 20 characters)
<b>Domain Name</b>	None	IOS	Field populated upon initial device discovery or upon refreshing settings. Enable this option from <b>AMP Setup &gt; Network</b> page to display this field on the <b>APs/Devices &gt; Manage</b> page, with fully-qualified domain names for IOS APs. This field is used in conjunction with <b>Domain</b> variable in IOS templates.
<b>Location</b>	Read from the device	All	The SNMP location set on the device.

**Table 83** *APs/Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
<b>Latitude</b>	None	All	Text field for entering the latitude of the device. The latitude is used with the Google Earth integration.
<b>Longitude</b>	None	All	Text field for entering the longitude of the device. The longitude is used with the Google Earth integration.
<b>Altitude</b> (meters)	None	All	Text field for entering the altitude of the device when known. This setting is used with the Google Earth integration. Specify altitude in meters.
<b>Group</b>	Default Group	All	Drop-down menu that can be used to assign the device to another Group.
<b>Folder</b>	Top	All	Drop-down menu that can be used to assign the device to another Group.
<b>Auto Detect Upstream Device</b>	Yes	All	Selecting <b>Yes</b> enables automatic detection of upstream device, which is automatically updated when the device is polled. Selecting <b>No</b> displays a drop-down menu of upstream devices.
<b>Down Status Message</b>	None	All	Enter a text message that provides information to be conveyed if the device goes down.
<b>Automatically clear Down Status Message when device comes back up</b>	None	All	Whether the message entered in the <b>Down Status Message</b> field should be removed after the device returns to the Up status.
<b>Administrative Status</b>	Enable	All	Enables or disables administrative mode for the device.
<b>Mode</b>	Local	All	Designates the mode in which the device should operate. Options include the following: <ul style="list-style-type: none"> <li>• Local</li> <li>• H-REAP</li> <li>• Monitor</li> <li>• Rogue Detector</li> <li>• Sniffer</li> </ul>

4. Complete additional settings on the **APs/Devices > Manage** page, to include H-REAP, certificates, radio settings, and network settings. [Table 84](#) describes many of the possible fields.



For complete listing and discussion of settings applicable only to Aruba devices, see the *Aruba Configuration Guide*.

**Table 84** *APs/Devices > Manage, Additional Settings*

Setting	Default	Device Type	Description
<b>Mesh Role</b>	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP as shown: <ul style="list-style-type: none"> <li>• <b>Mesh AP</b> — The AP will act like a mesh client. It will use other APs as its uplink to the network.</li> <li>• <b>Portal AP</b> — The AP will become a portal AP. It will use a wired connection as its uplink to the network and serve it over the radio to other APs.</li> <li>• <b>None</b> — The AP will act like a standard AP. It will not perform meshing functions</li> </ul>

**Table 84 APs/Devices > Manage, Additional Settings (Continued)**

Setting	Default	Device Type	Description
<b>Mesh Mobility</b>	Static	Mesh Devices	Select <b>Static</b> if the AP is static, as in the case of a device mounted on a light pole or in the ceiling. Select <b>Roaming</b> if the AP is mobile. Two examples would be an AP mounted in a police car or utility truck.
<b>Receive Antenna</b>	Diversity	Cisco	Drop-down menu for the receive antenna provides three options: <b>Diversity</b> — Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the <b>Diversity</b> setting should be used for both receive and transmit antennas. <b>Right</b> — If your device has removable antennas and you install a high-gain antenna on the device's right connector (the connector on the right side when viewing the back panel of the device), use this setting for receive and transmit. <b>Left</b> — If your device has removable antennas and you install a high-gain antenna on the device's left connector, use this setting for both receive and transmit.
<b>Transmit Antenna</b>	Diversity	Cisco	See description in <b>Receive Antenna</b> above.
<b>Antenna Diversity</b>	Primary Only	Symbol 4131	Drop-down menu provides the following options: <b>Full Diversity</b> — The AP receives information on the antenna with the best signal strength and quality. The AP transmits on the antenna from which it last received information. <b>Primary Only</b> — The AP transmits and receives on the primary antenna only. Secondary Only: The AP transmits and receives on the secondary antenna only. <b>Rx Diversity</b> — The AP receives information on the antenna with the best signal strength and quality. The AP transmits information on the primary antenna only.
<b>Transmit Power Reduction</b>	0	Proxim	Transmit Power Reduction determines the APs transmit power. The max transmit power is reduced by the number of decibels specified.
<b>Channel</b>	6	All	Represents the AP's current RF channel setting. The number relates to the center frequency output by the AP's RF synthesizer. Contiguous APs should be set to different channels to minimize "crosstalk," which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance. 802.11b's 2.4-GHz range has a total bandwidth of 80-MHz, separated into 11 center channels. Of these channels, only 3 are non-overlapping (1, 6, and 11). In the United States, most organizations use only these non-overlapping channels.
<b>Transmit Power Level</b>	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage radius of the access point by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the AP will interfere with neighboring APs. Supported values are: <b>Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW)</b>

**Table 84 APs/Devices > Manage, Additional Settings (Continued)**

Setting	Default	Device Type	Description
<b>Radio Enabled</b>	Yes	All	The Radio Enabled option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. AMP will still monitor the Ethernet page and ensure the AP stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at an AP-Level or Group-Level. <b>NOTE:</b> You cannot disable radios unless rogue scanning is disabled in <b>Groups &gt; Radio</b> .
<b>Use DHCP</b>	Yes	All	If enabled, the AP will be assigned a new IP address using DHCP. If disabled, the AP will use a static IP address. For improved security and manageability, disable DHCP and using static IP addresses.
<b>LAN IP</b>	None	All	The IP Address of the AP Ethernet interface. If One-to-One NAT is enabled, AMP will communicate with the AP on a different address (the IP Address defined in the <b>Device Communication</b> section). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
<b>Subnet Mask</b>	None	All	Provides the IP subnet mask to identify the sub-network so the IP address can be recognized on the LAN. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
<b>Gateway</b>	None	All	The IP address of the default internet gateway. If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.

5. Locate the **Template Options** area on the **APs/Devices > Manage** page.



This section only appears for IOS APs, Symbol and Aruba controllers in groups with Aruba GUI Config disabled.

Table 85 describes field settings, default values, and additional information for this page.

**Table 85 APs/Devices > Manage > Template Options Fields and Default Values**

Setting	Default	Device Type	Description
<b>WDS Role</b>	Client	Cisco IOS Wireless LAN Controllers only	Set the WDS role for this AP. Select Master for the WDS master APs and Client for the WDS Client. Once this is done you can use the %if wds_role= % to push the client, master, or backup lines to appropriate WDS APs.
<b>SSL Certificate</b>	None	Cisco IOS	AMP will read the SSL Certificate off of the AP when it comes UP in AMP. The information in this field will defines what will be used in place of %certificate%.
<b>Extra Device Commands</b>	None	Cisco IOS	Defines the lines that will replace the %ap_include_1% variable in the IOS template. This field allows for unique commands to be run on individual APs. If you have any settings that are unique per AP like a MOTD you can set them here.
<b>switch_command</b>	None	Cisco Catalyst switches	Defines lines included for each of the members in the stack. This field appears only on the master's <b>Manage</b> page. The information in this field will determine what is used in place of the %switch_command% variable.

6. For Cisco WLC devices, go to the interfaces section of the **APs/Devices > Manage** page. Select **Add new Interface** to add another controller interface, or select the **pencil** icon to edit an existing

controller interface. [Table 86](#) describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by AMP, refer to the Cisco WLC product documentation.

**Table 86** *APs/Devices > Manage > Interface Fields and Descriptions for Cisco WLC Devices*

Field	Default	Description
<b>Name</b>	None	The name of the interface on the controller.
<b>VLAN ID</b>	None	The VLAN ID for the interface on the controller.
<b>Port</b>	None	The port on the controller to access the interface.
<b>IP Address</b>	None	The IP address of the controller.
<b>Subnet Mask</b>	None	The subnet mask for the controller.
<b>Gateway</b>	None	The controller's gateway.
<b>Primary and Secondary DHCP Servers</b>	None	The DHCP servers for the controller.
<b>Guest LAN</b>	Disabled	Indicates a guest LAN.
<b>Quarantine VLAN ID</b>	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.
<b>Dynamic Device Management</b>	Enabled	When enabled, makes the interface an AP-manager interface. Cisco calls this feature Dynamic AP Management.

## Setting a Maintenance Window for a Device

AirWave can automate the manual action of putting multiple devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode.

Maintenance windows can be set as a one-time or recurring event on the **APs/Devices > Manage** and **Groups > Basic** page. You can also use the **Modify Devices** link to add or delete maintenance windows to multiple selected devices at once. Additionally, this feature can be used on Master Console to set maintenance windows for multiple AMPs.

To set a maintenance window for a single device in **APs/Devices > Manage**, follow these steps:

1. Navigate to the **APs/Devices > Manage** page for a device.
2. At the bottom of the page, locate the Maintenance Windows section.
3. Select **Add New AP Maintenance Window**.

**Figure 102** *Add New Maintenance Window in APs/Devices > Manage page*

Maintenance Windows		
Name	Duration	Scheduled
Yearly maintenance	15 minutes	Every January 10th at 12:30 am

4. Enter a name for the maintenance window.
5. In the **Occurs** field, specify whether the maintenance window should occur one time, or daily, weekly, monthly, or annually.
6. Set the desired start time and the duration (in minutes) of the maintenance window.
7. Select **Add**.



## Configuring Device Interfaces for Switches

When you go to the **APs/Devices > Interfaces** page for a switch, you can add a Virtual interface by selecting **Add** and entering the appropriate information in the page that then appears, as shown in [Figure 103](#).

**Figure 103 Add Virtual Interfaces Page for Wired Devices**

New physical and virtual interfaces are discovered using SNMP polling as described in [“SNMP/HTTP Scanning” on page 108](#). To refresh and reload all current interface information from a device, select **Import Interfaces** on the bottom of the page as shown in [Figure 104](#).

**Figure 104 Import Interfaces for Refresh and Reload (lower portion of page)**

	Interface	Name	Type ▲	Interface Type	Description	Interface Labels	Shutd
	Nu0	Null0	other	-	Null0	Nu0	-
<input type="checkbox"/>	VI50	Vlan50	propVirtual	Catalyst VLAN	-	VI50	No
<input type="checkbox"/>	VI51	Vlan51	propVirtual	Catalyst VLAN	-	VI51	No
<input type="checkbox"/>	VI59	Vlan59	propVirtual	Catalyst VLAN	-	VI59	No
<input type="checkbox"/>	VI50	Vlan50	propVirtual	Catalyst VLAN	Vlan50	VI50	No
<input type="checkbox"/>	VI1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	VI1	No
<input type="checkbox"/>	VI59	Vlan59	propVirtual	Catalyst VLAN	Vlan59	VI59	No
<input type="checkbox"/>	VI51	Vlan51	propVirtual	Catalyst VLAN	Vlan51	VI51	No
<input type="checkbox"/>	VI1	Vlan1	propVirtual	Catalyst VLAN	-	VI1	No

1-9 ▼ of 9 Interfaces Page 1 ▼ of 1

Select All - Unselect All

Delete

Import Interfaces

You can view details for each interface on a wired device from its individual interface page as well. For details, see [“Understanding the APs/Devices > Interfaces Page” on page 132](#).

You can configure interface settings individually or in groups. For individual settings, select the pencil icon next the interface name in **AP/Devices > Interfaces**.

This takes you to the **Interfaces Monitoring and Configuration** window which has a slightly different appearance depending on whether you are configuring a physical or virtual interface, as shown in [Figure 105](#) and [Figure 106](#).

**Figure 105 Physical Interfaces Monitoring and Configuration Sections**

### Interface Monitoring

Auto Detect Interface Capacity: ☒ Yes ☐ No

Interface capacities will automatically be updated when the device is polled.

Combined Bandwidth: ☐ Yes ☒ No

Interface Labels:

Mode:

### Interface Configuration

Description:

Shutdown: ☐ Yes ☒ No

Interface Type: FastEthernet IEEE 802.3

Switchport Access VLAN:

Switchport Mode:

Switchport Trunk Native VLAN:

Switchport Trunk Allowed VLANs:

Switchport Trunk Pruning VLANs:

Switchport Trunk Encapsulation:

Speed:

Additional Commands:

ip dhcp snooping trust

Save

Cancel

**Figure 106 Virtual Individual Interfaces Configuration Section**

### Interface Configuration

Description:

Interface Type: Catalyst VLAN

Save

Cancel


To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 107.

**Figure 107 Edit Multiple Interfaces**




Interface Summary for **ArubaS3500** in group **aruba gui no wms** in folder **Top > aruba > corvina**

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution	Up	Down
ArubaS3500	27	16	11	26	15	11	1	1	0

#### Physical Interfaces


 [Edit Interfaces](#)

1-3 ▼ of 24 Interfaces Page 1 ▼ of 8 > > | [Reset filters](#) [Choose columns](#) [Export CSV](#)




Interface ▲	Mode	Name	Operational Status ▼	Type ▼
 gigabitethernet0/0/1	Distribution	corvina uplink	Up	ethernetCs
 gigabitethernet0/0/20	Access	GE0/0/20	Down	ethernetCs
 gigabitethernet0/0/21	Access	GE0/0/21	Down	ethernetCs

1-3 ▼ of 24 Interfaces Page 1 ▼ of 8 > > | [Reset filters](#)

#### Virtual Interfaces

 [Edit Interfaces](#)

1-3 ▼ of 3 Interfaces Page 1 ▼ of 1 [Reset filters](#) [Choose columns](#) [Export CSV](#)

Interface ▲	Name	Type ▼	MAC Address	Admin Status ▼	0
 mgmt	MGMT	rfc877x25	00:0B:86:6A:62:01	Up	D
 tunnel0	Tunnel Interface	tunnel	00:0B:86:6A:62:00	Up	U
 vlan51	802.1Q VLAN	l3ipvlan	00:0B:86:6A:62:00	Up	U

1-3 ▼ of 3 Interfaces Page 1 ▼ of 1 [Reset filters](#)

#### VLANs

You will remain on the same page, but will have the option to make changes to the most commonly edited settings in batch mode, as shown in [Figure 108](#).

**Figure 108** Multiple Interface Editing Page Illustration

	Interface	Name	Type	Interface Type	Description	Interface Labels	Shutdown	IP Address
<input type="checkbox"/>	Vl50	Vlan50	propVirtual	Catalyst VLAN		Vl50	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Vl51	Vlan51	propVirtual	Catalyst VLAN		Vl51	<input type="radio"/> Yes <input checked="" type="radio"/> No	10.51.0.26
<input type="checkbox"/>	Vl59	Vlan59	propVirtual	Catalyst VLAN		Vl59	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Vl50	Vlan50	propVirtual	Catalyst VLAN	Vlan50	Vl50	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Vl1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	Vl1	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Vl59	Vlan59	propVirtual	Catalyst VLAN	Vlan59	Vl59	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Nu0	Null0	other	-	Null0	Nu0	<input type="radio"/> Yes <input type="radio"/> No	-
<input type="checkbox"/>	Vl51	Vlan51	propVirtual	Catalyst VLAN	Vlan51	Vl51	<input type="radio"/> Yes <input checked="" type="radio"/> No	-
<input type="checkbox"/>	Vl1	Vlan1	propVirtual	Catalyst VLAN		Vl1	<input type="radio"/> Yes <input checked="" type="radio"/> No	-

1-9 of 9 Interfaces Page 1 of 1

Select All - Unselect All

AMP assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on templates, see [Chapter 6, “Creating and Using Templates”](#) on page 151.

## Individual Device Support and Firmware Upgrades

Perform the following steps to configure AP communication settings for individual Aruba device types.

1. Locate the **Device Communication** area on the **APs/Devices > Manage** page.
2. Specify the credentials to be used to manage the AP. [Figure 109](#) illustrates this page.

**Figure 109** APs/Devices > Manage > Device Communication

Device Communication

View Device Credentials

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:

SNMP Port:

If this device is down because the credentials on the device have changed, update the fields below with the correct information.

This device is currently using SNMP version 1

Community String:

Confirm Community String:

Auth Password:

Confirm Auth Password:

Privacy Password:

Confirm Privacy Password:



NOTE

The **Device Communication** area may appear slightly different depending on the particular vendor and model of the APs being used.

3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View AP Credentials** link in AMP by the root user. Contact AirWave support for detailed instructions to disable the link.
5. (Optional.) Enter the appropriate SSH and Telnet credentials if you are configuring Dell, Aruba Networks, Alcatel-Lucent or any Cisco device except Cisco WLAN controllers.
6. Select **Apply**, then **Confirm Edit** to apply the changes to the AP immediately, **Schedule** to schedule the changes during a specific time, or **Cancel** to return to **APs/Devices > Manage**.



NOTE

Some AP configuration changes may require the AP to be rebooted. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.

Select the **Update Firmware** button at the bottom right of the page to upgrade the device's firmware.

Figure 110 illustrates the page that opens and Table 87 describes the settings and default values.



The **Update Firmware** button only appears if 1) the AMP Administrator has enabled **Allow firmware upgrades in monitor-only mode** in **AMP Setup > General**, 2) if you are looking at an **APs/Devices > Manage** page for a controller or autonomous AP that supports firmware upgrades in AMP. See the “Supported Wireless Firmware Versions” document (the AMP Firmware Matrix) in **Home > Documentation** to see all of the AMP-supported devices that can perform firmware upgrades. In most cases, you cannot upgrade firmware directly on thin APs.

**Table 87** *APs/Devices > Manage > Firmware Upgrade Fields and Default Values*

Setting	Default	Description
<b>Desired Version</b>	None	Specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the <b>Device Setup &gt; Upload Firmware &amp; Files</b> page.
<b>Job Name</b>	None	Sets a user-defined name for the upgrade job. Use a meaningful and descriptive name.
<b>Use “/safe” flag for Cisco IOS firmware upgrade command</b>	No	Enables or disables the /safe flag when upgrading IOS APs. The /safe flag must be disabled on older APs for the firmware file to fit in flash memory.
<b>Email Recipients</b>	None	Displays a list of email addresses that should receive alert emails if a firmware upgrade fails.
<b>Sender Address</b>	None	Displays the <b>From</b> address in the alert email.

**Figure 110** *APs/Devices > Manage Firmware Upgrades*

**Desired Version**

Choose the desired firmware version to be applied to **Cisco-19:5F:2B** (10.51.3.128). Upload firmware files on the Device Setup [Upload Firmware & Files](#) page.

Current Version:

12.4(21a)JA1

Desired Version:

-- Select firmware version

**Firmware Upgrade Job Options**

Job name:

Firmware upgrade for Cisco-19

Use “/safe” flag for Cisco IOS firmware upgrade command:

☒ Yes
☐ No

Serve firmware files from this interface:

10.2.32.10

**Failure Notification Options**

To be notified when upgrades fail and when a job is stopped, enter email addresses of the form user@domain. Separate multiple addresses by spaces, commas, or semicolons.

Email Recipients:

user@example.com

Sender Address:

me@networks.com

Initiating a firmware upgrade will change the **Firmware Status** column for the device to Pending in **APs/Devices > List**. You can review the status of all recent firmware upgrade jobs in **System > Firmware Upgrade Jobs**.

## Troubleshooting a Newly Discovered Down Device

If the device status on the **APs/Devices > List** page remains **Down** after it has been added to a group, the most likely source of the problem is an error in the SNMP community string being used to manage the device. Perform the following steps to troubleshoot this scenario.

1. Select the **Name** of the down device in the list of devices on the **APs/Devices > List** or **APs/Devices > Down** page. This automatically directs you to the **APs/Device > Monitor** page for that device.
2. Locate the **Status** field in the **Device Info** section. If the Status is **Down**, it includes a description of the cause of the problem. Some of the common system messages are as follows in [Table 88](#):

**Table 88** Common System Messages for Down Status

Message	Meaning
<b>AP is no longer associated with controller</b>	This means the AP no longer shows up in any controller's AP list (on the AirWave server). Either the AP was removed from the controller, or it has roamed to another controller that AirWave does not have visibility to, or it is offline.
<b>Controller is Down</b>	When a controller goes down, AMP automatically marks all associated thin APs down (because communication to thin APs are via the controller and AirWave assumes that if the Controller has gone offline then all associated APs are down as well until reassociated another Controller).
<b>Downloading</b>	The AP is in the process of downloading firmware or configuration (only applies to Cisco WLC thin APs and some Symbol APs).
<b>Error fetching existing configuration</b>	AMP could not fetch a config for the AP. Usually this is because the AMP has incorrect credentials and was not able to log in.
<b>ICMP Ping Failed (after SNMP Get Failed)</b>	The device is not responding and is likely offline.
<b>SNMP Get Failed</b>	SNMP credentials and/or configuration may be incorrect. Verify that SNMP is enabled and that credentials and access ports are configured correctly on both the target device and in AirWave.
<b>SNMP Trap</b>	AMP received an SNMP trap from the controller indicating that the AP is no longer associated to the controller.
<b>Telnet Error: command timed out</b>	Telnet/SSH username and password specified for that device is incorrect.
<b>Unexpected LAN MAC Address found at this device's IP address</b>	<p>If AMP detects that the LAN MAC address of a device has changed this error message will appear. This usually indicates that a physical hardware change has occurred (while reusing the same IP Address) without using the <b>Replace Hardware</b> feature in AirWave. This error may also indicate an IP address conflict between two or more devices.</p> <p>When an unexpected LAN MAC address is seen in a device's IP address, its <b>APs/Devices &gt; Manage</b> page displays the message "Click <b>Replace Hardware</b> (preferred) or <b>Reset MAC Address</b> to reset the LAN MAC address if this device has been replaced with new hardware" at the top of the page. Use the <b>Replace Hardware</b> button at the bottom of that page in order to avoid this message.</p>

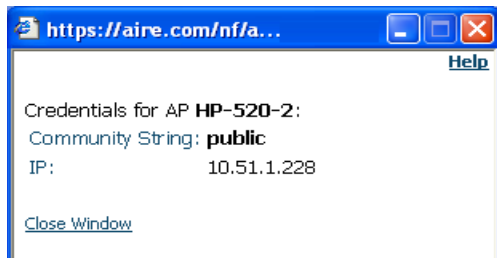


To view the detailed status of all your down devices at once, navigate to **APs/Devices > Down** (try the **Down** top header stats link) and look at the **Detailed Status** column for the list of down devices. This column can be sorted using the **Filter** icon

3. If the **SNMP Get Failed** message appears, select the **APs/Devices > Manage** tab to go to the management page for that device.
4. If visible, select the **View Device Credentials** link in the **Device Communications** section of **APs/Devices > Manage**. This displays the credentials AMP is using unsuccessfully to communicate with the device. This link can be removed from AMP for security reasons by setting a flag in AMP. Only users

with root access to the AMP command line can show or hide this link. To disable this feature, please contact AirWave support. [Figure 111](#) illustrates this page.

**Figure 111 View Device Credentials Window**



The **View Device Credentials** message may appear slightly different depending on the vendor and model.

5. If the credentials are incorrect, return to the **Device Communications** area on the **APs/Devices > Manage** page. Enter the appropriate credentials, and select **Apply**.
6. Return to the **APs/Devices > List** page to see if the device appears with a Status of **Up**.

## Setting up Aruba Spectrum Analysis in AMP

The spectrum analysis software modules on Aruba AP models AP-105, RAP-5WN, the AP-12x series, the AP-13x series and the AP-9x series can examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

The spectrum analyzer is used in conjunction with Aruba's Adaptive Radio Management (ARM) technology. While the spectrum analyzer identifies and classifies Wi-Fi and non-Wi-Fi sources of interference, ARM automatically ensures that APs serving clients will stay clear of interference.

Individual APs or groups of APs can be converted to dedicated spectrum monitors through the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile.

Each 802.11a and 802.11g radio profile references a spectrum profile, which identifies the spectrum band the radio will monitor and analyze, and defines the default ageout times for each monitored device type. By default, an 802.11a radio profile references a spectrum profile named **default-a** (which configures the radio to monitor the upper channels of the 5 GHz radio band), and an 802.11g radio profile references a spectrum profile named **default-g** (which configures the radio to monitor all channels the 2.4 GHz radio band).

Most interference will occur in the 2.4 GHz radio band.

For more information about Spectrum analysis and ARM technology, refer to the *ArubaOS 6.0 User Guide*.

## Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in spectrum mode in AMP:

- The AP must be in **Manage Read/Write** mode.
- The AP's associated controller must have an RFprotect license, and must run ArubaOS 6.0 or later.
- Aruba GUI Config must be enabled for that AP's group in the **Groups > Basic** page.

There are three main situations in which you would set one or more devices to Spectrum mode in AMP:

- Aruba AP Groups running permanently with the default Spectrum profile
- Individual APs running temporarily in Spectrum mode while part of an Aruba AP Group set to ap-mode

- Controller-level Spectrum Overrides (an alternative to creating new Aruba AP groups or new radio profiles for temporary changes)

## Setting up a Permanent Spectrum Aruba AP Group

If you have multiple supported Aruba APs in multiple controllers that you want to run in Spectrum mode over the long run, you create a special Aruba AP group and set up a profile that is set to **spectrum-mode** and references the default **Spectrum** profile. Set up more than one profile if you want to utilize both radio bands in Spectrum mode.

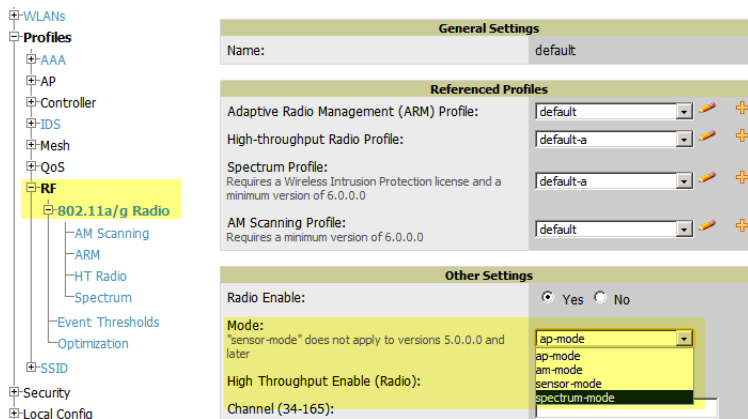
If you use an 802.11a or 802.11g radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile will be set to spectrum mode. Therefore, best practices are to create a new 802.11a or 802.11g radio profile just for spectrum monitors.

If you have Global Aruba Configuration enabled in **AMP Setup > General**, create the configuration below, then go to the controller's group's **Aruba Config** page and select the newly created Aruba AP Group.

Perform these steps to set the AP group to use the default Spectrum profile settings:

1. In **Groups > Aruba Config**, select **Add New Aruba AP Group**.
2. Give the new Group a name (like "Spectrum APs") and select the plus sign next to the **802.11a Radio Profile** to create a new radio profile.
3. Enter a name under the General Settings section of **Profiles > RF > 802.11a/g Radio**.
4. In the **Other Settings** section, change the **Mode** field from ap-mode to **spectrum-mode**, as illustrated in Figure 112. Then select **Save**.

**Figure 112** Spectrum mode in Aruba Configuration



The above steps will use the defaults in the referenced **Spectrum Profile**. To change the defaults, navigate to **Groups > Aruba Config > Profiles > RF > 802.11a/g Radio > Spectrum** and create a new Spectrum profile with non-default settings. In most cases, you should not change the settings in the default profile.

If all of the devices in this Aruba AP Group are managed by the same controller and you want to temporarily override one or more profile settings in your spectrum-mode APs, you can set up a controller override.

To disable spectrum mode in this group, change the referenced radio profile back to **default**.

## Configuring an Individual AP to run in Spectrum Mode

If you want to temporarily set an individual radio in an AP to run in Spectrum mode without creating or changing Aruba AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Aruba AP:

1. Go to the **APs/Devices > Manage** page for a Spectrum-supported Aruba AP (-105, -120, -130, -90).
2. After checking the Audit page, set the AP to **Manage Read/Write** mode.



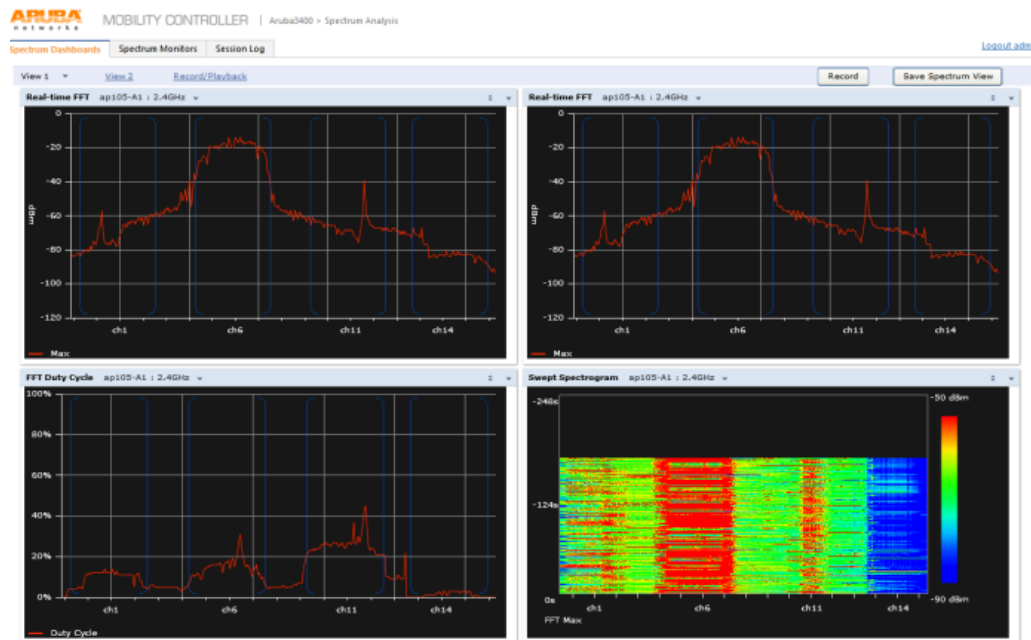
3. Select **Yes** on the **Spectrum Override** field for one or both radios, depending on the band and channels you want it to analyze.
4. Select the band that should run in spectrum. If you selected the 5GHz band in the 802.11an Radio section, choose the lower, middle, or upper range of channels that you want to be analyzed by this radio.
5. Select **Save and Apply** and confirm your edit.

This overrides the current **Mode** setting for that AP (ap-mode or am-mode).

After making this change, you can view the **Radio Role** field that will appear in the **Radios** section of the **APs/Devices > Monitor** page.

The new role, **Spectrum Sensor**, is a link to the Spectrum Analysis page for the controller that manages this AP, as illustrated in [Figure 113](#).

**Figure 113** Spectrum Analysis on Controller Dashboard



This chart is only available for AP models AP-105, AP-90, and the AP-130 Series.

To disable Spectrum mode on this individual AP after it has collected data, return to the **APs/Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

## Configuring a Controller to use the Spectrum Profile

You can use AMP to customize individual fields in the profile instance used by a particular controller without having to create new Aruba AP groups and new radio profiles. To do this, you can set a controller-level override for its referenced Spectrum profile, as illustrated in [Figure 114](#). This will affect all Spectrum-supported APs managed by this controller.

**Figure 114** *Override Section of a Supported Controller's Manage Page*

**Aruba Overrides**

New Aruba Controller Override

1-1 ▼ of 1 Aruba Controller Overrides Page 1 ▼ of 1 [Choose Columns](#)

	Profile	Instance	Field	Value
<input type="checkbox"/>	Spectrum Profile	default-a	Bluetooth	12

1-1 ▼ of 1 Aruba Controller Overrides Page 1 ▼ of 1

[Select All](#) - [Unselect All](#)

Perform these steps to override individual profile settings for an Aruba controller that is part of a spectrum-mode Aruba AP group:

1. Select a Spectrum-supported Aruba controller that is referencing a Spectrum profile, and go to its **APs/ Devices > Manage** page. Set it to **Manage Read/Write** mode.
2. Under the **Aruba Overrides** section, select **Add New Aruba Controller Override**.
3. In the **Profile** drop-down menu, select the **Spectrum Profile** type.
4. In the **Profile Instance** drop-down menu, select the instance of the Spectrum profile used by the controller.
5. In the **Field** drop-down menu, select the setting you would like to change (such as an Age-Out setting or a Spectrum Band), and enter the overriding value below it.
6. Select **Add** to save your changes.
7. To create additional overrides for this controller, select **Add New Aruba Controller Override** again.
8. When you have finished, select **Save and Apply**.

You can also use the above procedure to turn on Spectrum mode for radio profiles on one particular controller, or use the overrides to point your radio profile to a non-default Spectrum profile for just this controller.

This chapter provides an overview and several tasks supporting the use of device configuration templates in AMP, and contains the following topics:

- “Group Templates” on page 151
- “Viewing and Adding Templates” on page 152
- “Configuring General Template Files and Variables” on page 155
- “Configuring Cisco IOS Templates” on page 160
- “Configuring Cisco Catalyst Switch Templates” on page 162
- “Configuring Symbol Controller / HP WESM Templates” on page 163
- “Configuring a Global Template” on page 165

## Group Templates

### Supported Device Templates

Templates are helpful configuration tools that allow AMP to manage virtually all device settings. A template uses variables to adjust for minor configuration differences between devices.

The **Groups > Templates** configuration page allows you to create configuration templates for the following types of devices:

- Dell PowerConnect W
- Aruba
- Alcatel-Lucent



---

Use the graphical Aruba Config feature in support of Aruba devices, particularly for AOS 3.3.2.x and later. Refer to the *Aruba Configuration Guide* for additional information.

---

- Cisco Aironet IOS autonomous APs
- Cisco Catalyst switches
- HP ProCurve 530 and WeSM controllers
- Nomadix
- Symbol
- Trapeze
  - 3Com
  - Nortel
  - Enterasys

### Template Variables

Variables in templates configure device-specific properties, such as name, IP address and channel.

Variables can also be used to configure group-level properties, such as SSID and RADIUS server, which may differ from one group to the next. The AMP template understands many variables including the following:

- %ap\_include\_1% through %ap\_include\_10%

- %channel%
- %hostname%
- %ip\_address%
- %ofdmPOWER%

The variable settings correspond to device-specific values on the **APs/Devices > Manage** configuration page for the specific AP that is getting configured.



Changes made on the other **Group** pages (Radio, Security, VLANs, SSIDs, and so forth) are not applied to any APs that are configured by templates.

## Viewing and Adding Templates

Perform these steps to display, add, or edit templates.

1. Go to the **Groups > List** page, and select a group for which to add or edit templates. This can be a new group, created with the **Add** button, or you can edit an existing group by selecting the corresponding pencil icon. The **Groups > Basic** page for that group appears. Additional information about adding and editing groups is described in “Configuring and Using Device Groups in AMP” on page 71.
2. From the AMP navigation pane, select **Templates**. The **Templates** page appears. Figure 115 illustrates the **Groups > Templates** configuration page, and Table 89 describes the columns.

**Figure 115 Groups > Templates Page Illustration for a Sample Device Group**

Group: **Acme Corporation**

**Note:** No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JA2.  
**Note:** No template is available for Cisco Aironet 1200 IOS devices with firmware version 12.3(8)JEC.  
**Note:** No template is available for Cisco Aironet 1240 IOS devices with firmware version 12.4(10b)JDA.  
**Note:** No template is available for Aruba 5000 devices with firmware version 3.3.2.10.  
**Note:** No template is available for Aruba 5000 devices with firmware version 3.3.2.4.  
**Note:** No template is available for Aruba 2400 devices with firmware version 3.3.2.10.  
**Note:** No template is available for Symbol WS5100 devices with firmware version 3.2.0.0-040R.  
**Note:** No template is available for Aruba 3600 devices with firmware version 3.3.2.7.  
**Note:** No template is available for Cisco Aironet 1250 IOS devices with firmware version 12.4(10b)JA3.  
**Note:** No template is available for Aruba 3400 devices with firmware version 3.3.2.7.  
**Note:** No template is available for Aruba 3200 devices with firmware version 3.3.2.8-m-3.0.  
**Note:** No template is available for Symbol RFS7000 devices with firmware version 1.1.1.0-003R.  
**Note:** No template is available for Cisco Aironet 871W devices with firmware version 12.4(4)T7.

New Template

Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Symbol and Trapeze devices in this group using a configuration file. Variables in the templates are used to configure device-specific properties (like name, IP address and channel) as well as group level properties (ssid, radius server, etc).

	Name ▲	Device Type	Status	Fetch Date	Version Restriction
<input type="checkbox"/>	Aruba 200	Aruba 200	Template saved	1/19/2008 11:43 PM	3.2.0.3
<input type="checkbox"/>	Aruba 200 - 3.3.1.1	Aruba 200	Template saved	2/28/2008 6:24 AM	None
<input type="checkbox"/>	Aruba 3600 - 3.2.0.3	Aruba 3600	Template saved	1/18/2008 11:06 AM	3.2.0.3
<input type="checkbox"/>	Aruba 800	Aruba 800	Template saved	2/27/2008 10:58 PM	None
<input type="checkbox"/>	Aruba 800 - 3.1.1.7	Aruba 800	Template saved	1/20/2008 2:09 AM	3.1.1.7

**Table 89 Groups > Templates Fields and Default Values**

Setting	Description
<b>Notes</b>	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Select the link from such a note to launch the <b>Add Template</b> configuration page for that device.
<b>Name</b>	Displays the template name.
<b>Device Type</b>	Displays the template that applies to APs or devices of the specified type. If <b>vendor (Any Model)</b> is selected, the template applies to all models from that vendor that do not have a version specific template defined. If there are two templates that might apply to a device, the template with the most restrictions takes precedence.
<b>Status</b>	Displays the status of the template.
<b>Fetch Date</b>	Sets the date that the template was originally fetched from a device.

**Table 89** *Groups > Templates Fields and Default Values (Continued)*

Setting	Description
<b>Version Restriction</b>	Designates that the template only applies to APs running the version of firmware specified. If the restriction is <b>None</b> , then the template applies to all the devices of the specified type in the group. If there are two templates that might apply to a device the template with the most restrictions takes precedence. If there is a template that matches a devices firmware it will be used instead of a template that does not have a version restriction.

3. To create a new template and add it to the AMP template inventory, go to the **Groups > List** page, and select the group name, and the **Details** page appears. Select **Templates**, then **Add**.
4. Complete the configurations illustrated in [Figure 116](#), and the settings described in [Table 90](#).

**Figure 116 Groups > Templates > Add Template Page Illustration**

Group: **Routers/Switches**

Cisco Catalyst (Any Model)

Name:

Device Type: Cisco Catalyst (Any Model) ▾

Reboot devices after configuration changes: ☒ Yes ☐ No

Restrict to this version: ☐ Yes ☒ No

Template firmware version:

Template Select

Fetch template from device: -- Select Device -- ▾

Fetch

Template

The following variables may be used in the template value of each variable is configured on the APs/IC Manage page for each device in the group. Each must be surrounded by percent signs: `%hostname`, `%if...` statements must be terminated by `%endif` cannot be nested.

```
<ignore_and_do_not_push></ignore_and_do_not_push>
<push_and_exclude></push_and_exclude>
```

tags can be used to achieve a good configuration refer to the User Guide for more information.

**Available Variables:**

ap_include_1	contact
ap_include_10	domain
ap_include_2	gateway
ap_include_3	hostname
ap_include_4	interfaces
ap_include_5	location
ap_include_6	manager_ip
ap_include_7	ssl_cert
ap_include_8	
ap_include_9	
chassis_id	

Credentials

Change credentials the AMP uses to contact devices after successful config push.

Community String:

Confirm Community String:

Telnet/SSH Username:

Telnet/SSH Password:

Confirm Telnet/SSH Password:

"enable" Password:

Confirm "enable" Password:

SNMPv3 Username:

Auth Password:

Confirm Auth Password:

SNMPv3 Auth Protocol:

MD5 ▾

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol:

DES ▾

Add

Cancel

**Table 90 Groups > Templates > Add Template Fields and Default Values**

Setting	Default	Description
<b>Use Global Template</b>	No	Uses a global template that has been previously configured on the <b>Groups &gt; Templates</b> configuration page. Available templates will appear in the drop-down menu. If <b>Yes</b> is selected you can also configure global template variables. For Symbol devices you can select the groups of thin APs to which the template should be applied. For more information about global templates, see the <b>Groups &gt; Templates</b> section of the <i>User Guide</i> .

Table 90 **Groups > Templates > Add Template Fields and Default Values** (Continued)

Setting	Default	Description
<b>Fetch</b>	None	Selects an AP from which to fetch a configuration. The configuration will be turned into a template with basic AP specific settings like channel and power turned into variables. The variables are filled with the data on the <b>APs/Devices &gt; Manage</b> page for each AP.
<b>Name</b>	None	Defines the template display name.
<b>AP Type</b>	Cisco IOS (Any Model)	Determines that the template applies to APs or devices of the specified type. If <b>Cisco IOS (Any Model)</b> is selected, the template applies to all IOS APs that do not have a version specific template specified.
<b>Reboot APs After Configuration Changes</b>	No	Determines reboot when AMP applies the template, copied from the new configuration file to the startup configuration file on the AP. If <b>No</b> is selected, AMP uses the AP to merge the startup and running configurations. If <b>Yes</b> is selected, the configuration is copied to the startup configuration file and the AP is rebooted. This field is only visible for some devices.
<b>Restrict to this version</b>	No	Restricts the template to APs of the specified firmware version. If <b>Yes</b> is selected, the template only applies to APs on the version of firmware specified in the <b>Template Firmware Version</b> field.
<b>Template firmware version</b>	None	Designates that the template only applies to APs running the version of firmware specified.
<b>Community String</b>	None	If the template is updating the community strings on the AP, enter the new community string AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>Telnet/SSH Username</b>	None	If the template is updating the <b>Telnet/SSH Username</b> on the AP, enter the new username AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>Telnet/SSH Password</b>	None	If the template is updating the <b>Telnet/SSH password</b> on the AP, enter the new Telnet/SSH password AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>"enable" Password</b>	None	If the template is updating the enable password on the AP, enter the new enable password AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>SNMPv3 Username</b>	None	If the template is updating the <b>SNMP v3 Username</b> password on the AP, enter the new SNMP Username password here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>Auth Password</b>	None	If the template is updating the <b>SNMP v3 Auth</b> password on the AP, enter the new SNMP Username password here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>Privacy Password</b>	None	If the template is updating the <b>SNMP v3 Privacy</b> password on the AP, enter the new SNMP Username password here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
<b>SNMPv3 Auth Protocol</b>	MD5	Specifies the <b>SNMPv3 Auth</b> protocol, either <b>MD5</b> or <b>SHA-1</b> .
<b>SNMPv3 Privacy Protocol</b>	DES	Specifies the <b>SNMPv3 Privacy</b> protocol, either <b>DES</b> or <b>AES</b> .

## Configuring General Template Files and Variables

This section describes the most general aspects of configuring AP device templates and the most common variables:

- [Configuring General Templates](#)
- [Using Template Syntax](#)
- [Using Directives to Eliminate Reporting of Configuration Mismatches](#)
- [Using Conditional Variables in Templates](#)



- [Using Substitution Variables in Templates](#)
- [Using AP-Specific Variables](#)

## Configuring General Templates

Perform the following steps to configure Templates within a Group.

1. Select a Group to configure.




---

Start with a small group of access points and placing these APs in Monitor Only mode, which is read-only. Do this using the **Modify Devices** link until you are fully familiar with the template configuration process. This prevents configuration changes from being applied to the APs until you are sure you have the correct configuration specified.

---

2. Select an AP from the Group to serve as a *model* AP for the others in the Group. You should select a device that is configured currently with all the desired settings. If any APs in the group have two radios, make sure to select a model AP that has two radios and that both are configured in proper and operational fashion.
3. Go to the **Groups > Templates** configuration page. Select **Add** to add a new template.
4. Select the type of device that will be configured by this template.
5. Select the model AP from the drop-down list, and select **Fetch**.
6. AMP automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to [“Using Template Syntax” on page 157](#). These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact AirWave support before proceeding.
7. Specify the device types for the template. The templates only apply to devices of the specified type.
  - Specify whether AMP should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then AMP instructs the AP to copy the configuration from AMP to the startup configuration file of the AP and reboot the AP.
  - If the **Reboot Devices after Configuration Changes** option is not selected, then AMP instructs the AP to copy the configuration to the startup configuration file and then tell the AP to copy the startup configuration file to the running configuration file.
  - Use the **reboot** option when there are changes requiring reboot to take effect, for example, removing a new SSID from a Cisco IOS device. Copying the configuration from startup configuration file to running configuration file merges the two configurations and can cause undesired configuration lines to remain active on the AP.
8. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select **Yes** and enter the firmware version in the **Template Firmware Version** text field.
9. Select **Save and Apply** to push the configuration to all of the devices in the group. If the devices are in monitor-only mode (which is recommended while you are crafting changes to a template or creating a new one), then AMP will audit the devices and compare their current configuration to the one defined in the template.




---

If you set the reboot flag to **No**, then some changes could result in configuration mismatches until the AP is rebooted.

---

For example, changing the SSID on Cisco IOS APs requires the AP to be rebooted. Two other settings that require the AP to be rebooted for configuration change are Logging and NTP. A configuration mismatch results if the AP is not rebooted.

If logging and NTP service are not required according to the Group configuration, but are enabled on the AP, you would see a configuration file mismatch as follows if the AP is not rebooted:

## IOS Configuration File Template

```
...
(no logging queue-limit)
...
```

## Device Configuration File on APs/Devices > Audit Configuration Page

```
...
    line con 0
    line vty 5 15
actual logging 10.51.2.1
actual logging 10.51.2.5
actual logging facility local6
actual logging queue-limit 100
actual logging trap debugging
    no service pad
actual ntp clock-period 2861929
actual ntp server 209.172.117.194
    radius-server attribute 32 include-in-access-req format %h
...
```

10. Once the template is correct and all mismatches are verified on the **APs/Devices > Audit** configuration page, use the **Modify Devices** link on the **Groups > Monitor** configuration page to place the desired devices into **Management** mode. This removes the APs from Monitor mode (read-only) and instructs the AP to pull down its new startup configuration file from AMP.



---

Devices can be placed into Management mode individually from the **APs/Devices > Manage** configuration page.

---

## Using Template Syntax

Template syntax is comprised of the following components, described in this section:

- [Using AP-Specific Variables](#)
- [Using Directives to Eliminate Reporting of Configuration Mismatches](#)
- [Using Conditional Variables in Templates](#)
- [Using Substitution Variables in Templates](#)

## Using Directives to Eliminate Reporting of Configuration Mismatches

AMP is designed to audit AP configurations to ensure that the actual configuration of the access point exactly matches the Group template. When a configuration mismatch is detected, AMP generates an automatic alert and flags the AP as having a **Mismatched** configuration status on the user page.

However, when using the templates configuration function, there will be times when the running-config file and the startup-config file do not match under normal circumstances. For example, the `ntp clock-period` setting is almost never identical in the running-config file and the startup-config file. You can use directives such as `<ignore_and_do_not_push>` to customize the template to keep AMP from reporting mismatches for this type of variance.

AMP provides two types of directives that can be used within a template to control how AMP constructs the startup-config file to send to each AP and whether it reports variances between the running-config file and the startup-config file as "configuration mismatches." Lines enclosed in `<push_and_exclude>` are included

in the AP startup-config file but AMP ignores them when verifying configurations. Lines enclosed in **<ignore\_and\_do\_not\_push>** cause AMP to ignore those lines during configuration verification.

### Ignore\_and\_do\_not\_push Command

The `ignore and do not push` directive should typically be used when a value cannot be configured on the device, but always appears in the running-config file. Lines enclosed in the `ignore and do not push` directive will not be included in the startup-config file that is copied to each AP.

When AMP is comparing the running-config file to the startup-config file for configuration verification, it will ignore any lines in the running-config file that start with the text within the directive. Lines belonging to an ignored and unpushed line, the lines immediately below the line and indented, are ignored as well. In the example below, if you were to bracket NTP server, the NTP clock period would behave as if it were bracketed because it belongs or is associated with the NTP server line.



---

The line `<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>` will cause lines starting with "ntp clock-period" to be ignored. However, the line `<ignore_and_do_not_push>ntp </ignore_and_do_not_push>` causes all lines starting with "ntp" to be ignored, so it is important to be as specific as possible.

---

### Push\_and\_exclude Command

Instead of using the full tags you may use the parenthesis shorthand, (substring). The `push and exclude` directive is used to push commands to the AP that will not appear in the running-config file. For example, some **no** commands that are used to remove SSIDs or remove configuration parameters do not appear in the running-config file of a device. A command inside the `push and exclude` directive are included in the startup-config file pushed to a device, but AMP excludes them when calculating and reporting configuration mismatches.



---

The opening tag may have leading spaces.

---

Below are some examples of using directives:

```
...
line con 0
  </push_and_exclude>no stopbits</push_and_exclude>
line vty 5 15
!
ntp server 209.172.117.194
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>
end
```

### Using Conditional Variables in Templates

Conditional variables allow lines in the template to be applied only to access points where the enclosed commands will be applicable and not to any other access points within the Group. For example, if a group of APs consists of dual-radio Cisco 1200 devices (802.11a/b) and single-radio Cisco 1100 (802.11b) devices, it is necessary to make commands related to the 802.11a device in the 1200 APs conditional. Conditional variables are listed in the table below.

The syntax for conditional variables is as follows, and syntax components are described in [Table 91](#):

```
%if variable=value%
...
%endif%
```

**Table 91** *Conditional Variable Syntax Components*

Variable	Values	Meaning
<b>interface</b>	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
<b>radio_type</b>	a	Installed 5GHz radio module is 802.11a
	b	Installed 2.4GHz radio module is 802.11b only
	g	Installed 2.4GHz radio module is 802.11g capable
<b>wds_role</b>	backup	The WDS role of the AP is the value selected in the dropdown menu on the <b>APs/Devices &gt; Manage</b> configuration page for the device.
	client	
	master	
<b>IP</b>	Static	IP address of the device is set statically on the AP Manage configuration page.
	DHCP	IP address of the device is set dynamically using DHCP

## Using Substitution Variables in Templates

Substitution variables are used to set AP-specific values on each AP in the group. It is obviously not desirable to set the IP address, hostname, and channel to the same values on every AP within a Group. The variables in [Table 92](#) are substituted with values specified on each access point's **APs/Devices > Manage** configuration page within the **AMP User** page.

Sometimes, the running-config file on the AP does not include the command for one of these variables because the value is set to the default. For example, when the “transmission power” is set to maximum (the default), the line “power local maximum” will not appear in the AP running-config file, although it will appear in the startup-config file. AMP would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent AMP from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, AMP suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way AMP suppresses lines enclosed in parentheses, which is explained below). A list of the default values that causes lines to be suppressed when reporting configuration mismatches is shown in [Table 92](#).

**Table 92** *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
<b>hostname</b>	Name	hostname %hostname%	-
<b>channel</b>	Channel	channel %channel%	-
<b>ip_address</b> <b>netmask</b>	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp ...	
<b>gateway</b>	Gateway	ip default-gateway %gateway%	-
<b>antenna_receive</b>	Receive antenna	antenna receive %antenna_receive%	diversity
<b>antenna_transmit</b>	Transmit antenna	antenna transmit %antenna_transmit%	diversity
<b>cck_power</b>	802.11g radio module CCK power level	power local cck %cck_power%	maximum
<b>ofdm_power</b>	802.11g radio module OFDM power level	power local ofdm %ofdm_power%	maximum

**Table 92** *Substitution Variables in Templates (Continued)*

Variable	Meaning	Command	Suppressed Default
<b>power</b>	802.11a and 802.11b radio module power level	power local %power%	maximum
<b>location</b>	The location of the SNMP server.	snmp-server location %location%	-
<b>contact</b>	The SNMP server contact.	snmp-server contact %contact%	
<b>certificate</b>	The SSL Certificate used by the AP	%certificate%	-
<b>ap include</b>	The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the <b>APs/Devices &gt; Manage</b> configuration page replace this variable.	%ap_include_1% through %ap_include_10%	-
chassis id			
domain			
interfaces			
location			

## Using AP-Specific Variables

When a template is applied to an AP all variables are replaced with the corresponding settings from the **APs/Devices > Manage** configuration page. This enables AP-specific settings (such as Channel) to be managed effectively on an AP-by-AP basis. The list of used and available variables appears on the template detail configuration page. Variables are always encapsulated between % signs. The following example illustrates this usage:

```
hostname %hostname%
...
interface Dot11Radio0
...
power local cck %CCK_POWER%
power local ofdm %OFDM_POWER%
channel %CHANNEL%
...
```

The `hostname` line sets the AP hostname to the hostname stored in AMP.

The `power` lines set the power local `cck` and `ofdm` values to the numerical values that are stored in AMP.

## Configuring Cisco IOS Templates

Cisco IOS access points have hundreds of configurable settings. AMP enables you to control them via the **Groups > Templates** configuration page. This page defines the startup-config file of the devices rather than using the AMP normal **Group** configuration pages. AMP no longer supports making changes for these devices via the browser-based page, but rather uses templates to configure all settings, including settings that were controlled formerly on the AMP **Group** configuration pages. Perform these steps to configure a Cisco IOS Template for use with one or more groups, and the associated devices.

This section includes the following topics:

- [Applying Startup-config Files](#)
- [WDS Settings in Templates](#)

- [SCP Required Settings in Templates](#)
- [Supporting Multiple Radio Types via a Single IOS Template](#)
- [Configuring Single and Dual-Radio APs via a Single IOS Template](#)

## Applying Startup-config Files

Each of the APs in the Group copies its unique startup-config file from AMP via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then AMP instructs the AP to copy the configuration from AMP to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then AMP instructs the AP to copy the configuration to the startup-config file and then tell the AP to copy the startup config file to the running-config file. Use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.




---

Changes made on the standard AMP Group configuration pages, to include Basic, Radio, Security, VLANs, and so forth, are not applied to any template-based APs.

---

## WDS Settings in Templates

A group template supports Cisco WDS settings. APs functioning in a WDS environment communicate with the Cisco WLSE via a WDS master. IOS APs can function in Master or Slave mode. Slave APs report their rogue findings to the WDS Master (AP or WLSM which reports the data back to the WLSE. On the **APs/ Devices > Manage** configuration page, select the proper role for the AP in the WDS Role drop down menu.

The following example sets an AP as a WDS Slave with the following lines:

```
%if wds_role=client%
wlccp ap username wlse password 7 XXXXXXXXXXXX
%endif%
```

The following example sets an AP as a WDS Master with the following lines:

```
%if wds_role=master%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 200 interface BV11
wlccp ap username wlse password 7 095B421A1C
%endif%
```

The following example sets an AP as a WDS Master Backup with the following lines:

```
%if wds_role=backup%
aaa authentication login method_wds group wds
aaa group server radius wds server
10.2.25.162 auth-port 1645 acct-port 1646
wlccp authentication-server infrastructure method_wds
wlccp wds priority 250 interface BV11
wlccp ap username wlse password 7 095B421A1C
%endif%
```

## SCP Required Settings in Templates

A few things must be set up before enabling SCP on the **Groups > Basic** configuration page. The credentials used by AMP to login to the AP must have level 15 privileges. Without them AMP is not able to communicate with the AP via SCP. The line "aaa authorization exec default local" must be in the APs

configuration file and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP's configuration file:

- username Cisco privilege 15 password 7 0802455D0A16
- aaa authorization exec default local
- ip scp server enable

The username line is a guideline and will vary based on the username being set, in this case Cisco, and the password and encoding type, in this case 0802455D0A16 and 7 respectively.

These values can be set on a group wide level using Templates and TFTP. Once these lines are set, SCP can be enabled on the **Groups > Basic** configuration page without problems.

## Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to 802.11g vs. 802.11b. For instance, lines related to speed rates that mention rates above 11.0Mb/s do not work for 802.11b radios that cannot support these speeds. Use the "%IF variable=value% ... %ENDIF%" construct to allow a single IOS configuration template to configure APs with different radio types within the same Group as illustrated below:

```
interface Dot11Radio0
...
%IF radio_type=g%
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
%ENDIF%
%IF radio_type=b%
speed basic-1.0 2.0 5.5 11.0
%ENDIF%
%IF radio_type=g%
power local cck %CCK_POWER%
power local ofdm %OFDM_POWER%
%ENDIF%
...
```

## Configuring Single and Dual-Radio APs via a Single IOS Template

To configure single and dual-radio APs using the same IOS config template, you can use the interface variable within the %IF...% construct. The below example illustrates this usage:

```
%IF interface=Dot11Radio1%
interface Dot11Radio1
bridge-group 1
bridge-group 1 block-unknown-source
bridge-group 1 spanning-disabled
bridge-group 1 subscriber-loop-control
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
no ip address
no ip route-cache
rts threshold 2312
speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 36.0 48.0 54.0
ssid decibel-ios-a
authentication open
guest-mode
station-role root
%ENDIF%
```

## Configuring Cisco Catalyst Switch Templates

Cisco Catalyst Switch templates are configured much like Cisco IOS templates with the addition of the interfaces and switch\_command (for stacked switches) variables. Interfaces can be configured on the Device Interface pages, as shown in [“Configuring Device Interfaces for Switches” on page 142](#). You can



import interface information as described in this section or by fetching a template from that device, as described in [“Configuring General Templates” on page 156](#).



---

Just one template is used for any type of Cisco IOS device, and another is used for any type of Catalyst Switch regardless of individual model.

---

## Configuring Symbol Controller / HP WESM Templates

This section describes the configuration of templates for Symbol controllers and HP WESM devices.

Symbol controllers (RFS x000, 5100 and 2000) can be configured in AMP using templates. AMP supports Symbol thin AP firmware upgrades from the controller's manage page.

A sample running-configuration file template is provided in this topic for reference. A template can be fetched from a model device using the Cisco IOS device procedure described in [“Configuring Cisco IOS Templates” on page 160](#). Cisco IOS template directives such as `ignore_and_do_not_push` can also be applied to Symbol templates.

Certain parameters such as `hostname` and `location` are turned into variables with the `%` tags so that device-specific values can be read from the individual manage pages and inserted into the template. They are listed in Available Variable boxes on the right-hand side of the template fields.

Certain settings have integrated variables, including `ap-license` and `adoption-preference-id`. The radio preamble has been template-integrated as well. An option on the **Group > Templates** page reboots the device after pushing a configuration to it.

A sample Symbol controller partial template is included below for reference.

```
!  
! configuration of RFS4000 version 4.2.1.0-005R  
!  
version 1.4  
!  
!  
aaa authentication login default local none  
service prompt crash-info  
!  
network-element-id RFS4000  
!  
username admin password 1 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8  
username admin privilege superuser  
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f  
!  
!  
access-list 100 permit ip 192.168.0.0/24 any rule-precedence 10  
!  
spanning-tree mst cisco-interopability enable  
spanning-tree mst configuration  
    name My Name  
!  
ip dns-server-forward  
wwan auth-type chap  
no bridge multiple-spanning-tree enable bridge-forward  
country-code us  
aap-ipfilter-list no port 3333 plz  
aap-ipfilter-list no port 3333 tcp plz  
    deny tcp src-start-ip 0.0.0.0 src-end-ip 255.255.255.255 dst-start-ip 0.0.0.0 dst-end-ip  
255.255.255.255 dst-start-port 3333 dst-end-port 3334 rule 1  
%redundancy_config%  
logging buffered 4  
logging console 4  
snmp-server engineid netsnmp 6b8b45674b30f176  
snmp-server location %location%  
snmp-server contact %contact%  
snmp-server sysname %hostname%  
snmp-server manager v2
```

```

snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpmanager v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpoperator v3 encrypted auth md5 0xb03b1ebfa0e3d02f50e2b1c092ab7c9f

```

A sample Symbol Smart RF template is provided below for reference:

```

radio %radio_index% radio-mac %radio_mac%
%if radio_type=11a%
    radio %radio_index% coverage-rate 18
%endif%
%if radio_type=11an%
    radio %radio_index% coverage-rate 18
%endif%
%if radio_type=11b%
    radio %radio_index% coverage-rate 5p5
%endif%
%if radio_type=11bg%
    radio %radio_index% coverage-rate 6
%endif%
%if radio_type=11bgn%
    radio %radio_index% coverage-rate 18
%endif%

```

A sample Symbol thin AP template is provided below for reference and for the formatting of `if` statements.

```

radio add %radio_index% %lan_mac% %radio_type% %ap_type%
radio %radio_index% radio-number %radio_number%
radio %radio_index% description %description%
%if radio_type=11a%
radio %radio_index% speed basic6 9 basic12 18 basic24 36 48 54
radio %radio_index% antenna-mode primary
radio %radio_index% self-heal-offset 1
radio %radio_index% beacon-interval 99
radio %radio_index% rts-threshold 2345
radio %radio_index% max-mobile-units 25
radio %radio_index% admission-control voice max-perc 76
radio %radio_index% admission-control voice res-roam-perc 11
radio %radio_index% admission-control voice max-mus 101
radio %radio_index% admission-control voice max-roamed-mus 11
%endif%
%if radio_type=11an%
radio %radio_index% speed basic11a 9 18 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
%endif%
%if radio_type=11b%
radio %radio_index% speed basic1 basic2 basic5p5 basic11
%endif%
%if radio_type=11bg%
radio %radio_index% speed basic1 basic2 basic5p5 6 9 basic11 12 18 24 36 48 54
radio %radio_index% on-channel-scan
radio %radio_index% adoption-pref-id 7
radio %radio_index% enhanced-beacon-table
radio %radio_index% enhanced-probe-table
%endif%
%if radio_type=11bgn%
radio %radio_index% speed basic11b2 6 9 12 18 24 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
%endif%
radio %radio_index% channel-power indoor %channel% %transmit_power% %channel_attribute%
%detector%
%adoption_pref_id%
radio %radio_index% enhanced-beacon-table
radio %radio_index% on-channel-scan
%ap_include_4%

```

## Configuring a Global Template

Global templates allow AMP users to define a single template in a global group that can be used to manage APs in subscriber groups. They turn settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

Perform the following steps to create a global template, or to view or edit an existing global template:

1. Go to the **Group > Templates** configuration page for the global group that owns it.
2. Select **Add** to add a new template, or select the pencil icon next to an existing template to edit it.
3. Examine the configurations illustrated in [Figure 117](#).

**Figure 117** *Group > Templates > Add Page Illustration*

Group: global group

**Add** New Template

Templates allow you to manage the configuration of 3Com, Alcatel, Aruba, Cisco Aironet IOS, Enterasys, HP, Hirschmann, LANCOM, Nomadix, Nortel, Sprint and Tadiran devices in the group using a configuration file. Variables in the templates are used to configure device-specific properties (for example, IP address and channel) as well as group-level properties (ssid, radius server, etc.).

Name	Device Type	Template Name	Date Saved	Variable CSV Upload
Aruba 3600 - 3.3.1.11	Aruba 3600	Template saved	6/26/2008 6:10 PM	3.3.1.11
Aruba 3600 - 3.3.2.0	Aruba 3600	Template saved	7/23/2008 10:59 AM	3.3.2.09
Aruba 3600 - 3.3.2.0 - new	Aruba 3600	Template saved	8/12/2008 5:57 PM	None
Aruba 800 - 2.5.4.26	Aruba 800	Template saved	8/11/2008 5:39 PM	None
Cisco Aironet 1200 IOS - 12.2(20)04	Cisco Aironet 1200 IOS	Template saved	6/26/2008 6:02 PM	12.2(20)04
Cisco Aironet 1250 IOS - 12.4(10)1A3	Cisco Aironet 1250 IOS	Template saved	6/27/2008 10:38 AM	None
HP ProCurve 530 - WA.02.00.0160	HP ProCurve 530	Template saved	6/26/2008 6:15 PM	WA.02.00.0160

7 Templates

Select All - Unselect All

Delete

Save Save and Apply Discard

Group: global group

**Template Select**

Fetch template from device: Select Device Fetch

Cisco IOS (Any Model)

Name: Device Type: Cisco IOS (Any Model)

Reboot devices after configuration changes: Yes No

Restrict to this version: Yes No

Template firmware version:

**Template Variables**

Variable Name	Variable Value	Delete

Add

The following variables may be used with variables configured on the device in the group. Each variable is generated by the device. The generated by field and the variable name are used to generate a global configuration file for more information.

4. Use the drop-down menu to select a device from which to build the global template and select **Fetch**. The menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration populates the template field. Global template variables can be configured with the **Add** button in the **Template Variables** box, illustrated in [Figure 118](#).

**Figure 118** *Template Variables Illustration*

Variable Name	Variable Value	Delete

Add

The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered is the default value, but can be changed on a per-group basis later. You can also populate global template variables by uploading a CSV file (see below).

5. Once you have configured your global template, select **Add**. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, select **Apply Changes Now**. If you do not want to add the template, select **Cancel and Discard Changes**. Canceling from the confirmation configuration page causes the template and all of the template variables to be lost.
7. Once you have added a new global template, you can use a CSV upload option to configure global template variables. Go to the **Groups > Templates** configuration page and select the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.
  - **Group Name**—the name of the subscriber group that you wish to update.
  - **Variable Name**—the name of the group template variable you wish to update.
  - **Variable Value**—the value to set.

For example, for a global template with a variable called "ssid\_1", the CSV file might resemble what follows:

```
Group Name, ssid_1
Subscriber 1, Value 0
```

8. Once you have defined and saved a global template, it is available for use by any local group that subscribes to the global group. Go to the **Groups > Template** configuration page for the local group and select the pencil icon next to the global template in the list. [Figure 119](#) illustrates this page.

**Figure 119** *Groups > Templates Edit, Upper Portion*

Group: **SG aruba**

Aruba 3600	
Name:	Aruba 3600 - 3.3.1.11
Device Type:	Aruba 3600
Restrict to this version:	Yes
Template firmware version:	3.3.1.11

Group Template Variables	
location:	<input type="text" value="Building1.floor1"/>

9. To make template changes, go to the **Groups > Template** configuration page for the global group and select the pencil icon next to the template you wish to edit. Note that you cannot edit the template itself from the subscriber group's **Groups > Templates** tab.
10. If group template variables have been defined, you are able to edit the value for the group on the **Groups > Templates, Add** configuration page in the **Group Template Variables** box. For Symbol devices, you are also able to define the template per group of APs.

For more information on using templates in AMP, see the previous section of this chapter. It is also possible to create local templates in a subscriber group—using global groups does not mean that global templates are mandatory.

This chapter provides an overview to rogue device and IDS event detection, alerting, and analysis using RAPIDS, and contains the following sections:

- “Introduction to RAPIDS” on page 167
- “Viewing Rogues on the RAPIDS > List Page” on page 176
- “Setting Up RAPIDS” on page 169
- “Defining RAPIDS Rules” on page 172
- “Score Override” on page 180
- “Using the Audit Log” on page 181
- “Additional Resources” on page 182

## Introduction to RAPIDS

Rogue device detection is a core component of wireless security. With RAPIDS rules engine and containment options, you can create a detailed definition of what constitutes a rogue device, and quickly act on a rogue AP for investigation, restrictive action, or both. Once rogue devices are discovered, RAPIDS alerts your security team of the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- Over the Air
  - Using your existing enterprise APs
  - Optional AirWave Management Client (AMC)
- On the Wire
  - Polling routers and switches to identify, classify, and locate unknown APs
  - Using HTTP and SNMP scanning



NOTE

---

To set up a scan, refer to “Discovering and Adding Devices” on page 107.

---

- Using the controller’s wired discovery information

Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Aruba WIP**—Aruba Networks, Inc.’s Wireless Intrusion Protection (WIP) module integrates wireless intrusion protection into the mobile edge infrastructure. The WIP module provides wired and wireless AP detection, classification and containment; detects DoS and impersonation attacks; and prevents client and network intrusions.
- **Cisco WLSE** (1100 and 1200 IOS)—AMP fetches rogue information from the HTTP interface and gets new AP information from SOAP API. This system provides wireless discovery information rather than rogue detection information.
- **AirMagnet Enterprise**—Retrieves a list of managed APs from AMP.
- **AirDefense**—Uses the AirWave XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from AMP.

## Viewing Overall Network Health on RAPIDS > Overview

The **RAPIDS > Overview** page displays a page of RAPIDS summary information (see [Figure 120](#)). [Table 93](#) defines the summary information that appears on the page.

**Figure 120 RAPIDS > Overview Page Illustration**

### IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Deauth Broadcast	0	1	33
Power Save DoS Attack	0	2	2
Station Associated to Rogue AP	0	2	3
Station Unassociated from Rogue AP	0	1	1
Wireless Bridge Detected	8	128	252
5 Attack Types	8	134	291

### Rogue Data

#### Device Count by RAPIDS Classification



☐ Unclassified 91.1%  
☐ Neighbor 8.9%

RAPIDS Classification	Devices
Rogue	0
Suspected Rogue	0
Unclassified	1918
Suspected Neighbor	0
Neighbor	187
Suspected Valid	0
Valid	0
Total	2105

#### RAPIDS Devices by OS



☐ Unknown 66.7%  
☐ Linux 33.3%

Operating System	Devices
Linux	1
Unknown	2
Not scanned	2102

#### Acknowledged RAPIDS Devices



☐ Unacknowledged 100.0%  
☐ Acknowledged 0.0%

### RAPIDS Changes ([view RAPIDS audit log](#))

Time	User	Event
Mon May 23 03:40:30 2011	admin	seas_config (id 1): rapids_rogue_bssid_window: '0' => '8'
Mon May 23 03:39:51 2011	admin	seas_config (id 1): rapids_rogue_bssid_window: '4' => '0'

**Table 93** *RAPIDS > Overview Fields and Descriptions*

Summary	Description
<b>IDS Events</b>	Displays a list of attack types for the designated folder and subfolders. Field displays events from the past two hours, the past 24 hours, and total IDS events. Names of attacks link to summary pages with more details. <b>Note:</b> AMP should be configured as the SNMP trap receiver on the controllers to receive IDS traps. See the <i>AirWave and Aruba Best Practices Guide</i> for details.
<b>Device Count by RAPIDS Classification</b>	A pie chart of rogue device percentages by RAPIDS classification.
<b>RAPIDS Classification</b>	A summary list with details of the statistics depicted in the Device Count by RAPIDS Classification pie chart. Click the linked classification name to be taken to a filtered rogue list.
<b>RAPIDS Devices by OS</b>	A pie chart of RAPIDS percentages by the detected operating system.
<b>Operating System</b>	Detected operating systems represented in this summary listing. Click on the linked Operating System name to see the rogues list filtered by that classification. OS scans can be run manually or enabled to run automatically on the <b>RAPIDS &gt; Setup</b> page.
<b>Acknowledged RAPIDS Devices</b>	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
<b>RAPIDS Changes</b>	Tracks every change made to RAPIDS including changes to rules, manual classification, and components on the <b>RAPIDS &gt; Setup</b> page. A link at the top of the list directs you to the <b>RAPIDS &gt; Audit Log</b> page.

## Setting Up RAPIDS

The **RAPIDS > Setup** page allows you to configure your AMP server for RAPIDS. Complete the settings on this page as desired, and select **Save**. Most of the settings are internal to how AMP will process rogues.

### Basic Configuration

On the **RAPIDS > Setup** page, the **Basic Configuration** section allows you to define RAPIDS behavior settings. [Figure 121](#) illustrates this page and [Figure 121](#) describes the fields:



**Figure 121 RAPIDS > Setup Page Illustration**

Basic Configuration	
ARP IP Match Timeout (1-168 hours):	<input type="text" value="24"/>
RAPIDS Export Threshold:	<input type="text" value="Suspected Rogue"/>
Wired-to-Wireless MAC Address Correlation (0-8 bits): Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fx). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).	<input type="text" value="4"/>
Wireless BSSID Correlation (0-8 bits): Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. <b>Note:</b> When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.	<input type="text" value="4"/>
Delete Rogues not detected for (0-14 days, zero disables): Cannot be larger than the rogue discovery event expiration (14) configured on the <a href="#">AMP Setup</a> page, unless that value is set to 0.	<input type="text" value="0"/>
Automatically OS scan rogue devices:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Classification Options	
Acknowledge Rogues by Default:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Manually Classifying Rogues Automatically Acknowledges Them:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Containment Options	
Manage rogue AP containment: When enabled, RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS, including the "Contain" classification.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Manage rogue AP containment in monitor-only mode: Containment updates will always be pushed to devices running WMS offload, regardless of this setting.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Maximum number of APs to contain a rogue: The maximum number of APs that will contain a rogue on Cisco WLC controllers.	<input type="text" value="3"/>

Filtering Options	
Filter Ad-hoc Rogues:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Filter Rogues by Signal Strength:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Minimum Signal Strength (Less than or equal to 0): Enter minimum signal strength in dBm. Rogues will not be recorded until they exceed this signal strength.	<input type="text"/>
Filter Rogues Discovered by Remote APs:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Filter IDS Events from Remote APs:	<input checked="" type="radio"/> Yes <input type="radio"/> No

**Table 94 RAPIDS > Setup > Basic Configuration Fields**

Field	Default	Description
<b>ARP IP Match Timeout</b>	24	If you have routers and switches on the AMP, and it's scanning them for ARP tables, this can assign a rogue IP address information. This timeout specifies how recent that information needs to be for the IP address to be considered valid. Note that the default ARP poll period is long (several hours).
<b>RAPIDS Export Threshold</b>	Suspected Rogue	Exported rogues will be sent to VisualRF for location calculation.
<b>Wired-to-Wireless MAC Address Correlation</b>	4	Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fx). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).
<b>Wireless BSSID Correlation</b>	4	Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. <b>Note:</b> When you change this value, RAPIDS will not immediately combine (or un-combine) rogue records. Changes will occur during subsequent processing of discovery events.
<b>Delete Rogues not detected for (0-14 days, zero disables):</b>	0	This value cannot be larger than the rogue discovery event expiration (14) configured on the <b>AMP Setup</b> page, unless that value is set to 0.
<b>Automatically OS scan rogue devices</b>	No	Whether to scan the operating system of rogues. Enabling this feature will cause RAPIDS to perform an OS scan when it gets in IP address for a rogue device. The OS scan will be run when a rogue gets an IP address for the first time or if the IP address changes.

**Table 95 RAPIDS > Setup > Classification Options Fields**

Field	Default	Description
<b>Acknowledge Rogues by Default</b>	No	Sets RAPIDS to acknowledge rogue devices upon initial detection, prior to their classification.
<b>Manually Classifying Rogues Automatically Acknowledges them</b>	Yes	Defines whether acknowledgement happens automatically whenever a rogue device receives a manual classification.

Filtered rogues are dropped from the system before they are processed through the rules engine. This can speed up overall performance but will eliminate all visibility into these types of devices.

**Table 96** *RAPIDS > Setup > Filtering Options*

Field	Default	Description
<b>Ignore Ad-hoc rogues</b>	No	Filters rogues according to ad-hoc status.
<b>Ignore Rogues by Signal Strength</b>	No	Filters rogues according to signal strength. Since anything below the established threshold will be ignored and possibly dangerous, Aruba does not recommend enabling this setting. Instead, incorporate signal strength into the classification rules on the <b>RAPIDS &gt; Rules</b> page.
<b>Ignore Rogues Discovered by Remote APs</b>	No	Filters rogues according to the remote AP that discovers them. Enabling this option causes AirWave to drop all rogue discovery information coming from remote APs.
<b>Ignore IDS Events from Remote APs</b>	No	Filters IDS Events discovered by remote APs.

## Rogue Containment Options

Using RAPIDS, AMP can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Aruba controllers (running AOS versions 3.x and later). AMP will alert you to the appearance of the rogue device and identify any mismatch between controller configuration and the desired configuration.



WMS Offload is not required to manage containment in AMP.

Table 97 shows the Containment Options section of the **RAPIDS > Setup** page.

**Table 97** *RAPIDS > Setup > Containment Options Fields and Default Values*

Field	Default	Description
<b>Manage rogue AP Containment</b>	Yes	Rogue APs on Cisco WLC and Aruba controllers as defined by the Rules engine will be classified as a Contained Rogue. AMP pushes the containment status of a rogue device to the controller and the controller takes the appropriate action. For the rogue device to be contained, you may need to configure containment on the controller.
<b>Manage rogue AP containment in monitor-only mode</b>	No	If disabled, AMP will display the desired containment settings but will not push them to devices. This may result in mismatches in device classifications. This can be useful for administrators that want to see what RAPIDS would push to the controller without making any changes to their network.  If enabled, AMP will push the desired containment settings to the controllers in Monitor-Only mode, as well as the devices in <b>Managed</b> mode.
<b>Maximum number of APs to contain a rogue</b>	3	Sets the maximum number of APs that will contain a rogue on Cisco WLC controllers.

1. Navigate to the **RAPIDS > Setup** page.
2. From the **Containment Options** section, select **Yes** in the **Manage rogue AP containment** field. Once this is done, the Contained Rogue classification will appear as an option in the classification drop down menu as shown in [Figure 122](#).

Additionally, once this option been enabled, the option to manage contained APs in **Monitor-Only** mode becomes available. Containment in Monitor-Only mode means configuration changes will still be pushed to the controller, even though it is in monitor-only mode.

**Figure 122** *RAPIDS > Classification Rule Menu with Containment*

RAPIDS Classification Rule

Rule name:

Classification: Unclassified

Threat Level:

Enabled:

Detected on WLAN ▼

From the **APs/Devices > Rogues Contained** page, you can see the containment status information, as shown in [Figure 123](#).



The Rogue Containment device tab is only present for devices that support containment.

**Figure 123** *Rogue Containment Status Page*

Rogue Containment Status

1-5 ▼ of 5 Rogue BSSIDs Page 1 ▼ of 1 Choose Columns Export to CSV

Rogue ▲	BSSID	Containment State	Desired Containment State	Classifying Rule	Location
Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Enterasys-36:5C:18	00:01:F4:36:5C:18	Contained	Not Contained	Signal strength > -75 dBm	-
Enterasys-37:4A:C3	00:01:F4:37:4A:C3	Contained	Not Contained	Signal strength > -75 dBm	-
Locally Ad-71:BA:90	02:20:A6:71:BA:90	Contained	Not Contained	Signal strength > -75 dBm	-
Locally Ad-71:BA:90	02:20:A6:71:BA:91	Contained	Not Contained	Signal strength > -75 dBm	-

1-5 ▼ of 5 Rogue BSSIDs Page 1 ▼ of 1

## Additional Settings

Additional RAPIDS settings such as role filtering and performance tuning are available in the following locations:

- Use the **AMP Setup > Roles > Add/Edit Role Page** to define the ability to use RAPIDS by user role. Refer to [“Creating AirWave User Roles”](#) on page 46.
- Use the **AMP Setup > General > Performance Tuning** page to define the processing priority of RAPIDS in relation to AirWave as a whole (see [Table 18](#) on page 42).

## Defining RAPIDS Rules

The **RAPIDS > Rules** page is one of the core components of RAPIDS. This feature allows you to define rules by which any detected device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful.

This section contains the following topics:

- [“Controller Classification with WMS Offload”](#) on page 172
- [“Device OUI Score”](#) on page 173
- [“Rogue Device Threat Level”](#) on page 173
- [“Viewing and Configuring RAPIDS Rules”](#) on page 174
- [“Recommended RAPIDS Rules”](#) on page 176
- [“Using RAPIDS Rules with Additional AirWave Functions”](#) on page 176

### Controller Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Aruba WLAN switches. Controller classification of this type remains distinct from RAPIDS classification. WLAN switches feed

wireless device information to AirWave, which AirWave then processes. AMP then pushes the WMS classification to all of the ArubaOS controllers that are WMS offload enabled.

WMS Offload ensures that a particular BSSID has the same classification on all of the controllers. WMS Offload removes some load from master controllers and feeds 'connected-to-lan' information to the RAPIDS classification engine. RAPIDS classifications and controller classifications are separate and often are not synchronized.



---

RAPIDS classification is not pushed to the devices.

---

The following table compares how default classification may differ between AMP and ArubaOS for scenarios involving WMS Offload.

**Table 98** *Rogue Device Classification Matrix*

AirWave	AOS (ARM)
Unclassified (default state)	Unknown
Rogue	Rogue
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Valid	Valid
Contained Rogue	DOS

For additional information about WMS Offload, refer to the *Aruba and AirWave Best Practices Guide* in **Home > Documentation**.

## Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score. The OUI score of each device is viewable from each rogue's detail page. [Table 99](#) provides list the OUI scores definitions.

**Table 99** *Device OUI Scores*

Score	Description
Score of 1	Indicates any device on the network; this is the lowest threat level on the network.
Score of 2	Indicates any device in which the OUI belongs to a manufacturer that produces wireless (802.11) equipment.
Score of 3	Indicates that the OUI matches a block that contains APs from vendors in the Enterprise and small office/ small home market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces small office/ small home access points.

## Rogue Device Threat Level

The threat level classification adds granularity for each general RAPIDS classification. Devices of the same classification can have differing threat scores based on the classifying rule, ranging from 1 to 10 with a default value of 5. This classification process can help identify the greater threat. Alerts can be defined and sorted by threat level.

Threat level and classification are both assigned to a device when a device matches a rule. Once classified, a device's classification and threat level change only if it is classified by a new rule or is manually changed. Threats levels can be manually defined on the **RAPIDS > Detail** page when the RAPIDS classification is manually overridden or you can edit the rule to have a higher threat level.

## Viewing and Configuring RAPIDS Rules

To view the RAPIDS rules that are currently configured on AMP, navigate to the **RAPIDS > Rules** page (Figure 124).

**Figure 124** *RAPIDS > Rules Page Illustration*

Default RAPIDS Classification: Unclassified

Change the priority order of rules by dragging and dropping rows.

Add New RAPIDS Classification Rule

	Rule name	Classification	Threat Level	Enabled	
<input type="checkbox"/>	Protect my SSID	Rogue	10	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	Fingerprint scan	Rogue	5	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	Detected wirelessly and on LAN	Rogue	5	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	Signal strength > -75 dBm	Suspected Rogue	5	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	Detected Wirelessly	Suspected Neighbor	5	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes	⬆️⬆️⬆️
<input type="checkbox"/>	OUI block does not contain APs	Suspected Valid	5	Yes	⬆️⬆️⬆️

7 RAPIDS Classification Rules

Select All - Unselect All

Delete

Save and Apply Revert

Table 100 defines the fields in the **RAPIDS > Rules** page.

**Table 100** *RAPIDS > Rules Page*

Field	Description
<b>Default Classification</b>	Sets the classification that a rogue device receives when it does not match any rules.
<b>Add New RAPIDS Classification Rule</b>	Select this button to create a RAPIDS classification rule.
<b>Rule Name</b>	Displays the name of any rule that has been configured. Rule names should be descriptive and should convey the core purpose for which it was created.
<b>Classification</b>	Displays the classification that devices receive if they meeting the rule criteria.
<b>Threat Level</b>	Displays the numeric threat level for the rogue device that pertains to the rule. Refer to <a href="#">"Rogue Device Threat Level"</a> on page 173 for additional information.
<b>Enabled</b>	Displays the status of the rule, whether enabled or disabled.
<b>Reorder Drag and Drop Icon</b> ⬆️⬆️⬆️	Changes the sequence of rules in relation to each other. Select, then drag and drop, the icon for any rule to move it up or down in relation to other rules. A revised sequence of rules must be saved before rogues are classified in the revised sequence. <b>NOTE:</b> The sequence of rules is very important for proper rogue classification. A device gets classified by the first rule to which it complies, even if it conforms to additional rules later in the sequence.

To create a new rule, select the **Add** button next to **New RAPIDS Classification Rule** to launch the **RAPIDS Classification Rule** page (see Figure 125).

**Figure 125** *Classification Rule Page*

**RAPIDS Classification Rule**

Rule name:

Classification: Valid

Threat Level: 5

Enabled: ☒ Yes ☐ No

Detected on WLAN Add

Fill in the settings described in Table 100 then select an option from the drop down menu.

Table 101 defines the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 125). Once all rule settings are defined, select **Add**. The new rule automatically appears in the **RAPIDS > Rules** page.

**Table 101** *Properties Drop Down Menu*

Option	Description
<b>Wireless Properties</b>	
<b>Detected on WLAN</b>	Classifies based on how the rogue is detected on the wireless LAN.
<b>Detecting AP Count</b>	Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select <b>At Least</b> or <b>At Most</b> .
<b>Encryption</b>	Classifies based on the rogue matching a specified encryption method. Note that you can select for 'no encryption' with a rule that says "Encryption does not match WEP or better".
<b>Network type</b>	Rogue is running on the selected network type, either <b>Ad-hoc</b> or <b>Infrastructure</b> .
<b>Signal Strength</b>	Rogue matches signal strength parameters. Specify a minimum and maximum value in dBm.
<b>SSID</b>	Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression. <b>NOTE:</b> For SSID matching functions, AirWave processes only alpha-numeric characters and the asterisk wildcard character (*). AirWave ignores all other non-alpha-numeric characters. For example, the string of <b>ethersphere-*</b> matches the SSID of <b>ethersphere-wpa2</b> but also the SSID of <b>ethersphere_this_is_an_example</b> (without any dashes).
<b>Detected Client Count</b>	Classifies based on the number of valid clients.
<b>Wireline Properties</b>	
<b>Detected on LAN</b>	Rogue is detected on the wired network. Select <b>Yes</b> or <b>No</b> .
<b>Fingerprint Scan</b>	Rogue matches fingerprint parameters.
<b>IP Address</b>	Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.
<b>OUI Score</b>	Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Select <b>remove</b> to remove one or both criteria, as desired.
<b>Operating System</b>	Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.
<b>Wireless/Wireline Properties</b>	
<b>Manufacturer</b>	Rogue matches the manufacturer information of the rogue device. Specify matching or non-matching manufacturer criteria.
<b>MAC Address</b>	Rogue matches the MAC address. Specify matching or non-matching address criteria, or use a wildcard (*) for partial matches.
<b>Aruba Controller Properties</b>	
<b>Controller Classification</b>	Rogue matches the specified controller classification.
<b>Confidence</b>	Rogue falls within a specified minimum and maximum confidence level, ranging from 1 to 100.

After creating a new rule, select **Add** to return to the **RAPIDS > Rules** page. Select **Save and Apply** to have the new rule take effect.

## Deleting or Editing a Rule

To delete a rule from the RAPIDS rules list, go to the **RAPIDS > Rules** page. Select the check box next to the rule you want to delete, and select **Delete**. The rule is automatically deleted from **RAPIDS > Rules**.

To edit any existing rule, select its pencil icon to launch the **RAPIDS Classification Rule** page (see [Figure 125](#)). Edit or revise the fields as necessary, then select **Save**.

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

## Recommended RAPIDS Rules

- **If Any Device Has Your SSID, Then Classify as Rogue**

The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by AirWave. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.

- **If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, Then Classify as Rogue**

This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.

- **If More Than Four APs Have Discovered a Device, Then Classify as Rogue**

By default, AirWave tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.


The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact AirWave support.

## Using RAPIDS Rules with Additional AirWave Functions

Rules that you configure on the **RAPIDS > Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in AirWave, with additional information:

- **RAPIDS > List**—Lists rogue devices as classified by rules.
- **RAPIDS > Rules**—Displays the rules that classify rogue devices.
- **RAPIDS > Overview**—Displays general rogue device count and statistical information.
- **System > Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports > Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

## Viewing Rogues on the RAPIDS > List Page

To view a rogue AP, select the **RAPIDS > List** tab and select a rogue device type from the **Minimum Classification** drop-down menu (see [Figure 126](#)). You can sort the table columns (up/down) by selecting the column head. Most columns can be filtered using the funnel icon (). The active links on this page launch additional pages for RAPIDS configuration or device processing.



**Figure 126 RAPIDS > List Page Illustration (partial view)**

Minimum Classification: Rogue

[Modify Devices](#)

1-2 of 2 Rogue APs Page 1 of 1 [Choose Columns](#) [CSV Export](#)

Ack	RAPIDS Classification	Threat Level	Name	Classifying Rule	Controller Classification	WMS Classification AP	WMS
<span>- All -</span>	<span>- All -</span>	<span>- All -</span>		<span>- All -</span>	<span>- All -</span>		
No	Rogue	5	HANGZHOU H-49:17:C0	Detected Wirelessly and on LAN	Valid	00:1a:1e:c0:1a:dc	1/7/2
No	Rogue	5	HANGZHOU H-32:1F:60	Detected Wirelessly and on LAN	Valid	00:24:6c:c8:70:b5	1/7/2

1-2 of 2 Rogue APs Page 1 of 1

[View Ignored Rogues](#)

Table 102 details the column information displayed in Figure 126. For additional information about RAPIDS rules, refer to “Defining RAPIDS Rules” on page 172.

**Table 102 RAPIDS > List Column Definitions**

Column	Description
<b>Ack</b>	Displays whether or not the rogue device has been acknowledged. Devices can be acknowledged manually or you can configure RAPIDS so that manually classifying rogues will automatically acknowledges them. Additionally, devices can be acknowledged by using <b>Modify Devices</b> link at the top of the <b>RAPIDS &gt; List</b> page. Rogues should be acknowledged when the AirWave user has investigated them and determined that they are not a threat (see “Basic Configuration” on page 169).
<b>RAPIDS Classification</b>	Displays the current RAPIDS classification. This classification is determined by the rules defined on the <b>RAPIDS &gt; Rules</b> page.
<b>Threat Level</b>	This field displays the numeric threat level of the device, in a range from 1 to 10. The definition of threat level is configurable, as described in “Rogue Device Threat Level” on page 173. The threat level is also supported with Triggers (see “Monitoring and Supporting AMP with the System Pages” on page 183).
<b>Name</b>	Displays the alpha-numeric name of the rogue device, as known. By default, AirWave assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. Clicking the linked name will redirect you to the <b>RAPIDS &gt; Detail</b> page for that rogue device. Refer to “Overview of the RAPIDS > Detail Page” on page 179.
<b>Classifying Rule</b>	Displays the RAPIDS Rule that classified the rogue device (see “Viewing and Configuring RAPIDS Rules” on page 174).
<b>Current Associations</b>	The number of current rogue client associations to this device.
<b>Max associations</b>	The highest number of rogue client associations ever detected at one time.
<b>Controller Classification</b>	Displays the classification of the device based on the controller’s hard-coded rules. <b>NOTE:</b> This column is hidden unless <b>Offload WMS Database</b> is enabled by at least one group on the <b>Groups &gt; Basic</b> page.
<b>WMS Classification AP</b>	The AP that provided the information used to classify the device. Click the linked device name to be redirected to the <b>APs/Devices &gt; Monitor</b> page for that AP.
<b>WMS Classification Date</b>	The date that WMS set the classification.
<b>Confidence</b>	The confidence level of the suspected rogue. How confidence is calculated varies based on the version of ArubaOS. When an ArubaOS controller sees evidence that a device might be on the wire it will up the confidence level. If ArubaOS is completely sure that it is on the wire, it gets classified as a rogue.
<b>Wired</b>	Displays whether the rogue device has been discovered on one of your wired networks by polling routers/switches, your SNMP/HTTP scans, or Aruba WIP information. This column displays <b>Yes</b> or is blank if wired information was not detected.
<b>Detecting APs</b>	Displays the number of AP devices that have wirelessly detected the rogue device. A designation of heard implies the device was heard over the air.
<b>Location</b>	If the rogue has been placed in VisualRF, this column will display the name of the floor plan the rogue is on as a link to the VisualRF Floor Plan View page.

**Table 102 RAPIDS > List Column Definitions (Continued)**

Column	Description
<b>SSID</b>	Displays the most recent SSID that was heard from the rogue device.
<b>Signal</b>	Displays the strongest signal strength detected for the rogue device.
<b>RSSI</b>	Displays Received Signal Strength Indication (RSSI) designation, a measure of the power present in a received radio signal.
<b>Network Type</b>	<p>Displays the type of network in which the rogue is present, for example:</p> <ul style="list-style-type: none"> <li>● <b>Ad-hoc</b>—This type of network usually indicates that the rogue is a laptop that attempts to create a network with neighboring laptops, and is less likely to be a threat.</li> <li>● <b>AP</b>—This type of network usually indicates an infrastructure network, for example. This may be more of a threat.</li> <li>● <b>Unknown</b>—The network type is not known.</li> </ul>
<b>Encryption Type</b>	<p>Displays the encryption that is used by the device. Possible contents of this field include the following encryption types:</p> <ul style="list-style-type: none"> <li>● <b>Open</b>—No encryption</li> <li>● <b>WEP</b>—Wired Equivalent Privacy</li> <li>● <b>WPA</b>—Wi-Fi Protected Access</li> </ul> <p>Generally, this field alone does not provide enough information to determine if a device is a rogue, but it is a useful attribute. If a rogue is not running any encryption method, you have a wider security hole than with an AP that is using encryption.</p>
<b>Ch</b>	Indicates the most recent RF channel on which the rogue was detected. <b>Note:</b> it may be detected on more than one channel if it contains more than one radio.
<b>LAN MAC Address</b>	The LAN MAC address of the rogue device.
<b>LAN Vendor</b>	Indicates the LAN vendor of the rogue device, when known.
<b>Radio MAC Address</b>	Displays the MAC address for the radio device, when known.
<b>Radio Vendor</b>	Indicates the radio vendor of the rogue device, when known.
<b>OS</b>	This field displays the OS of the device, as known. OS is the result of a running an OS port scan on a device. An IP addresses is required to run an OS scan. The OS reported here is based on the results of the scan.
<b>Model</b>	Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available.
<b>IP Address</b>	Displays the IP address of the rogue device. The IP address data comes from fingerprint scans or ARP polling of routers and switches.
<b>Last Discovering AP</b>	Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in AirWave. Click the linked device name to be redirected to the <b>APs/Devices &gt; Monitor</b> page for that AP.
<b>Switch/Router</b>	Displays the switch or router where the device's LAN MAC address was last seen.
<b>Port</b>	Indicates the physical port of the switch or router where the rogue was last seen.
<b>Notes</b>	Indicates any notes about the rogue device that may have been added.
<b>Last Seen</b>	Indicates the date and time the rogue device was last seen.

## Overview of the RAPIDS > Detail Page

Select a device Name in the **RAPIDS > List** page to view the **Detail** page (Figure 127).

**Figure 127 RAPIDS > Detail Page Illustration**

Name:

7D:2C:50

Model:

-

First Discovered:

10/10/2011 3:37 PM

Acknowledge:

☐ Yes ☒ No

Controller Classification:

Suspected Rogue

IP Address:

-

First Discovery Method:

Wireless AP scan

SSID:

qa\_hyb

Confidence:

20

First Discovery Agent:

Spectrum-AP105-d7:9b

RAPIDS Classification:

Suspected Rogue

Channel:

6

Last Discovered:

10/20/2011 1:16 PM

Classification Rule:

Signal strength > -75 dBm

WEP:

No

Last Discovery Method:

Wireless AP scan

RAPIDS Classification Override:

- No Override -

WPA:

No

Last Discovery Agent:

Spectrum-AP93-06:bd

Threat Level:

5

Network Type:

AP

Threat Level Override:

1

Radio MAC Address:

00:0B:86:7D:2C:50

Current Associations:

2

Radio Vendor:

Netron

Max Associations:

5

LAN MAC Address:

-

LAN Vendor:

-

OUI Score:

-

Operating System:

-

OS Detail:

-

Last Scan:

-

Notes:

Update

Ignore

Delete

Refresh this page for updated results.

Location: Srimi > Srimi > 3.dwg (Floor 1)

Enlarge

Last Placed: 10/20/2011 12:26 PM

### Current Rogue Client Associations

1-2 of 2 Rogue Client Associations Page 1 of 1 Choose columns Export CSV

MAC Address	Username	First Heard	Last Heard	BSSID	SSID	Location
00:21:6A:4B:E2:88	pdedhia	10/17/2011 2:41 PM	10/20/2011 1:15 PM	00:0B:86:7D:2C:50	qa_hyb	Srimi > Srimi > 3.dwg
00:24:D7:EB:0B:48	-	10/17/2011 1:22 PM	10/20/2011 12:56 PM	00:0B:86:7D:2C:50	qa_hyb	Srimi > Srimi > 3.dwg

1-2 of 2 Rogue Client Associations Page 1 of 1

### Discovery Events


1-5 of 35 Discovery Events Page 1 of 7 > > | Reset filters Choose columns Export CSV

RSSI	Signal	Channel	SSID	WEP	WPA	BSSID	Network Type	IP Address	Time	Discovery Method	Discovery Agent
24	-88	6	qa_hyb	No	No	00:0B:86:7D:2C:50	AP	-	10/20/2011 1:16 PM	Wireless AP scan	AM65-e5:e0
39	-50	6	qa_hyb	No	No	00:0B:86:7D:2C:50	AP	-	10/20/2011 1:16 PM	Wireless AP scan	Spectrum-AP93
37	-75	6	qa_hyb	No	No	00:0B:86:7D:2C:50	AP	-	10/20/2011 1:01 PM	Wireless AP scan	1341-AP39-QA
13	-83	6	qa_hyb	No	No	00:0B:86:7D:2C:50	AP	-	10/20/2011 1:01 PM	Wireless AP scan	1341-AP38
37	-75	6	qa_hyb	No	No	00:0B:86:7D:2C:50	AP	-	10/20/2011 1:01 PM	Wireless AP scan	1341-AP36-QA

1-5 of 35 Discovery Events Page 1 of 7 > > | Reset filters

Important things to remember regarding the information in the device detail page are:

- Users with the role of **Admin** can see all rogue AP devices.
- Active rogue clients associated with this AP are listed in the **Current Rogue Client Associations** table. Selecting a linked MAC address will take you to the **Clients > Client Detail** page, where you can view fingerprinting and device details.
- Users with roles limited by folder can *see* a rogue AP if there is at least one discovering device that they can see.
- The discovery events displayed are from APs that you can see on the network. There may be additional discovery events that remain hidden to certain user roles.
- Each rogue device frequently has multiple discovery methods, all of which are listed.
- As you work through the rogue devices, use the **Name** and **Notes** fields to identify the AP and document its location.
- You can use the global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.

- VisualRF uses the heard signal information to calculate the physical location of the device.
- If the device is seen on the wire, RAPIDS reports the switch and port for easy isolation.
- If you find that the rogue belongs to a neighboring business, for example, you can override the classification to a neighbor and acknowledge the device. Otherwise, it is strongly recommended that you extract the device from your building and delete the rogue device from your system. If you delete a rogue, you will be notified the next time it is discovered.
- Most columns in the **Discovery Events** list table on this page can be filtered using the funnel icon ().

To update a rogue device:

1. Select the **Identify OS for Suspected Rogues** option if an IP address is available to obtain operating system information using an nmap scan. Note that if you are running wireline security software on your network, it may identify your AMP as a threat, which you can ignore.
2. Select the **Ignore** button if the rogue device is to be ignored. Ignored devices will not trigger alerts if they are rediscovered or reclassified.
3. Select the **Delete** button if the rogue device is to be removed from AirWave processing.

## Viewing Ignored Rogue Devices

The **RAPIDS > List** page allows you to view ignored rogues—devices that have been removed from the rogue count displayed by AirWave. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, select **View Ignored Rogues** at the bottom left of the page.

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

## Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. AirWave performs a port scan on the device and attempts to determine the operating system (see “[Setting Up RAPIDS](#)” on page 169)

You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.

- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To manage the rogue, remove it from the network and acknowledge the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.




---

Not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

---

## Score Override

On **RAPIDS > Score Override** page you can change the OUI scores that are given to MAC addresses detected during scans of bridge forwarding tables on routers or switches. [Figure 128](#), [Figure 129](#), and [Table 103](#) illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.



Note that rescoreing a MAC Address Prefix poses a security risk. The block has received its score for a reason. Any devices that fall within this block receive the new score.

1. Navigate to the **RAPIDS > Score Override** page. This page lists all existing overrides if they have been created.

**Figure 128 RAPIDS > Score Override Page**

1-11 of 11 Score Overrides Page 1 of 1 Edit Columns

	MAC Address Prefix	Vendor	Score
<input type="checkbox"/>	00:02:2D	Agere Systems	2 - OUI: manufacturer block contains wireless clients, WIFI tags or scanners
<input type="checkbox"/>	00:02:6F	Senao International Co., Ltd.	4 - OUI: manufacturer block contains SOHO access points
<input type="checkbox"/>	00:03:03	JAMA Electronics Co., Ltd.	3 - OUI: manufacturer block contains enterprise access points
<input type="checkbox"/>	00:0D:54	3COM	4 - OUI: manufacturer block contains SOHO access points
<input type="checkbox"/>	00:10:40	INTERMEC CORPORATION	1 - Any device on the network not categorized with a higher score
<input type="checkbox"/>	00:13:72	Dell	1 - Any device on the network not categorized with a higher score
<input type="checkbox"/>	00:14:69	Cisco	4 - OUI: manufacturer block contains SOHO access points
<input type="checkbox"/>	00:15:2B	Cisco Systems	4 - OUI: manufacturer block contains SOHO access points
<input type="checkbox"/>	00:30:65	Apple Computer	3 - OUI: manufacturer block contains enterprise access points
<input type="checkbox"/>	00:30:89	Spectrapoint Wireless, LLC	4 - OUI: manufacturer block contains SOHO access points
<input type="checkbox"/>	00:C0:49	U.S. ROBOTICS, INC.	4 - OUI: manufacturer block contains SOHO access points

1-11 of 11 Score Overrides Page 1 of 1

2. Select **Add** to create a new override or select the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears (Figure 129).

**Figure 129 Add/Edit Score Override Page**

**Score Override**

MAC Address Prefix:

Score: 

4 - OUI: manufacturer block contains SOHO access points  
4 - OUI: manufacturer block contains SOHO access points  
3 - OUI: manufacturer block contains enterprise access points  
2 - OUI: manufacturer block contains wireless clients, WIFI tags or scanners  
1 - Any device on the network not categorized with a higher score

**Table 103 RAPIDS > Add/Edit Score Override Page Fields**

Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. Select **Add** to create the new override, or select **Save** to retain changes to an existing override. The new or revised override appears on the **RAPIDS > Score Override** page.
5. To remove any override, select that override in the checkbox and select **Delete**.

## Using the Audit Log

The Audit Log is a record of any changes made to the RAPIDS rules, setup page, and manual changes to specific rogues. This allows you to see how something is changes, when it changed, and who made the alteration. The Audit Log can be found at **RAPIDS > Audit Log**. For more information, see Figure 130.

**Figure 130** *Audit Log Page Illustration*

RAPIDS Changes		
Time	User	Event
Wed Feb 17 10:21:12 2010	admin	rapids_classification_rule (id 39): classification: '70' => '80'
Wed Feb 17 10:20:20 2010	admin	seas_config (id 1): rapids_manage_containment: '0' => '1'
Fri Feb 12 08:19:00 2010	jason	rapids_classification_rule (id 39): classification: '80' => '70'
Fri Feb 12 08:19:00 2010	jason	seas_config (id 1): rapids_manage_containment: '1' => '0'
Tue Feb 9 15:53:57 2010	admin	rapids_classification_rule (id 39): manufacturer: 'proxim*' => '3Com*'; name: 'Contain Proxim' => 'Contain 3Com'
Tue Feb 9 15:53:03 2010	admin	rapids_classification_rule (id 39): classification: '70' => '80'
Thu Feb 4 15:59:12 2010	admin	seas_config (id 1): rapids_manage_containment: '0' => '1'
Mon Feb 1 13:55:36 2010	admin	rapids_classification_rule (id 39): classification: '80' => '70'
Mon Feb 1 13:55:36 2010	admin	seas_config (id 1): rapids_manage_containment: '1' => '0'
Thu Jan 28 15:48:54 2010	admin	rogue_ap (id 154880): Cisco-AD:61:FE: 'Identify Operating System'

## Additional Resources

The following AirWave tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to [“Viewing, Delivering and Responding to Triggers and Alerts” on page 186](#).
- **Reports**—The **New Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see [“Using the New Rogue Devices Report” on page 242](#).

For additional security-related features and functions, see the following topics in this guide.

- [“Configuring Group Security Settings” on page 82](#)
- [“Configuring Cisco WLC Security Parameters and Functions” on page 96](#)
- [“Configuring Group SSIDs and VLANs” on page 84](#)
- [“Monitoring and Supporting AMP with the System Pages” on page 183](#)

Daily WLAN administration often entails network monitoring, supporting WLAN and AirWave users, and monitoring AMP system operations.

This chapter contains the following administration procedures:

- “Monitoring and Supporting AMP with the System Pages” on page 183
- “Monitoring and Supporting WLAN Clients” on page 196
- “Evaluating and Diagnosing User Status and Issues” on page 203
- “Managing Mobile Devices with SOTI MobiControl and AirWave” on page 207
- “Monitoring and Supporting AMP with the Home Pages” on page 209
- “Supporting AMP Servers with the Master Console” on page 220
- “Upgrading AirWave” on page 222
- “Backing Up AMP” on page 223
- “Using AirWave Failover for Backup” on page 224
- “Logging out of AirWave” on page 225

## Monitoring and Supporting AMP with the System Pages

The **System** pages provide a centralized location for system-wide AMP data and settings. Apart from **Triggers**, **Alerts**, and **Backups** pages that are described elsewhere in this chapter, the remaining pages of the **System** section are as follows:

- **System > Status**—Displays status of all AMP services and links to their log pages. Refer to “Using the System > Status Page” on page 184.
- **System > Syslog & Traps**—Displays all syslog messages and SNMP traps that AMP receives. Refer to “Viewing Device Events in System > Syslog & Traps” on page 185.
- **System > Event Log**—This useful debugging tool keeps a list of recent AMP events, including APs coming up and down, services restarting, and most AMP-related errors as well as the user that initiated the action. Refer to “Using the System > Event Log Page” on page 186.
- **System > Triggers**—View and edit triggering conditions that cause AMP to send out alert notifications. Refer to “Viewing, Delivering and Responding to Triggers and Alerts” on page 186.
- **System > Alerts**—View or acknowledge alerts sent out by the system and use the Triggering Agent links to drill down to the device that triggered the alert. Refer to “Viewing Alerts” on page 194.
- **System > Backups**—View the backup files that are run nightly. Refer to “Backing Up AMP” on page 223.
- **System > Configuration Change Jobs**—Manages configuration changes in AMP. Refer to “Using the System > Configuration Change Jobs Page” on page 215.
- **System > Firmware Upgrade Jobs**—Displays information about current and scheduled firmware upgrades. Refer to “Using the System > Firmware Upgrade Jobs Page” on page 215.
- **System > Performance**—Displays basic AMP hardware information as well as resource usage over time. Refer to “Using the System > Performance Page” on page 216.



## Using the System > Status Page

The **System > Status** page displays the status of all of AirWave services. Services will either be **OK**, **Disabled**, or **Down**. If any service is **Down** (displayed in red) please contact AirWave support. The **Reboot System** button provides a graceful way to power cycle your AMP remotely when it is needed. The **Restart AMP** button will restart the AMP services without power cycling the server or reloading the OS. [Figure 131](#) illustrates this page.

**Figure 131** *System > Status Page Illustration*

Refresh

Diagnostic report file for sending to customer support: [diagnostics.tar.gz](#)  
VisualRF diagnostics report file: [VisualRFdiag.tar.gz](#)

Service ▲	Status	Log
Airbus Message Server	OK	/var/log/airbus.log
Alert Cache Builder	OK	/var/log/alerts_stats_cacher
Alert Monitor	OK	/var/log/alertd
Asynchronous Work Scheduler	OK	/var/log/tuple_scheduler
At	OK	/var/log/at
AWMS News Fetcher	OK	/var/log/awms_news_fetcher
Cisco ACS	OK	/var/log/acs
Cisco WLSE Poller	OK	/var/log/wlse
Client Monitor Worker	OK	/var/log/async_logger_client
Configuration Monitor	OK	/var/log/config_verifier
Configuration Server	OK	/var/log/config_pusher
Cron	OK	/var/log/amp_cron
Database	OK	/var/log/pgsql
Device List Cacher	OK	/var/log/ap_list_cacher
Device Monitor	OK	/var/log/ap_watcher
Device Monitor (Poll Now)	OK	/var/log/ap_watcher_poll_now
Discovery Event Existing-AP Cacher	OK	/var/log/discovery_event_cacher
DNS Fetcher	OK	/var/log/dns_fetcher
DNS Refresh	OK	/var/log/dns_refresh
Fallover Monitor	Disabled	/var/log/amp_watcher
Firmware Server	OK	/var/log/firmware_enforcer
FTP Server	Disabled	/var/log/xferlog
Guest User Credential Enabler	OK	/var/log/guest_user_pusher
HTTP/SNMP Scanner	OK	/var/log/ap_scanner
LWAPP Managed Certificate Builder	OK	/var/log/lwapp_rebuild
Master Console	Disabled	/var/log/mc_stat_collector
MC Report Runner	OK	/var/log/mc_report_runner
Mobile Device Management Engine	Disabled	/var/log/mdm.log
NTP Client	OK	
PAPI Message Processor	OK	/var/log/papi
PAPI Message Router	OK	/var/log/msgHandler.log
Parallel HTTP Fetcher	Disabled	/var/log/http_fetcher
Performance Monitor	OK	/var/log/perf_collector
Persistent TupleSpaces Server	OK	/var/log/persistent_tuple_spaces
Postfix Mail Server	OK	/var/log/maillog
RADIUS Accounting Server	OK	/var/log/radius/radius.log
Report Runner	OK	/var/log/amp_report_runner
Rogue Filter	OK	/var/log/rogue_filter
RTLS Collector	OK	/var/log/rtls
SNMP Enabler	OK	/var/log/snmp_enabler
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher
SNMP Trap Handler	OK	/var/log/snmp_trap_handler
Synchronous Event Handler	OK	/var/log/syncd
Tag Expiration	OK	/var/log/expire_wifi_tags
TupleSpaces Server	OK	/var/log/tuple_spaces
VisualRF Engine	OK	/var/log/visualrf.log
Web Server	OK	/var/log/httpd/ssl_error_log
WEP Key Setter	OK	/var/log/wep_key_setter
Whitelist Collector	Disabled	/var/log/whitelist_collector
Work Queue Collision Logger	OK	/var/log/work_queue_clobber_logger

**Additional Log Files**

Description ▲	Log
Nightly Maintenance	/var/log/nightly_maintenance
System Audit Log	/var/log/system_audit_log
Telnet Commands	/var/log/telnet_cmds
Upgrade to 6.4_beta6	/tmp/AMP-6.4_beta6-upgrade.log

4 Additional Log Files

[Restart AWMS](#) [Reboot System](#)


- The link **diagnostics.tar.gz** contains reports and logs that are helpful to Aruba support in troubleshooting and solving problems. Your Aruba support representative may ask for this file along with other logs that are linked on this page.
- Similarly, the **VisualRFdiag.zip** link contains VisualRF diagnostic information that might be requested by Aruba support.
- A summary table lists logs that appear on the **System > Status** page. These are used to diagnose AMP problems. Additional logs are available via SSH access in the /var/log and /tmp directories; Aruba

support engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. [Table 104](#) describes some of the most important logs:

**Table 104** A Sample of Important Status Logs

Log	Description
<b>pgsql</b>	Logs database activity.
<b>error_log</b>	Reports problems with the web server. Also linked from the internal server error page that displays on the web page; please send this log to Aruba support whenever reporting an internal server error.
<b>maillog</b>	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
<b>radius</b>	Displays error messages associated with RADIUS accounting.
<b>async_logger</b>	Tracks many device monitoring processes, including user-AP association.
<b>async_logger_client</b>	Logs device configuration checks.
<b>config_pusher</b>	Logs errors in pushing configuration to devices.
<b>visualrf.log</b>	Details errors and messages associated with the VisualRF application.

## Viewing Device Events in System > Syslog & Traps

Admins can use the **System > Syslog & Traps** page to review all syslog messages and SNMP traps that AMP receives from the trigger type **Device Event**. These device events are listed by time, type, source device, AP, severity, facility, category, and message. Most columns can be filtered using the funnel icon () , and messages can be filtered by substring using the **Search** field, as seen in [Figure 132](#).

You can change the historical data retention from the **Device Events (Syslog, Traps)** field in **AMP Setup > General**.

**Figure 132** System > Syslog & Traps Page Illustration

Device Events

1-10 ▼ of 41967 Device Events Page 1 ▼ of 4197 > > | [Reset filters](#) [Choose columns](#)

Time ▼	Type ▼	Source Device ▼	AP ▼	User	Severity ▼	Facility ▼	Category ▼	Message
								<input type="text" value="Search"/>
5/24/2011 7:40 PM	SNMP Trap	<Unknown>	00:24:6c:c4:c1:50.testdomain	-	-	-	AP Status	wlsxNAccessPointIsDown wlsxTrapAPM wlsxTrapTime: 5/24/2011 22:41:25 U1
5/24/2011 7:40 PM	SNMP Trap	<Unknown>	ap125-c0:50:78	-	-	-	AP Status	wlsxNAccessPointIsDown wlsxTrapAPM wlsxTrapTime: 5/24/2011 22:41:25 U1
5/24/2011 7:40 PM	SNMP Trap	<Unknown>	00:24:6c:c4:c1:50.testdomain	-	-	-	Rogue Detection	wlsxAPEntryChanged wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:41:25 U1 delete(2), wlsxTrapTableGenNumber.0
5/24/2011 7:40 PM	SNMP Trap	<Unknown>	ap125-c0:50:78	-	-	-	Rogue Detection	wlsxAPEntryChanged wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:41:25 U1 delete(2), wlsxTrapTableGenNumber.0
5/24/2011 7:39 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:2b:34	-	-	-	AP Status	wlsxNAccessPointIsUp wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:40:29 U1
5/24/2011 7:39 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:2b:34	-	-	-	Rogue Detection	wlsxAPEntryChanged wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:40:29 U1 create(1), wlsxTrapTableGenNumber.0
5/24/2011 7:39 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:2b:34	-	-	-	Rogue Detection	wlsxAPEntryChanged wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:40:25 U1 delete(2), wlsxTrapTableGenNumber.0
5/24/2011 7:39 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:2b:34	-	-	-	Rogue Detection	wlsxAPEntryChanged wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:40:29 U1 modify(3), wlsxTrapTableGenNumber.C
5/24/2011 7:39 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:2b:34	-	-	-	AP Status	wlsxNAccessPointIsDown wlsxTrapAPM wlsxTrapTime: 5/24/2011 22:40:25 U1
5/24/2011 7:38 PM	SNMP Trap	<Unknown>	00:1a:1e:c0:55:46	-	-	-	AP Status	wlsxNAccessPointIsUp wlsxTrapAPMacA wlsxTrapTime: 5/24/2011 22:39:49 U1

1-10 ▼ of 41967 Device Events Page 1 ▼ of 4197 > > | [Reset filters](#)

[Table 105](#) describes the columns and the information provided in each:

**Table 105** System > Syslog & Traps Columns and Descriptions

Column	Description
<b>Time</b>	The timestamp of the device event.
<b>Type</b>	Either Syslog or SNMP Trap.
<b>Source Device</b>	The name of the device that sent the message. Will be a link if you have visibility to the device. Can be empty if AMP could not correlate the source IP.

**Table 105** *System > Syslog & Traps Columns and Descriptions (Continued)*

Column	Description
<b>AP</b>	Contains a link to the <b>APs/Devices &gt; Monitor</b> page for a device other than the source device that was correlated from some data contained in the message (by LAN MAC, BSSID, or IP Address). Can be blank, and will only be a link if you have visibility to the device.
<b>Client</b>	Displays a user's MAC address if one was found in the message. Can be blank, and will be a link if you have visibility to the user's AP.
<b>Severity</b>	The severity level of the event: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info
<b>Facility</b>	Part of the syslog spec - sort of the logical source of the message. From controllers, will always be one of local0-local7 (you can configure on the controller when sending syslog messages to a particular receiver which facility you want to use in the messages).
<b>Category</b>	If SNMP Trap: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection. For Syslog messages, a category is based on the process name on the controller that sent the syslog message. The categorization for traps and syslog messages only works for events from an Aruba controller.
<b>Message</b>	The raw trap message including the AP MAC Address, time sent, and other information. For syslogs, AMP does not display the numbers at the beginning of the message that indicate the severity and facility. For traps, AMP will attempt to translate them to human-readable format when possible. AMP will not receive processed SNMP traps into the Device Event framework if the AMP doesn't have MIB file to translate the trap.  Use the Search field at the top of the column to filter the messages by a substring.

Syslog messages also appear in the **APs/Devices > Monitor** page for controllers and in **Clients > Client Detail** pages under the **Association History** section.

## Using the System > Event Log Page

The **System > Event Log** page is a very useful debugging tool containing a list of recent AMP events including APs coming up and down, services restarting, and most AMP-related errors as well as the user that initiated the action. [Figure 133](#) illustrates this page, and [Table 106](#) describes the page components.

**Figure 133** *System > Event Log Page Illustration*

Refresh

Time	User	Type	Event	Device ID	Folder
Tue Jan 18 19:33:34 2011	System	Device	Symbol 7131 AP-7131N-1 Error in SNMP polling: Counter length too long (5 bytes)	59914	Top > symbol > fat aps
Tue Jan 18 19:31:00 2011	System	Device	HP ProCurve 2626-PWR other-hp-poe-switch.dev Un-setting upstream device	51805	Top > Routers and switches
Tue Jan 18 19:30:40 2011	System	Device	Dell PowerConnect W-3400 Aruba-3400 Configuration verification: configuration on device does not match desired configuration	60061	Top > aruba > guest user
Tue Jan 18 19:28:48 2011	System	Device	Aruba 651 Intel651-medium Configuration verification: configuration on device does not match desired configuration	60301	Top > aruba
Tue Jan 18 19:28:45 2011	System	Device	Aruba 3200 Aruba3200-3.121 Configuration verification: configuration on device does not match desired configuration	60123	Top > aruba > arm
Tue Jan 18 19:28:37 2011	System	Device	Symbol 7131 AP-7131N-1 Error in SNMP polling: Counter length too long (5 bytes)	59914	Top > symbol > fat aps
Tue Jan 18 19:28:14 2011	System	Device	Aruba 651 Aruba651 Telnet/SSH Error: pattern match timed-out	60215	Top > aruba

**Table 106** *Event Log Fields*

Column	Description
<b>Time</b>	Date and time of the event.
<b>User</b>	The AirWave user that triggered the event. When AirWave itself is responsible, <b>System</b> is displayed.
<b>Type</b>	Displays the Type of event recorded, which is one of four types, as follows: <ul style="list-style-type: none"> <li>● <b>Device</b>—An event localized to one specific device.</li> <li>● <b>Group</b>—A group-wide event.</li> <li>● <b>System</b>—A system-wide event.</li> <li>● <b>Alert</b>—If a trigger is configured to report to the log, an <b>Alert</b> type event will be logged here.</li> </ul>
<b>Event</b>	The event AirWave observed; useful for debugging, user tracking, and change tracking.

## Viewing, Delivering and Responding to Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

- [Viewing Triggers](#)
- [Creating New Triggers](#)

- [Delivering Triggered Alerts](#)
- [Viewing Alerts](#)
- [Responding to Alerts](#)

AirWave monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, AMP generates (or triggers) alerts that enable you to address problems, frequently before users have a chance to report them.

## Viewing Triggers

To view defined system triggers, navigate to the **System > Triggers** page. [Figure 134](#) illustrates this page.

**Figure 134** *System > Triggers Page Illustration (partial view)*

Triggers:

	Type	Trigger	Additional Notification Options	NMS Trap Destinations
<input type="checkbox"/>	Device Resources	Percent CPU Utilization >= 85 % for 15	Email	-
<input type="checkbox"/>	Device Up	Device Type is Access Point	-	-
<input type="checkbox"/>	Inactive Tag	for >= 2 hrs 0 mins	-	-
<input type="checkbox"/>	Device IDS Events	Count > 100 for 30 minutes	-	-
<input type="checkbox"/>	New User	New User Association	NMS	10.51.1.7
<input type="checkbox"/>	Device Down	All device types	NMS	-
<input type="checkbox"/>	Device RADIUS Authentication Issues	Count >= 20 for 15 secs	NMS	10.51.1.7
<input type="checkbox"/>	802.11 Frame Counters	WEP Undecryptable Rate >= 100 frames/sec for 1 hour	-	-
<input type="checkbox"/>	Rogue Device Classified	Classification = Rogue	NMS	10.51.1.7
<input type="checkbox"/>	Radio Down	-	NMS	10.51.1.7

## Creating New Triggers

Perform the following steps to create and configure one or more new triggers. These steps define settings that are required for any type of trigger.

1. To create a new trigger, select the **Add New Trigger** button from the **System > Triggers** page. The page that appears is illustrated in [Figure 135](#).

**Figure 135 Add New Trigger Page Illustration**

**Trigger**

Type:

Severity:

Send Alerts for Thin APs when Controller is Down: ☐ Yes ☒ No

**Conditions**

Matching conditions: ☒ All ☐ Any

Available Conditions: Device Type

New Trigger Condition

Option	Condition	Value
Device Type	is	Access Point

**Trigger Restrictions**

Folder:

Include Subfolders: ☒ Yes ☐ No

Group:

**Alert Notifications**

Additional Notification Options: ☒ Email ☒ NMS

NMS Trap Destinations: ☐ acceptance-test.corp.airwave.com ☒ gauss.corp.airwave.com

[Select All](#) [Unselect All](#)

Sender Address:

Enter multiple email addresses of the form user@domain separated by spaces, commas, or semicolons.

Recipient Email Addresses:

Logged Alert Visibility:

Suppress Until Acknowledged: ☒ Yes ☐ No

2. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.
  - a. The **Trigger Restrictions** settings establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. [Table 107](#) describes the options for trigger restrictions.

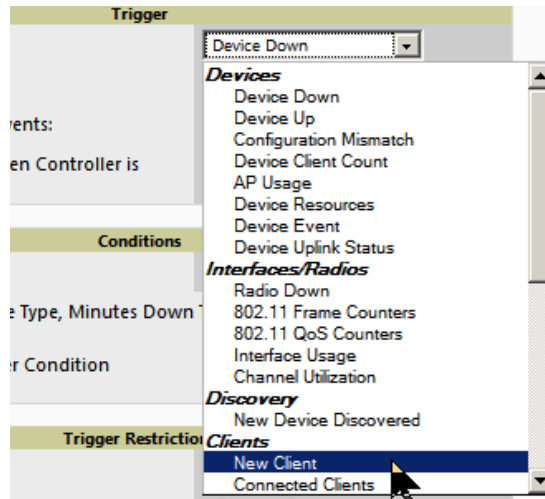
**Table 107 System > Trigger Details Fields and Default Values**

Notification Option	Description
<b>Folder</b>	Sets the trigger to apply only to APs/Devices in the specified folder or subfolders depending on the <b>Include Subfolders</b> option. <b>NOTE:</b> If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.
<b>Include Subfolders</b>	Sets the trigger to apply to all devices in the specified folder and all of the devices in folders under the specified folder.
<b>Group</b>	Sets the trigger to apply only to APs/Devices in the specified group. <b>NOTE:</b> If the trigger is restricted by folder and group, it only applies to the intersection of the two—it only applies to APs in the group and in the folder.

- b. In addition to appearing on the **System > Alerts** page, the **Alert Notifications** settings can be configured to distribute to email or to a network management system (NMS), or to both.
  - If you select **Email**, you are prompted to set the sender and recipient email addresses.
  - If you select **NMS**, you are prompted to choose one or more of the pre-defined trap destinations, which are configured on the **AMP Setup > NMS** page.

- Define the **Logged Alert Visibility**, in which you can choose how this trigger is distributed. The trigger can distribute according to how it is generated (**triggering agent**), or by the **role** with which it is associated.
  - The **Suppress Until Acknowledged** setting defines whether the trigger requires manual and administrative acknowledgement to gain visibility. If **No**, a new alert will be created every time the trigger criteria are met. If **Yes**, an alert will only be received the first time the criteria is met. A new alert for the device is not created until the initial one is acknowledged.
3. In the **Trigger** section, choose the desired trigger **Type** and **Severity**. [Figure 136](#) illustrates some of the supported trigger types. Severity levels are indicated in the email alerts. The alert summary information at the top of the AMP screen can be configured to separately display severe alerts. Refer to [“Configuring Your Own User Information with the Home > User Info Page”](#) on page 213 for more details.

**Figure 136** *System > Triggers > Add Trigger Type Drop-down Menu*



Once you have selected a trigger type, the **Add Trigger** page changes. In many cases, you must configure at least one **Condition** setting. Conditions, settings, and default values vary according to trigger type. Triggers with conditions can be configured to fire if any criteria match as well as if all criteria match.

- Some trigger types share common settings, such as **Duration** (which can be expressed in hours, minutes, seconds, or a combination of these) and **Severity** (from Normal to Critical).
- After you select **Save**, the trigger appears on your next viewing of the **System > Triggers** page with all other active triggers.
- You can edit or delete any trigger as desired from the **System > Triggers** page.
  - To edit an existing trigger, select the pencil icon next to the respective trigger and edit settings in the **Trigger Detail** page described in [Table 108](#).
  - To delete a trigger, check the box next to the trigger to remove, and select **Delete**.

Repeat this procedure for as many triggers and conditions as desired.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- [“Setting Triggers for Devices”](#) on page 190
- [“Setting Triggers for Interfaces and Radios”](#) on page 191
- [“Setting Triggers for Discovery”](#) on page 191
- [“Setting Triggers for Clients”](#) on page 192
- [“Setting Triggers for RADIUS Authentication Issues”](#) on page 193
- [“Setting Triggers for IDS Events”](#) on page 193
- [“Setting Triggers for AMP Health”](#) on page 194

## Setting Triggers for Devices

Perform the following steps to configure device-related triggers.

- a. Choose a device type from the **Devices** listed in the **Type** drop-down menu. See [Figure 136. Table 108](#) itemizes and describes device trigger options and condition settings.

**Table 108** *Device Trigger Types*

Option	Description
<b>Device Down</b>	<p>This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from AMP.</p> <p>To set the conditions for this trigger type, select <b>Add</b> in the <b>Conditions</b> section. Complete the conditions with the <b>Option</b>, <b>Condition</b>, and <b>Value</b> drop-down menus. The conditions establish the device type. Multiple conditions can apply to this type of trigger. The Device Down trigger can be configured to send alerts for thin APs when the controller is down; this behavior is turned off by default.</p> <p>Triggers with the <b>Minutes Down</b> condition enabled will compare the amount of time an AP has been down to the value (in minutes) set for the condition.</p> <p>When the <b>Limit by number of down events</b> is enabled, you can set the number of down events that activate the trigger, as well as the duration of the time window to be measured. AMP will then count the number of times that the device has gone from Up to Down in the specified span of time and display this in the Device Down alert.</p>
<b>Device Up</b>	<p>This trigger type activates when an authorized, previously down AP is now responding to SNMP queries. To set the conditions for this trigger type, select <b>Add</b> in the <b>Conditions</b> section.</p>
<b>Configuration Mismatch</b>	<p>This trigger type activates when the actual configuration on the AP does not match the defined <b>Group</b> configuration policy.</p> <p>To set the conditions for this trigger type, select <b>Add</b> in the <b>Conditions</b> section.</p>
<b>Device Client Count</b>	<p>Activates when a device reaches a user-count threshold for more than a specified period (such as more than 10 users associated for more than 60 seconds).</p>
<b>AP Usage</b>	<p>Activates when the total bandwidth through the device has exceeded a predefined threshold for more than a specified period (such as more than 1500kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting this type displays the following new fields in the <b>Type</b> section. Define these settings.</p> <ul style="list-style-type: none"> <li>• <b>Alert if Device Bandwidth &gt;= (kbps)</b>—This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole.</li> <li>• <b>Bandwidth Direction</b>—Choose <b>In</b>, <b>Out</b>, or <b>Combined</b>. This bandwidth is monitored on the device itself, not on the network as a whole.</li> </ul>
<b>Device Resources</b>	<p>This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined percentage for a specified period of time.</p>
<b>Device Event</b>	<p>This trigger is used for alerting based on SNMP traps and syslog messages, which are displayed in <b>System &gt; Syslogs &amp; Traps</b>, <b>APs/Devices &gt; Monitor</b> for affected devices, and in <b>Clients &gt; Client Detail</b>. The conditions supported are:</p> <ul style="list-style-type: none"> <li>• <b>Event Contents</b> (case insensitive substring matches on message content)</li> <li>• <b>Event Type</b> (syslog or trap)</li> <li>• <b>Syslog Severity</b>: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info</li> <li>• <b>Syslog Category</b></li> <li>• <b>SNMP Trap Category</b>: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection</li> </ul> <p><b>NOTE:</b> During the process of upgrading or installation for non-Master Console/Failover AMPs, AMP creates two default trigger definitions for Device Events:</p> <ul style="list-style-type: none"> <li>• SNMP Trap Category of <b>Hardware</b> or <b>Software</b></li> <li>• Event Type is <b>Syslog</b> and Syslog Severity &gt;= <b>Critical</b></li> </ul>
<b>Device Uplink Status</b>	<p>This trigger deploys whenever a RAP's active uplink changes from Ethernet to USB or vice versa. The corresponding events are captured in a RAP's <b>APs/Devices &gt; Monitor</b> page.</p>

- b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 187](#) to create a new trigger.



## Setting Triggers for Interfaces and Radios

To configure radio- and interface-related triggers, choose a trigger type from the **Interfaces/Radios** category, listed in the **Type** drop-down menu. [Table 109](#) itemizes and describes the radio trigger types and condition settings.

**Table 109** *Radio-Related Trigger Types*

Radio Trigger Options	Description
<b>Radio Down</b>	Indicates that a device's radio is down on the network. Once you choose this trigger type, select <b>Add New Trigger Condition</b> to create at least one condition. This type requires that a radio capability be set as a condition. The <b>Value</b> drop-down menu supports several condition options.
<b>802.11 Frame Counters</b>	Enables monitoring of traffic levels. There are multiple rate-related parameters for which you define conditions including ACK Failures, Retry Rate, and Rx Fragment Rate. See the <b>Option</b> drop-down menu in the <b>Conditions</b> section of the trigger page for a complete list of parameters. Select <b>Add New Trigger Condition</b> to access these settings. Define at least one condition for this trigger type.
<b>802.11 QoS Counters</b>	Enables monitoring of Quality of Service (QoS) parameters on the network, according to traffic type. The rate of different parameters includes ACK Failures, Duplicated Frames and Transmitted Fragments. See the drop-down field menu in the conditions section of the trigger page for a complete list of parameters. Select <b>Add New Trigger Condition</b> to access these settings. Define at least one condition for this trigger type.
<b>Interface Usage</b>	Interface labels defined on the trigger page will be used to set up triggers on one or more interfaces and/or radios. Available conditions are <b>Device Type</b> , <b>Interface Description</b> , <b>Interface Label</b> , <b>Interface Mode</b> , <b>Interface Speed In (Mbps)</b> , <b>Interface Speed Out (Mbps)</b> , <b>Interface Type</b> , and <b>Radio Type</b> .
<b>Channel Utilization</b>	Indicates that channel utilization has crossed particular thresholds. Available conditions are <b>Interference (%)</b> , <b>Radio Type</b> , <b>Time Busy (%)</b> , <b>Time Receiving (%)</b> , and <b>Time Transmitting (%)</b> .

## Setting Triggers for Discovery

Perform the following steps to configure triggers related to device discovery.

- Choose a trigger type from the **Discovery** category, listed in the **Type** drop-down menu. See [Figure 136](#).

**Table 110** *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	Description
<b>New Device Discovered</b>	This trigger type flags the discovery of a new AP, router or switch connected to the network (an device that AMP can monitor and configure). Once you choose this trigger type, select <b>Add New Trigger Condition</b> to specify a <b>Device Type</b> (Access Point, Controller, Remote AP, or Router/Switch)

- Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers”](#) on page 187 to create a new trigger.

## Setting Triggers for Clients

Perform the following steps to configure user-related triggers.

- a. Choose a trigger type from the **Clients** category, listed in the **Type** drop-down menu. See [Figure 136](#). [Table 111](#) itemizes and describes the Client-related trigger types, and condition settings for each discovery trigger type.

**Table 111** Client Trigger Types and Condition Settings

Client Trigger Option	Description
<b>New Client</b>	This trigger type indicates a new user has associated to a device within a defined set of groups or folders. A Filter on connection mode field appears to allow you to filter by <b>Wired</b> or <b>Wireless</b> clients. Note that the <b>New Client</b> trigger type does not require the configuration of any condition settings, so the <b>Condition</b> section disappears.
<b>Connected Clients</b>	This trigger type indicates a device (based on an input list of MAC addresses) has associated to the wireless network. It is required to define one or more MAC addresses with the field that appears.
<b>Client Usage</b>	<p>This trigger type indicates that the sustained rate of bandwidth used by an individual user has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500kbps for more than 120 seconds).</p> <p>Once you choose this trigger type, select <b>Add New Trigger Condition</b> to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The <b>Value</b> field requires that you input a numerical figure for kilobits per second (kbps).</p>
<b>New VPN User</b>	This trigger type indicates a new VPN user has associated to a device within a defined set of groups or folders. Note that the <b>New VPN User</b> trigger type does not require the configuration of any condition settings, so the <b>Condition</b> section disappears.
<b>Connected VPN Users</b>	This trigger type indicates a VPN device (based on an input list of MAC addresses) has associated to the VPN network. It is required to define one or more VPN usernames with the field that appears.
<b>VPN Session Usage</b>	<p>This trigger type indicates that the sustained rate of bandwidth used in an individual VPN session has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500kbps for more than 120 seconds).</p> <p>Once you choose this trigger type, select <b>Add New Trigger Condition</b> to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The <b>Value</b> field requires that you input a numerical figure for kilobits per second (kbps).</p>
<b>Inactive Tag</b>	This trigger type flags events in which an RFID tag has not been reported back to AMP by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.
<b>IPv4 Link-Local Addresses</b>	When enabled, this trigger checks whether the total count of self-assigned IP addresses has crossed a set threshold for clients within a selected folder or group. The alert deployed by this trigger includes a link to search for IP addresses containing 169.254.x.x.
<b>Client Goodput</b>	This trigger type indicates that the goodput for an individual client has exceeded a predefined threshold. Available conditions are Usage Kbps (combined), Usage Kbps (in), and Usage Kbps (out).
<b>Client Speed</b>	This trigger type indicates that the speed for an individual client has exceeded a predefined threshold. The available condition for this trigger is Speed Mbps.

- b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 187](#) to create a new trigger.

## Setting Triggers for RADIUS Authentication Issues

Perform the following steps to configure RADIUS-related triggers.

- a. Choose a trigger type from the **RADIUS Authentication Issues** list in the drop-down **Type** menu. [Table 112](#) itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

**Table 112** *RADIUS Authentication Trigger Types and Condition Settings*

Option	Description
<b>Client RADIUS Authentication Issues</b>	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Select <b>Add New Trigger Condition</b> to specify the count characteristics that trigger an alert. The <b>Option</b> , <b>Condition</b> , and <b>Value</b> fields allow you to define the numeric value of user issues.
<b>Device RADIUS Authentication Issues</b>	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The <b>Option</b> , <b>Condition</b> , and <b>Value</b> fields allow you to define the numeric value of user issues.
<b>Total RADIUS Authentication Issues</b>	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices.

- b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 187](#) to create a new trigger.

## Setting Triggers for IDS Events

Perform the following steps to configure Intrusion Detection System (IDS)-related triggers.

- a. Choose the **Device IDS Events** trigger type from the drop-down **Type** menu. See [Figure 136](#). [Table 113](#) describes condition settings for this trigger type.

**Table 113** *Device IDS Events Authentication Trigger Types and Condition Settings*

IDS Trigger Options	Description
<b>Device IDS Events</b>	This trigger type is based on the number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Alerts can also be generated for traps based on name, category or severity. Select <b>Add New Trigger Condition</b> to specify the count characteristics that trigger an IDS alert.
<b>Rogue Device Classified</b>	This trigger type indicates that a device has been discovered with the specified Rogue Score. Ad-hoc devices can be excluded automatically from this trigger by selecting <b>Yes</b> . See <a href="#">“Using RAPIDS and Rogue Classification” on page 167</a> for more information on score definitions and discovery methods.  Once you choose this trigger type, select <b>Add New Trigger Condition</b> to create one or more conditions. A condition for this trigger enables you to specify the nature of the rogue device in multiple ways.
<b>Client on Rogue AP</b>	This trigger type indicates that a client has associated to a rogue AP. Available conditions include rogue classification, and whether the client is valid.

- b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 187](#) to create a new trigger.

## Setting Triggers for AMP Health

After completing steps 1-3 in “[Creating New Triggers](#)” on page 187, perform the following steps to configure IDS-related triggers.

- a. Choose the **Disk Usage** trigger type from the drop-down **Type** menu. See [Figure 136](#) for trigger types. [Table 114](#) describes the condition settings for this trigger type.

**Table 114** *Disk Usage Trigger and Condition Settings*

AMP Health Trigger	Description
<b>Disk Usage</b>	This trigger type is based on the disk usage of AMP. This type of trigger indicates that disk usage for the AMP server has met or surpassed a defined threshold. Select <b>Add New Trigger Condition</b> to specify the disk usage characteristics that trigger an alert. Set one of these triggers at <b>90%</b> so you receive a warning before AMP suffers performance degradation due to lack of disk space.

- b. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “[Creating New Triggers](#)” on page 187 to create a new trigger.

## Delivering Triggered Alerts

AMP uses Postfix to deliver alerts and reports via email because it provides a high level of security and queues email locally until delivery. If AMP is located behind a firewall, preventing it from sending email directly to a specified recipient, use the following procedures to forward email to a smarthost.

1. Add the following line to `/etc/postfix/main.cf`:

```
relayhost = [mail.example.com]
where mail.example.com is the IP address or hostname of your smarthost
```

2. Run `service postfix restart`.

3. Send a test message to an email address:

```
Mail -v user@example.com
Subject: test mail
.
CC:
```

4. Press **Enter**.

5. Check the mail log to ensure mail was sent:

```
tail -f /var/log/maillog
```

## Viewing Alerts

Apart from visiting **System > Alerts**, AMP displays alerts and provides alert details in two additional ways:

1. The **Alert Summary** table is available on the following AMP pages, and is illustrated in [Figure 137](#):
  - **APs/Devices > List**
  - **Groups > Monitor**
  - **Home > Overview**
  - **Clients > Connected** or **Client Detail**

**Figure 137 Alert Summary Table Illustration**

Alert Summary				
Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	138	2300	2950	10/17/2011 2:47 PM
IDS Events	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

This table displays alerts as follows; select the alert **Type** to display alert details:

- **AMP Alerts**—Displays details for all device alerts.
- **IDS Events**—Displays details of all Intrusion Detection System (IDS) events and attacks under the RAPIDS tab. You must be enabled as a RAPIDS user to see this page.
- **RADIUS Authentication Issues**—Displays RADIUS-related alerts for devices in the top viewable folder available to the AMP user. The detailed list displays the MAC address, username, AP, radio, controller, RADIUS server, and time of each event. Alerts can be sorted by any column.

- The **Alerts** and **Severe Alerts** top header stats in the **Status** bar at the top of all AMP pages, illustrated in Figure 138. The Severe Alert Threshold can be configured on the **Home > User Info** page. Refer to “Setting Severe Alert Warning Behavior” on page 34.

**Figure 138 Alerts in the AMP Status Bar (highlighted)**

New Devices: 210	Up: 278	Down: 139	Mismatched: 117	Rogue: 1945	Users: 61	Alerts: 2710	Severe Alerts: 87
------------------	---------	-----------	-----------------	-------------	-----------	--------------	-------------------

Select the **Alerts** or the **Severe Alerts** counter or navigate to the **System > Alerts** page. Figure 139 illustrates this page.

**Figure 139 System > Alerts Page Illustration**

	Trigger Type	Trigger Summary	Triggering Agent	Time ▼	Severity
<input type="checkbox"/>	User Bandwidth	>= 100 kbps for 30 seconds	00:18:DE:09:B9:09	2/12/2007 12:54 PM	Warning
<input type="checkbox"/>	Device Up		hp-530-1	2/12/2007 12:32 PM	Normal
<input type="checkbox"/>	Device Down		hp-530-1	2/12/2007 12:27 PM	Critical
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Unknown Lo-72:8F:26	2/12/2007 11:51 AM	Minor
<input type="checkbox"/>	Device Up		roamabout-4102-3	2/12/2007 10:24 AM	Normal
<input type="checkbox"/>	Device Down		roamabout-4102-3	2/12/2007 10:19 AM	Critical

For each new alert, the **System > Alerts** page displays the items listed in Table 115.

**Table 115 System > Alerts Fields and Default Settings**

Field	Description
<b>Trigger Type</b>	Displays and sorts triggers by the type of trigger.
<b>Trigger Summary</b>	Provides an additional summary information related to the trigger.
<b>Triggering Agent</b>	Lists the name of the AP that generated the trigger. Select the name to display its <b>APs/ Devices &gt; Manage</b> page.
<b>Time</b>	Displays the date and time the trigger was generated.
<b>Severity</b>	Displays the severity code associated with that trigger.

## Responding to Alerts

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active status if it is unresolved. The alert remains on the **New Alerts** list until you acknowledge or delete it. If an alert already exists, the trigger for that AP or user does not create another alert until the existing alert has been acknowledged or deleted.
- Move the alert to the Alert Log by selecting it and selecting **Acknowledge**.
- You may see all logged alerts by selecting the **View logged alerts** link at the top of the **System > Alerts** page. Select the **New Alerts** link to return to the list of new alerts.
- Delete the alert by selecting it from the list and selecting **Delete**.

## Monitoring and Supporting WLAN Clients

The AMP **Users** pages support WLAN users in AMP. This section describes the **Clients** pages as follows:

- Overview of the Clients Pages
- Monitoring WLAN Users in the Clients > Connected and Clients > All Pages
- Supporting Guest WLAN Users With the Clients > Guest Users Page
- Supporting RFID Tags With the Clients > Tags Page
- See also [Evaluating and Diagnosing User Status and Issues](#).

For information about creating AMP users and AMP user roles, refer to:

- [Creating AirWave Users](#)
- [Creating AirWave User Roles](#)

If you need to create an AMP user account for frontline personnel who are to support Guest WLAN users, refer to [“Supporting Guest WLAN Users With the Clients > Guest Users Page” on page 199](#).

### Overview of the Clients Pages

The **Clients** pages display multiple types of user data for existing WLAN clients and VPN users. The data comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and AMP-generated data. AMP supports the following **Clients** pages:

- **Clients > Connected**—Displays active users that are currently connected to the WLAN. Refer to [“Monitoring WLAN Users in the Clients > Connected and Clients > All Pages” on page 196](#).
- **Clients > All**—Displays all users of which AMP is aware, with related information. Non-active users are listed in gray text. For a description of the information supported on this page, refer to [“Monitoring WLAN Users in the Clients > Connected and Clients > All Pages” on page 196](#).
- **Clients > Guest Users**—Displays all guest users in AMP and allows you to create, edit, or delete guest users. See [“Supporting Guest WLAN Users With the Clients > Guest Users Page” on page 199](#).
- **Clients > Client Detail**—Displays client device information, alerts, signal quality, bandwidth, and association history. This page appears when you select a user’s MAC address link from these list tables:

- **Clients > Connected**
- **Clients > All**
- **Home > Search** page results that display the user MAC address

See [“Evaluating User Status with the Clients > Client Detail Page” on page 203](#).

- **Clients > Diagnostics**—Displays possible client device issues, diagnostic summary data, user counts, AP information, 802.11 counters summary, and additional information. This page appears when you select a user’s MAC address from one of the following pages:

- **Clients > Connected**
- **Clients > All**
- **Home > Search** page results or **Search** field results that display the user MAC address

See [“Evaluating Client Status with the Clients > Diagnostics Page” on page 207](#).

- **Clients > Tags**—Displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that is monitored by AMP. [“Supporting RFID Tags With the Clients > Tags Page” on page 202](#).

### Monitoring WLAN Users in the Clients > Connected and Clients > All Pages

The **Clients > Connected** page displays all users currently connected in AMP, and is illustrated in [Figure 140](#) and described in [Table 116](#). This page contains the following information at a glance:

- The Folder field shows the current folder of Connected Clients you are viewing. You can view users under a particular folder from the Go to folder dropdown menu.



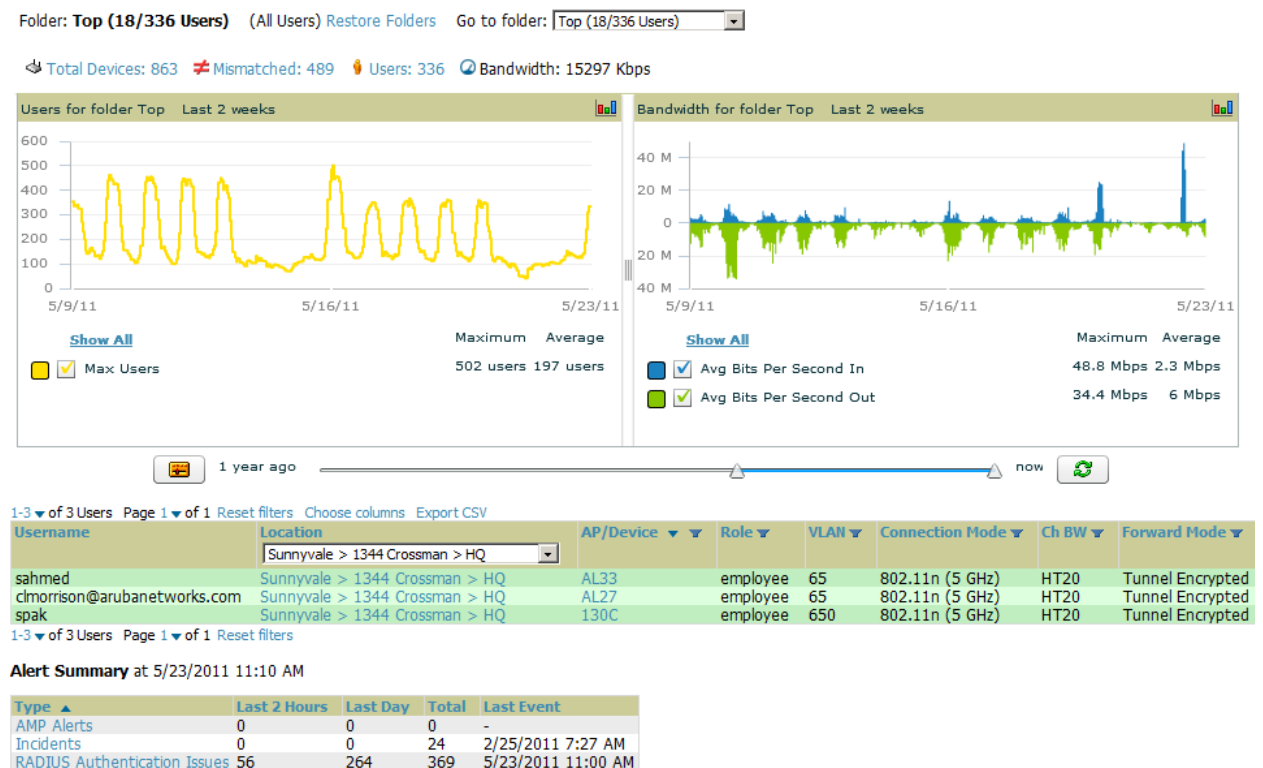
- Links under the Folder fields showing the **Total Devices**, **Mismatched**, **Clients**, and **Bandwidth** (a static, unlinked statistic) summarize the device information for this folder. Select these links to be taken to detail pages for each: **Total Devices** redirects to the **APs/Devices > List** for that folder, **Mismatched** redirects to the list in **APs/Devices > Mismatched** for that folder, and selecting **Clients** refreshes the page but expands to include users in the subfolders.
- Interactive graphs display average and max **Clients** over time, and **Usage** in and out for the selected folder over time.
- Below the Clients and Usage graphs is the list of connected users

The information on this page can be adjusted in the following ways:

- Drag the slider to pick the time range on the interactive graphs, and select **Show All** to select other options to display.
- The **Alert Summary** section displays custom configured alerts that were defined in the **System > Alerts** page.
- Use the **Filter** icon (🔍) next to certain columns (**AP/Device**, **Role**, **VLAN**, **Connection Mode**, and others) to filter the results by one of the values under that column. You can filter the list by substring match under the **Username** column.

The **Clients > Connected** page includes SSID information for users, and can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

**Figure 140 Clients > Connected Page Illustration (Partial View)**



**Table 116 Clients > Connected Table Columns and Links (Alphabetical)**

Field	Description
<b>AOS Device Type</b>	The type of client device determined by the Aruba controller -- a fallback in case the rules set in <b>AMP Setup &gt; Device Type Setup</b> were unable to determine the device type.
<b>AP/Device</b>	Displays the name of the AP to which the MAC address is associated as a link to this AP's <b>APs/Devices &gt; Monitor</b> page.
<b>Association Time</b>	The first time AMP recorded the user for this association.



**Table 116** *Clients > Connected Table Columns and Links (Continued)(Alphabetical)*

Field	Description
<b>Auth. Time</b>	The how long ago the user authenticated. <b>NOTE:</b> This value displays as a negative number for unauthenticated users.
<b>Auth. Type</b>	The type of authentication employed by the user: <ul style="list-style-type: none"> <li>WPA2 (EAP-PEAP) is the standard setting.</li> <li>EAP is reported by Aruba devices via SNMP traps.</li> <li>RADIUS accounting servers integrated with AMP will provide the RADIUS Accounting Auth type.</li> <li>Web (PAP) - Captive Portal.</li> <li>All others are considered to be not authenticated.</li> </ul>
<b>Usage</b>	The average bandwidth consumed by the MAC address.
<b>Ch BW</b>	The channel bandwidth that currently supports 802.11n users.
<b>Cipher</b>	Displays WEP with keys. This data is also displayed in the <b>Client Session</b> report in the <b>Session Data By Client</b> section.
<b>Connection Mode</b>	The Radio mode used by the user to associate to the AP for 802.11n clients.
<b>Device Type</b>	The type of device determined by <b>AMP Setup &gt; Device Type Setup</b> rules.
<b>Duration</b>	The length of time the MAC address has been associated.
<b>EAP Supplicant</b>	The party being authenticated in the Extensible Authentication Protocol.
<b>Forward Mode</b>	Forwarding mode for the port: Bridge, Tunnel, or Split Tunnel.
<b>Goodput</b>	The ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.
<b>Group</b>	The group containing the AP that the user is associated with.
<b>Guest User</b>	Specifies whether the user is a guest.
<b>Interface</b>	The interface on the device to which the user is connected.
<b>LAN Hostname</b>	The LAN hostname of the user MAC.
<b>LAN IP Address</b>	The IP assigned to the user MAC. AMP gathers it from the association table of APs.
<b>Location</b>	If a value appears here, the location of this user's client has been mapped on VisualRF. Select the location to open a new VisualRF Floor Plan Location window.
<b>MAC Address</b>	The radio MAC address of the user associated to APs as a link to the <b>Users &gt; Detail</b> page for this user.
<b>Manufacturer</b>	The manufacturer of the user's device.
<b>Model</b>	The model of the user's device.
<b>Name</b>	The product of the user's device.
<b>Network Chipset</b>	The chipset indicates the functions the device was designed to perform.
<b>Network Driver</b>	Driver name or other information.
<b>Notes</b>	Free notes about the user.
<b>OS</b>	The device's operating system type.
<b>OS Detail</b>	Additional information on the operating system such as version numbers.
<b>Phone Number</b>	Contact number for the user.
<b>Role</b>	Specifies the role that an Aruba controller assigned to the connected user, such as "employee".

**Table 116** *Clients > Connected Table Columns and Links (Continued)(Alphabetical)*

Field	Description
<b>Serial Number</b>	Serial number of the device.
<b>Service End</b>	Ending timestamp of the device usage.
<b>Service Start</b>	Beginning timestamp of the device usage.
<b>Sig. Qual.</b>	The average signal quality the user experienced.
<b>SSID</b>	The SSID with which the user is associated.
<b>Speed</b>	The packet and byte counts of data frames successfully transmitted to and received from associated stations.
<b>Tunneled Controller</b>	If a user is connected to an Aruba Mobility Switch, indicates which controller the user is authenticated to.
<b>Username</b>	Displays the name of the user associated to the AP. AMP gathers this data from device traps, SNMP polling, or RADIUS accounting. Usernames appear in italics when a username for that MAC address has been stored in the database from a previous association, but AMP is not getting a username for the current association. This may indicate that the user has not yet been authenticated for this session or AMP may not be getting a username from an external source.
<b>VLAN</b>	Displays the VLAN assigned to the user, if available.

## Supporting Guest WLAN Users With the Clients > Guest Users Page

AMP supports guest user provisioning for Dell PowerConnect W, Aruba Networks, Inc., Alcatel-Lucent and Cisco WLC devices. This allows frontline staff such as receptionists or help desk technicians to grant wireless access to WLAN visitors or other temporary personnel.



The Guest User Preferences section on **AMP Setup > Roles**, as well as the **Clients > Guest Users** subtab, will not appear if **Guest User Configuration** is globally disabled in **AMP Setup > General**.

Perform the following steps in the pages described to configure these settings.

1. Navigate to the **AMP Setup > Roles** page and select the **Read-Only Monitoring & Auditing** role type. Under **Guest User Preferences**, enable **Allow creation of Guest Users**.
2. Next, navigate to the **AMP Setup > Users** page and create a new user with the role that was just created. [Figure 141](#) illustrates this page.

**Figure 141** *AMP Setup > Users Page Illustration*

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users.
4. The next step in creating a guest access user is to navigate to the **Users > Guest Clients** tab. From this tab, you can add new guest users, you can edit existing users, and you can repair guest user errors.

This page displays a list of guest users and data, to include the expiration date, the SSID (for Cisco WLC) and other information. [Figure 142](#) illustrates this page and [Table 117](#) describes the information.

**Figure 142** *Clients > Guest Users Page Illustration*

**Guest Users:**

[Repair guest user errors](#)

[Add](#) New Guest User

1-4 ▼ of 4 Guest Users Page 1 ▼ of 1

		Username	Enabled	Email	Company Name	Sponsor Name	Expiration	Profile ▼	Status
<input type="checkbox"/>		rzajnnqw	Yes	vfranc@airess.com	Airess	vfranc	Never	-	Error - Failed to Configure
<input type="checkbox"/>		zserkxmm	Yes	-	-	bob	Never	-	Error - Failed to Configure
<input type="checkbox"/>		bobob	No	bobob@nowhere.com	arus networks	arus	5/27/2009 12:00 AM	-	User Expired
<input type="checkbox"/>		jestwrqg	Yes	-	-	Oriol	6/5/2009 12:00 PM	-	User Expired

Select All - Unselect All

[Print](#) [Delete](#)

**Table 117** *Clients > Guest Users Fields*

Field	Description
<b>Repair Guest User Errors</b>	Sets AMP to attempt to push the guest user again in an attempt to repair any errors in the <b>Status</b> column.
<b>Add New Guest User</b>	Adds a new guest user to a controller via AMP.
<b>Username</b>	Randomly generates a user name for privacy protection. This name appears on the <b>Guest User</b> detail page.
<b>Enabled</b>	Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled).
<b>Email</b>	Displays the optional email address of the user.
<b>Company Name</b>	Displays the optional company name for the user.
<b>Sponsor Name</b>	Displays the name of the sponsor for the guest user. This setting is optional.
<b>Expiration</b>	Displays the date the guest user's access is to expire.
<b>WLAN Profile</b>	Sets the SSID that the guest user can access. This setting applies to Cisco WLC only.
<b>Status</b>	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and select the <b>Repair guest user errors</b> button.

Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **Guest User** column. The **Client Detail** page for a guest user also contains a box with the same guest information that appears for each user on the **Clients > Guest Users** list.



**NOTE**

The **Enabled**, **Sponsor Name**, **WLAN Profile**, and **Status** columns can be filtered using the funnel icon (🔍).

- To add a new guest user, select **Add**, and complete the fields illustrated in [Figure 143](#). [Table 117](#) above describes most fields. The first three fields are required, and the remaining fields are optional.

**Figure 143 Clients > Guest Users > Add New Guest User Page Illustration**

Guest User

Username:

Generate

Password:

Generate

Name:

Enabled:

☒ Yes ☐ No

Email:

Company Name:

Sponsor Name:

Specify numeric dates with optional 24-hour times (like **7/4/2003** or **2003-07-04** for July 4th, 2003, or **7/4/2003 13:00** for July 4th, 2003 at 1:00 PM.), or specify relative times (like **tomorrow at noon** or **next tuesday at 4am**). Other input formats may be accepted.

Expiration: Blank means no expiration

WLAN Profile:

Description:

Email Options

Email Credentials:

☐ Yes ☒ No

Add

Cancel

To make the Username or Password anonymous and to increase security, complete these fields then select **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

6. Select **Add** to complete the new guest user, or select **Cancel** to back out of new user creation. The **Clients > Guest Users** page appears and displays results, as applicable.

## Supporting VPN Users with the Clients > VPN Sessions Page

The **Clients > VPN Sessions** page shows active VPN Sessions along with device type and HTTP fingerprinting information.

**Figure 144 Clients > VPN Sessions Page Illustration**

Folder: [Top \(0/9 VPN Sessions\)](#) > **VPN (9)** [Expand folders to show all VPN Sessions](#) Go to folder:

Total Devices: 2

Mismatched: 2

VPN Sessions: 9

Clients for folder VPN Last 17 hours

Show All

☒ Avg VPN Sessions

Maximum

Average

33 sessions

19 sessions

☒ Max VPN Sessions

Maximum

Average

33 sessions

19 sessions

Usage for folder VPN Last 17 hours

Show All

☒ Avg Bits Per Second In for VPN Sessions

Maximum

Average

1.4 Mbps

302.5 kbps

☒ Avg Bits Per Second Out for VPN Sessions

Maximum

Average

0 bps

0 bps

☒ Max Bits Per Second In for VPN Sessions

Maximum

Average

1.4 Mbps

302.5 kbps

☒ Max Bits Per Second Out for VPN Sessions

Maximum

Average

0 bps

0 bps

1 year ago

now

1-5 of 9 VPN Sessions Page 1 of 2 > | [Reset filters](#) [Choose columns](#) [Export CSV](#)

Controller	Group	Folder	Type	VLAN	Duration	Usage	AOS Device Type	IP Address	Username	Aruba HTTP Finger
hq-via-01	VPN	Top > VPN	VPN	1	1 day 2 hrs 58 mins	79.61 Kbps	OS X	10.240.105.224	cjoseph	Mozilla/5.0 (Macint
hq-via-01	VPN	Top > VPN	VPN	1	3 hrs 41 mins	29.86 Kbps	OS X	10.240.104.54	hstonebraker	Mozilla/5.0 (Macint
hq-via-01	VPN	Top > VPN	VPN	1	3 days 8 hrs 56 mins	23.28 Kbps	OS X	10.240.105.250	jziegler	Mozilla/5.0 (Macint
hq-via-01	VPN	Top > VPN	VPN	1	1 hr 39 mins	18.56 Kbps	OS X	10.240.104.164	ctang	Mozilla/5.0 (Macint
hq-via-01	VPN	Top > VPN	VPN	1	1 hr 3 mins	15.43 Kbps	OS X	10.240.104.207	eparker	Mozilla/5.0 (Macint

1-5 of 9 VPN Sessions Page 1 of 2 > | [Reset filters](#)

Alert Summary at 10/24/2011 6:48 PM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-

When a VPN username is selected, a **Clients > VPN User Detail** displays with current VPN sessions, a user and bandwidth interactive graph, and a historical VPN sessions list table.

AirWave | User Guide

Performing Daily Administration in AirWave | 201

## Supporting RFID Tags With the Clients > Tags Page

Radio Frequency Identification (RFID) supports identifying and tracking wireless devices with radio waves. RFID uses radio wave tags for these and additional functions. Active tags have a battery and transmit signals autonomously, and passive tags have no battery. RFID tags often support additional and proprietary improvements to network integration, battery life, and other functions.



Guest users being pushed to large numbers of controllers may take a very long time to push.

The **Clients > Tags** page displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that AMP monitors. AMP displays the information it receives from the controller in a table on this page. [Figure 145](#) illustrates this page, and [Table 118](#) describes fields and information displayed.



The **Vendor**, **Battery Level**, and **Chirp Interval** columns can be filtered using the funnel icon ( ).

**Figure 145** *Clients > Tags Page Illustration*

Tags

1-5 ▼ of 5 Tags Page 1 ▼ of 1

Name	MAC Address	Vendor	Battery Level	Chirp Interval	Last Seen ▼	Closest AP
CD-Burner	00:14:7E:00:14:7E	PanGo Networks, Inc.	Normal	2 mins	1/23/2009 1:19 PM	HQ-Engineering
-	00:14:7E:00:14:7E	InnerWireless	Normal	4 mins	1/23/2009 6:44 AM	-
Water-Cooler	00:14:7E:00:14:7E	Aeroscout Ltd.	-	12 secs	1/22/2009 5:35 AM	-
-	00:14:7E:00:14:7E	InnerWireless	Normal	1 min	1/20/2009 4:13 PM	-

**Table 118** *Clients > Tags Fields*

Field	Description
<b>Name</b>	Displays the user-editable name associated with the tag.
<b>MAC Address</b>	Displays the MAC address of the AP that reported the tag.
<b>Vendor</b>	Displays the vendor of the tag (Aeroscout, PanGo and Newbury)—display all or filter by type.
<b>Battery Level</b>	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.
<b>Chirp Interval</b>	Displays the tag chirp frequency or interval, filterable from the drop-down menu at the top of the column. Note that the chirp interval from the RFID tag influences the battery life of active tags as well as search times. If a tag chirps with very long chirp interval, it may take longer time for the location engine to accurately measure x and y coordinates.
<b>Last Seen</b>	Date and time the tag was last reported to AMP.
<b>Closest AP</b>	The AP that last reported the tag to the controller (linked to the AP monitoring page in AMP).

- To edit the name of the tag, or to add notes to the tag's record, select the pencil icon next to the entry in the list. You can then add or change the name and add notes like “maternity ward inventory” or “Chicago warehouse,” as two examples.
- The **Inactive Tag** trigger can be used to generate an alert if a tag is not reported to AMP after a certain interval. This can help to identify lost or stolen inventory. For more information about enabling this trigger, refer to the section “[Monitoring and Supporting AMP with the System Pages](#)” on page 183.

## Evaluating and Diagnosing User Status and Issues

If a WLAN user reports difficulty with the wireless network, the administration or Helpdesk personnel can view and process related user information from the **Client Detail** and **Diagnostic** pages. This section describes these two pages as follows:

- [Evaluating User Status with the Clients > Client Detail Page](#)
- [Evaluating Client Status with the Clients > Diagnostics Page](#)

### Evaluating User Status with the Clients > Client Detail Page

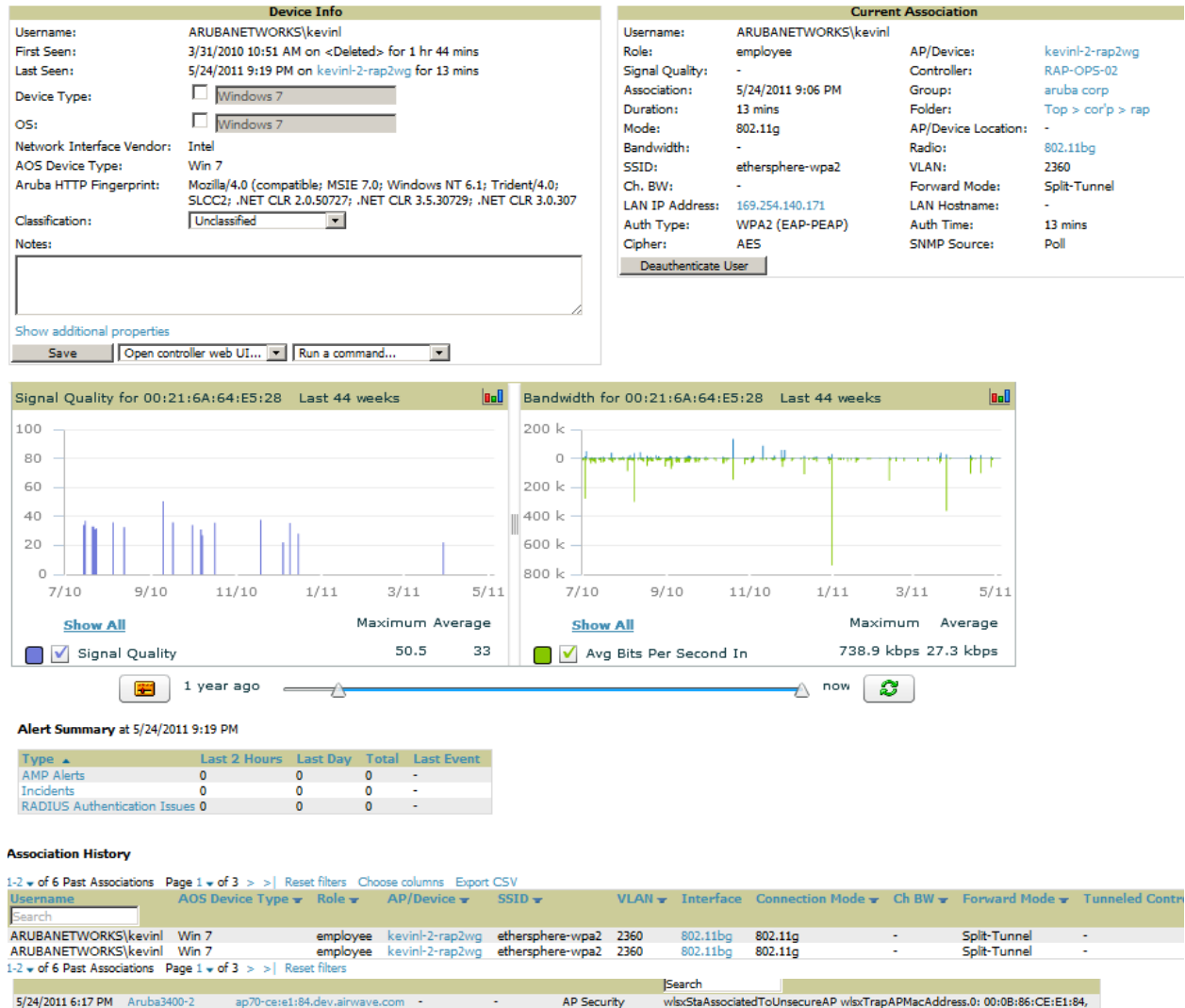
The **Clients > Client Detail** page is a focused subtab that becomes visible when you select a specific WLAN user. Access the **Clients > Client Detail** page by selecting the **MAC Address** link for a specific user from one of the following pages:

- **Clients > Connected**
- **Clients > All**
- **Home > Search** page results or **Search** field **Client** results that display the user MAC address

This page provides information for the wireless device, signal quality, and bandwidth consumption. This page also provides an AP association history and current association status. Finally, if VisualRF is enabled in **AMP Setup > General**, this page provides a graphical map of the user location and facility information.

[Figure 146](#) illustrates the contents of **Clients > Client Details** page.

**Figure 146** *Clients > Client Detail Page Illustration (partial view)*



## Mobile Device Access Control in Clients > Client Detail and Clients > Connected

Mobile Device Access Control (MDAC) secures, provisions and manages network access for Apple® iOS and other employee-owned mobile devices by enabling device fingerprinting, device registration, and increased device visibility. Refer to <http://www.arubanetworks.com/technology/mobile-device-access-control/> for more information on MDAC.

Use the checkbox next to these fields to enable them in **Clients > Client Detail**:

- Device Type
- OS
- OS Detail
- Manufacturer

To see more options, select the **Show additional properties** link. The results are illustrated in [Figure 147](#):



**Figure 147** *Device Info* section in **Clients > Client Detail** after **Show additional properties** is selected

Detail for **DC:2B:61:5E:A1:13**

Device Info	
Name:	<input type="checkbox"/> <input type="text"/>
Username:	jhao
First Seen:	11/15/2010 4:09 PM on 1154-Q for 1 hr 1 min
Last Seen:	5/25/2011 2:14 PM on 78C for 2 mins
Device Type:	<input type="checkbox"/> Apple iPhone
OS:	<input type="checkbox"/> iOS
OS Detail:	<input type="checkbox"/> 4.3.1 (4; 16GB)
Manufacturer:	<input type="checkbox"/> Apple
Model:	<input type="checkbox"/> iPhone
Serial Number:	<input type="checkbox"/> <input type="text"/>
Phone Number:	<input type="checkbox"/> <input type="text"/>
Network Interface Vendor:	Apple
Network Chipset:	<input type="checkbox"/> <input type="text"/>
Network Driver:	<input type="checkbox"/> <input type="text"/>
EAP Supplicant:	<input type="checkbox"/> <input type="text"/>
Asset ID:	<input type="checkbox"/> <input type="text"/>
Asset Group:	<input type="checkbox"/> <input type="text"/>
Asset Category:	<input type="checkbox"/> <input type="text"/>
Service Start:	<input type="checkbox"/> <input type="text"/>
Service End:	<input type="checkbox"/> <input type="text"/>
AOS Device Type:	iPhone
Aruba HTTP Fingerprint:	iTunes-iPhone/4.3.1 (4; 16GB)
Classification:	<input type="text" value="Valid"/>
Notes:	<div></div>

[Hide additional properties](#)

## Classifying Aruba Devices in Client Detail

If you have deployed Aruba controllers and have WMS Offload enabled on the network, the **Clients > Client Detail** page allows you to classify the device in the **Device Information** section, and to push this configuration to the Aruba controllers that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—If the **Protect Valid Stations** option is enabled, this setting designates the device as a legitimate network device. Once this **Valid** setting is pushed, this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—When this status is pushed to the device, Aruba controllers will attempt to keep it contained from the network.

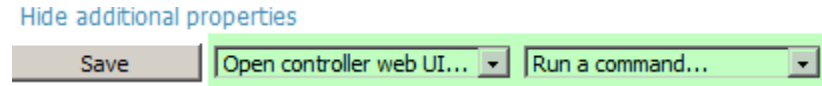
You can classify the user regardless of whether WMS Offload is enabled. If WMS Offload is enabled, the classification will get pushed up to the controller.

## Quick Links for Clients on Aruba Devices

In **Clients > Client Detail**, two drop-down menus were added in AirWave 7.3 next to the **Save** button in the **Device Info** section:

- **Open controller web UI:** A drop-down menu that allows you to jump to the controller's UI in a new window. Thin APs link to **Controller > Access Points** when not operating in mesh mode, or **Controller > Mesh Nodes** otherwise. Controllers show several more pages in this menu (**Security Dashboard**, for instance) if the controller is running AOS version 6.1 or greater.
- **Run a command:** A drop-down menu with a list of CLI commands you can run directly from the **APs/Devices > Monitor** page.

**Figure 148** *Open controller web UI and Run a command Menus in Clients > Client Detail*



## Using the Deauthenticate Client Feature

Some displays of the **Clients > Client Detail** page include the **Deauthenticate Client** feature in the **Current Association** section. Specifically, those displays are for devices which support this operation, namely Aruba and Cisco WLC with firmware version v4.0.0.0 or later.

Select **Deauthenticate Client** to use this feature, as shown in [Figure 149](#):

**Figure 149** *Deauthenticate Client button in Current Association section of Clients > Client Detail*

Current Association			
Username:	gfesta	AP/Device:	00:24:6c:c8:63:7a
Role:	employee	Controller:	sjcwifi01
Signal Quality:	18	Group:	Ethersphere
Association:	11/3/2011 1:13 PM	Folder:	Top > Ethersphere
Duration:	21 mins	AP/Device Location:	-
Mode:	802.11n (2.4 GHz)	Radio:	802.11bgn
Usage:	-	VLAN:	65
SSID:	ethersphere-wpa2	Forward Mode:	Tunnel Encrypted
Ch. BW:	HT20	LAN Hostname 1:	gerard-festa.arubanetworks.com
LAN IP 1:	10.6.5.49	Auth Time:	21 mins
Auth Type:	WPA2/EAP	SNMP Source:	Poll
Cipher:	AES		
Deauthenticate Client			

## Viewing a Client's Association History

Past association details of a client are tracked in the **Association History** table, which is located under the VRF QuickView illustration (if available) and the **Alert Summary** in **Clients > Client Detail**.

The columns in this table, shown in [Figure 150](#), are the same as the fields in the **Current Association** section for this user.

**Figure 150** *Association History in Clients > Client Detail*

Association History										
1-2 of 5 Past Associations Page 1 of 2 >   Reset filters Choose columns Export CSV										
Username	AOS Device Type	Role	AP/Device	SSID	VLAN	Interface	Connection Mode	Ch BW	Forward Mode	Tunneled Controller
ARUBANETWORKS\sdas	Windows 7	employee	1154-Q	ethersphere-wpa2	105	802.11an	802.11n (5 GHz)	HT40	Tunnel Encrypted	-
ARUBANETWORKS\sdas	Windows 7	employee	sdas-rap2vvg	ethersphere-wpa2	2360	802.11bg	802.11g	-	-	-
1-2 of 5 Past Associations Page 1 of 2 >   Reset filters										

## Viewing the Rogue Association History for a Client

Past association details of a rogue client are tracked in the **Rogue Association History** table, which is located under the Association History table in **Clients > Client Detail**.

**Figure 151 Rogue Association History table in Clients > Client Detail**

**Rogue Association History**

1-3 ▼ of 5 Past Rogue Associations Page 1 ▼ of 2 > | Choose columns Export CSV

Rogue AP ▼	SSID	BSSID	First Heard	Last Heard	Location	Signal	SNR	Connection Mode	Ch BW	Channel
Aruba-97:33:F0	lyncl	00:1A:1E:97:33:F0	8/30/2011 10:25 AM	8/30/2011 10:25 AM	-	-71	15	802.11n (5 GHz)	HT40	44
Aruba-80:86:00	RSN2OfficeWLAN	00:24:6C:80:86:08	9/1/2011 12:24 PM	9/1/2011 12:24 PM	-	-	-	802.11n (5 GHz)	HT40	40
Aruba-80:86:00	RSN2OfficeWLAN	00:24:6C:80:86:08	9/1/2011 1:54 PM	9/1/2011 1:54 PM	-	-80	12	802.11n (5 GHz)	HT40	48

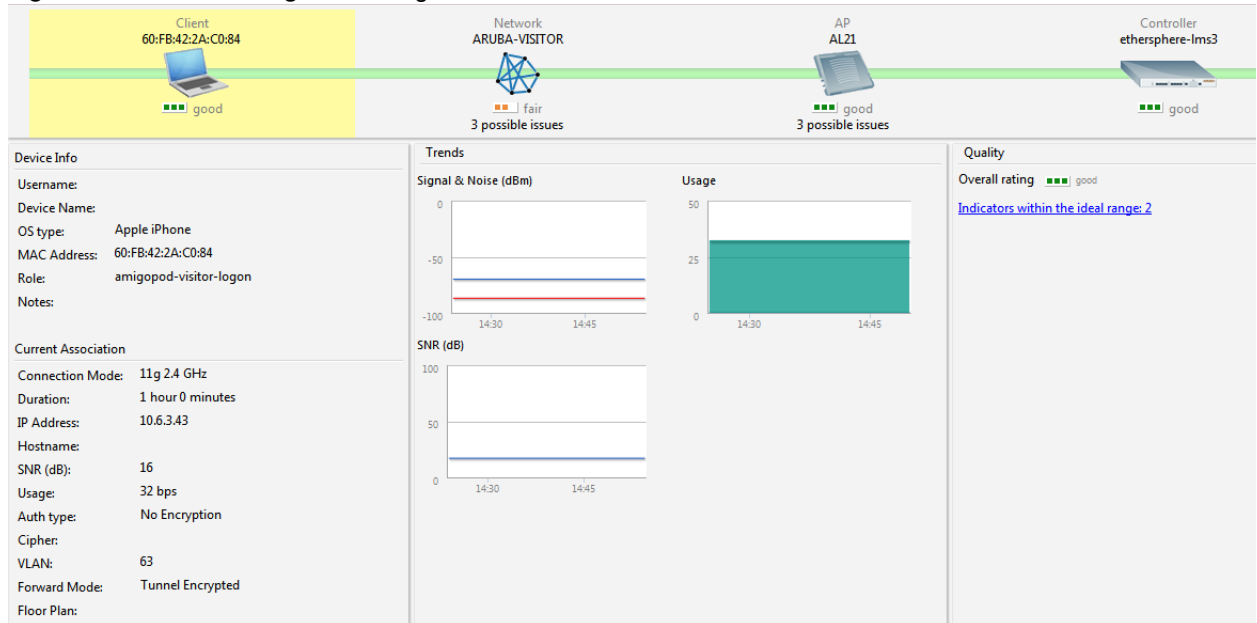
1-3 ▼ of 5 Past Rogue Associations Page 1 ▼ of 2 > |

## Evaluating Client Status with the Clients > Diagnostics Page

The **Clients > Diagnostics** page is accessible from the **Clients > Client Detail** page. You can also search for a user and select the associated MAC address from the search results.

This page provides an overview of a WLAN user's general status and connectivity on the network, as illustrated in [Figure 152](#).

**Figure 152 Clients > Diagnostics Page Illustration**



Each section of the **Clients > Diagnostics** page displays information by which to evaluate possible user issues.

## Managing Mobile Devices with SOTI MobiControl and AirWave

### Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Apple, and Android devices, has been integrated into AirWave to provide direct access to the MobiControl Web Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

### Prerequisites for Using MobiControl with AirWave

In order to use the MobiControl integration in AirWave, the following is required:

- An AMP running version 7.2.3 or later
- An MDM server with SOTI MobiControl Console 8.0x

- A client device that is:
  - associated with WLAN infrastructure managed by the AMP server running 7.2.3 or later
  - being actively managed by the SOTI MobiControl server

For more information about setting up MobiControl, please see <http://www.soti.net/mc/help/>.

In order to use SOTI MobiControl from within AirWave, you must first add your MDM server and designate it as a MobiControl.

## Adding a Mobile Device Management Server for MobiControl

1. To add an MDM server to AMP, navigate to **AMP Setup > MDM Server** and select **Add**. Complete the fields on this page. [Table 119](#) describes the settings and default values:

**Table 119** *AMP Setup > MDM Server > Add Fields and Descriptions*

Field	Description
<b>Hostname/IP Address</b>	The address or DNS hostname configured for your MobiControl Web Console.
<b>Protocol</b>	Whether HTTP or HTTPS is to be used when polling the MDM server. The port on which to connect to the MDM server is inferred from the protocol: with HTTP, AirWave will connect to port 80 of the SOTI server; with HTTPS, AirWave will connect to port 443.
<b>URL Context</b>	The URL context appended to the server URL to build the URL when connecting with the SOTI server. For MobiControl v8.0x the default URL Context is "MobiControlWeb". For MobiControl v8.5x the default URL Context is "MobiControl".
<b>Enabled</b>	Whether this server can be polled by AirWave. Make sure it is set to <b>Yes</b> .
<b>Username/Password</b>	The login credentials for accessing the web console of the MobiControl system.
<b>Polling Period</b>	The frequency in which AirWave polls the MDM server. The default is 5 minutes.

2. When finished, select **Add**.

The list page for the MDM server also displays:

- **Last Contacted** – The last time AirWave was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, AMP will obtain a list of all device IDs and their WLAN MAC addresses. The information about device OS, device OS Detail, Manufacturer, Model, Name are retrieved from MobiControl and populated to the **Clients > Client Detail** page for supported mobile devices. A **View device in SOTI MobiControl** link provides direct access to the MobiControl Web Console for additional details about the device. MobiControl information overrides data obtained from ArubaOS 6.0 controllers.

## Accessing MobiControl from the Clients > Client Detail Page

In order to access the MobiControl web console for a SOTI-managed mobile device from within AirWave, follow these steps:

1. Navigate to a page that lists clients. This can include:
  - **Clients > Connected** or **Clients > All**
  - Search results that display user MAC address
2. Select the MAC address in the **Clients** list table. The **Clients > Client Detail** page displays.
3. Under the Classification field, select the **View device in SOTI MobiControl** link. A new window will display the MobiControl Web Console for this device.

## Monitoring and Supporting AMP with the Home Pages

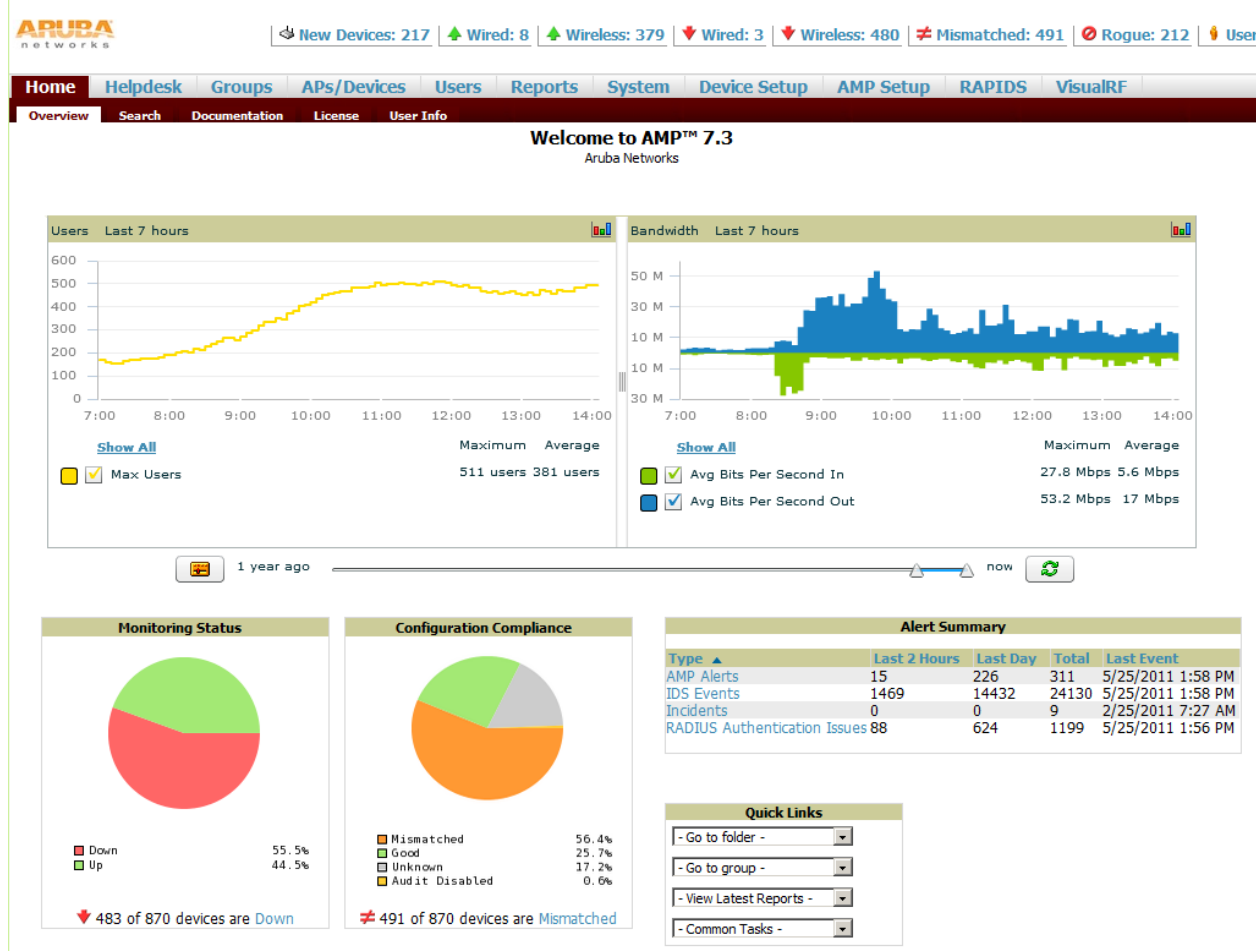
The **Home** tab of AMP provides the most frequent starting point for monitoring network status and establishing primary AMP functions once AMP configuration is complete. From the Home tab, you can access the following pages:

- The **Home > Overview** page condenses a large amount of information about your AMP. You can view the health and usage of your network and use shortcuts to view system information. Refer to [Monitoring AMP with the Home > Overview Page](#) below.
- The **Home > Search** page provides a simple way to find users, managed devices, groups, and rogues. Refer to “Searching AMP with the Home > Search Page” on page 211.
- The **Home > Documentation** page contains all relevant AMP documentation. See “Accessing AirWave Documentation” on page 213.
- The **Home > License** page provides product licensing information. See “The Customize link on the upper-right side of the page allows you to customize the widgets on the Home > Overview page. See “Customizing the Dashboard” on page 32.” on page 211.
- The **Home > User Info** page is where logged-in users can configure their name, contact information, rogue count filter level, customized header columns, severe alert threshold, personalized search preferences, record display preferences, and the refresh rate of the console. See “Configuring Your Own User Information with the Home > User Info Page” on page 213.

### Monitoring AMP with the Home > Overview Page

To view your overall network health, navigate to **Home > Overview** page. [Figure 153](#) illustrates this page, and [Table 120](#) describes the contents. The information that displays varies depending on your role.

Figure 153 *Home > Overview Page Illustration*



**Table 120** *Home > Overview Sections and Charts*

Section	Description
<b>Clients</b>	<p>This chart is a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Select <b>Show All</b> to display a list of data series that this graph can display, such as the user count by SSID.</p> <p>Clear the <b>Max Clients</b> or <b>Avg Clients</b> checkbox to change the display of the graph. The graph displays the maximum number of users by default. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.</p>
<b>Usage</b>	<p>This adjustable chart displays bandwidth data over time. To remove bandwidth in or out from the graphical display, clear the check box for <b>Avg Bits Per Second In</b> or <b>Out</b>.</p> <p>To display details for specific devices, select <b>Show All</b> and select the devices to be included in the graphical bandwidth summary chart. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.</p>
<b>Monitoring Status</b>	<p>This pie chart shows the percentage of all devices that are up and down on the network. To review devices that are down, select <b>Down</b> in the legend or the chart, and the <b>APs/Devices &gt; Down</b> page displays.</p>
<b>Configuration Compliance</b>	<p>The pie chart displays all known device configuration status on the network. Devices are classified as <b>Good</b>, <b>Unknown</b>, <b>Mismatched</b>, or <b>Audit Disabled</b>. Select the <b>Mismatched</b> link to see the <b>APs/Devices &gt; Mismatched</b> page.</p>
<b>Alert Summary</b>	<p>This section displays all known and current alerts configured and enabled in the <b>System &gt; Alerts</b> page (refer to “<a href="#">Viewing, Delivering and Responding to Triggers and Alerts</a>” on page 186). Alerts can be sorted using the column headers (<b>Type</b>, <b>Last 2 Hours</b>, <b>Last Day</b>, <b>Total</b>, or <b>Last Event</b>). The <b>Alert Summary</b> field displays three types of alerts:</p> <ul style="list-style-type: none"> <li>● <b>AMP Alerts</b></li> <li>● <b>IDS Events</b></li> <li>● <b>RADIUS Authentication Issues</b></li> </ul> <p>Select any alert type for more information.</p>
<b>Quick Links</b>	<p>The <b>Quick Links</b> section provides drop-down menus that enable you to move to the most common and frequently used pages in AMP, as follows:</p> <ul style="list-style-type: none"> <li>● <b>Go to folder</b>—This menu lists all folders defined in AMP from the <b>APs/Devices List</b> page. See “<a href="#">Using Device Folders (Optional)</a>” on page 134.</li> <li>● <b>Go to group</b>—This menu lists all groups defined in AMP, and enables you to display information for any or all of them. Use the <b>Groups</b> pages to edit, add, or delete groups that appear in this section. See “<a href="#">Configuring and Using Device Groups in AMP</a>” on page 71.</li> <li>● <b>View Latest Reports</b>—AMP supports creating custom reports or viewing the latest daily version of any report. Select any report type to display the daily version. See “<a href="#">Creating, Running, and Emailing Reports</a>” on page 227.</li> <li>● <b>Common Tasks</b>—This menu lists quick links to the most heavily used task-oriented pages in AMP, to include the following: <ul style="list-style-type: none"> <li>■ <b>Configure Alert Thresholds</b>—This link takes you to the <b>System &gt; Triggers</b> page. See “<a href="#">System &gt; Performance—Displays basic AMP hardware information as well as resource usage over time. Refer to “Using the System &gt; Performance Page” on page 216.”</a>” on page 183.</li> <li>■ <b>Configure Default Credentials</b>—This link takes you to the <b>Device Setup &gt; Communication</b> page. See “<a href="#">Configuring Communication Settings for Discovered Devices</a>” on page 54.</li> <li>■ <b>Discover New Devices on Your Network</b>—This link takes you to the <b>Device Setup &gt; Discover</b> page. See “<a href="#">Discovering, Adding, and Managing Devices</a>” on page 107.</li> <li>■ <b>Supported Devices and Features</b>—This link displays a PDF that summarizes all supported devices and features in chart format for AMP.</li> <li>■ <b>Upload Device Firmware</b>—This link displays the <b>Device Setup &gt; Upload Firmware &amp; Files &amp; Files Upload</b> page. See “<a href="#">Overview of the Device Setup &gt; Upload Firmware &amp; Files Page</a>” on page 56.</li> <li>■ <b>View Event Log</b>—This link displays the <b>System &gt; Event Log</b> page. See “<a href="#">Using the System &gt; Event Log Page</a>” on page 186.</li> </ul> </li> </ul>

The **Customize** link on the upper-right side of the page allows you to customize the widgets on the **Home > Overview** page. See “[Customizing the Dashboard](#)” on page 32.

## Viewing and Updating License Information

Navigate to the **Home > License** page using the standard AMP menu. [Figure 154](#) illustrates this page, and [Table 121](#) describes the contents.

Please be aware that you cannot enter multiple licenses. To combine multiple license entitlements into one new license, contact AirWave support.

**Figure 154** *Home > License Page Illustration*

System Overview	
System Name:	aire.com
Organization:	Aire Networks
Hostname:	aire.com
IP Address:	10.19.19.19
Time:	9/23/2009 7:25 PM
Uptime:	1 day 12 hrs 50 mins
Version:	6.4
OS:	CentOS release 5

This is a licensed version of AirWave Wireless Management Suite.

Refer to your license agreement for complete information about the terms of this license.  
Contact AirWave Technical Support at [support@airwave.com](mailto:support@airwave.com) or 1-866-943-4267 (866-WIFI-AMP) for more information.

Enter New License:

```
--- Begin AMP License Key ---  
Product: AWMS Professional  
Organization: Aruba Networks  
Hardware_ID: 00:21:9B:8B:B2:C4  
APs: 1000  
RAPIDS: Yes  
VisualRF: Yes  
Generated: Wed Mar 4 22:48:19 2009 UTC by VPKasf4K/eXQisetIOc+Aw  
--- Signature ---  
iD8DBQFJrwUzvN8PdJTKS2ERAuZmAJ9EwAYfhciAI7C3oPCOYjoAipUZxgCfaw9q  
UmDiGqRmGOH7s3S2F37H2d0=  
=6V+l  
--- End AMP License Key ---
```

**Table 121** *Home > License Static Fields and Descriptions*

Field	Description
<b>System Name</b>	Displays a user-definable name for AMP. The System Name can be configured from the <b>AMP Setup &gt; General</b> page.
<b>Organization</b>	Displays the organization listed on your license key.
<b>Hostname</b>	Displays the DNS name assigned to AMP.
<b>IP Address</b>	Displays the static IP address assigned to AMP. The IP Address can be configured from the <b>AMP Setup &gt; Network</b> page.
<b>Time</b>	Displays the current date and time set on AMP.
<b>Uptime</b>	Displays the amount of time since the operating system was last booted.
<b>Version</b>	Displays the version number of AMP code currently running.
<b>OS</b>	Displays the version of Linux installed on the server.

## Searching AMP with the Home > Search Page

While the **Search** field at the top of every AMP page allows you to perform a quick search across a small number of common categories, the **Home > Search** page conducts a deep system-wide search to find



connected and historical clients, VPN users, managed devices, rogue devices, rogue clients, groups, folders, and tags.

Search performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP address of all the APs, as well as the client MAC, VPN user, Client, LAN IP and VPN IP fields. [Figure 155](#) illustrates this page.

**Figure 155** Home > Search Page Illustration with Sample Hits on “00.”

Search for managed devices and wireless users. A single substring match is used. To search by MAC address, include colons (e.g. 00:00:00).

00: Search

APs/Devices: Modify Devices

1-45 of 45 APs/Devices Page 1 of 1

Device	Status	Users	BW (kbps)	Uptime	Configuration	Group	Folder	Controller	Master Controller
00:00:86:66:03:4e	Down	0	0	-	Unknown	Access Points	.arespace	-	-
00:00:86:c1:a0:52	Up	0	0	16 hrs 59 mins	Mematched	Access Points	.arespace	-	-
1250-91:14:3a	Up	0	0	8 days 19 hrs 3 mins	Mematched	lwic thin aps	.arespace	arespace-4400-1	-
1250-91:14:42	Up	0	0	12 days 20 hrs 18 mins	Mematched	lwic thin aps	.arespace	arespace-4400-1	-
Arespace-4012-2	Up	0	0	54 days 22 hrs 46 mins	Mematched	Access Points	.arespace	-	-
arespace-4400-1	Up	0	0	12 days 21 hrs 28 mins	Mematched	4400	.arespace	-	-

Users: 1-50 of 325 Users Page 1 of 7 >

Username	Role	MAC Address	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time	Duration
lgon	-	00:00:48:39:96:08	00:00:86:c1:a0:52	abaca-abaca	51	802.11bg	802.11g	0	2/13/2009 12:50 PM	-
-	-	00:04:23:4C:C1:33	AP2	ws100_102	1	802.11b	802.11b	-	3/10/2009 5:22 PM	-
-	-	00:05:4E:4B:14:2E	-	-	-	-	-	-	-	-
-	-	00:05:4E:4D:9D:6A	-	-	-	-	-	-	-	-
-	-	00:05:4E:4F:86:81	-	-	-	-	-	-	-	-
GuestLogon	-	00:06:25:2C:A5:A0	00:00:86:c1:a0:52	guest	51	802.11bg	802.11b	0	1/23/2009 9:07 AM	-
-	-	00:09:EF:05:1E:82	-	-	-	-	-	-	-	-
-	-	00:09:EF:05:20:CF	-	-	-	-	-	-	-	-
lgon	-	00:0A:88:7F:08:11	00:00:86:c1:a0:52	dpb_test_guest	51	802.11bg	802.11b	0	1/29/2009 2:25 PM	-
GuestLogon	-	00:0A:88:7F:08:11	ap-Not set	-	-	-	-	-	1/29/2009 2:19 PM	-
-	-	00:0A:88:7F:08:1E	-	-	-	-	-	-	-	-
-	-	00:0C:F1:38:0F:A6	-	-	-	-	-	-	-	-
-	-	00:0E:38:49:08:31	RADIO1	101	1	802.11b	802.11b	0	3/5/2009 3:18 PM	-
-	-	00:0E:38:49:08:3E	ap-Not set	guest	51	802.11a	802.11a	0	2/24/2009 1:08 PM	-
-	-	00:0E:98:0C:CE:F3	-	-	-	-	-	-	-	-
-	-	00:0E:98:07:35:8A	ap	open-ops	0	802.11a	802.11a	-	1/29/2009 8:59 AM	-
-	-	00:0F:86:81:D5:3F	-	-	-	-	-	-	-	-
-	-	00:0F:C8:82:33:A4	-	-	-	-	-	-	-	-
-	-	00:11:24:06:28:82	-	-	-	-	-	-	-	-
-	-	00:11:F5:53:AE:0F	-	-	-	-	-	-	-	-
-	-	00:13:02:1E:67:15	RADIO1	101	1	802.11b	802.11b	-	2/5/2009 5:30 PM	-
-	-	00:13:02:84:39:8D	ap	open-ops	0	802.11bg	802.11bg	-	1/28/2009 7:41 PM	-
-	-	00:13:02:AD:0C:3E	-	-	-	-	-	-	-	-
-	-	00:13:02:C2:39:28	-	-	-	-	-	-	-	-
-	-	00:13:02:CD:F3:D5	00:00:86:c1:a0:52	guest	51	802.11a	802.11a	0	2/20/2009 7:59 AM	-
-	-	00:13:CE:45:91:A0	ap-Not set	guest	51	802.11bg	802.11g	0	1/29/2009 4:00 PM	-

No Folders found  
No Groups found.

Rogues: Modify Devices

1-50 of 187 Rogue Devices Page 1 of 4 >

ACK	RAPIDS Classification	Threat Level	Name	Classifying Rule	Device Classification	Wired	#APs hearing	SSID
No	Valid	-	Enterways-68:FA:C3	<user set>	Unclassified	-	6	test012
No	Suspected Neighbor	5	Tropos Net-04:0F:BB	Suspected Neighbor - detected wirelessly	Unclassified	-	5	TroposNetworks
No	Suspected Neighbor	5	Cisco Syst-A7:8B:ED	Suspected Neighbor - detected wirelessly	Unclassified	-	3	disshop-arespace-open
No	Valid	-	Aruba Netw-88:88:32	<user set>	Unclassified	-	5	ethersphere-voip
No	Valid	-	Enterways-27:F6:48	<user set>	Unclassified	-	6	Roamabout Default Network Name
No	Suspected Neighbor	5	SYMBOL TEC-07:64:A6	Suspected Neighbor - detected wirelessly	Unclassified	-	6	ws100_102
No	Valid	-	NOMADIX IN-05:02:D0	<user set>	Unclassified	-	6	Normadix
No	Valid	-	Meru Netwo-B9:CC:05	<user set>	Unclassified	-	6	BetsyFromPike

Tags: 1-5 of 5 Tags Page 1 of 1

Name	MAC Address	Vendor	Battery Level	Chrg Interval	Last Seen	Closest AP
-	00:0C:CC:5E:7F:9E	Aerocout Ltd.	-	45 secs	3/12/2009 10:25 AM	1250-91:14:42
-	00:14:7E:00:4C:DC	InnerWireless	Normal	1 mn	3/12/2009 10:24 AM	1250-91:14:42
-	00:0C:CC:7A:38:8A	Aerocout Ltd.	-	50 secs	3/12/2009 10:24 AM	lwapp-1250:13:21:1e
-	00:14:7E:00:4C:B9	InnerWireless	Normal	2 mins	3/12/2009 10:23 AM	lwapp-1250:13:21:1e
-	00:14:7E:00:4C:F2	InnerWireless	Normal	0 mins	3/10/2009 10:00 AM	-

1. Enter the keyword or text with which to search. If searching for a MAC address, enter it in colon-delimited format.



The AMP Search utility is case-insensitive when single or double quotes are not used. For exact case-sensitive matches, use quotes around the search phrase.

2. Select **Search**, and the results display after a short moment. Results support several hypertext links to additional pages, and the **Filter** icon over some columns allow for additional filtering of search returns. Search results are categorized in the following sequence. Categories of search results can be customized on the **Home > User Info** page to limit the scope of information returned. Not all categories below may offer returns for a given search:

- Devices
- Clients
- VPN Users
- Rogues and Rogue Clients
- Tags
- Folders and Groups

## Accessing AirWave Documentation

The **Home > Documentation** page provides easy access to all relevant AirWave documentation. All of the documents on this page are hosted locally by your AirWave server and can be viewed by any PDF viewer. If you have any questions that are not answered by the documentation, please contact AirWave support.

## Configuring Your Own User Information with the Home > User Info Page

The **Home > User Info** page displays information about the user that is logged into AirWave. This page includes the authentication type (local user, RADIUS, or TACACS+) and access level. This page enables customization some of the information displayed in AMP, and is the place to change your password.

The logged-in users can customize the information displayed in the AMP header. [Figure 156](#) illustrates the **Home > User Info** page, and [Table 122](#) lists the fields.

**Figure 156** *Home > User Info Page Illustration*

**admin** is logged in as a local database user with role *AMP Administration* and Administrator access to RAPIDS.

The screenshot displays the 'Home > User Info' page in the AirWave interface. It is divided into four main sections: 'User Information', 'Top Header Stats', 'Search Preferences', and 'Display Preferences'. The 'User Information' section includes fields for Name (Admin), New Password, Confirm New Password, Email Address (admin@mycompany.com), Phone, and Notes. The 'Top Header Stats' section allows customization of the AMP header, including a filter level for rogue count (Valid), a 'Customize Header Columns' section with checkboxes for various stats like New Devices, Up/Down (Wired & Wireless), Up/Down (Wireless), Mismatched, Rogues, Clients, VPN Sessions, Alerts, and Severe Alerts, and a 'Severe Alert Threshold' set to Major. The 'Search Preferences' section includes a 'Customize Search' checkbox and a list of search criteria like Aps/Devices, Clients (Connected), Clients (Historical), VPN Sessions (Connected), VPN Sessions (Historical), Rogue Clients, Folders, Groups, Tags, and Rogues. The 'Display Preferences' section includes a 'Default Number of Records per List' set to All records, a 'Reset List Preferences' button, a 'Customize Columns for Other Roles' checkbox, a 'Console Refresh Rate' set to 1 minute, and an 'Idle Timeout' set to 60 minutes. At the bottom, there are 'Save' and 'Revert' buttons.

User Information	
Name:	Admin
New Password:	
Confirm New Password:	
Email Address:	admin@mycompany.com
Phone:	
Notes:	

Top Header Stats	
Filter Level For Rogue Count:	Valid
Customize Header Columns:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Stats:	<input checked="" type="checkbox"/> New Devices <input checked="" type="checkbox"/> Up (Wired & Wireless) <input checked="" type="checkbox"/> Up (Wired) <input checked="" type="checkbox"/> Up (Wireless) <input checked="" type="checkbox"/> Down (Wired & Wireless) <input checked="" type="checkbox"/> Down (Wired) <input checked="" type="checkbox"/> Down (Wireless) <input checked="" type="checkbox"/> Mismatched <input checked="" type="checkbox"/> Rogues <input checked="" type="checkbox"/> Clients <input checked="" type="checkbox"/> VPN Sessions <input checked="" type="checkbox"/> Alerts <input checked="" type="checkbox"/> Severe Alerts
	Select All - Unselect All
Severe Alert Threshold:	Major
Include Device Types:	<input checked="" type="checkbox"/> Fat APs <input checked="" type="checkbox"/> Thin APs <input checked="" type="checkbox"/> Controllers <input checked="" type="checkbox"/> Switches <input checked="" type="checkbox"/> Others
	Select All - Unselect All

Search Preferences	
Customize Search:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Search Preferences:	<input checked="" type="checkbox"/> Aps/Devices <input checked="" type="checkbox"/> Clients (Connected) <input checked="" type="checkbox"/> Clients (Historical) <input checked="" type="checkbox"/> VPN Sessions (Connected) <input checked="" type="checkbox"/> VPN Sessions (Historical) <input checked="" type="checkbox"/> Rogue Clients <input checked="" type="checkbox"/> Folders <input checked="" type="checkbox"/> Groups <input checked="" type="checkbox"/> Tags <input checked="" type="checkbox"/> Rogues
	Select All - Unselect All

Display Preferences	
Default Number of Records per List:	All records
Reset List Preferences:	Reset
Customize Columns for Other Roles:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Console Refresh Rate:	1 minute
Idle Timeout (5 mins to 240 mins):	60
	Save Revert

**Table 122** *Home > User Info Fields and Descriptions*

Field	Description
<b>Top Header Stats</b>	
<b>Filter Level For Rogue Count</b>	Specifies the minimum classification that will cause a device to be included in the rogue count header information. More about the classifications can be found in <a href="#">“Controller Classification with WMS Offload” on page 172</a> .
<b>Customize Header Columns</b>	Enables/disables the ability to control which statistics hyperlinks (also known as Top Header Stats) are displayed at the top of every AMP screen.
<b>Stats</b>	Select the specific data you would like to see in the Top Header Stats. Refer to <a href="#">“Status Section” on page 22</a> . <b>Note:</b> This field only appears if you selected <b>Yes</b> in the previous field.
<b>Severe Alert Threshold</b>	Configures the minimum severity of an alert to be included in the Severe Alerts count. See <a href="#">“Setting Severe Alert Warning Behavior” on page 34</a> for details. <b>Note:</b> The severe alerts count header info will only be displayed if ‘Severe Alerts’ is selected in the <b>Stats</b> section above. <b>Note:</b> This field only appears if you selected <b>Yes</b> in the <b>Customize Header Columns</b> field.
<b>Include Device Types</b>	Configures the types of devices that should be included in the header stats. If a device type is not selected then it will not be included in the header stats. <b>Note:</b> This field only appears if you selected <b>Yes</b> in <b>Customize Header Columns</b> .
<b>Search Preferences</b>	
<b>Customize Search</b>	Set to <b>No</b> by default; when set to <b>Yes</b> , you can select which search categories to display when “Full” search results are returned.
<b>Display Preferences</b>	
<b>Default Number of Records per List</b>	Defines the number of rows to appear in any list by default. If a row count is manually set, it will override the default setting.
<b>Reset List Preferences</b>	Reset all list preferences including number of records per list, column order and hidden column information.
<b>Customize Columns for Other Roles</b>	Allows admin users to determine the columns that should be displayed and the order they should be displayed for specific user roles. To customize lists for other users, navigate to that list and select <b>Choose Columns for roles</b> above the list. Make the desired column changes; select the roles to update and <b>Save</b> .
<b>Console Refresh Rate</b>	The frequency in which lists and charts automatically refresh on a page.
<b>Idle Timeout</b> (5 mins to 240 mins)	Number of minutes of idle time until AMP automatically ends the user session. This setting only the logged-in user of this AMP. The default is 60 minutes. To set the max idle timeout for all users of this AMP, see <a href="#">“Setting Up Login Configuration Options” on page 49</a> .

Perform the following steps to configure your own user account with the **Home > User Info** page:

- In the **User Information** section, enter the following information:
  - Name**—Enter the ID by which you log into and operate in AMP.
  - Email Address**—Enter the email address to be used for alerts, triggers, and additional AMP functions that support an email address.
  - Phone**—Enter the area code and phone number, if desired.
  - Notes**—Enter any additional text-based information that helps other AMP users or administrators to understand the functions, roles, or other rights of the user being created.

## Using the System > Configuration Change Jobs Page

Schedule configuration change jobs are summarized on the **System > Configuration Change Jobs** page. Perform the following steps to use this page, illustrated in [Figure 157](#).

**Figure 157** *System > Configuration Change Jobs Page Illustration*

Subject: AP02, Description: Change Radio Status on AP "AP02" 802.11bg and AP "AP02" 802.11a, Scheduled Time: September 9th 2007 at 12:00 am, User: admin, Folder: Top > controller thin ap > trapeze, Group: Access

To run at: September 9th 2007 at 12:00 am

AP "AP02" 802.11bg  
Radio: (none) Enabled

AP "AP02" 802.11a  
Radio: (none) Enabled

Apply Changes Now Delete Cancel

**Schedule**  
Specify numeric dates with optional 24-hour times (like 7/4/2003 or 2003-07-04 for July 4th, 2003, or 7/4/2003 13:00 for July 4th, 2003 at 1:00 PM.), or specify relative times (like at noon, tomorrow at midnight, or next tuesday at 4am). Other input formats may be accepted.  
Start Date/Time: September 9th 2007 at 12:00  
Schedule

1. To edit an existing configuration change job select on the linked description name. On the subsequent edit page you can choose to run the job immediately by selecting **Apply Changes Now**, reschedule the job by selecting **Schedule**, **Delete** the job, or **Cancel** the job edit.
2. Select the linked AP or group name under the **Subject** column to go to its monitoring page.
3. Select the linked group and folder names under **Folder** or **Group** to go to the AP's folder or group page.
4. Scheduled configuration change jobs will also appear on the **Manage** page for an AP or the **Monitoring** page for a group.

## Using the System > Firmware Upgrade Jobs Page

The **System > Firmware Upgrade Jobs** page displays a list of recent firmware upgrade jobs that have been initiated in the **APs/Devices > Manage** page or **Modify Devices** page for a controller or autonomous AP that supports firmware upgrades in AMP.

Successful upgrade jobs are not archived on this page – generally you visit this page to review failed or pending firmware upgrade jobs.

Users with the **AP/Device Manager** role and higher can view this page. Audit-only users cannot view this page or tab.

**Figure 158** *System > Firmware Upgrade Jobs Page Illustration*

Firmware upgrade jobs:

Add new firmware files on the [Firmware & File Upload](#) page. Initiate a firmware upgrade job from the APs/Device Manage page of a device or from the Modify Devices actions on a list of devices.

Firmware Server Log

	Name	Role	Username	Created	Status	Scheduled Start Time	Total Devices	Pending	In Progress	Completed	Failed
<input type="checkbox"/>	Firmware upgrade for 5500-6.0.196.0	AMP Administration	admin	4/7/2011 2:57 PM	Failed	-	1	0	0	1	0
<input type="checkbox"/>	Firmware upgrade for Cisco4400	AMP Administration	admin	4/6/2011 3:07 PM	Failed	-	1	0	0	0	1
<input type="checkbox"/>	Firmware upgrade for Cisco4400	AMP Administration	admin	4/6/2011 3:12 PM	Failed	-	1	0	0	0	1
<input type="checkbox"/>	Firmware upgrade for Cisco4400	AMP Administration	admin	4/6/2011 3:22 PM	Failed	-	1	0	0	0	1

4 Firmware Upgrade Jobs

Select All - Unselect All

Restart Failed Jobs Cancel and Delete Jobs

Firmware Server Log

You can perform the following operations on this page:

- To restart failed firmware upgrade jobs, select the checkboxes next to the rows you want to restart and select the **Restart Failed Jobs** button.
- To stop a pending upgrade job and remove it from the list, select the **Cancel and Delete Jobs** button.
- Use additional links on the page as shortcuts to the **Device Setup > Upload Firmware & Files** page, or the complete raw text of the Firmware Server Log

- To view additional details about an individual upgrade job including the devices being upgraded, select the name of an upgrade job from the Name column to go to the **System > Firmware Upgrade Job Detail** page, illustrated in [Figure 159](#).

From here you can click the device name to go to its **APs/Devices > Monitor** page, or the link under **Firmware File** column to go to the **Device Setup > Upload Firmware & Files** page.

**Figure 159** *System > Firmware Upgrade Job Detail Page Illustration*

[Firmware Server Log](#)

Details for firmware upgrade job **Firmware upgrade for 5500-6.0.196.0**

Firmware upgrade job is stopped because too many upgrades have failed. [Restart the upgrade job](#)

**Job Information:**

Role	Username	Created	Status	Scheduled Start Time	Total Devices	Pending	In Progress	Completed	Failed
<a href="#">AMP Administration</a>	admin	4/7/2011 2:57 PM	Failed	-	1	0	0	1	0

**Devices being upgraded:**

There are 3 APs that you cannot see. 0 of those APs are currently being upgraded.

		Order in Queue ▲	Current Version	Desired Version	Current Secondary Version	Desired Secondary Version	Firmware File
<input type="checkbox"/>	wlc 5500	1	7.0.116.0	6.0.199.4	1.0.1		<a href="#">0_AIR-CT5500-K9-6-0-199-4.aes</a>

[Select All](#) - [Unselect All](#)

[Cancel and Delete Upgrades](#)

## Using the System > Performance Page

The **System > Performance** page displays basic AirWave hardware information as well as resource usage over time. AMP logs performance statistics such as load average, memory and swap data every minute.

The historical logging is useful to determine the best usable polling period and track the health of AirWave over time.

The page is divided into four sections:

- System Information
- Performance Graphs
- Database Statistics
- Disk Usage

[Figure 160](#) illustrates this page and [Table 123](#) describes fields and information displayed.

Figure 160 System > Performance Page Illustration (Partial Screen)

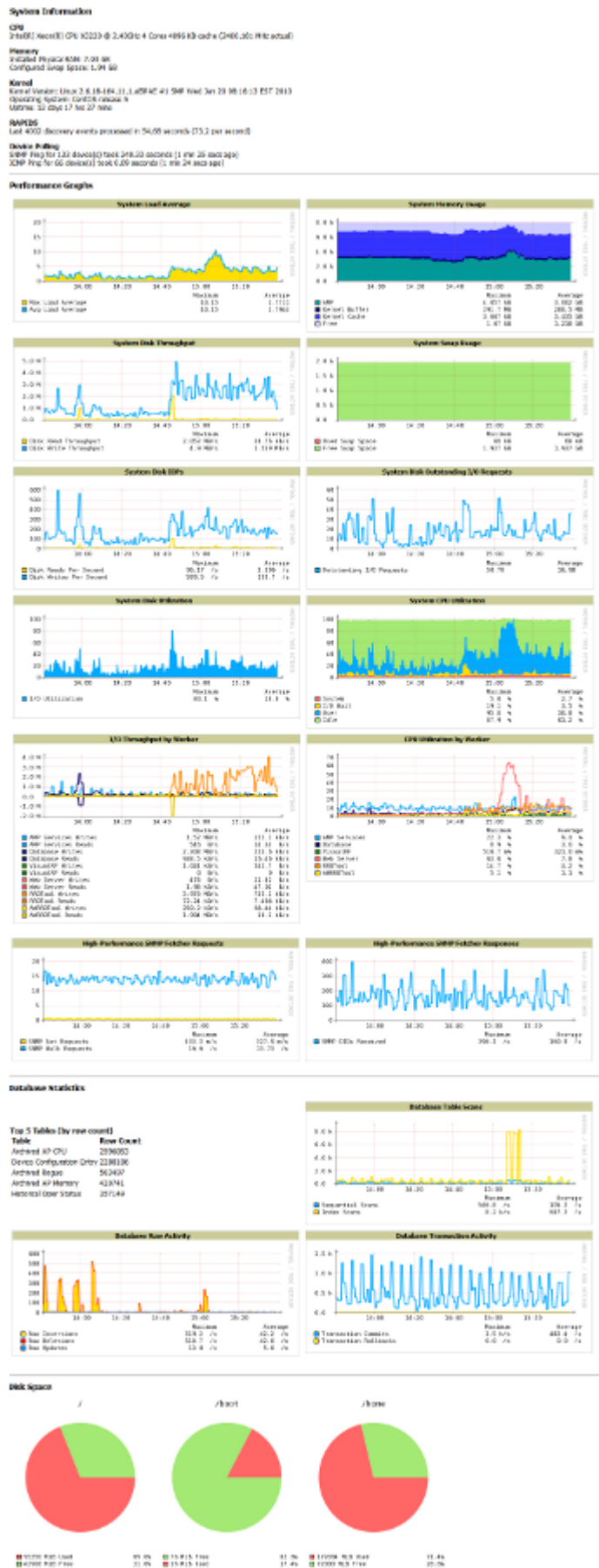


Table 123 **System > Performance** Page Fields and Graphs

Field	Description
<b>System Information</b>	
<b>CPU(s)</b>	Basic CPU information as reported by the operating system.
<b>Memory</b>	The amount of physical RAM and Swap space seen by the operating system. Refer to the <i>AirWave Server Hardware Guide</i> for hardware requirements.
<b>Kernel</b>	The version of the Linux kernel running on the box.
<b>Architecture</b>	The AMP's architecture information.
<b>Device Polling</b>	Displays some AP/Device polling statistics.
<b>Performance Graphs</b>	
<b>System Load Average</b>	The number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical AMP load is around 2-3 times the number of CPU cores you have in your system. A constant load of 4x to 5x is cause for concern. A load above 6x is a serious issue and will probably result in AMP becoming unusable. To lower the load average, try increasing a few polling periods in the <b>Groups &gt; Basic</b> page.
<b>System Memory Usage</b>	The amount of RAM that is currently used broken down by usage. It is normal for AMP to have very little free RAM. Linux automatically allocates all free RAM as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer.
<b>System Disk Utilization</b>	The amount of data read from the disk and written to the disk.
<b>System Disk IOPs</b>	The number of disk reads and writes per second.
<b>System Disk Throughput</b>	The rate of reading and writing from and to the disk in bytes per second.
<b>System Disk Outstanding I/O Requests</b>	The average number of outstanding I/O requests (queue depth). If it's high, it means that I/O requests (disk reads/writes) aren't being serviced as fast as they're being asked for.
<b>System Swap Usage</b>	The amount of Swap memory used by AMP. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If an AMP consistently uses swap, you should consider installing additional RAM.
<b>System CPU Utilization</b>	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
<b>I/O Throughput by Worker/by Service</b>	Displays reads and writes for workers (AMP services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (AMP, VisualRF and web server).
<b>CPU Utilization by Worker/by Service</b>	Displays reads and writes for workers (AMP services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (AMP, VisualRF and web server).
<b>System Network Bandwidth</b>	All traffic in and out measured in bits per second of your primary network interface (Eth0 being the most common).
<b>Bandwidth by Protocol</b>	Displays the amount of traffic used by Telnet, HTTPS and SNMP used by your primary network interface (Eth0 being the most common).
<b>Legacy SNMP Fetcher Requests</b>	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
<b>Legacy SNMP Fetcher Responses</b>	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
<b>High Performance SNMP Fetcher Requests</b>	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
<b>High Performance SNMP Fetcher Responses</b>	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.



**Table 123** *System > Performance Page Fields and Graphs (Continued)*

Field	Description
<b>Database Statistics</b>	
<b>Top 5 Tables (by row count)</b>	The five largest tables in AMP. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Decreasing the length of time client data is stored on the AMP page is recommended if a user/client table exceeds 250,000 rows.
<b>Database Table Scans</b>	The number of database table scans performed by the database.
<b>Database Row Activity</b>	The number of insertions, deletions and updates performed to the database.
<b>Database Transaction Activity</b>	The number of commits and rollbacks performed by the database.
<b>Disk Space</b>	
<b>Disk Space</b>	Pie charts that display the amount of used and free hard drive space for each partition. If a drive reaches over 80% full, you may want to lower the <b>Historical Data Retention</b> settings on the <b>AMP Setup &gt; General</b> page or consider additional drive space.

There are several initial steps that you can take to troubleshoot AMP performance problems, including slow page loads and timeout errors. Initial troubleshooting steps would include the following:

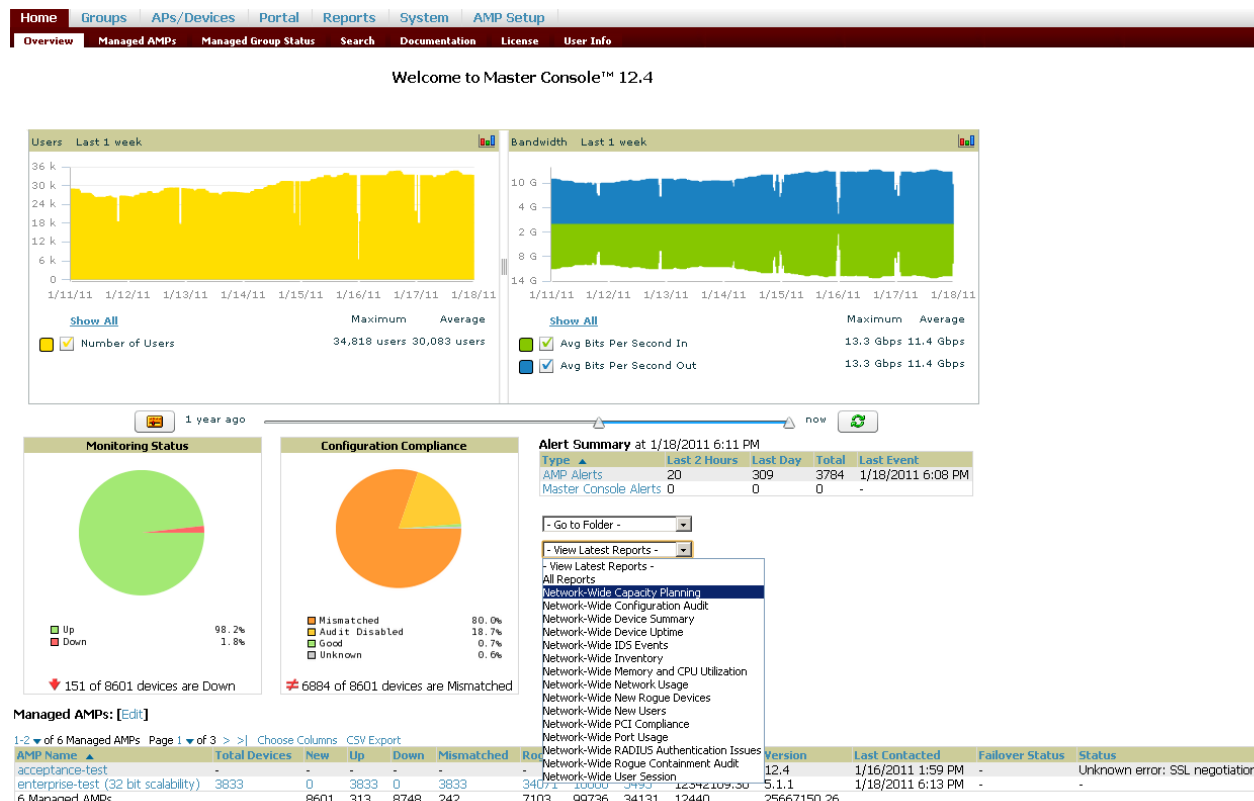
- Increasing the polling period settings on the **Groups > Basic** page.
- Increasing the polling period time for groups with routers and switches.
- Adding additional memory to the server. Please consult the sizing information in the latest edition of the *AirWave Server Sizing Guide* or contact AirWave support for the latest recommendations.

## Supporting AMP Servers with the Master Console

The **Master Console (MC)** is used to monitor multiple AMP stations from one central location. The Master Console is designed for customers running multiple AMP servers. Once an AMP station has been added to the MC, it will be polled for basic AMP information.

Much like the normal **Home > Overview** page, the **Master Console Home > Overview** page provides summary statistics for the entire network at a glance. [Figure 161](#) illustrates the Overview page:

**Figure 161** Master Console **Home > Overview** Page Illustration



- Reports can be run from the **Master Console** to display information from multiple AMP stations; because such reports can be extremely large, reports can also be run as **summary only** so that they generate more quickly and finish as a manageable file size.
- The Master Console can also be used to populate group-level configuration on managed AMP installations using the **Global Groups** feature.
- The Master Console offers a display of devices that are in a **Down** or **Error** state anywhere on the network. This information is supported on Master Console pages that display device lists such as **Home > Overview** and **APs Devices > List**.
- The Master Console and Failover servers can be configured with a **Managed AMP Down** trigger that generates an alert if communication is lost to a managed or watched AMP station. The Master Console or Failover server can also send email or NMS notifications about the event. See [“System > Performance—Displays basic AMP hardware information as well as resource usage over time. Refer to “Using the System > Performance Page” on page 216.” on page 183.](#)



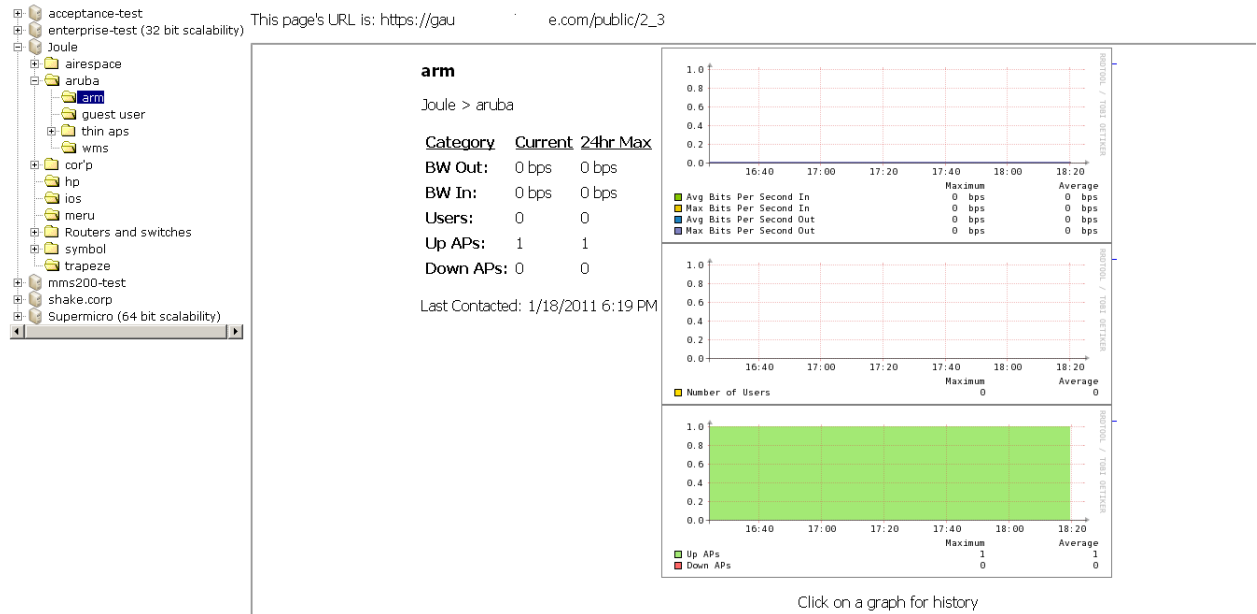
The license key determines if the server will behave as a Master Console or as a standard AMP server.

## Using the Public Portal on Master Console

The Master Console also contains an optional Public Portal which allows any user to view basic group-level data for each managed AMP. This feature is disabled by default for security reasons; no AMP or Master Console login is required to view the public portal. The Public Portal can be enabled in **AMP Setup >**

**General** in the **Master Console** section. Once enabled, a new **Portal** tab will appear to the right of the **Groups** tab (refer to the navigation section in [Figure 161](#) in the previous page). The URL of the public portal will be <https://your.AMP.name/public>. When you upgrade to the latest version of AMP, the public portal is disabled by default, regardless of the type of license.

**Figure 162** *Public Portal Page Illustration*



The **Public Portal** supports configuration of the iPhone interface. This can be configured using the Master Console AMP page. See “[Defining General AirWave Server Settings](#)” on page 35.

## Adding a Managed AMP with the Master Console

Perform the following steps to add a managed AMP console.

1. Navigate to the **Home > Managed AMPs** page.
2. Select the pencil icon to edit or reconfigure an existing AMP console, or select **Add New Managed AMP** to create a new AMP console. The **Managed AMP** page appears. Complete the settings on this page as described in [Table 124](#).

**Table 124** *Managed AMP Fields and Default Values*

Field	Default	Description
<b>Hostname / IP Address</b>	N/A	Enter the IP address or Hostname of the AMP server to be managed.
<b>Polling Enabled</b>	Yes	Enables or disables the Master Console polling of managed AMP server.
<b>Polling Period</b>	5 minutes	Determines how frequently the Master Console polls the managed AMP server.
<b>Username</b>	N/A	The username used by the Master Console to login to the managed AMP server. The user needs to be an AP/Device Manager or AMP Administrator.
<b>Password</b> (Confirm Password)	N/A	The password used by the Master Console to login to the managed AMP.
<b>HTTP Timeout</b> (5-1000 sec)	60	Defines the timeout period used when polling the managed AMP server.
<b>Manage Group Configuration</b>	No	Defines whether the Master Console can manage device groups on the managed AMP server.

3. When finished, select **Add** to return to the **Managed AMPs** list page.

## Using Global Groups with Master Console

To push configurations to managed groups using the AMP Global Groups feature, follow these steps:

1. Navigate to the Master Console's **Groups > List** page.
2. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group.
3. Select the **Duplicate** icon to create a new group with identical configuration to an existing group.  
Groups created on the Master Console will act as Global Groups, or groups with master configurations that can be pushed out to subscriber groups on managed AMPs. Global groups are visible to all users, so they cannot contain APs (which can be restricted based on user role).
4. Selecting the name of an existing group on the Master Console loads the subtabs for **Basic**, **Security**, **SSIDs**, **AAA Servers**, **Templates**, **Radio**, **Cisco WLC Config**, **Proxim Mesh**, and **MAC ACL** pages, if such pages and configurations are active for the devices in that group.

These subtabs contain the same fields as the group subtabs on a monitored AMP, but each field also has a checkbox. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the [Chapter 6, “Creating and Using Templates”](#), except that there is no process by which templates can be fetched from devices in the subscriber group on managed AMPs. Instead, the template must be copied and pasted into the Master Console Global Group.

When a Global Group is pushed from the Master Console to subscriber groups on managed AMPs, all settings will be static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. For list pages, override options are available only on the **Add** page for each list. It will take several minutes for changes to Global Groups on the Master Console to be pushed to the managed AMPs; make sure that the **Manage Group Configuration** option is enabled for each managed AMP.

Once Global Groups have been configured on the Master Console, groups must be created or configured on the managed AMPs to subscribe to a particular Global Group. To configure subscriber groups, enable **Use Global Groups** on the **Group > Basic** page of a group on a managed AMP. Select the name of the Global Group from the drop-down menu, and then select **Save and Apply**. Note that the MC doesn't push anything when you create new subscriber groups; the copy of the Global Group already on the managed AMP provides the information.

Once the configuration is pushed, the non-overridden fields from the Global Group will appear on the subscriber group as static values and settings. Only fields that had the override checkbox selected in the Global Group will appear as fields that can be set at the level of the subscriber group. Any changes to a static field must be made on the Global Group.

The Global Groups feature can also be used without the Master Console. For more information about how this feature works, refer to [“Configuring and Using Device Groups in AMP” on page 71](#).

## Upgrading AirWave

The AirWave upgrade process may change. Please contact support and consult the latest AirWave release announcement for detailed instructions and changes.

### Upgrade Instructions

To upgrade AirWave:

1. Log in to the AirWave server as the root user.
2. Run the following command (where x.x.x is equal to the latest AMP version)

```
# start_amp_upgrade -v x.x.x
```

## Upgrading Without Internet Access

If your AirWave cannot get to the Internet:

1. Download the latest AMP version from our download page: [www.airwave.com/support/download](http://www.airwave.com/support/download)
2. Copy the file to AMP /root directory using WinSCP.
3. On the AMP, run the following command:

```
# start_amp_upgrade -v x.x.x
```

The `start_amp_upgrade` script will check the `/root` directory for the latest update. If the update is not found, the script will attempt to download it from the AirWave support page. The script will then extract the version specific upgrade script. The version specific script will deploy all needed files, update the database, perform any data migrations and restart the AirWave services.

## Backing Up AMP

AMP creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **AMP Setup > General** page under **Nightly Maintenance Time**.

Although AMP only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. AMP creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other AMP settings.

## Viewing and Downloading Backups

To view current AirWave backup files, go to the **System > Backups** page. [Figure 163](#) illustrates this page.

**Figure 163** *System > Backups Page Illustration*

Backups are run nightly.

[nightly\\_data001.tar.gz](#) Backup of 1071445503 bytes made 15 hrs 15 mins ago.  
[nightly\\_data002.tar.gz](#) Backup of 1045819243 bytes made 1 day 15 hrs 15 mins ago.  
[nightly\\_data003.tar.gz](#) Backup of 987593884 bytes made 2 days 15 hrs 15 mins ago.  
[nightly\\_data004.tar.gz](#) Backup of 1054778324 bytes made 3 days 15 hrs 15 mins ago.

To download a backup file, select the filename URL and the **File Download** popup page appears.

Regularly save the data backup file to another machine or media. This process can be automated easily with a nightly script.



---

Nightly maintenance and `amp_backup` scripts back up the full AMP data and save the file as `nightly_data00[1-4].tar.gz`. In previous AMP versions, the scripts created both config backup and data backup files. In order to restore the AMP data, it is only necessary to have most recent data backup file, and AMP no longer uses or supports the config backup file, effective as of AMP 6.3.2 and later AMP versions.

---

## Running Backup on Demand

To create an immediate backup:

1. Log into the AMP system as **root**.
2. Run the backup script by typing `amp_backup`.

This creates a backup of the system located in `/alternative/databackup.tar.gz`.

## Restoring from a Backup

To restore a backup file on a new machine:

1. Use your AirWave Installation CD to build a new machine. The new machine must be running the same version as the AMP that created the backup file.
2. Copy the nightly\_data00[1-4].tar.gz file to the /tmp directory in the new AMP.  
A file transfer client that supports SFTP/SCP for Windows is WinSCP: <http://winscp.sourceforge.net/eng/>  
WinSCP allows you to transfer the nightly00[1-4].tar.gz file from your local PC to the new AMP using the secure copy protocol (SCP).
3. Log onto the new server as **root**.
4. Change to the scripts directory by typing **scripts**.
5. Run the restore script by typing **./amp\_restore -d /tmp/nightly\_data00[1-4].tar.gz**.



Network administrators can now use the nightly backup from a 32-bit AMP to restore AMP on a 64-bit installation, rather than having to create a special backup file or use the special restore script.

## Using AirWave Failover for Backup

The failover version of AMP provides a “many to one” hot backup server. The Failover AMP polls the watched AMPs to verify that each is up and running. If the watched AMP is unreachable for the specified number of polls, the Failover AMP automatically restores the most recent saved backup from the watched AMP and begins polling its APs.

### Navigation Section of AMP Failover

The **Navigation** section displays tabs to all main GUI pages within AMP Failover. The top bar is a static navigation bar containing tabs for the main components of AMP, while the lower bar is context-sensitive and displays the subtabs for the highlighted tab. [Table 125](#) describes the contents of this page.

**Table 125** Contents of the Navigation Section of Failover

Main Tab	Description	Subtabs
<b>Home</b>	The <b>Home</b> page provides basic AMP Failover information including system name, hostname, IP address, current time, running time, software version, and watched AMP information.	<ul style="list-style-type: none"> <li>● <b>Overview</b></li> <li>● <b>User Info</b></li> <li>● <b>Watched AMPs</b></li> <li>● <b>License</b></li> </ul>
<b>System</b>	The <b>System</b> page provides information related to AMP operation and administration including overall system status, performance monitoring, and backups.	<ul style="list-style-type: none"> <li>● <b>Status</b></li> <li>● <b>Triggers</b></li> <li>● <b>Alerts</b></li> <li>● <b>Event Log</b></li> <li>● <b>Backups</b></li> <li>● <b>Performance</b></li> </ul>
<b>AMP Setup</b>	The <b>Setup</b> page provides all information relating to the configuration of AMP itself and its connection to your network.	<ul style="list-style-type: none"> <li>● <b>General</b></li> <li>● <b>Network</b></li> <li>● <b>Users</b></li> <li>● <b>TACACS+</b></li> </ul>

### Adding Watched AMP Stations

Navigate to the **Home > Watched AMPs** page to begin backing up and monitoring AMP stations. Once an AMP installation has been added to the Watched AMP list, the Failover AMP will download the most recent backup and begin polling. The Failover AMP and the Watched AMP must be on the same version or else the watched AMP will be unable to restore properly. If any of the watched AMPs are not on the same version of AMP, you will need to upgrade. The Failover AMP will need HTTPS access (port 443) to the watched AMP to verify that the web page is active and to fetch downloads.

Once the Failover AMP determines that the Watched AMP is not up (based on the user-defined missed poll threshold) it will restore the data backup of the Watched AMP and begin monitoring the watched AMP APs and devices. There are many variables that affect how long this will take including how long client historical data is being retained, but for an AMP with 1,000 APs it might take up to 10 minutes. For an AMP with 2,500 APs, it might take as long as 20 minutes. The Failover AMP will retain its original IP address.

In summary, the Failover AMP could take over for the Watched AMP in as little as five minutes; it might take up to an additional 10-20 minutes to unpack the watched AMP data and begin monitoring APs. The most important factors are the missed poll threshold, which is defined by the user, and the size of the watched AMP backup, which is affected by the total number of APs and by the amount of data being saved, especially client historical data.

To restore the Watched AMP, run the backup script from the command line and copy the current data file and the old Watched AMP configuration file to the Watched AMP. Then run the restore script. More information about backups and restores can be found in [“Backing Up AMP” on page 223](#).

**Table 126** *Home > Watched Page Fields and Default Values*

Setting	Default	Description
<b>IP/Hostname</b>	None	The IP address or Hostname of the watched AMP. The Failover AMP needs HTTPS access to the watched AMPs.
<b>Username</b>	None	A username with management rights on the watched AMP.
<b>Password</b>	None	The password for the username with management rights specified above.
<b>HTTP Timeout (5-1000 Sec)</b>	60	The amount of time before AMP considers a polling attempt failed.
<b>Polling Enabled</b>	Yes	Enables or disables polling of the Watched AMP. <b>NOTE:</b> You do not need to disable polling of the watched AMP system if it is set to be down during nightly maintenance or is being upgraded.
<b>Polling Period</b>	5 minutes	The amount of time between polls of the Watched AMP.
<b>Missed Poll Threshold</b>	None	The number of polls that can be missed before the failover AMP will begin actively monitoring the Watched AMP APs.

## Logging out of AirWave

To log out of AirWave, select the **Logout** link on the upper right hand corner of every AirWave page.

You will be logged off automatically based on the number of minutes set in the **Idle Timeout** setting of **Home > User Info**. Refer to [“Configuring Login Message, TACACS+ and RADIUS Authentication” on page 49](#).





This chapter describes AirWave reports, including access, creation, scheduling, and distribution.

This chapter includes the following sections:

- “Overview of AMP Reports” on page 227
- “Using Daily Reports” on page 230
- “Defining Reports” on page 252
- “Emailing and Exporting Reports” on page 255

AirWave ships with several reports enabled by default. Default reports may run nightly or weekly, depending on the AMP release. Review the list of defined and scheduled reports with the **Reports > Generated** and **Reports > Definition** pages to determine if default reports are desired. If not, you can delete, disable, or reschedule any of them.

AirWave supports additional specialized reports as follows:

- **System > Status** page supports the diagnostic report file for sending to customer support: diagnostics.tar.gz.
- **System > Status** page supports the VisualRF diagnostics report file: VisualRFdiag.tar.gz.
- **VisualRF > Network View** supports the Bill of Materials (BOM) report. Refer to [Chapter 10, “Using VisualRF”](#) on page 257.

## Overview of AMP Reports

Reports are powerful tools in network analysis, user configuration, device optimization, and network monitoring on multiple levels. Among their benefits, reports provide an interface for multiple configurations.

AirWave reports have the following general parameters:

- AMP runs daily versions of all reports during predefined windows of time. All reports can be scheduled to run in the background.
- The daily version of any report is available instantly in the **Reports > Generated** page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that don’t span a period of time. Instead, these two reports provide a snapshot of the current state of the network.
- Users can create all other reports over a custom time period on the **Reports > Definitions** page. All reports can be emailed or exported to XML format for easy data manipulation using a spreadsheet.

### Reports > Definitions Page Overview

The **Reports > Definitions** page allows you to define new reports and see the reports already defined.

The **Definitions** page includes these sections:

- **Report definitions** section—The **Add** button allows you to define a custom report using the **Custom Options** drag and drop interface, or from any of the report types in the dropdown menu. The **Report Definitions** table has a complete list of all saved report definitions with an option to return to each definition’s table to further customize your report.
  - **Add and Run** allows you to create a report definition and run that report immediately.

- **Run Now** (visible from the expanded **Report Definitions** menu) allows immediate running of a custom report as soon as you set the parameters. You must save its definition separately, if you want to remember the parameters.
- **Report definitions for other roles** section—This section, supported for **admin** users, displays additional reports that have been scheduled for other roles. This section of the page adds the **Role** column, and other columns are the same.

Each pane includes a **Latest Report** column with the most recently run reports for each definition and role created. **Run** and **Delete** buttons allow you to select a report from the definitions table to run or delete. Once you define a report from the **Definition** page, it appears on the **Generated** page. The **Reports > Definition** page is shown in [Figure 164](#), and [Table 127](#) describes the fields available when you select a specific report definition.

**Table 127 Reports > Definition Page Fields and Descriptions**

Field	Description
<b>Report Definition</b>	Displays a field for entering report title and dropdown menu, shown in <a href="#">Figure 165</a> , displaying all possible report types.
<b>Report Restrictions</b>	Displays dynamic fields that include spaces for selecting attributes and entering data relevant to your selected report type scope such as groups, folders, SSID, Device Search filter, report start and end times.
<b>Scheduling Options</b>	Reveals options for one time or regularly scheduled reporting by selecting <b>Yes</b> . Options include report frequency, start time, and current system time.
<b>Report Visibility</b>	Allows you to determine a report's visibility according to user role.
<b>Email Options</b>	Reveals email address preferences for sending reports by selecting <b>Yes</b> .
<b>Add and Run</b>	Allows you to create a report definition and run that report right then.
<b>Run Now</b>	Allows you to run any report that has been defined on the spot without saving settings or creating a new report definition.
<b>Add</b>	Saves report definition you just created.

**Figure 164 Reports > Definitions Page Illustration (Split View)**

Report definitions:

New Report Definition

Reports are available on the [Generated Reports](#) page after they have been run.

1-20 ▼ of 45 Report Definitions Page 1 ▼ of 3 > >|

	Title ▲	Type	Subject
<input type="checkbox"/>	VoWLAN Devices	Device Summary	SSID intranet-voip
<input type="checkbox"/>	VoWLAN Usage	Network Usage	SSID intranet-voip
<input type="checkbox"/>	VoWLAN User Sessions	User Session	SSID intranet-voip
<input type="checkbox"/>	Avir-uptime	Device Uptime	Group HQ
<input type="checkbox"/>	Capacity Planning Max Values	Capacity Planning	All Groups, Folders and SSIDs
<input type="checkbox"/>	Custom Device Summary Report	Device Summary	Group HQ
<input type="checkbox"/>	Custom IDS Events Report	IDS Events	All Groups and Folders

Latest Report	Report Start	Report End	Last Run Time	Scheduled
VoWLAN Devices	2 weeks ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
VoWLAN Usage	1 week ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
VoWLAN User Sessions	2 weeks ago	now	5/15/2009 3:00 PM	Every Friday at 3:00 pm PDT
Avir-uptime	last week	today	5/19/2009 12:19 AM	-
Capacity Planning Max Values	3/1/2009	12:00 a.m. today	5/21/2009 12:15 AM	Daily at 12:15 am PDT
Custom Device Summary Report	2 weeks ago	now	5/14/2009 6:36 AM	-
Custom IDS Events Report	5/14/09 22:00	5/14/09 23:00	5/15/2009 7:13 AM	-

Select All - Unselect All

Report definitions for other roles:

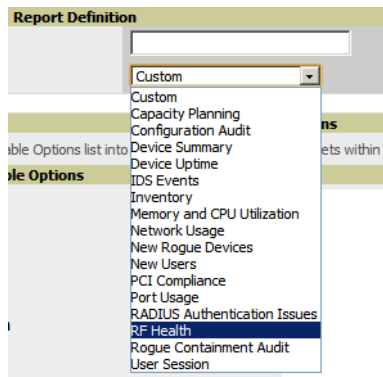
1-4 ▼ of 4 Report Definitions Page 1 ▼ of 1

	Role ▲	Title	Type	Subject
<input type="checkbox"/>	corp-users-via-radius	Radius Auth Problems	RADIUS Authentication Issues	All Groups, Folders and SSIDs
<input type="checkbox"/>	Partner	Device Summary Report	Device Summary	All Groups, Folders and SSIDs
<input type="checkbox"/>	Partner	RADIUSReport	RADIUS Authentication Issues	Group <a href="#">Research Lab</a> and Folder <a href="#">Top &gt; Sunnyvale HQ &gt; HQ Cisco LWAPP</a> and SSID <a href="#">wpa2</a>
<input type="checkbox"/>	Partner	PCICompliance-Detailed-3wks-Acme	PCI Compliance	Group HQ

Latest Report	Report Start	Report End	Last Run Time	Scheduled
-	yesterday	now	4/27/2009 2:21 PM	-
Device Summary Report	5/5/2009	5/8/2009	5/8/2009 10:58 AM	-
-	1/1/2009	3/31/2009	3/31/2009 6:08 AM	-
PCICompliance-Detailed-3wks-Acme	3 weeks ago	now	4/28/2009 7:12 AM	-

Select All - Unselect All

**Figure 165 Report Type Drop-down Menu in Reports > Definitions Illustration**



Only **admin** users have complete access to all report information. The AMP reports and online displays of information can vary with configuration, User Roles, and Folders.

## Reports > Generated Page Overview

The **Reports > Generated** page displays reports that have been run, as well as the most recent daily version of any report. An **Admin** user can see and edit all report definitions in AMP. Users with **Monitor Only** roles can see reports and definitions only if they have access to all devices in the reports.

The **Reports > Generated** page contains three primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The latest daily reports for immediate online viewing

**Figure 166 Reports > Generated Page Example**

**Generated reports:**  
Visit the [Report Definitions](#) page to run new reports.  
1-20 ▼ of 959 Reports Page 1 ▼ of 48 > >|

<input type="checkbox"/>	Generation Time ▼	Title	Type	Subject	Report Start	Report End
<input type="checkbox"/>	5/21/2009 3:24 AM	test	Network Usage	All Groups, Folders and SSIDs	11/21/2008 2:51 AM	5/21/2009 2:51 AM
<input type="checkbox"/>	5/21/2009 3:05 AM	yourdomain.user session	User Session	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 3:05 AM	yourdomain.radius authentication issues	RADIUS Authentication Issues	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 2:48 AM	yourdomain.new users	New Users	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 2:48 AM	yourdomain.new rogue devices	New Rogue Devices	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 2:48 AM	yourdomain.network usage	Network Usage	All Groups, Folders and SSIDs	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 2:24 AM	yourdomain.memory and cpu utilization	Memory and CPU Utilization	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM
<input type="checkbox"/>	5/21/2009 2:23 AM	yourdomain.inventory	Inventory	All Groups and Folders	-	-
<input type="checkbox"/>	5/21/2009 2:23 AM	yourdomain.ids-event	IDS Events	All Groups and Folders	5/20/2009 2:00 AM	5/21/2009 2:00 AM

Select All - Unselect All

---

**Generated reports for other roles:**  
1-5 ▼ of 5 Reports Page 1 ▼ of 1

<input type="checkbox"/>	Role ▲	Generation Time	Title	Type	Subject	Report Start	Report End
<input type="checkbox"/>	Admin Team	4/24/2009 9:19 AM	Capacity Report From Cron	Capacity Planning	All Groups, Folders and SSIDs	4/23/2009 12:00 AM	4/24/2009 12:00 AM
<input type="checkbox"/>	Admin Team	Failed	Capacity Report From Cron	Capacity Planning	All Groups, Folders and SSIDs	4/23/2009 12:00 AM	4/24/2009 12:00 AM
<input type="checkbox"/>	Partner	4/28/2009 7:15 AM	PCICompliance-Detailed-3wks-Acme	PCI Compliance	Group Acme HQ	4/7/2009 7:12 AM	4/28/2009 7:12 AM

Select All - Unselect All

**Figure 167** *Reports > Generated Page with Single-click Report Viewing Options*

Latest Capacity Planning Report  
Latest Configuration Audit Report  
Latest Custom Report  
Latest Device Summary Report  
Latest Device Uptime Report  
Latest IDS Events Report  
Latest Inventory Report  
Latest Memory and CPU Utilization Report  
Latest Network Usage Report  
Latest New Rogue Devices Report  
Latest New Users Report  
Latest PCI Compliance Report  
Latest Port Usage Report  
Latest RADIUS Authentication Issues Report  
Latest RF Health Report  
Latest User Session Report

## Using Daily Reports

This section describes the default and custom-scheduled reports supported in AMP. These reports can be accessed from the **Reports > Generated** page.

### Viewing Generated Reports

The **Reports > Generated** page supports the following general viewing options:

- By default, the reports on the **Reports > Generated** page are sorted by **Generation Time**. You can sort reports by any other column header in sequential or reverse sequential order. You can also choose columns, export the Generated Reports list in CSV, and modify the pagination of this list.
- The **Reports > Detail** page launches when you select any report title from this page.

The **Generated Reports** page contains fewer columns and information than the **Definitions** page. [Table 128](#) describes each column for the **Reports > Generated** page.

**Table 128** *Reports > Generated Page Fields and Descriptions*

Field	Description
<b>Generated Time</b>	Displays the date and time of the last time the report was run, or when the latest report is available. Selecting the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and selecting <b>Run</b> .
<b>Title</b>	Displays title of the report. This is a user-configured field when creating the report.
<b>Type</b>	Displays the type of the report.
<b>Subject</b>	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
<b>Report Start</b>	Displays the beginning of the time period covered in the report.
<b>Report End</b>	Displays the end of the time period covered in the report.
<b>Role</b>	In the <b>Reports definitions for other roles</b> section, this column indicates the roles for which additional reports are defined.

### Using Custom Reports

Custom reports allow users to specify the data that should be included in a report.

Perform these steps to create a Custom Report.

1. Navigate to the **Reports > Definitions** page.
2. Select **Add**.
3. By default, the Custom option will be selected in the Type drop-down menu, and the **Custom Options** section appears below as shown in [Figure 168](#).

**Figure 168 AMP Custom Options Page Illustration**

Available Options	Selected Options
<ul style="list-style-type: none"> <li>Aruba License</li> <li>Capacity Planning</li> <li>Client Inventory</li> <li>Client Session</li> <li>Configuration Audit</li> <li>Device Summary</li> <li>Device Uptime</li> <li>IDS Events</li> <li>Inventory</li> <li>Memory and CPU Utilization</li> <li>Network Usage</li> <li>New Clients</li> <li>New Rogue Devices</li> <li>Port Usage</li> <li>RADIUS Authentication Issues</li> <li>RF Health</li> <li>Rogue Clients</li> <li>Rogue Containment Audit</li> <li>VPN Session</li> </ul>	<ul style="list-style-type: none"> <li>VPN Session: Summary</li> <li>VPN Session: Session Data by VPN Type (Charts)</li> <li>VPN Session: Session Data by VLAN (List)</li> <li>VPN Session: Session Data by VLAN (Charts)</li> <li>VPN Session: Session Data by VPN Type (List)</li> <li>VPN Session: Session Data by Controller (Charts)</li> <li>VPN Session: Session Data by Controller (List)</li> <li>VPN Session: Session Data by HTTP Fingerprint (List)</li> <li>VPN Session: Session Data by HTTP Fingerprint (Charts)</li> <li>VPN Session: Session Data by AOS Device Type (Charts)</li> <li>VPN Session: Sessions</li> <li>VPN Session: Session Data by AOS Device Type (List)</li> <li>VPN Session: Session Data by Users</li> </ul>

The left pane of the **Custom Options** section lists all available data that can be included in the report. For example, if the data you want to include is in the RF Health report, select **RF Health** to view a list of all available radio frequency information. Then, simply drag the desired data from the **Available Options** list on the left to the **Selected Options** pane on the right.

The order of the data in the **Selected Options** section is the order that it will appear in the report. The data can be reordered by dragging an item up or down the list.

- Below the Custom Options panes are the **Report Restrictions**, **Scheduling Options**, **Report Visibility**, and **Email Options** sections. Choose the parameters as needed for your report, especially a **Report Start** and **Report End**.
- When finished, select **Add and Run** to add the report to your list and run it immediately, **Run Now** to run without being added to the list, **Add** to add but not run the report, or **Cancel** to exit this page.

## Using the Aruba License Report

A new Aruba License Report has been added in the Reports tab to track licenses on Aruba devices in your network. This report includes information on the type, quantity, percent used, installation date, expiration date, and the license keys.

**Figure 169** *Aruba License Report Detail Page*

Aruba License Report for All Groups and Folders						
Generated on 5/26/2011 5:07 PM						
Details for Aruba800 in Group aruba gui no wms and Folder Top > aruba with Max #of APs 16						
1-8 ▼ of 8 Aruba800 Page 1 ▼ of 1 Export CSV						
License Type	License Qty	License Used (%)	Install Date	Expires	Flag	Key
AP Developers Module	-	-	2009-08-25 02:14:37	Never	E	bmo7joNC-2j0sUjxC-/rT8j2tm-Wwojkppa-8W001hkq-2zc
Voice Services Module	-	-	2009-08-25 02:14:23	Never	E	nFfoa6E5-pg6qxISM-/VtaNIp9-8wu4hM0u-Ohtnj1yP-XV\
External Services Interface	-	-	2009-08-26 03:00:14	Never	E	rw15Lw/A-EmZZHHsj-7IivmPeY-kBzU8Pkq-ZmiYaSMZ-Hv
MMC AP	-	-	2009-08-26 03:00:12	Never	E	c+8HJ9lp-cuHr79mk-8ytsOHO/-5TuLvZ9/-E5sTP/Un-A2k
xSec Module	-	-	2009-08-26 03:00:12	Never	E	dYh7cFQv-RsUH5jCA-+WUaGwyW-CTrYyhYl-QjFk7Gti-ge
Client Integrity Module	-	-	2009-08-26 03:00:13	Never	E	Oh5fstC-Xm/E763-2dSXW9Z-ATrbAjtT-IrQrsGQ-sew
Wireless Intrusion Protection	-	-	2009-08-26 03:00:13	Never	E	P4hkbzw-pZ4Uro5Z-OJ38dnL9-I0tLD/fX-Ku92sldt-oPw
VPN Server	-	-	2009-08-26 03:00:13	Never	E	HbnXkYdF-MOaoUls5-d6eweXq2-ZIVc8QK0-nHR4Fz/H-Fv
1-8 ▼ of 8 Aruba800 Page 1 ▼ of 1						
Details for 10.15.76.8 in Group 10.15.76.8 and Folder Top > 10.15.76.8 with Max #of APs 32						
1-1 ▼ of 1 10.15.76.8 Page 1 ▼ of 1 Export CSV						
License Type	License Qty	License Used (%)	Install Date	Expires	Flag	Key
Policy Enforcement Firewall for VPN users	-	-	2011-01-18 15:26:31	Never	E	dTjudtrN-908tVTT2-+JKsZhr1-K+n3r0XS-J
1-1 ▼ of 1 10.15.76.8 Page 1 ▼ of 1						
Details for Aruba3600-Master in Group aruba gui no wms and Folder Top > aruba > guest user with Max #of APs 16						
1-1 ▼ of 1 Aruba3600-Master Page 1 ▼ of 1 Export CSV						
License Type	License Qty	License Used (%)	Install Date	Expires	Flag	Key
Policy Enforcement Firewall for VPN users	-	-	2011-02-28 13:37:04	Never	E	kh+aiHT9-u8oKILF1-M+fEjnjH-aIeOfSU-BzZ
1-1 ▼ of 1 Aruba3600-Master Page 1 ▼ of 1						

## Using the Capacity Planning Report

The **Capacity Planning Report** tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. This report assists in analyzing device capacity and performance on the network, and such analysis can help to achieve network efficiency and improved experience for users.

This report is based on interface-level activity. The information in this report can be sorted by any column header in sequential or reverse-sequential order by selecting the column heading.

Refer also to the “Using the Network Usage Report” on page 241 for additional bandwidth information.

The following figures and Table 129 illustrate and describe the contents of the **Capacity Planning Report**.



Figure 170 Capacity Planning Report Detail Page

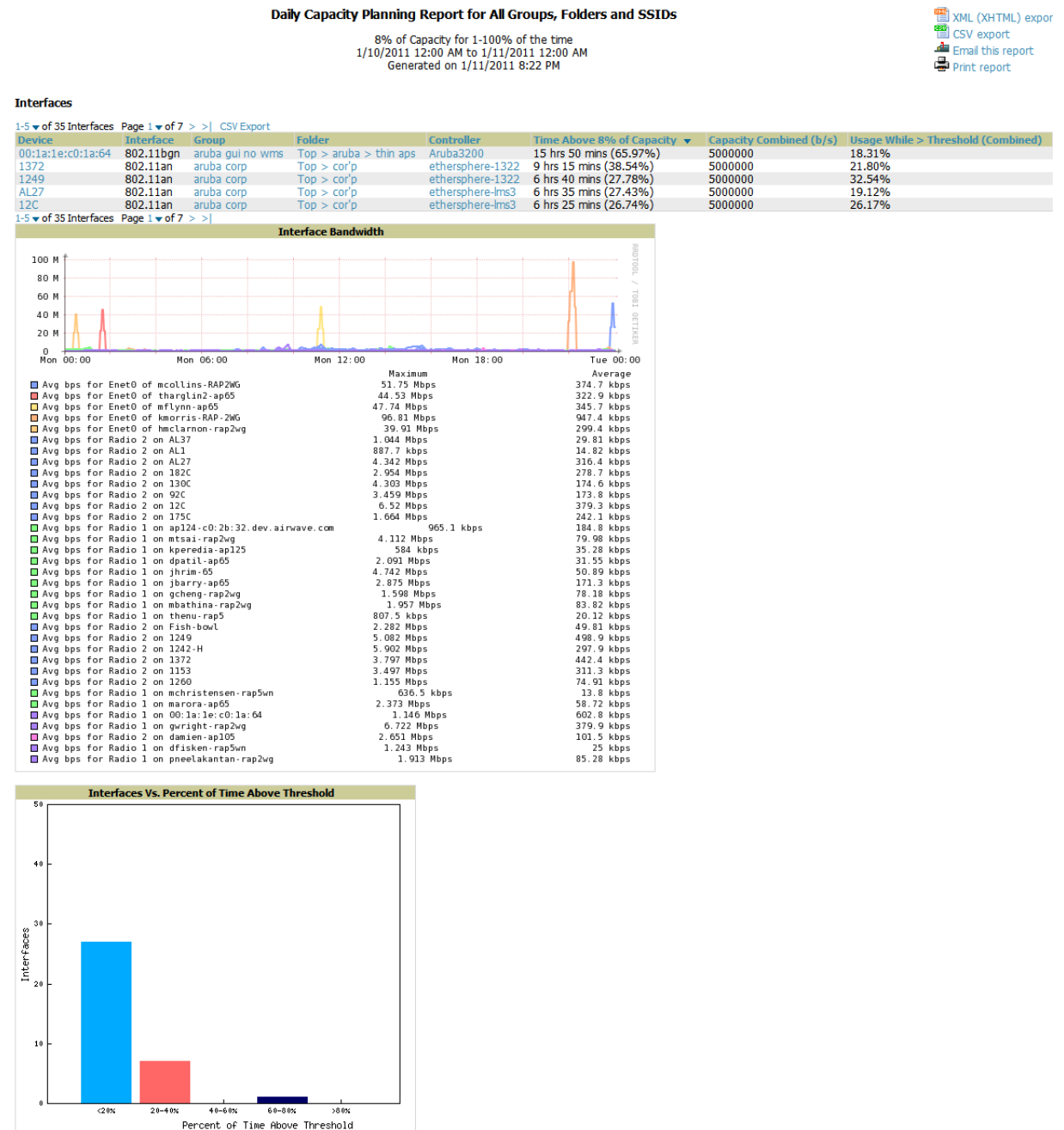


Table 129 Capacity Planning Report Fields and Contents, Top Portion

Field	Description
<b>Device</b>	Displays the device type or name.
<b>Interface</b>	Displays the type of 802.11 wireless service supported by the device.
<b>Group</b>	Displays the device group with which the device is associated.
<b>Folder</b>	Displays the folder with which the device is associated.
<b>Controller</b>	Displays the controller with which a device operates.
<b>Time Above 1% of Capacity</b>	Displays the time duration in which the device has functioned above 0% of capacity. A low percentage of use in this field may indicate that a device is under-used or poorly configured in relation to its capacity, or in relation to user needs.
<b>Capacity Combined (b/s)</b>	Displays the combined capacity in and out of the device, in bits-per-second.

**Table 129 Capacity Planning Report Fields and Contents, Top Portion (Continued)**

Field	Description
<b>Usage While &gt; Threshold (Combined)</b>	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
<b>Overall Usage (Combined)</b>	Displays the overall usage of the device, both combined in and out traffic.
<b>Usage While &gt; Threshold (in)</b>	Displays device usage that exceeds the defined and incoming threshold capacity.
<b>Overall Usage (In)</b>	Displays overall device usage for incoming data.
<b>Usage While &gt; Threshold (Out)</b>	Displays device usage for outgoing data that exceeds defined thresholds.
<b>Overall Usage (Out)</b>	Displays device usage for outgoing data.

## Using the Configuration Audit Report

The **Configuration Audit Report** provides an inventory of device configurations on the network, enabling you to display information one device at a time, one folder at a time, or one device group at a time. This report links to additional configuration pages.

Perform these steps to view the most recent version of the report, then to configure a given device using this report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and select **Latest Configuration Audit Report** to display **Detail** device configuration information for all devices. The ensuing **Detail** report can be very large in size, and provides multiple links to additional device configuration or information display pages.
3. You can display device-specific configuration to reduce report size and to focus on a specific device. When viewing configured devices on the **Detail** page, select a device in the **Name** column. The device-specific configuration appears.
4. You can create or assign a template for a given device from the **Detail** page. Select **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Select **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Select **Show Archived Device Configuration**.

Figure 171 and Table 130 illustrate and describe the general **Configuration Audit** report and related contents.

**Figure 171** *Reports > Generated > Daily Configuration Audit Report Page, abbreviated example*

XML (XHTML)
 export
 CSV export
 Email this report
 Print report

**Daily Configuration Audit Report for All Groups, Folders and SSIDs**

Generated on 5/21/2009 2:21 AM

1-20 of 360 Items
 Page 1 of 18
 > >|

Name	Folder	Group	Mismatches									
11.1.3	Top > Sunnyvale HQ	Corp HQ	<table> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None</td> <td>Mesh AP</td> </tr> </table>		Current Device Configuration	Desired Device Configuration	Location	(failed to fetch)	Not Available	Mesh Role	None	Mesh AP
	Current Device Configuration	Desired Device Configuration										
Location	(failed to fetch)	Not Available										
Mesh Role	None	Mesh AP										
11.1.4	Top > HQ	Corp HQ	<table> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None</td> <td>Mesh AP</td> </tr> </table>		Current Device Configuration	Desired Device Configuration	Location	(failed to fetch)	Not Available	Mesh Role	None	Mesh AP
	Current Device Configuration	Desired Device Configuration										
Location	(failed to fetch)	Not Available										
Mesh Role	None	Mesh AP										
11.1.5	Top > HQ	Corp HQ	<table> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None</td> <td>Mesh AP</td> </tr> </table>		Current Device Configuration	Desired Device Configuration	Location	(failed to fetch)	Not Available	Mesh Role	None	Mesh AP
	Current Device Configuration	Desired Device Configuration										
Location	(failed to fetch)	Not Available										
Mesh Role	None	Mesh AP										
11.1.6	Top > HQ	Corp HQ	<table> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None</td> <td>Mesh AP</td> </tr> </table>		Current Device Configuration	Desired Device Configuration	Location	(failed to fetch)	Not Available	Mesh Role	None	Mesh AP
	Current Device Configuration	Desired Device Configuration										
Location	(failed to fetch)	Not Available										
Mesh Role	None	Mesh AP										
1210-5	Top > HQ > Lab	Corp HQ	<table> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> <tr> <td>Location</td> <td>(failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Mesh Role</td> <td>None</td> <td>Mesh AP</td> </tr> </table>		Current Device Configuration	Desired Device Configuration	Location	(failed to fetch)	Not Available	Mesh Role	None	Mesh AP
	Current Device Configuration	Desired Device Configuration										
Location	(failed to fetch)	Not Available										
Mesh Role	None	Mesh AP										
Template: <div>             Actual aaa accounting network acct_methods start-stop group rad_acct              Actual aaa authentication login eap_methods group rad_eap              Actual aaa authentication login eap_methods4 group rad_eap4              Actual aaa authentication login mac_methods local              Actual aaa authorization exec default local              Actual aaa cache profile admin_cache              Actual all              Actual aaa group server radius dummy              Actual aaa group server radius rad_acct              Actual aaa group server radius rad_admin              Actual cache authentication profile admin_cache              Actual cache authorization profile admin_cache              Actual cache expiry 1              Actual aaa group server radius rad_eap              Actual aaa group server radius rad_eap4              Actual server 10.2.25.180 auth-port 1645 acct-port 1646              Actual server 10.2.25.180 auth-port 1812 acct-port 1813           </div>												

Airwave\_Cisco\_LWAPP

Top > Sunnyvale HQ > HQ Cisco LWAPP

Research Lab

	Current Device Configuration	Desired Device Configuration
802.11a Channel Assignment Method	Automatic	Static
802.11a Coverage Measurement	180	300
802.11a DCA Channel 165	Disabled	Enabled
802.11a DCA Channel 190	Disabled	Enabled
802.11a DCA Channel 196	Disabled	Enabled
802.11a DTPC Support	Enabled	Disabled
802.11a Data Fragmentation Threshold	2346	2337
802.11a Global Default Transmit Power Level	1	5
802.11a Load Measurement	60	300
802.11a Noise Measurement	180	300
802.11a Power Level Assignment Method	Automatic	Fixed

**Table 130** *Daily Configuration Audit Report*

Field	Description
<b>Name</b>	Displays the device name for every device on the network. Selecting a given device name in this column allows you to display device-specific configuration.
<b>Folder</b>	Displays the folder in which the device is configured in AMP. Selecting the folder name in this report displays the <b>APs/Devices &gt; List</b> page for additional device, folder and configuration options.
<b>Group</b>	Displays the group with which any given device associates. Selecting the group for a given device takes you to the <b>Groups &gt; Monitor</b> page for that specific group, to display graphical group information, modification options, alerts, and an audit log for the related group.
<b>Mismatches</b>	This field displays configuration mismatch information. When a device configuration does not match ideal configuration, this field displays the ideal device settings compared to current settings.

## Using the Device Summary Report

The **Device Summary Report** identifies devices that are the most or least used devices, and a comprehensive list of all devices. One potential use of this report is to establish more equal bandwidth distribution across multiple devices. This report contains the following five lists of devices.

- **Most Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that support the highest numbers of users. This list provides links to additional information or configuration pages for each device to make adjustments, as desired.

- **Most Utilized by Bandwidth**—By default, this list displays the 10 devices that consistently have the highest bandwidth consumption during the time period defined for the report. This list provides links to additional information or configuration pages for each device.
- **Least Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—By default, this list displays the 10 devices that are the least used, according to the bandwidth throughput.
- **Devices**—This list displays all devices in AMP. By default it is sorted alphabetically by device name.



---

You can specify the number of devices that appear in each of the first four categories in the **Reports > Definitions > Add** page.

---

Any section of this report can be sorted by any of the columns. For example, you can specify a location and then sort the **Devices** list by the **Location** column to see details by location, or you can see all of the APs associated with a particular controller by sorting on the **Controller** column. If the AP name contains information about the location of the AP, you can sort by AP name.

If sorting the **Devices** list does not provide you with sufficient detail, you can specify a **Group** or **Folder** in the report **Definition** of a custom report. If you create a separate Group or Folder for each set of master and local controllers, you can generate a separate report for each Group or Folder. With this method, the summary sections of each report contain only devices from that Group or Folder.

and [Table 131](#) illustrate and describe the **Reports > Generated > Device Summary Detail** page.

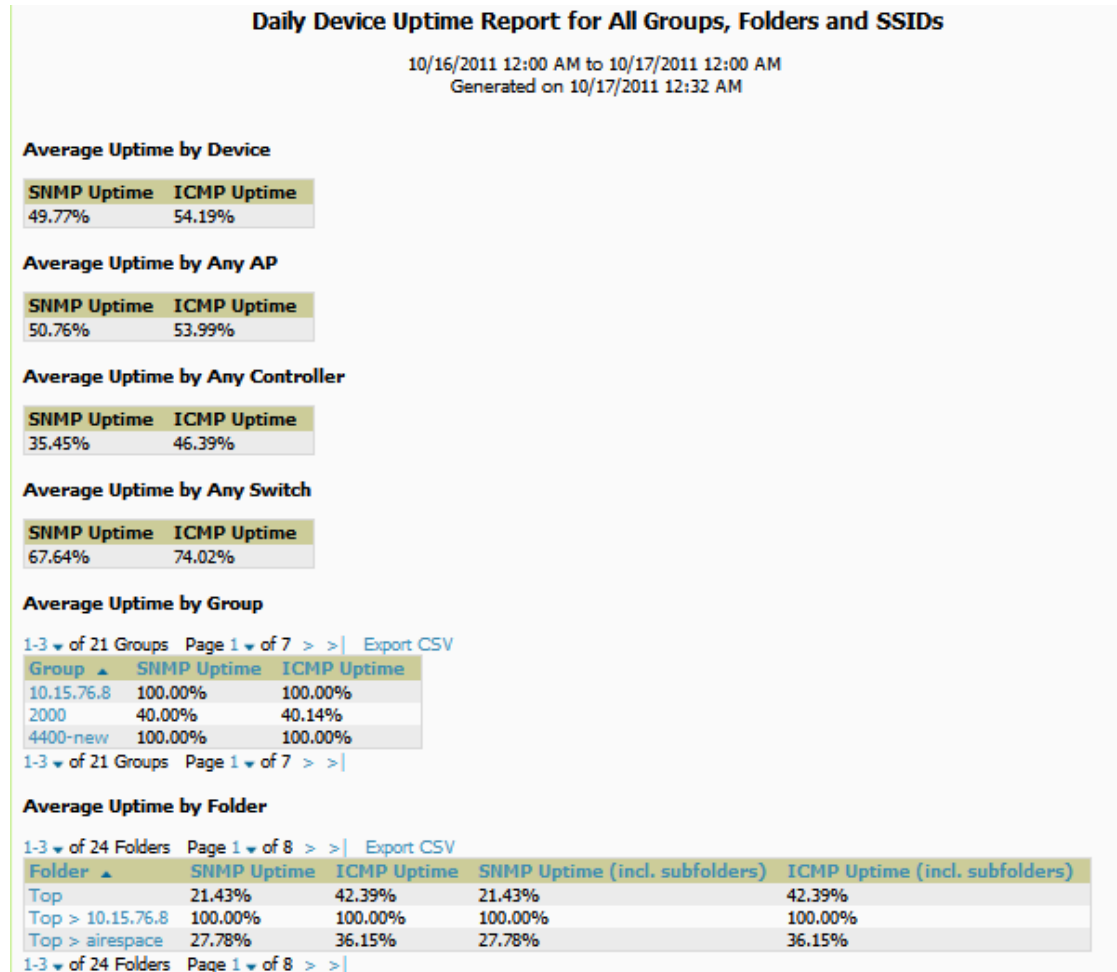


You can use this report as the central starting point to improve uptime by multiple criteria. This report covers protocol-oriented, device-oriented, or SSID-oriented information. This report can help to monitor and optimize the network in multiple ways. It can demonstrate service parameters, can establish locations that have superior or problematic uptime availability, and can help with additional analysis in multiple ways. Locations, device groups, or other groupings within a network can be identified as needing attention or can be proven to have superior performance when using this report.

As of AirWave 7.4, the Device Uptime Report contains four new columns that track bootstrap count (number of times the device has gone down for a firmware change), reboot count, downtime duration, and downtime duration percent. As mentioned above, you can optionally ignore device downtime during planned maintenance periods in this report, and you can restrict the report to business days only.

Figure 173 and Table 131 illustrate and describe the **Device Uptime** report.

**Figure 173 Device Uptime Report Illustration**



**Table 132 Reports > Generated > Device Uptime Report Unique Fields and Descriptions**

Field	Description
<b>SNMP Uptime</b>	Displays the percentage of time the device was reachable via ICMP. AMP polls the device via SNMP at the rate specified on the <b>Groups &gt; Basic</b> page.
<b>ICMP Uptime</b>	Displays the percentage of time the device was reachable via ICMP. If the device is reachable via SNMP it is assumed to be reachable via ICMP. AMP only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
<b>Time Since Last Boot</b>	The uptime as reported by the device at the end of the time period covered by the report.

## Using the IDS Events Report

The **IDS Events Report** lists and tracks IDS events on the network involving APs or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response.



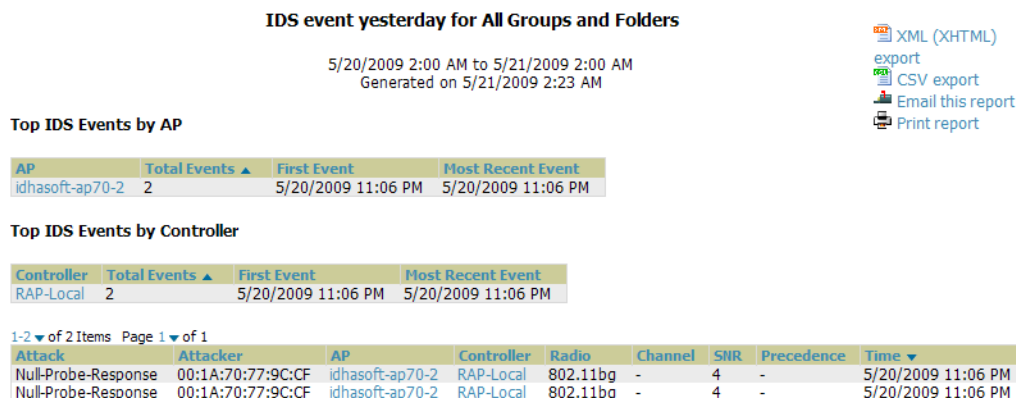
Your role must be enabled to view RAPIDS to see this report.

The **Home > Overview** page also cites IDS events, and triggers can be configured for IDS events. Refer to “[Setting Triggers for IDS Events](#)” on page 193 for additional information.

Selecting the AP device or controller name takes you to the **APs/Devices > List** page.

[Figure 174](#) and [Table 133](#) illustrate and describe the **Reports > Generated > IDS Events Detail** page.

**Figure 174** *Reports > Generated > IDS Events Report Illustration*



**Table 133** *Reports > Generated > IDS Events Detail Unique Fields and Descriptions*

Field	Description
Attack	Displays the name or label for the IDS event.
Controllers	This column lists the controllers for which IDS events have occurred in the prior 24 hours, and provides a link to the <b>APs/Devices &gt; Monitor</b> page for each.
Attacker	Displays the MAC address of the device that generated the IDS event.
Radio	Displays the 802.11 radio type associated with the IDS event.
Channel	Displays the 802.11 radio channel associated with the IDS event, when known.
SNR	Displays the signal-to-noise (SNR) radio associated with the IDS event.
Precedence	Displays precedence information associated with the IDS event, when known.
Time	Displays the time of the IDS event.

## Using the Inventory Report

The **Inventory Report** itemizes all devices and firmware versions on the network, to include vendor information and graphical pie-chart summaries. The primary sections of this report are as follows:

- Vendor Summary—Lists the vendors for all devices or firmware on the network.
- Firmware Version Summary—Lists the firmware version for all firmware used on the network.
- Model Summary—Lists the model numbers for all devices or firmware on the network.

See [Figure 175](#) for an illustration of a sample report.

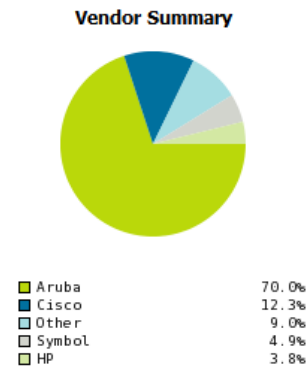


Figure 175 Reports > Generated > Inventory Report Illustration (Edited View)

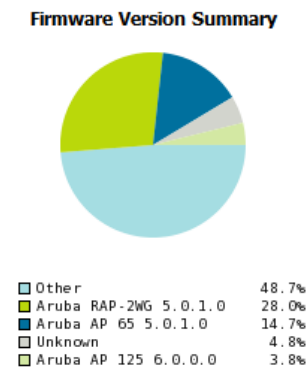
### Daily Inventory Report for All Groups and Folders

Generated on 1/10/2011 12:27 AM

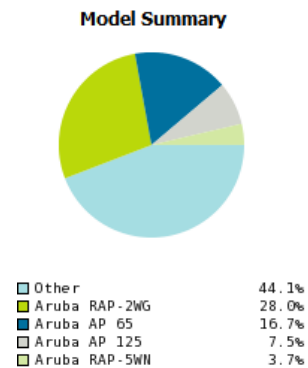
XML (XHTML) exp  
CSV export  
Email this report  
Print report



Vendor	Count	% of Total
Aruba	382	69.96%
Cisco	67	12.27%
Symbol	27	4.95%
HP	21	3.85%
Meru	7	1.28%
Proxim	6	1.10%
Router/Switch	6	1.10%
Enterasys	4	0.73%
3Com	4	0.73%
Trapeze	4	0.73%
Nortel	3	0.55%
Nomadix	3	0.55%
LANCOM	3	0.55%
Alcatel-Lucent	2	0.37%
APC	2	0.37%
D-Link	1	0.18%
Netgear	1	0.18%
Dell	1	0.18%
Juniper	1	0.18%
Hirschmann	1	0.18%
20 Vendors	546	100.00%



Firmware Version	Count	% of Total
3Com AP2750 7.0.4.4.0	1	0.18%
3Com AP3750 7.0.4.4.0	1	0.18%
3Com WX1200 7.0.4.4.0	1	0.18%
Alcatel-Lucent AP 124 5.0.1.0	1	0.18%
Alcatel-Lucent OAW-4308 5.0.1.0	1	0.18%
APC AP7900 v3.7.0	2	0.37%
Aruba 200 5.0.2.0	3	0.55%
Aruba 2400 3.1.1.7	1	0.18%
Aruba 2400 3.4.3.1	1	0.18%
Aruba 2400 5.0.1.0	1	0.18%
Aruba 3200 3.3.2.24-m-3.1.11	1	0.18%
Aruba 3200 6.0.0.1	1	0.18%
Aruba 3200 6.0.1.0	1	0.18%
Aruba 3400 3.3.2.24-m-3.1.12	1	0.18%
Aruba 3600 5.0.1.0	5	0.92%
Aruba 3600 6.0.0.0	2	0.37%
Aruba 6000 3.4.4.0	1	0.18%
Aruba 6000 6.0.0.0	1	0.18%
Aruba 620 3.4.2.5	1	0.18%
Aruba 651 3.4.3.0	1	0.18%
Aruba 651 6.0.0.0	1	0.18%
Aruba 800 2.5.6.20	1	0.18%
Aruba 800 3.3.2.19-FIPS	1	0.18%
Aruba 800 5.0.2.0	2	0.37%
Aruba AP 105 3.4.4.0	8	1.47%
Aruba AP 105 5.0.1.0	2	0.37%
Aruba AP 105 6.0.1.0	1	0.18%
164 Versions	546	100.00%



Model	Count	% of Total
Aruba RAP-2WG	153	28.02%
Aruba AP 65	91	16.67%
Aruba AP 125	41	7.51%
Aruba RAP-5WN	20	3.66%
Aruba AP 70	16	2.93%
Aruba AP 105	12	2.20%
Cisco Aironet 1030 LWAPP	9	1.65%
Cisco Aironet 1000 LWAPP	8	1.47%
Aruba 3600	7	1.28%
Aruba AP 61	6	1.10%
Unknown	6	1.10%
Cisco Catalyst 3750-24TS	5	0.92%
Symbol 5131	4	0.73%
Symbol AP 100	4	0.73%
Aruba 800	4	0.73%
HP ProCurve 420	3	0.55%
Proxim AP-700	3	0.55%
118 Models	546	100.00%

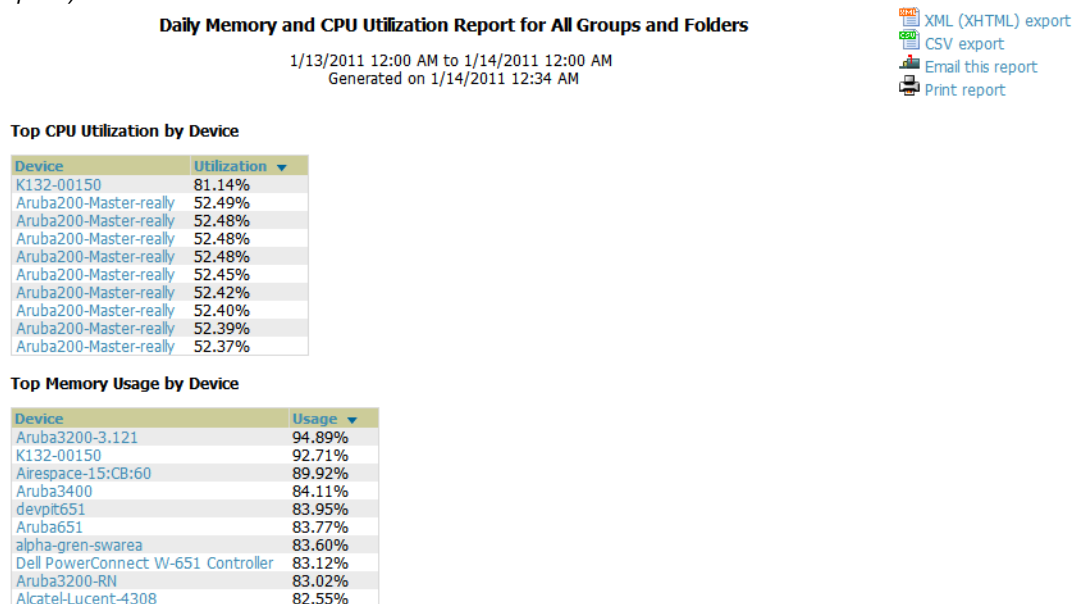
## Using the Memory and CPU Utilization Report

The **Memory and CPU Utilization Report** displays the top memory usage by device, and CPU usage on the network by device. Both are by percentage.

To create a scheduled and generated report of this type, refer to “Using Daily Reports” on page 230.

Figure 176 illustrates the **Reports > Detail** page for this report.

**Figure 176 Reports > Generated > Daily Memory and CPU Usage Report Illustration (Contents Rearranged for Space)**



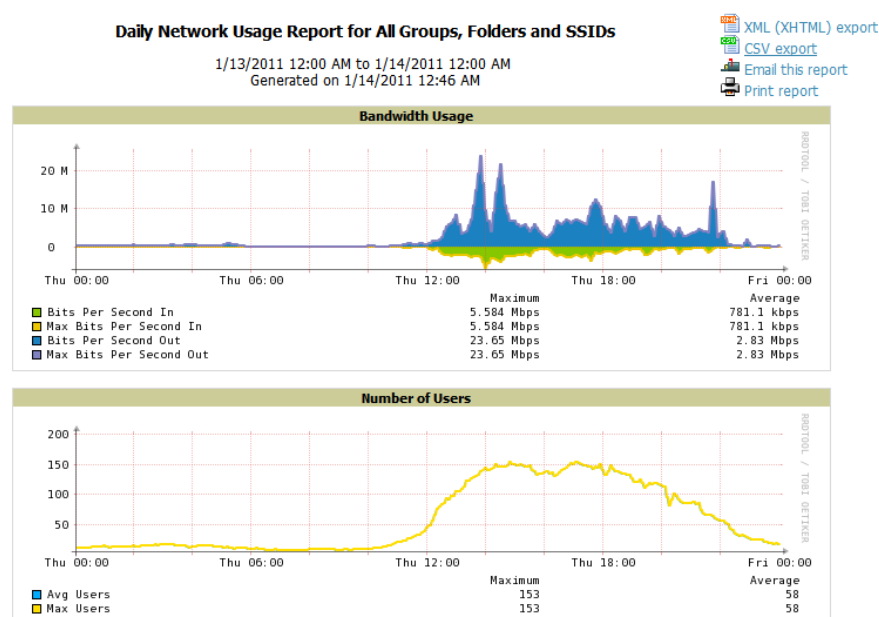
## Using the Network Usage Report

The **Network Usage Report** contains network-wide information in two categories:

- **Bandwidth usage by device**—maximum and average bandwidth in kbps
- **Number of users by time period**—average bandwidth in and out

Figure 177 illustrates the **Reports > Detail** page for the Daily Network Usage.

**Figure 177 Reports > Generated > Network Usage Report Illustration**



## Using the New Rogue Devices Report

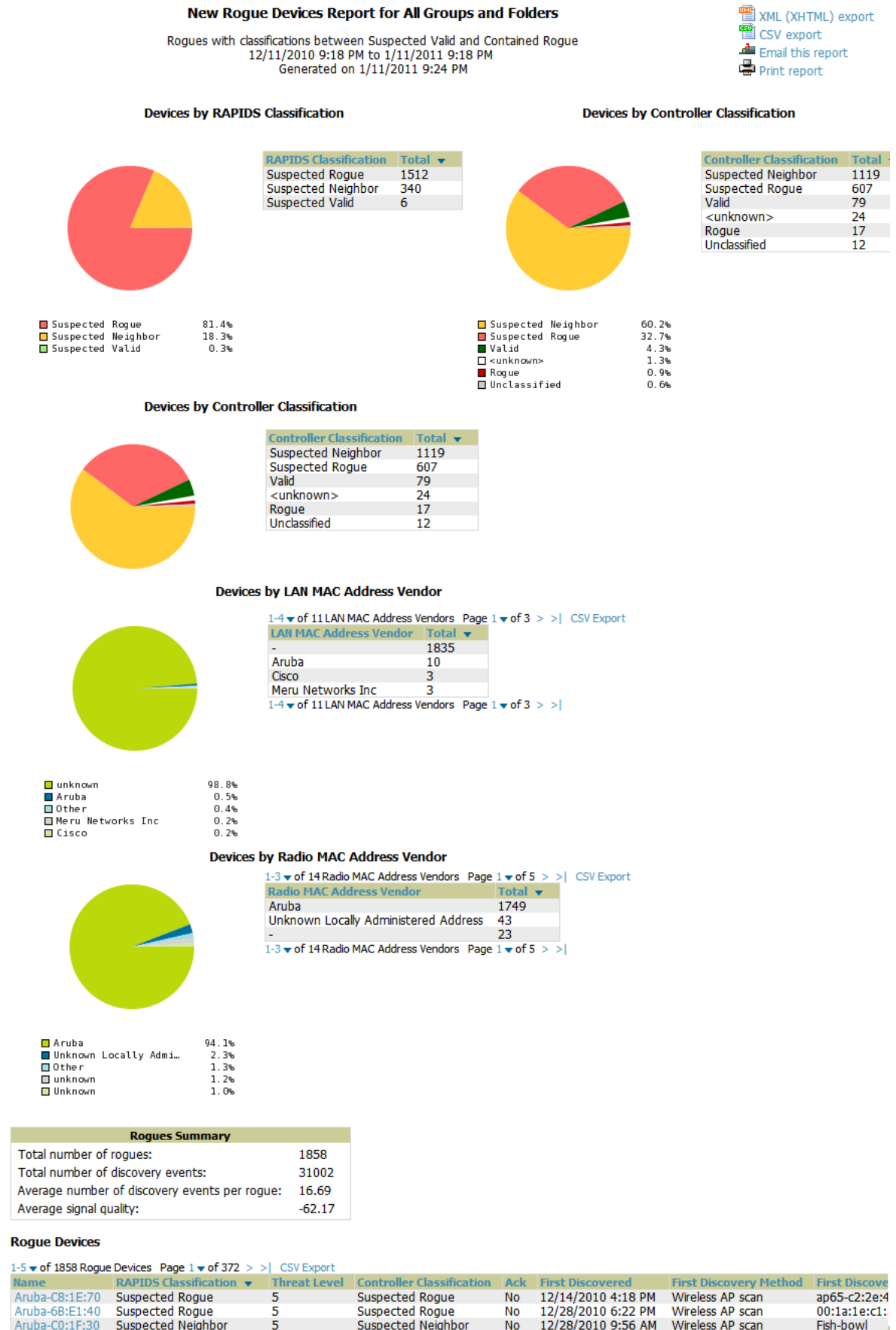
The **New Rogue Devices Report** summarizes rogue device information including the following categories of information:

- Rogue devices by RAPIDS classification—described in [“Using RAPIDS and Rogue Classification” on page 167](#)
- Top rogue devices by number of discovering APs
- Top rogue devices by signal strength
- Graphical summary of rogue devices by LAN MAC address vendor
- Graphical summary of rogue devices by radio MAC address vendor
- Text-based table summary of rogue device counts
- Detailed and text-based table of rogue devices discovered only wirelessly with extensive device parameters and hyperlink interoperability to additional AMP pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional AMP pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional AMP pages

This report is not run by default, but is available after you define it.

Refer to [Figure 178](#) for a sample illustration of this report.

**Figure 178 Reports > Generated > New Rogue Devices Report Illustration**



The rogue device inventories that comprise this report contain many fields, described in [Table 134](#).

**Table 134** *New Rogue Devices Report Fields*

Field	Description
<b>Name</b>	Displays the device name, as able to be determined.
<b>RAPIDS Classification</b>	Displays the RAPIDS classification for the rogue device, as classified by rules defined on the <b>RAPIDS &gt; Rules</b> page. Refer to <a href="#">“Using RAPIDS and Rogue Classification” on page 167</a> for additional information.
<b>Threat Level</b>	Displays the numeric threat level by which the device has been classified, according to rules defined on the <b>RAPIDS &gt; Rules</b> page. Refer to <a href="#">“Using RAPIDS and Rogue Classification” on page 167</a> for additional information.
<b>Ack</b>	Displays whether the device has been acknowledged with the network.
<b>First Discovered</b>	Displays the date and time that the rogue device was first discovered on the network.
<b>First Discovery Method</b>	Displays the method by which the rogue device was discovered.
<b>First Discovery Agent</b>	Displays the network device that first discovered the rogue device.
<b>Last Discovering AP</b>	Displays the network device that most recently discovered the rogue device.
<b>Model</b>	Displays the rogue device type when known.
<b>Operating System</b>	Displays the operating system for the device type, when known.
<b>IP Address</b>	Displays the IP address of the rogue device when known.
<b>SSID</b>	Displays the SSID for the rogue device when known.
<b>Network Type</b>	Displays the network type on which the rogue was detected, when known.
<b>Channel</b>	Displays the wireless RF channel on which the rogue device was detected.
<b>WEP</b>	Displays WEP encryption usage when known.
<b>RSSI</b>	Displays Received Signal Strength (RSSI) information for radio signal strength when known.
<b>Signal</b>	Displays signal strength when known.
<b>LAN MAC Address</b>	Displays the MAC address for the associated LAN when known.
<b>LAN Vendor</b>	Displays LAN vendor information associated with the rogue device, when known.
<b>Radio MAC Address</b>	Displays the MAC address for the radio device, when known.
<b>Radio Vendor</b>	Displays the vendor information for the radio device when known.
<b>Port</b>	Displays the router or switch port associated with the rogue device when known.
<b>Last Seen</b>	Displays the last time in which the rogue device was seen on the network.
<b>Total Discovering APs</b>	Displays the total number of APs that detected the rogue device.
<b>Total Discovery Events</b>	Displays the total number of instances in which the rogue device was discovered.

## Using the New Users Report

The **New Users Report** lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more. The report definition can filter on connection mode (wired, wireless or both).

Figure 179 illustrates the fields and information in the **New Users Report**.

Figure 179 **Reports > Generated > New Users Report Illustration**

Daily New Users Report for All Groups, Folders, SSIDs and Roles

2/6/2010 12:00 AM to 2/7/2010 12:00 AM

Generated on 2/7/2010 12:16 AM

New Users

1-9 of 9 New Users Page 1 of 1

Username	Role	MAC Address	Vendor	AP/Device	Association Time	Duration
-	VoFi	00:03:2A:00:03:2A	UniData Communication Systems, Inc.	Operations-AL25	1/20/2009 6:25 PM	38 mins
NETWORKS\abc	employee	00:16:CF:00:16:CF	Hon Hai Precision Ind. Co., Ltd.	ExecutiveSuite-AL16	1/20/2009 5:17 PM	17 mins
-	-	00:03:2A:00:03:2A	Cisco-Linksys LLC	HQ-Engineering	1/20/2009 2:46 PM	5 mins
wifiphone	employee	00:16:CF:00:16:CF	UniData Communication Systems, Inc.	Haystack-AL29	1/20/2009 1:44 PM	10 hrs 31 m
employee@networks.com	employee	00:03:2A:00:03:2A	Nokia Danmark AS	Area51-AL33	1/20/2009 11:17 AM	6 mins
58224	visitor	00:16:CF:00:16:CF	Intel	Facilities-AL37	1/20/2009 11:11 AM	2 hrs 33 m

XML (XHTML)

export

CSV export

Email this report

Print report

XML (XHTML)  
 export  
 CSV export  
 Email this report  
 Print report

## Using the PCI Compliance Report

AMP supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The **PCI Compliance Report** displays current PCI configurations and status as enabled on the network. Verify that AMP is enabled to monitor compliance with PCI requirements, as described in the “[Enabling or Disabling PCI Auditing](#)” on page 68.

In addition to citing simple pass or fail status with regard to each PCI requirement, AMP introduces very detailed diagnostic information to recommend the specific action or actions required to achieve Pass status, when sufficient information is available. Refer to the “[Auditing PCI Compliance on the Network](#)” on page 66 for information about enabling PCI on the network. The configurations in that section enable or disable the contents of the PCI Compliance Report that is viewable on the **Reports > Generated** page.

Figure 180 illustrates the fields and information in a **PCI Compliance Report**.

Figure 180 **Reports > Generated > PCI Compliance Report Illustration Example**

Daily PCI Compliance Report for All Groups, Folders and PCI Requirements		
1/20/2009 12:00 AM to 1/21/2009 12:00 AM Generated on 1/21/2009 12:23 AM		
This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 1.2 requirements that are relevant to security in your network. PCI DSS standard requirements are available at <a href="https://www.pcisecuritystandards.org">https://www.pcisecuritystandards.org</a> .		
Disclaimer: The PCI Compliance Report must be completed by an authorized QSA. The sole purpose of this report is to provide IT administrators with an on-demand internal audit of components which are visible to AirWave Wireless Management Suite.		
Summary		
PCI Requirement	Description	Status
1.1	Configuration standards for router. A device fails if it is in read-write management mode and there are mismatches between the desired configuration and the configuration on the device.	Pass
1.2.3	Install firewalls between any wireless networks and the cardholder data environment. A device passes if it can function as a stateful firewall.	Pass
2.1	Always change vendor-supplied defaults. A device fails if the usernames, passwords or SNMP credentials being used by AWMS to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Pass
2.1.1	Change vendor-supplied defaults for wireless environments. A device fails if the passphrases, SSIDs or other security-related settings are on a list of forbidden values. The list includes common manufacturer defaults.	Pass
4.1.1	Use strong encryption in wireless networks. A device fails if the desired or actual configuration reflect that WEP is enabled or if associated users can connect with WEP.	Pass

XML (XHTML)  
 export  
 CSV export  
 Email this report  
 Print report

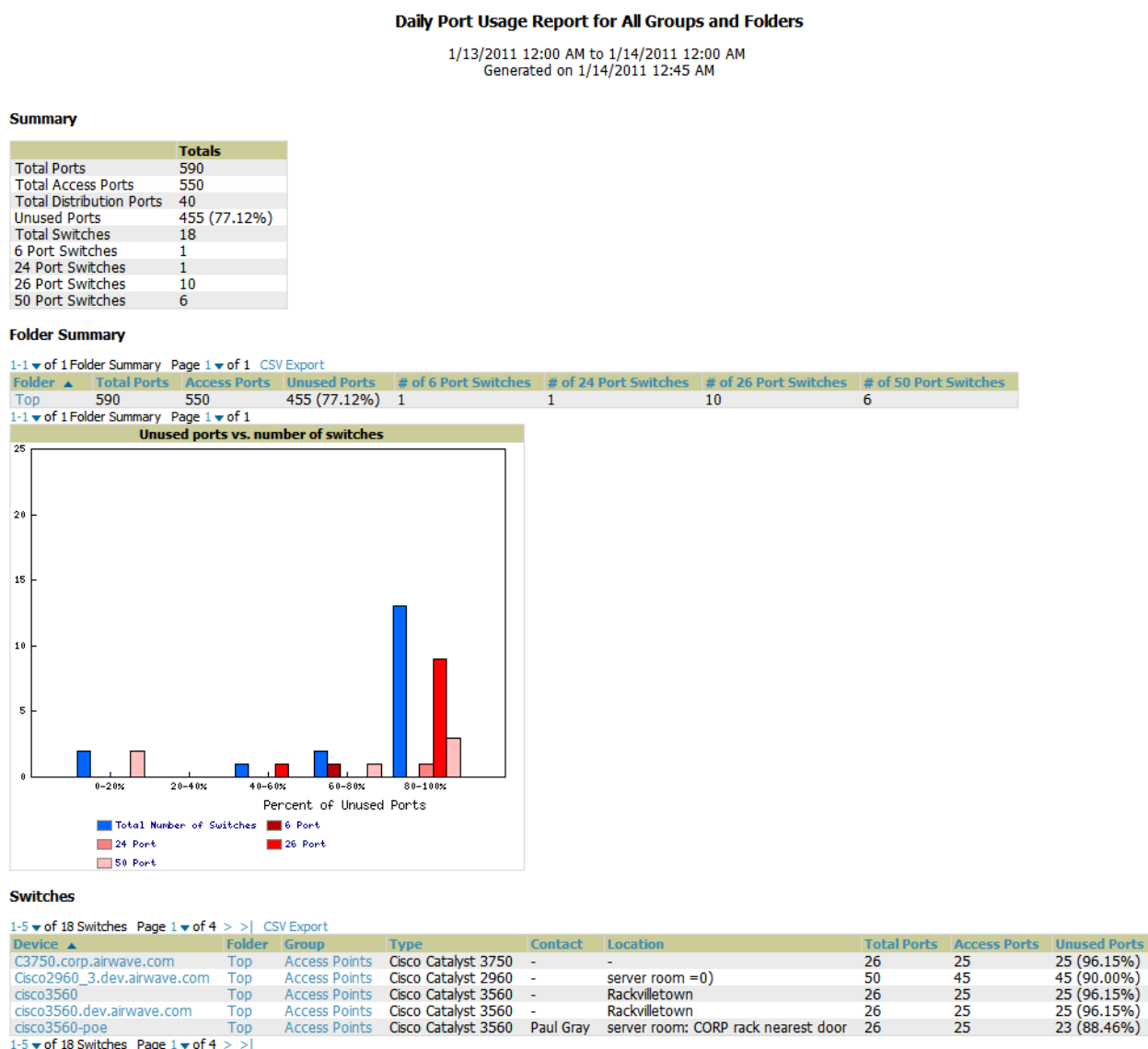
## Using the Port Usage Report

You can generate a wide array of port usage statistics from the **Port Usage Report** including each of the following:

- List of all the switches and ports in your network by folder
- List of unused ports
- List of access and distribution ports
- Histogram displaying unused ports vs. unused switches by type (access or distribution)
- List of most used switches
- List of most used ports

A sample of the types of information used to generate in a **Port Usage Report** appears in [Figure 181](#).

**Figure 181** *Reports > Generated > Port Usage Report Detail Page (partial view)*



## Using the RADIUS Authentication Issues Report

The **RADIUS Authentication Issues Report** contains issues that may appear with controllers, RADIUS servers, and users. [Figure 182](#) illustrates the fields and information in the **RADIUS Authentication Issues Report**.





## Figure 183 Reports > Detail > Daily RF Health Report Page Illustration

### Daily RF Health Report for All Groups and Folders

1/4/2011 12:00 AM to 1/5/2011 12:00 AM  
Generated on 1/5/2011 12:36 AM

XML (XHTML) export  
CSV export  
Email this report  
Print report

#### Problem 5 GHz Radios

Device	Channel Changes	Transmit Power Changes	Mode Changes	Average Noise	Average Channel Utilization	MAC/Phy Errors	Interfering Devices	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1394	1	1	0	-74.50	-	22636800	-	1	10138.00	-	ethersphere-1322	Top	Access Points
2198	4	1	0	-79.00	-	58752000	-	2	44596.00	-	ethersphere-1322	Top	Access Points

#### Problem 2.4 GHz Radios

Device	Channel Changes	Transmit Power Changes	Mode Changes	Average Noise	Average Channel Utilization	MAC/Phy Errors	Interfering Devices	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
00:1a:1e:c0:6c:a6	16	7	0	-77.00	-	4579200	-	0	0.00	-	Aruba3600-US	Top	Access Points
1154-Q	9	1	0	-71.50	-	123984000	-	1	419.00	-	ethersphere-1322	Top	Access Points
1350	1	5	0	-53.00	-	345600	-	0	0.00	-	ethersphere-1322	Top	Access Points
2103	3	1	0	-61.50	-	99100800	-	0	0.00	-	ethersphere-1322	Top	Access Points
2188	6	3	0	-73.50	-	60652800	-	1	308.00	-	ethersphere-1322	Top	Access Points

#### Most Noise (5 GHz)

Rank	Device	Average Noise	Channel Changes	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	1394	-74.50	1	-	1	10138.00	-	ethersphere-1322	Top	Access Points
2	2198	-79.00	4	-	2	44596.00	-	ethersphere-1322	Top	Access Points
3	1310	-86.00	1	-	15	2439711.00	-	ethersphere-1322	Top	Access Points
4	1350	-87.00	1	-	6	383120.00	-	ethersphere-1322	Top	Access Points
5	ap105-A1	-87.00	18	-	0	0.00	-	Aruba-3400	Top	Access Points
6	00:24:6c:c8:70:b5	-87.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
7	00:1a:1e:c0:1a:d0	-87.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
8	1260	-88.00	5	-	2	73432.00	-	ethersphere-1322	Top	Access Points
9	1242-H	-88.00	1	-	8	2098072.00	-	ethersphere-1322	Top	Access Points
10	1248	-88.00	13	-	1	6185.00	-	ethersphere-1322	Top	Access Points

#### Most Noise (2.4 GHz)

Rank	Device	Average Noise	Channel Changes	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	1350	-53.00	1	-	0	0.00	-	ethersphere-1322	Top	Access Points
2	2103	-61.50	3	-	0	0.00	-	ethersphere-1322	Top	Access Points
3	1154-Q	-71.50	9	-	1	419.00	-	ethersphere-1322	Top	Access Points
4	2188	-73.50	6	-	1	308.00	-	ethersphere-1322	Top	Access Points
5	RAD105	-73.50	1	-	0	0.00	-	67000-primary	Top	Access Points
6	00:1a:1e:c0:6c:a6	-77.00	16	-	0	0.00	-	Aruba3600-US	Top	Access Points
7	AP001d.a1fc.ca7a	-77.50	7	25.20	0	0.00	default location	5500-6.0.196.0	Top	Access Points
8	1372	-81.50	5	-	0	0.00	-	ethersphere-1322	Top	Access Points
9	00:1a:1e:c0:2b:34	-81.50	1	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
10	00:1a:1e:c1:52:0e	-82.00	1	-	1	2064.00	-	Aruba651	Top	Access Points

#### Most Utilized by Channel Usage (5 GHz)

Rank	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP10	3.15	3.15	0	0.00	Sales Office-hello	Cisco4400	Top	Access Points
2	AP0018.19bd.b1d0	1.57	1.57	0	0.00	ap lab	Cisco4400	Top	Access Points

#### Most Utilized by Channel Usage (2.4 GHz)

Rank	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP0018.19bd.b1d0	71.65	68.90	0	0.00	ap lab	Cisco4400	Top	Access Points
2	AP10	64.96	62.60	0	1.00	Sales Office-hello	Cisco4400	Top	Access Points
3	AP001d.a1fc.ca7a	22.83	20.47	0	0.00	default location	5500-6.0.196.0	Top	Access Points

#### Most MAC/Phy Errors (5 GHz)

Rank	Device	MAC/Phy Errors	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	2103	186865200	14	-88.00	-	0	672.00	-	ethersphere-1322	Top	Access Points
2	Fish-bowl	534810000	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
3	ap105-A1	471571200	18	-87.00	-	0	0.00	-	Aruba-3400	Top	Access Points
4	1153	308016000	1	-92.00	-	8	646989.00	-	ethersphere-1322	Top	Access Points
5	1154-Q	300328400	1	-89.50	-	0	142587.00	-	ethersphere-1322	Top	Access Points
6	1260	261792000	5	-88.00	-	2	73432.00	-	ethersphere-1322	Top	Access Points
7	2188	242697600	1	-91.00	-	4	110898.00	-	ethersphere-1322	Top	Access Points
8	1263	242524800	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
9	1372	233798400	2	-90.00	-	3	233005.00	-	ethersphere-1322	Top	Access Points
10	1350	232675200	1	-87.00	-	6	383120.00	-	ethersphere-1322	Top	Access Points

#### Most MAC/Phy Errors (2.4 GHz)

Rank	Device	MAC/Phy Errors	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	ap105-A1	240254800	6	-86.50	-	0	0.00	-	Aruba-3400	Top	Access Points
2	1154-Q	123984000	9	-71.50	-	1	419.00	-	ethersphere-1322	Top	Access Points
3	2103	99100800	3	-61.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
4	2188	60652800	6	-73.50	-	1	308.00	-	ethersphere-1322	Top	Access Points
5	1260	56505600	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
6	00:24:6c:c4:ce:a6	50889600	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
7	Fish-bowl	43632000	2	-86.00	-	1	83.00	-	ethersphere-1322	Top	Access Points
8	2198	34819200	4	-86.50	-	1	4616.00	-	ethersphere-1322	Top	Access Points
9	1242-H	32572800	2	-88.00	-	1	188.00	-	ethersphere-1322	Top	Access Points
10	00:08:86:C3:65:7A	30758400	1	-102.50	-	0	0.00	-	Aruba3400	Top	Access Points

#### Most Channel Changes (5 GHz)

Rank	Device	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	20	-90.00	-	0	337.00	-	Aruba651	Top	Access Points
2	ap105-A1	18	-87.00	-	0	0.00	-	Aruba-3400	Top	Access Points
3	2103	14	-88.00	-	0	672.00	-	ethersphere-1322	Top	Access Points
4	1248	13	-88.00	-	1	6185.00	-	ethersphere-1322	Top	Access Points
5	1263	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
6	Fish-bowl	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
7	1260	5	-88.00	-	2	73432.00	-	ethersphere-1322	Top	Access Points
8	2198	4	-79.00	-	2	44596.00	-	ethersphere-1322	Top	Access Points
9	ap65-c2:2e:4a	2	-104.50	-	0	0.00	chicken fingers	Aruba2400	Top	Access Points
10	1372	2	-90.00	-	3	233005.00	-	ethersphere-1322	Top	Access Points

#### Most Channel Changes (2.4 GHz)

Rank	Device	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
2	00:1a:1e:c0:6c:a6	16	-77.00	-	0	0.00	-	Aruba3600-US	Top	Access Points
3	1154-Q	9	-82.00	-	1	419.00	-	ethersphere-1322	Top	Access Points
4	1249	8	-88.00	-	1	56.00	-	ethersphere-1322	Top	Access Points
5	AP001d.a1fc.ca7a	7	-77.50	25.20	0	0.00	default location	5500-6.0.196.0	Top	Access Points
6	1260	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
7	2188	6	-83.50	-	1	308.00	-	ethersphere-1322	Top	Access Points
8	ap105-A1	6	-86.50	-	0	0.00	-	Aruba-3400	Top	Access Points
9	1372	5	-81.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
10	1153	5	-85.00	-	2	1200.00	-	ethersphere-1322	Top	Access Points

#### Most Transmit Power Changes (5 GHz)

Rank	Device	Transmit Power Changes	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	ap105-A1	31	18	-87.00	-	0	0.00	-	Aruba-3400	Top	Access Points
2	00:24:6c:c4:ce:a6	17	20	-90.00	-	0	337.00	-	Aruba651	Top	Access Points
3	2103	7	14	-88.00	-	1	6185.00	-	ethersphere-1322	Top	Access Points
4	00:1a:1e:c0:2b:34	6	1	-88.00	-	0	0.00	-	Aruba3200-3.121	Top	Access Points
5	00:1a:1e:c0:6c:a6	5	1	-89.50	-	0	0.00	-	Aruba3600-US	Top	Access Points
6	1248	5	13	-88.00	-	1	6185.00	-	ethersphere-1322	Top	Access Points
7	1263	4	6	-91.00	-	3	1493316.00	-	ethersphere-1322	Top	Access Points
8	Fish-bowl	3	6	-90.00	-	4	767319.00	-	ethersphere-1322	Top	Access Points
9	ap65-c2:2e:4a	2	2	-104.50	-	0	0.00	chicken fingers	Aruba2400	Top	Access Points
10	1242-H	1	1	-88.00	-	8	2098072.00	-	ethersphere-1322	Top	Access Points

#### Most Transmit Power Changes (2.4 GHz)

Rank	Device	Transmit Power Changes	Channel Changes	Average Noise	Average Channel Utilization	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	00:24:6c:c4:ce:a6	29	20	-82.00	-	0	0.00	-	Aruba651	Top	Access Points
2	00:1a:1e:c1:52:0e	13	1	-82.00	-	1	2064.00	-	Aruba651	Top	Access Points
3	1249	10	8	-90.50	-	0	65.00	-	ethersphere-1322	Top	Access Points
4	1248	8	4	-90.50	-	0	65.00	-	ethersphere-1322	Top	Access Points
5	00:1a:1e:c0:6c:a6	7	16	-77.00	-	0	0.00	-	Aruba3600-US	Top	Access Points
6	1394	5	1	-83.50	-	0	0.00	-	ethersphere-1322	Top	Access Points
7	1350	5	1	-53.00	-	0	0.00	-	ethersphere-1322	Top	Access Points
8	ap105-A1	5	6	-86.50	-	0	0.00	-	Aruba-3400	Top	Access Points
9	1260	3	6	-86.50	-	2	676.00	-	ethersphere-1322	Top	Access Points
10	2188	3	6	-73.50	-	1	308.00	-	ethersphere-1322	Top	Access Points

#### Least Utilized by Channel Usage (5 GHz)

Rank	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP0018.19bd.b1d0	1.57	1.57	0	0.00	ap lab	Cisco4400	Top	Access Points
2	AP10	3.15	3.15	0	0.00	Sales Office-hello	Cisco4400	Top	Access Points

#### Least Utilized by Channel Usage (2.4 GHz)

Rank	Device	Channel Busy	Interference	Number of Users	Bandwidth (bps)	Location	Controller	Folder	Group
1	AP001d.a1fc.ca7a	22.83	20.47	0	0.00	default location	5500-6.0.196.0	Top	Access Points
2	AP10	64.96	62.60	0	1.00	Sales Office-hello	Cisco4400	Top	Access Points
3	AP0018.19bd.b1d0	71.65	68.90	0	0.00	ap lab	Cisco4400	Top	Access Points

All tables in RF Health indicate the rank, device type, number of users, bandwidth, location, controller,

folder, and group, and all are sorted according to rank. Selecting a value under the **Device** column in any table will take you to the **APs/Devices > Monitor > Radio Statistics** page for the band indicated in the table title (5 GHz or 2.4 GHz).

- Every list contains Rank, Device (name, not type), Channel Changes, Average Noise, Average Channel Utilization, Clients, Usage, Location, Controller name, Speed, Goodput, Folder, and Group.
- The third column in the list (after Device) will be the column the list is sorted by.
- If that column would otherwise be in the list (Channel Changes), it does not show up in the list where it would otherwise.
- Note that sometimes the sorted column is not one of those common ones, such as the Interfering Devices section.

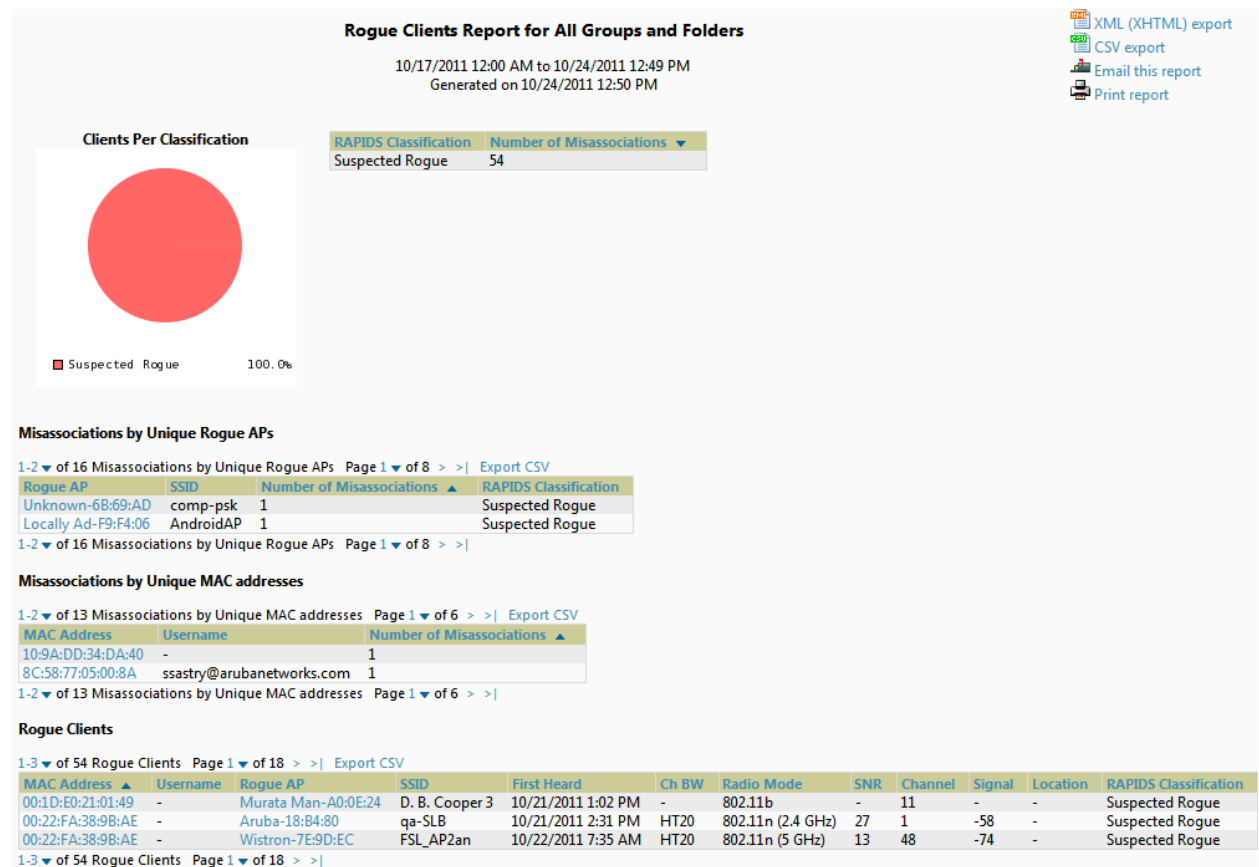
AMP limits data storage to 183 days (approximately six months) per radio. If you create an RF Health Report with a date range longer than 183 days, it will only include Channel Changes, Transmit Power Changes, Average Utilization, Mac/Phy Errors and Average Noise based on whatever part of the report intersects the last 183 days. This differs from most reports because other data (like bandwidth and users) maxes out at 425 days, and AMP validates reports so you can only run them over a 366-day duration.

## Using the Rogue Clients Report

The Rogue Clients report tracks the number of valid users that connected to rogues in the specified time frame, and can be filtered by rogue classification. Ad-hoc devices can be included, and specific details that should be included about the clients can be selected.

By default, the minimum RAPIDS classification is Suspected Rogue, and the maximum is Contained Rogue.

**Figure 184** *Reports > Detail > Rogue Clients Report Page Illustration*







## Using the Rogue Containment Audit Report

The rogue containment audit report that lets you know if any containment is failing. Figure 185 illustrates the fields and information in this report type.

**Figure 185** *Reports > Detail > Rogue Containment Audit Report Page Illustration*

**Rogue Containment Audit Report for All Groups and Folders**

Generated on 12/1/2009 4:33 PM

 XML (XHTML) export  
 CSV export  
 Email this report  
 Print report

1-8 ▼ of 8 Rogues Contained Page 1 ▼ of 1 Export to CSV

Controller	Rogue	BSSID	Containment State	Desired Containment State	Classifying Rule	Location
- All -	- All -	- All -	- All -	- All -	- All -	- All -
Airspace-5500	Apple-ED:38:17	00:03:93:ED:38:17	Contained	Not Contained	Signal strength > -75 dBm	-
Airspace-5500	Senao Inte-43:78:B1	00:02:6F:43:78:B1	Contained	Not Contained	Signal strength > -75 dBm	-
Airspace-5500	Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Aruba2400	Enterasys-36:5C:18	00:01:F4:36:5C:18	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Enterasys-37:4A:C3	00:01:F4:37:4A:C3	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Cisco-9F:75:90	00:1D:45:9F:75:90	Not Contained	Contained	Manual Classification Override	-
Aruba2400	Locally Ad-71:BA:90	02:20:A6:71:BA:90	Contained	Not Contained	Signal strength > -75 dBm	-
Aruba2400	Locally Ad-71:BA:90	02:20:A6:71:BA:91	Contained	Not Contained	Signal strength > -75 dBm	-

1-8 ▼ of 8 Rogues Contained Page 1 ▼ of 1

## Using the Client Session Report

The **Client Session Report** extensively itemizes user-level activity by session- any instance in which a user connects to the network. In list and chart form, this report tracks and display session information that can include any or all of the following:

- Session Data by OS (List or Chart)
- Session Data by OS Detail (List or Chart)
- Session Data by Model (List or Chart)
- Session Data by Manufacturer (List or Chart)
- Session Data by Device Type (List or Chart)
- Session Data by AOS Device Type (List or Chart)
- Session Data by Network Interface Vendor (List or Chart)
- Session Data by Network Chipset (List or Chart)
- Session Data by Network Driver (List or Chart)
- Session Data by EAP Supplicant (List or Chart)
- Session Data by Asset Group (List or Chart)
- Session Data by Asset Category (List or Chart)
- Session Data by Connection Mode (List or Chart)
- Session Data by SSID (List or Chart)
- Session Data by Role (List or Chart)
- Session Data by VLAN (List or Chart)
- Session Data by Cipher (List or Chart)
- Summary
- Sessions
- Session Data By Client

Figure 186 Client Session Detail, Partial View

#### Session Data by Cipher

1-3 of 3 Ciphers Page 1 of 1 Export CSV

Cipher	Number of Users	% of Users	Amount of Time	% of Time	MB Used	% of MB Used	Average Signal Quality	Number of Sessions
AES	153	83.61%	39 days 10 hrs 48 mins	73.34%	18779.90	98.87%	37.55	427
-	29	15.85%	13 days 15 hrs 16 mins	25.35%	214.46	1.13%	6.92	144
WEP	1	0.55%	16 hrs 52 mins	1.31%	0.04	0.00%	48.64	97
3 Ciphers		100.00%	53 days 18 hrs 57 mins	100.00%	-	100.00%		668

1-3 of 3 Ciphers Page 1 of 1

Number of Users by Cipher



■ AES  
■ unknown  
■ WEP

Amount of Time Spent by Cipher



■ AES  
■ unknown  
■ WEP

MB Used by Cipher



■ AES  
■ unknown  
■ WEP

#### User Session Summary

Number of sessions:	668
Number of unique users:	171
Number of guest users:	0
Number of unique APs:	124
Average session duration:	1 hr 55 mins
Total traffic (MB):	18994.40
Average traffic per session (MB):	28.43
Average traffic per user (MB):	111.08
Average bandwidth per user (Kbps):	51.06
Average signal quality:	38.25

#### Sessions

1-3 of 668 Sessions Page 1 of 223 > >| Export CSV

MAC Address	Username	Role	Device Name	Controller	Group	Folder	Device Location	Co
00:26:5A:09:4A:2D	-	logon	00:24:6c:c8:6e:dd	Aruba-3400	aruba gui no wms	Top > aruba > thin aps	changed	5/1
24:AB:81:F5:52:C0	shankarc	employee	shankarc-rap2wg	RAP-OPS-02	aruba corp	Top > cor/p > rap	-	5/1
00:26:C6:82:55:FA	ARUBANETWORKS\mrayanan	employee	mrayanan-rap2wg	RAP-OPS-02	aruba corp	Top > cor/p > rap	-	5/1

1-3 of 668 Sessions Page 1 of 223 > >|

#### Session Data by User

1-3 of 171 Session Data by User Page 1 of 57 > >| Export CSV

MAC Address	Username	Roles	Amount of Time	MB Used	Avg Bandwidth (Kbps)	Average Signal Quality	Vendor	Connection M
00:23:12:00:A4:91	aanderson	employee	3 hrs 6 mins	21.11	15.06	50.84	Apple	802.11g
D8:9E:3F:DD:F4:07	slekkala	employee	18 mins	1.03	7.63	16.89	Apple	802.11g
00:23:14:AC:16:F8	ARUBANETWORKS\hcho	employee	1 hr 0 mins	13.11	28.88	41.00	Intel	802.11g

1-3 of 171 Session Data by User Page 1 of 57 > >|

## Defining Reports

You can create reports in AMP for any time period you wish, to be run when you wish, and distributed to recipients that you define. Perform these steps to create and run custom reports. Reports created with the **Reports > Definition** page appear on this and on the **Reports > Generated** page once defined.

1. To create or edit a report, browse to the **Reports > Definition** page and select the **Add** button, or select the pencil icon to edit an existing report definition. [Figure 187](#) illustrates one view of the **Reports > Definition** page.

**Figure 187** *Defining a Report with **Reports > Definitions > Add Button***

**Report Restrictions**

Group: -- All Groups --

Folder: -- All Folders --

Device Search Filter:  
This report will be run against Devices that match this search.

**Report Restrictions** section varies according to report type.

Report Start:

Report End:

**Scheduling Options**

Schedule: ☐ Yes ☒ No

**Report Visibility**

Generated Report Visibility: By Role

**Email Options**

Email Report: ☐ Yes ☒ No

2. Complete the fields described in [Table 135](#) and any additional **Report Restrictions**. The **Report Restrictions** section changes according to the report type you choose. Additional information about each report type is described in [“Using Daily Reports”](#) on page 230.

**Table 135** ***Reports > Definitions > Add Page Fields***

Field	Default	Description
<b>Title</b>	Empty	Enter a <b>Report Title</b> . Use a title that is a meaningful and descriptive, so it may be found easily on the lists of reports that appear on either <b>Generated</b> or <b>Definitions</b> pages.
<b>Type</b>	Capacity	Choose the type of report you wish to create in the Report Type drop-down menu.
<b>Group</b>	All Groups	Specify the groups and folders to be covered in the report by choosing <b>All Groups</b> (or <b>All Folders</b> ) or specifying <b>Use selected groups</b> (or <b>Use selected folders</b> ) in the drop-down menu.  If <b>Use selected groups</b> is chosen, a menu with checkboxes appears, allowing you to choose the groups to include in the report.
<b>Folder</b>	All Folders	
<b>Device Search Filter</b>	Blank	Add a specific alpha numeric string for finding devices that match that which you entered. Note that once you enter a search string, new or deleted devices that match the search string will automatically be included or excluded in all future reports generated until you delete or change the search string.  For certain reports, such as <b>New User</b> and <b>Client Session</b> , will allow you to search devices associated with a specific user or device.
<b>Filter by device type</b>	All Device Types	Filter this report by device type. By selecting the second option - <b>Use selected device types</b> - you can select the checkboxes next to the specific device types you want to filter on: Access Points (such as campus APs remote APs, and different types of Mesh APs), Controllers (Master, Local, Standby, and Virtual), Switches & Routers (Aruba and non-Aruba), and Universal & Custom Devices.
<b>SSID</b>	All SSIDs	This field displays for most report types. When this field appears, and when you select <b>Use Selected IDs</b> , a new list of SSIDs displays. Check (select) the specific SSIDs to be included in the report.

**Table 135 Reports > Definitions > Add Page Fields (Continued)**

Field	Default	Description
<b>Report Start</b> <b>Report End</b>	Blank	These fields establish the time period to be covered by the report. These fields are supported for most report types. When these fields do not appear, the report provides a snapshot of current status rather than information covering a period of time  Times can be entered in relative or absolute form. A start date of 6 months 3 weeks 5 days 9 hours ago and an end time of 4 months 2 weeks 1 day ago is valid, as is a start date of 5/5/2008 13:00 and an end date of 6/6/2008 9:00. Absolute times must be entered in a 24-hour format. Other reports, like the Inventory Report, give a snapshot picture of the AMP at the present time.
<b>Schedule</b>	No	When you select <b>Yes</b> , new fields display that allow you to define a specific time for report creation. The report schedule setting is distinct from the <b>Report Start</b> and <b>Report End</b> fields, as these define the period of time to be covered by the report.  These <b>Schedule</b> fields establish the time that a report runs, independent of report scope: <ul style="list-style-type: none"> <li>• <b>Current Local Time</b>—Displays for reference the time of the AMP system.</li> <li>• <b>Desired Start Date/Time</b>—Sets the time the report runs, which may often be separate from the time period covered by the report. This allows you to run a report during less busy hours.</li> <li>• <b>Occurs</b>—Select whether the report is to be run one time, daily, weekly, monthly, or annually. Depending on the recurrence pattern selected, you get an additional drop-down menu. For example, if you select a recurrence of monthly, you get an additional drop-down menu that allows you to pick which day of the month (day 1, day 2, and so forth) the report should run.</li> </ul>
<b>Generated Report Visibility</b>	By Role	This field allows you to display the report either by user role, with the report appearing in User Role lists on the <b>Reports &gt; Generated</b> page.  Alternatively, this field allows you to display reports by <b>Subject</b> on the <b>Reports &gt; Generated</b> page.
<b>Email Report</b>	No	Select <b>Yes</b> to display sender and recipient fields. Enter the Sender Address where marked to indicate the address that appears in the <b>From</b> field of the emailed report. Enter recipient email addresses separated by commas when using multiple email addresses.  <b>NOTE:</b> AMP will not attempt to email a report with an excessively large number of rows in the detail section.

In the report restrictions section you can customize any detailed information contained in a chosen report. [Figure 188](#) shows a sample **Report Restrictions** page.

**Figure 188 Report Restrictions Illustration**

**Report Restrictions**

Group: -- All Groups --

Folder: -- All Folders --

SSID: -- All SSIDs --

Number of items to include in memory/CPU summary (Greater than or equal to 1): 10

Usage by SSID:

- ☒ Interval
- ☒ SSID
- ☒ Max Users
- ☒ Max BW In (kbps)
- ☒ Max BW Out (kbps)
- ☒ Avg Users
- ☒ Avg BW In (kbps)
- ☒ Avg BW Out (kbps)

By default all data will be included. Deselect the checkbox to hide specific information. The list can also be reordered by dragging and dropping the separate lines. The order displayed here will match the column order in the report.



3. Do one of the following:

- Select **Add and Run** to generate the report immediately, in addition to saving report settings.
- Select **Run Now** to generate the report immediately without creating a new report definition or saving the report settings.
- Select **Add (only)** to complete the report creation, to be run at the time scheduled.
- Select **Cancel** to exit from the **Add** page.

Table 136 describes the configurable settings for the custom report to be created. Select any of the report names to view additional information on that report type.

**Table 136** Report Types and Scheduling Options Supported for Custom Reports

Report Type	Can be Run by Time Period	Can be Run by Group/Folder	Description
Using Custom Reports	Yes	Yes	Summarizes devices based on which have exceeded a defined percentage of their maximum bandwidth capacity. Pulls data for AP radios or interfaces of universal devices (ifSpeed value).
Using the Capacity Planning Report	Yes	Yes	Tracks bandwidth capacity and consumption according to thresholds for data throughput. This is a device-oriented report.
Using the Configuration Audit Report	No	Yes	Provides a snapshot of the configuration of all specified access points in AMP, at report run time.
Using the Device Summary Report	Yes	Yes	Summarizes user and bandwidth statistics and lists devices in AMP.
Using the Device Uptime Report	Yes	Yes	Summarizes device uptime within defined groups or folders.
Using the IDS Events Report	Yes	Yes	Summarizes IDS events; can be limited to a summary of a certain number of events.
Using the Inventory Report	No	Yes	Provides an audit of vendors, models and firmware versions of devices in AMP.
Using the Memory and CPU Utilization Report	Yes	Yes	Summarizes usage for controllers for defined top number of devices; can be run with or without per-CPU details and details about device memory usage.
Using the Network Usage Report	Yes	Yes	Summarizes bandwidth data and number of users.
Using the New Rogue Devices Report	Yes	No	Shows new rogue devices by score, discovering AP, and MAC address vendor.
Using the New Users Report	Yes	No	Provides a summary list of new users, including username, role, MAC address, discovering AP, and association time.
Using the PCI Compliance Report	Yes	Yes	Provides a summary of network compliance with PCI requirements, according to the PCI requirements enabled in AMP using the <b>AMP Setup &gt; PCI Compliance</b> page.
Using the Port Usage Report	Yes	Yes	Summarizes switch and port information across the network. Generates information on the unused ports. Provides a detailed list of all available switches and ports in the network.
Using the RADIUS Authentication Issues Report	Yes	Yes	Summarizes RADIUS authentication issues by controller and by user, as well as a list of all issues.
Using the RF Health Report	Yes	Yes	Tracks problematic radios, changes, errors, and interfering devices.

**Table 136** Report Types and Scheduling Options Supported for Custom Reports (Continued)

Report Type	Can be Run by Time Period	Can be Run by Group/Folder	Description
<a href="#">Using the RF Health Report</a>	No	Yes	Identifies discrepancies between access point containment status specified in AMP compared to containment status identified by the controller at report run time.
<a href="#">Using the Client Session Report</a>	Yes	Yes	Summarizes user data by radio mode, SSID and VLAN, as well as lists all sessions.

## Emailing and Exporting Reports

This section describes three ways in which distribute reports from AMP:

- [Emailing Reports in General Email Applications](#)
- [Emailing Reports to Smarthost](#)
- [Exporting Reports to XML or CSV](#)

### Emailing Reports in General Email Applications

Perform these steps to set up email distribution of reports in AMP:

- All reports contain a link to export the report to an XML file and a text box where you may specify email addresses, separated by commas, to which reports are sent.
- Select **Email This Report** to email the report to the address specified in the text box above the button.

Additional information about email-based report generation is described in [“Defining Reports” on page 252](#), and in [“Emailing Reports to Smarthost” on page 255](#).

### Emailing Reports to Smarthost

AMP uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If AMP sits behind a firewall, which prevents it from sending email directly to the specified recipient, use the following procedure to forward email to a smarthost.

1. Add the following line to `/etc/postfix/main.cf`:

```
relayhost = [mail.example.com]
```

Where: `mail.example.com` is the IP address or hostname of your smarthost.

2. Run `service postfix restart`

3. Send a test message to an email address.

```
Mail -v xxx@xxx.com
Subject: test mail
.
CC:
```

4. Press **Enter**.

5. Check the mail log to ensure mail was sent by running this command:

```
tail -f /var/log/maillog
```

## Exporting Reports to XML or CSV

AMP allows you to export individual reports in XML (xhtml) or CSV. You can also export all reports at once and a zip file will be generated with all of the files in CSV format included. These files may be read by an HTML browser or opened in Excel. The CSV files can be opened in any text editor.



---

This method of exporting files supports graphics and links, and prevents **Missing File C:\filename.css** error messages.

---

## Transferring Reports Using FTP

Once reports are generated, you can also copy them to any ftp accessible destination using a sample script located in the /var/airwave/custom directory. For more information, contact AirWave support.

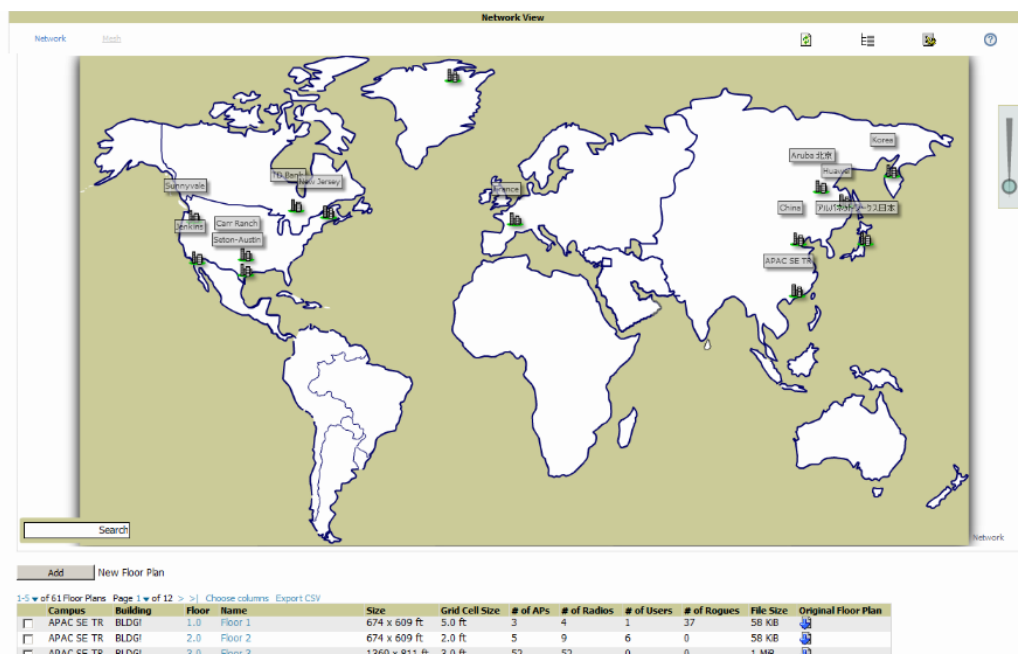
This chapter contains information about VisualRF, and includes the following topics:

- “Features” on page 258
- “Useful Terms” on page 258
- “Starting VisualRF” on page 259
- “Basic QuickView Navigation” on page 259
- “Using the Settings in the VisualRF > Setup Page” on page 264
- “Configuring QuickView Personal Preferences” on page 268
- “Increasing Location Accuracy” on page 269
- “Using QuickView to Assess RF Environments” on page 276
- “Planning and Provisioning” on page 281
- “Importing and Exporting in VisualRF” on page 291
- “VisualRF Location APIs” on page 294
- “About VisualRF Plan” on page 295

The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. To understand what is happening on your wireless network, you need to know where your users and devices are located, and you need to monitor the RF environment in those areas. VisualRF puts this information at your fingertips through integrated mapping and location data.

VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. Moreover, VisualRF does not require dedicated RF sensors or a costly additional location appliance - all the necessary information is gathered from your existing wireless access points and controllers.

**Figure 189** Example VisualRF Page Showing all networks



## Features

- VisualRF 7.3 adds a new Mesh monitoring page specially for viewing Aruba AirMesh devices. It automatically renders Mesh APs based on GPS coordinates.
- Floor plan upload wizard enables direct importation of JPEG, GIF, PNG, PDF and CAD files for floor plans.
- Batch upload wizard enables batch uploads of multiple CAD files with corresponding walls, and access points.
- Accurate calculation of the location of all client devices (laptops, RFID Tags, PDAs, Phones) using RF data from your existing APs and controllers. Further improvements in accuracy can be achieved with site surveys.
- Graphical navigation allows your Help Desk to view floor plans simply by clicking on the appropriate campus, building, or floor.
- Tree view allows you to navigate to a specific campus, building, or floor via a tree navigation.
- Heatmaps depict the strength of RF coverage in each location.
- Speed (data rate) view which depicts the highest possible speed at every location on a floor plan.
- Built into the AirWave for onscreen display of alerts and error conditions. For instance, an AP icon will display in red when a critical alert is active or when usage conditions exceed pre-defined thresholds.
- Location playback viewer which allows visual tracking of up to 24 hours of location history.
- Dynamically recalculates path loss and device locations based on real-time data from your wireless LAN, for increased location accuracy.
- Calibrates RF data from multiple vendors' APs (and across different product lines from the same vendor) for accurate display even in multi-vendor and multi-architecture environments.
- Full planning capabilities based on speed or signal requirements.

## Useful Terms

- **VisualRF** - The AirWave service that calculates location, calculates path loss, and provides floor plan editing capabilities.
- **VisualRF Plan** - Makes the planning portions of VisualRF available in an offline software package that does not require a server. For more information about VisualRF Plan, see [“About VisualRF Plan” on page 295](#).
- **QuickView** - Flash front-end for VisualRF which displays information generated by the backend service.
- **mW** - 1/1000 of a Watt. It is a linear measurement (always positive) generally used to represent transmission.
- **dB (Decibels)** - difference/ratio between two signal levels.
- **dBm** - dB as compared to 1 mW. It is a logarithmic measurement (integer) which is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so it is easy to evaluate performance between various vendors.
- **RSSI (Received Signal Strength Indicator)** - IEEE defines RSSI is a mechanism by which RF energy is to be measured by the circuitry on a wireless NIC (0-255). RSSI is not standard across vendors. Each vendor determines their own RSSI scale/values.
- **AP-to-AP Signal (Neighbor)** - Some APs/Controllers have the ability to report the signal strength of APs that they hear. AMP uses these signal strength readings to dynamically attenuate floor plans to increase the accuracy of client locations and heat maps.
- **Unassociated Client Information** - Some APs/Controllers have the ability to report the signal strength clients they hear, but that are associated to a radio on a neighboring AP. AMP also uses these signal strength readings to more accurately place clients.
- **Client Surveys** - Client surveys within VisualRF use access points to understand which clients they hear and at what signal strength.

- **Rogue Surveys** - Rogue surveys are facilitated by AMC, VisualRF and the client's radio to understand which access points they hear and what signal strength.

## Starting VisualRF

In order to launch VisualRF, it must be enabled within **AMP Setup** to display the VisualRF tab, and the VisualRF engine must be switched on in **VisualRF > Setup**. Both of these pages are visible to logged-in administrators only. By default, VisualRF is disabled in new AMP installations.

To enable VisualRF, follow these instructions while logged in as an administrator:

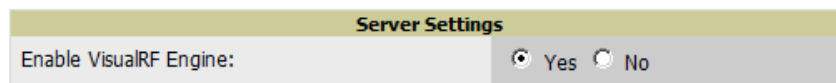
1. Go to **AMP Setup > General**.
2. Scroll down to the **AMP Features** section as shown in [Figure 190](#). In the field **Display VisualRF**, select **Yes**. Then select **Save**.

**Figure 190** *AMP Setup > General > AMP Features Page Illustration*



3. After the VisualRF tab is visible, navigate to **VisualRF > Setup**.
4. In the **Server Settings** section, select **Yes** in the **Enable VisualRF Engine** field. Then select **Save**.

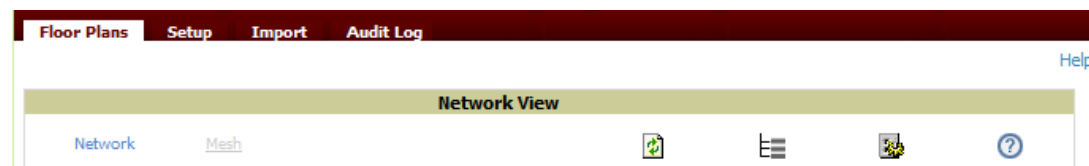
**Figure 191** *VisualRF > Setup > Server Settings Section*



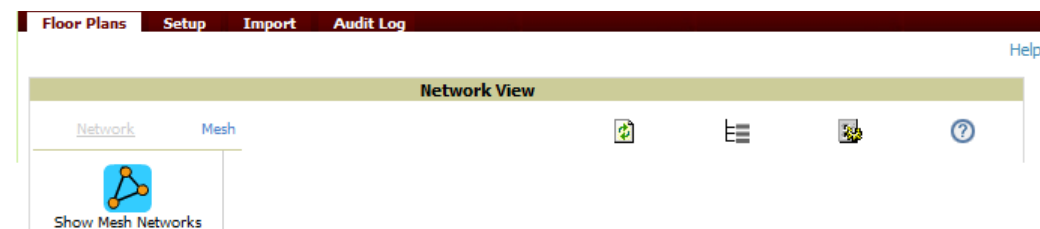
## Basic QuickView Navigation

The top-level menus of VisualRF are split into two major categories: Network and Mesh, as shown in [Figure 192](#) and [Figure 193](#). Selecting these menus will cause relevant submenus and sections to display below:

**Figure 192** *Default VisualRF Top Level Menu - Network View*





**Figure 193** *Default VisualRF Top Level Menu - Mesh View*





[Table 137](#) describes the top level icons and their functions on VisualRF.

**Table 137** *Top Level Icons and Descriptions*

Operation	Icon	Description
Refresh		Refresh the floor plan to see changes.
Open Site Tree		Display the Network Tree View Window on top of the floor plan.

**Table 137** Top Level Icons and Descriptions (Continued)

Operation	Icon	Description
Preferences		Configure personal viewing preferences. The Preferences menu allows you to configure user preferences (overlay types, grid lines, alerts, icon sizes). See <a href="#">“Configuring QuickView Personal Preferences”</a> on page 268 for more details.
Help		Launch the online help. <b>NOTE:</b> This User Guide currently contains the most up-to-date help information for the VisualRF interface.

## Network View Navigation

When viewing a floor plan in Network View, the top-level menu changes to **Overlays**, **Display**, and **Edit** toggles.

### Overlays

**Figure 194** Overlays Menu - Speed selected

The **Overlays** menu contains three common sections: **Type**, **Floors**, and **Frequencies**. Selecting options in these sections can display additional menu sections that affect the data overlays on the floor plan you are viewing.

#### Type section

- **Heatmap** - Evaluate coverage based on signal levels by providing the highest dBm (energy level) for all areas of a floor plan. When this option is selected, the **Signal Cutoff** drop-down menu displays.
- **Speed** - Evaluate coverage based on xmit power of client by providing the highest data rate a user will receive for all areas of a floor plan. When this option is selected, the **Client Transmit Power** drop-down menu displays. Additionally, a **Rates** interface appears with 54Mbps, 300Mbps, and 450Mbps.
- **Ch. Utilization** - View how much airtime is used in the environment. Airtime usage is a good measure of how busy an area is. When you select this option, a new **Data Set** menu appears where you can select the Current or Maximum Total, Receive, Transmit, or Interference information to display on the Floor Plan.
- **Sensor Coverage** - provides the farthest area which a sensor can hear. When this option is selected, the **Client Transmit Power** drop-down menu displays.
- **Voice** - provides color-coded overlay based on number of radios covering each grid cell based on the selected signal cutoff. When this option is selected, the **Signal Cutoff** drop-down menu displays.
- **Wired Range** - Displays the distance an Ethernet cable can be pulled from an IDF. The max range is equal to 300 feet minus 5 percent minus 1.1x the floor height.

#### Floors section

The Floors section shows the overlay information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Select all options to see all floors, or one or more of the following options:

- Above - show the data from APs located on the floor above
- Current (default)
- Below - show the data from APs located on the floor below



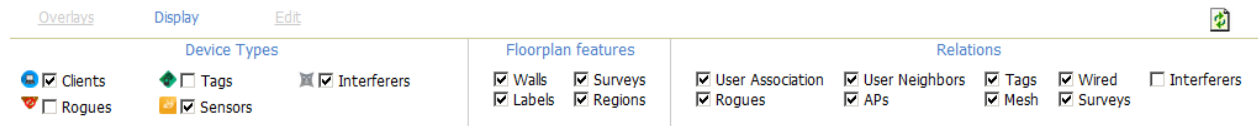
## Frequencies section

Select the desired frequency from the following options:

- 5 GHz (lines are always green)
- 2.4 GHz (lines are always blue)
- 2.4 + 5 GHz (lines are yellow)

## Display Menu

Figure 195 *Display Menu*



## Device Types section

- **Clients** - Turns the display of wireless users on or off. Clients on the floor plan are indicated by the icon.
- **Rogues** - Toggle rogue devices on or off. Rogues on the floor plan are indicated by the icon.
- **Tags** - Toggle WiFi Tags on or off. Tags on the floor plan are indicated by the icon.
- **Sensors** - Toggle sensors on or off. Sensors on the floor plan are indicated by the icon.
- **Interferers** - Toggle interferers on or off. Interferers on the floor plan are indicated by the icon.



Interferer indicators works for AOS customers running 6.1 or newer that have run the mgmt-server type AMP command, and have APs performing Spectrum analysis through hybrid scanning or dedicated spectrum monitors.

## Floorplan Features section

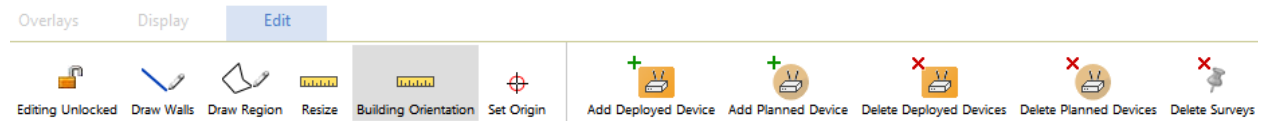
- **Regions** - Toggle regions on or off.
- **Surveys** - Toggle surveys on or off.
- **Walls** - Toggle walls on or off.
- **Labels** - Toggle labels on or off.

## Relations section

- **User Association** - Toggle line between the wireless user and AP of association.
- **Rogues** - Toggle lines between rogue APs and radios which hear the AP.
- **User Neighbors** - Toggle lines between client and radios which hear the client excluding the radio of association.
- **APs** - Toggle lines between APs which heard each other.
- **Tags** - Toggle lines between WiFi Tags and radios which hear the Tags. For Tags there is no radio of association.
- **Wired** - Toggle lines between APs/sensors and their IDF.
- **Mesh** - Toggle lines between Mesh portals and nodes.
- **Surveys** - Toggle lines between client (x,y) to APs by client during survey.
- **Interferers** - Toggle lines between interferers and the radios that have discovered them. For interferers, there is no radio of association.

## Edit Menu

**Figure 196** *Edit Menu Options*



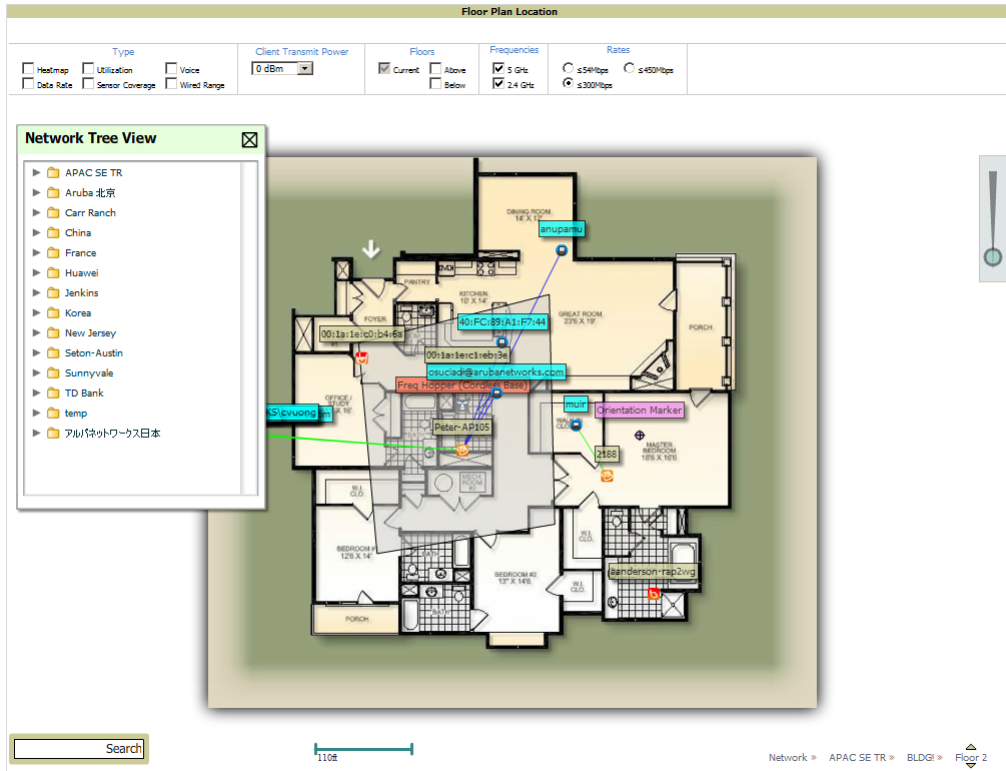
Options in the **Edit** menu allow you to add information to the floor plan. [Table 138](#) explains the options in the **Edit** menu:

**Table 138** *Edit Icons and Descriptions*

Operation	Description
<b>Edit Locked/Unlocked</b>	Lock a floor plan for editing.
<b>Draw Walls</b>	Add walls onto a floor plan. Refer to <a href="#">“Adding Exterior Walls”</a> on page 270.
<b>Draw Region</b>	Add region onto a floor plan. Region types include Planning, IDF, Location Probability, Location Testing and Informational.
<b>Resize</b>	Update the scale of the floor plan to properly reflect the accurate dimensions of the floor plan.
<b>Building Orientation</b>	Place the location of two GPS points in order to set latitude and longitude of a building. This will allow VisualRF to calculate the GPS coordinates for APs, clients, rogues, and RFID tags.
<b>Set Origin</b>	Set Orientation for proper vertical floor plan alignment.
<b>Add Deployed Device</b>	Provision APs onto a floor plan (APs monitored by AMP).
<b>Add Planned Device</b>	Manually plan APs onto a floor plan (APs not monitored by AMP).
<b>Delete Planned Devices/Delete Deployed Device</b>	Remove all specified devices on a floor plan.
<b>Delete Surveys</b>	Remove all surveys (rogue and client) on floor plan.

[Figure 197](#) shows additional navigation controls when viewing floor plans. In the bottom left corner of the window is the **Search** box. In the top right corner is the zoom control. You can also zoom by using Ctrl + your mouse wheel as well as the + and - keys. In the bottom right corner are navigation tools related to network, campus, and building.

**Figure 197** On-Screen Navigation Options



## Mesh View Navigation

Mesh view provides a visual Mesh monitoring page specially for viewing Aruba AirMesh devices. It automatically renders Mesh APs based on GPS coordinates.

Figure 198 displays an example of a Mesh Network view with a mouseover above a network icon:

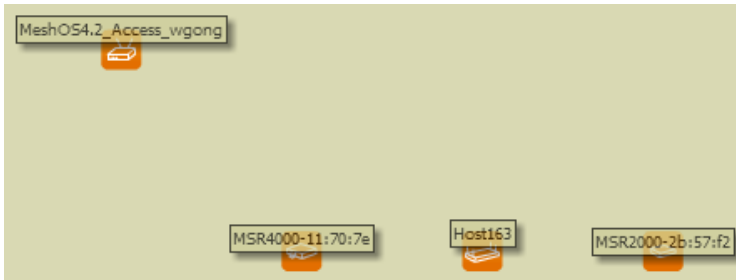
**Figure 198** Viewing Mesh Networks in VisualRF



You can mouse over each mesh network icon to view the number of APs, Users, and Bandwidth.

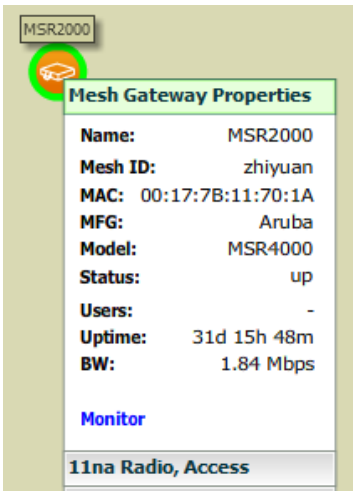
Clicking on an AirMesh network will display the APs with labels:

**Figure 199** *APs in a mesh network*



Select an AirMesh's AP icon to bring up the popup menu showing the Mesh Node Properties by default. This window shows the node's name, MeshID, MAC, Manufacturer, and other information. Click the blue **Monitor** link inside this window to be taken to the **APs/Devices > Monitor** page for more details.

**Figure 200** *Properties for a Mesh Gateway Illustration*



For radio-level status information on the AirMesh device in your network, select the menus in the AP's popup window for each radio (**11na Radio, Access**, and so forth).

## Using the Settings in the VisualRF > Setup Page

The **VisualRF > Setup** page, illustrated in [Figure 201](#), configures advanced settings for VisualRF. Please reconfigure these settings very carefully because these settings can impact your server's performance as well as your location accuracy.



**NOTE**

---

Selecting **Save** will cause VisualRF to restart, disrupting or delaying the usability for up to 5 minutes.

---

**Figure 201** *The VisualRF > Setup Page*

The screenshot displays the VisualRF Setup Page with the following sections:

- Server Settings:**
  - Enable VisualRF Engine: ☒ Yes ☐ No
  - Enable Multi-floor Bleed Through: ☒ Yes ☐ No
  - Dynamic Attenuation: ☒ Yes ☐ No
  - Use Metric Units: ☐ Yes ☒ No
  - Memory Allocation: 1 GB
  - Core Threads: 8
  - Location Caching Threads: 8
  - UI Threads: 8
  - Synchronization Timer: 15 minutes
  - Restrict visibility of empty floor plans to the role of the user who created them: ☐ Yes ☒ No
- Location Settings:**
  - Allowed deviation for client placement: 2 dB
  - Maximum Rogue APs per Floor Plan (approx.): 50
- Location Calculation Timer Settings:**
  - Legacy Laptop Min/Max (sec): 90/360
  - Legacy Laptop Number of Samples: 3
  - Laptop Min/Max (sec): 90/360
  - Laptop Number of Samples: 3
  - Phone Min/Max (sec): 60/240
  - Phone Number of Samples: 3
  - RFID Min/Max (sec): 30/120
  - RFID Number of Samples: 4
  - Scale Min/Max (sec): 500/2000
  - Scale Number of Samples: 3
  - Printer Min/Max (sec): 120/480
  - Printer Number of Samples: 3
  - Rogue Min/Max (sec): 500/2000
  - Rogue Number of Samples: 3
  - Default Min/Max (sec): 90/360
  - Default Number of Samples: 3
- Wall Attenuation Settings:**
  - Add New Wall Attenuation

Material	Attenuation	Color
brick	18	Chartreuse
Concrete	15	Red
Cubicle	4	Green
Drywall	6	Yellow
Glass	3	Blue
Re-Bar inforced Mesh poured concrete	100	Khaki
reinforced concrete	25	Maroon
shoji	3	Lavender
telefonica-wall	50	Azure
waterfall	94	Turquoise

  - 10 Wall Attenuations
  - Save Revert

To enable VisualRF and tune memory and performance, navigate to the **Server Settings** section on this page. The settings in this section are detailed in [Table 139](#):

**Table 139** *Server Settings Section of the VisualRF > Setup Page*

Setting	Default	Description
<b>Enable VisualRF Engine</b>	No	Enables or disables the VisualRF engine. This setting must be enabled to use VisualRF. If you do not have a license for VisualRF, this page will not appear.
<b>Enable Multi-floor Bleed-Through</b>	Yes	Enables or disables calculating the impact APs on floors above and below the currently viewed floor in the Quick View.
<b>Dynamic Attenuation</b>	Yes	Incorporate AP to AP readings as well as site survey information and dynamically recalculate the path loss of each radio to every grid cell on the floor plan, increasing coverage and location accuracy.
<b>Use Metric Units</b>	No	Instructs the VisualRF engine to display all units of measurements in metric

**Table 139** *Server Settings* Section of the **VisualRF > Setup** Page (Continued)

Setting	Default	Description
<b>Memory Allocation</b>	512 MB	<p>The amount of memory dedicate to VisualRF. It is not dynamically allocated and all the memory is consumed upon starting the service. Be sure to check the memory and swap utilization in the <b>Systems &gt; Performance</b> page before making any changes. The exact amount of memory used per floor plan will vary heavily based on the size, number of devices and number of grid cells on the floor plan.</p> <ul style="list-style-type: none"> <li>• 25 floors or less 512 MB</li> <li>• 50 to 75 floors 1 GB</li> <li>• 75 to 100 floors 1.5 GB</li> <li>• 100 to 200 floors 3GB</li> <li>• 200 to 300 floors 5 GB (64-bit only)</li> <li>• Above 300 8 GB (64-bit only)</li> </ul> <p><b>NOTE:</b> If you see Out of Memory errors in the SSL error log on the <b>System &gt; Status</b> page, you should increase memory allocation.</p>
<b>Core Threads</b>	1x number of cores	Number of threads that calculate path loss for each floor. These threads also regenerate a floor's RF properties when new APs, walls, or regions are added to a floor plan.
<b>Location Caching Threads</b>	1x number of cores	Number of threads that calculate the location of all clients associated with access points on this floor plan.
<b>UI Threads</b>	1x number of cores	<p>Number of threads that service the users accessing QuickView, as well as AMP-to-VisualRF communication.</p> <p><b>NOTE:</b> If users experience timeout errors while using QuickView, allocate additional UI Threads.</p>
<b>Synchronization Timer</b>	15 minutes	This timer indicates how often VisualRF will synchronize security for APs within AMP.
<b>Restrict visibility of empty floor plans to the role of the user who created them</b>	No	When enabled, only the creator can view an empty floor plan.

To tune location accuracy, go to the **Location Settings** section on this page as described in [Table 140](#):

**Table 140** *Location Settings* Section in **VisualRF > Setup**

Setting	Default	Description
<b>Allowed deviation for client placement</b>	4 dB	<p>When VisualRF locates a client or rogue it utilizes signal metrics from all the APs that hear the client or rogue device. VisualRF builds a fingerprint location for all clients with similar transmit-power capability. All subsequent clients that fall within the deviation is placed on the same location fingerprint or x, y coordinates.</p> <p><b>Example:</b> AP #1 hears client1 at -72, and AP #2 hears client 1 at -64. VisualRF calculates the client's location to be at coordinates 100, 200. Client2 is heard by AP#1 at -71 and AP#2 at -65. VisualRF will use the average of the difference in signals (AP#1 -72 and -71) to see if the client matches a pre-calculated location fingerprint. <math>1 + 1</math> (differences in signals) / 2 (# of APs) = 1 which falls within the deviation of 2, hence the client would be located at 100,200.</p>
<b>Maximum Rogue APs per Floor Plan</b>	20	<p>Sets the maximum number of rogues AMP will place on a Floor. Use this filter in combination with the <b>RAPIDS Export Threshold</b> configured on the <b>RAPIDS &gt; Setup</b> page to intelligently control the number of rogue devices displayed per floor.</p> <p><b>NOTE:</b> Increasing this value could increase the load on the server and the clutter on the screen.</p>

To tune the frequency for calculating device locations within the VisualRF UI, navigate to the **Location Calculation Timer Settings** section as described in [Table 142](#):

**Table 141** *Location Calculation Timer Settings Section of VisualRF > Setup*

Setting	Default	Description
<b>Legacy Laptop Min/Max (sec)</b>	90/360	<p>This timer determines how often to calculate location for legacy laptop devices. Taken with the data samples the calculation would follow:</p> <p>After minimum timer (90 seconds) check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples).</p> <p>If so (<b>Yes</b> to question above) then recalculate the client device's location based on the samples received.</p> <p>If not (<b>No</b> to the question above) then wait until the number of sample setting is met and recalculate. If the number of samples is never met, wait until the maximum timer (360 seconds) and recalculate.</p>
<b>Legacy Laptop Number of Samples</b>	3	See definition above.

All of the other device types (phone, printer, scale, and so on) use the same methodology as detailed above.

To edit the wall settings and select a color for wall types within the VisualRF UI, navigate to the **Wall Attenuation Settings** section and select the pencil icon next to each of these settings as described in [Table 142](#):

**Table 142** *Wall Attenuation Settings in VisualRF > Setup*

Setting	Default	Description
<b>Glass Attenuation (dB)</b>	2	<p>Specifies the attenuation for any glass walls that are drawn in VisualRF.</p> <p><b>NOTE:</b> All of these values are global variables that cannot be overridden for individual floor plans. VisualRF uses these values to calculate path loss and client locations. Walls within VisualRF are interpreted as pure dB loss without adjusting for wall thickness.</p>
<b>Cubicle Attenuation (dB)</b>	4	Specifies the attenuation for any cubicle walls drawn in VisualRF.
<b>Drywall Attenuation (dB)</b>	6	Specifies the attenuation for any drywall walls drawn in VisualRF.
<b>Concrete Attenuation (dB)</b>	15	Specifies the attenuation for any concrete walls drawn in VisualRF.

## VisualRF Resource Utilization

When tuning the VisualRF server, use the default settings as recommended. If you do change any of these settings above, change one at a time and see how the system performs. Each time you restart VisualRF, it will take at least 30 minutes to return to normal processing.

If you use the 'top' command to check on VisualRF resource utilization, ensure you use the 'l' and 'H' flags to show cores and threads. Remember 'top' also takes 1-2 minutes to normalize and provide accurate data.



It is normal for VisualRF to consume 20% of each core with a combination of threads. It will utilize excess CPU cycles on all cores when required.

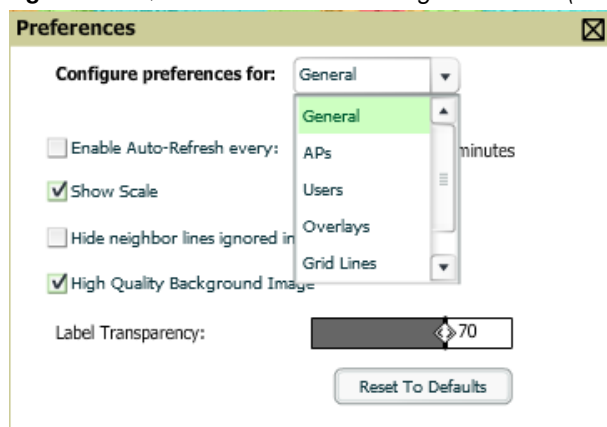


## Configuring QuickView Personal Preferences

To configure your personal preferences in QuickView, select the **Preferences** icon and choose from the following configuration options:

- **General** - select from the **Configure Preferences** drop-down menu, as shown in [Figure 202](#):
  - Enable auto-refresh toggle
  - Refresh Interval in minutes
  - Show Scale
  - Hide neighbor lines ignored in location calculation
  - High Quality Background Image - you can disable to increase rendering speed
  - Label Transparency

**Figure 202** QuickView Preferences Page Illustration (General preferences selected)



- **APs** - select from the **Configure Preferences** drop-down menu:
  - BW - select the kbps threshold for normal (green), high (yellow), and excessive (red)
  - # of Users - select the number of users threshold for normal (green), high (yellow), and excessive (red)
  - % of Uptime for the last 24 hours for normal (green) and excessive (red)
  - Radio Status - display red or green depending on the status of the radios within the AP
  - AP Status - display red or green in relation to up/down status of AP
  - Icon Size - select the size of the AP icon display on the floor plan
  - Show Channel in Label
  - Show Transmit Power in Label
- **Users** - select from the **Configure Preferences** drop-down menu:
  - BW - select the kbps threshold for normal (green), high (yellow), and excessive (red).
  - Signal Strength - select the dBm client threshold between excellent and poor
  - Icon Size - select the size of the client device icon display on the floor plan
- **Overlays** - select display type for Heatmaps, Speed, Sensor, Voice, and Ch. Utilization
  - Grid - non vector overlay
  - Vector - provides a more smooth overlay with mouse-over capabilities
- **Grid Lines** - Toggle grid lines on or off
  - Distance between grid lines
  - Color of grid lines

- **Navigation** - select from the Configure Preferences drop-down menu (campus and buildings):
  - % of APs Up for the last 24 hours for normal (green) and excessive (red)
  - Icon Size for campus, building and floor



These preferences are stored in the database, so they will be retained across browsers and machines.



The remaining sections in this chapter apply to networks, campuses, buildings, and floor plans that have already been set up in VisualRF. If you do not yet have any of this information in VisualRF for your network, refer to [“Planning and Provisioning” on page 281](#).

## Increasing Location Accuracy

The Location Service will use all RF information available to increase location accuracy of clients, tags, and rogue devices. Understanding your infrastructure's inherent capabilities helps you learn the extra effort required to ensure location accuracy.

There are three key elements read from controllers or access points that increase location accuracy: signal strength of a client as heard by the AP of association, signal strength of a client as heard by APs other than the AP of association, and signal strength at which an AP hears other APs.

These factors are detailed further in [Table 143](#):

**Table 143** Elements Read From Controllers to Increase Location Accuracy

MFG/Model	Client Signal Associated AP	AP-to-AP Signals (Dynamic Attenuation)	Unassociated Client Signal	Rogue AP Signal
Aruba	Yes	Yes	Yes	Yes
Cisco LWAPP	Yes	Yes	Yes	Yes
Cisco IOS	Yes	No	No	With WLSE
Cisco VxWorks	Yes	No	No	No
Trapeze	Yes	No	No	Yes
Meru	No	No	No	Yes
Proxim	Yes	Yes	Yes	Yes
Symbol Auton. AP	Yes	No	No	Yes
Symbol Thin AP	Yes	No	Yes	Yes
Proxim AP-2000	Yes	No	Yes	Yes
Proxim AP-4000	Yes	Yes	Yes	Yes
ProCurve WeSM	Yes	Yes	No	Yes
ProCurve 530	Yes	Yes	Yes	Yes
ProCurve 420	Yes	Yes	No	Yes

AirWave provides four main methods to increase accuracy once your access points are deployed:

- Adding Exterior Walls - increases location accuracy by reducing the statistical probability of placements outside the office confines. See [“Adding Exterior Walls” on page 270](#).
- Client Training for Stationary Devices - ensures non-mobile clients like desktops or scales will always remain in a defined static location. Statically assigning non-mobile devices reduces the CPU load on

your server because VisualRF does not evaluate any signal metrics for this MAC address when associated with an AP on the floor plan. See [“Location Training for Stationary Devices” on page 270](#).

- Remote Client Surveys - provides additional attenuation inputs for corners and low-coverage areas without the burden of actually carrying a laptop to the physical location. See [“Adding Client Surveys” on page 271](#).
- Location Probability Regions - Probability regions will increase or decrease the chances of a device being located within the region. See [“Adding Location Probability Regions” on page 272](#).

## Adding Exterior Walls

Because VisualRF utilizes much existing RF information, generally only external walls are required for accurate client locations. VisualRF's Dynamic Attenuation feature uses AP-to-AP information to calculate attenuation for interior areas, negating the need to enter interior walls. If your devices support AP-to-AP information in the table above, you should only draw exterior walls.

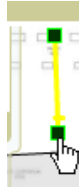
1. Select **Draw Walls** icon in the Edit menu.
2. The cursor changes to a crosshair. Use this to draw the wall directly over the floor plan, as shown in [Figure 203](#):

**Figure 203** Drawing a wall



3. To move or resize the wall, select the **Wall** icon in the Edit menu again. The cursor changes to a hand, and the ends of the wall is highlighted. Click and drag the end point handles to change the wall, as shown in [Figure 204](#):

**Figure 204** Moving and resizing an existing wall



- To change the attenuation of a wall, right-click the wall and select the appropriate building material.
  - To delete a wall, select the wall and press the Delete key.
4. Once all walls are provisioned on the floor plan, select **Save** (floppy disk icon above the zoom bar).



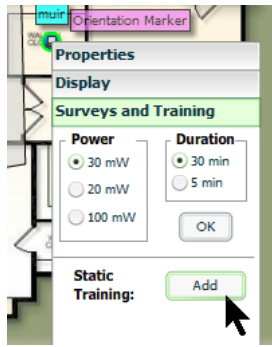
Drawing only outside walls is recommended. If you are seeing inaccurate client locations or heat maps after entering exterior walls, proceed to Client Surveys. If you still experience problems, then you can proceed to adding interior walls.

## Location Training for Stationary Devices

QuickView provides the ability to statically assign a permanent  $x, y$  coordinate to stationary devices like PCs, Scales, and Point-of-Sale terminals. This will reduce the calculation requirements on the VisualRF location service and increase the accuracy of the RF characteristics of individual floor plans.

1. Drag the client device to the proper location.
2. Select the device and a popup menu appears. From that menu, select **Surveys and Training**.
3. Click the **Add** button for Static Training, as shown in [Figure 205](#):

**Figure 205** *Surveys and Training menu for a client device*



To remove a statically trained device, select client, and select the Surveys and Training option. Select **Delete** button (which will have replaced the **Add** button) for Static Training.



The static locations are automatically saved, so the **Save** icon (floppy disk) will not appear.

## Adding Client Surveys

Client surveys provide a method for increasing the accuracy of the attenuation grid by taking real signal samplings from client devices associated with the WLAN.

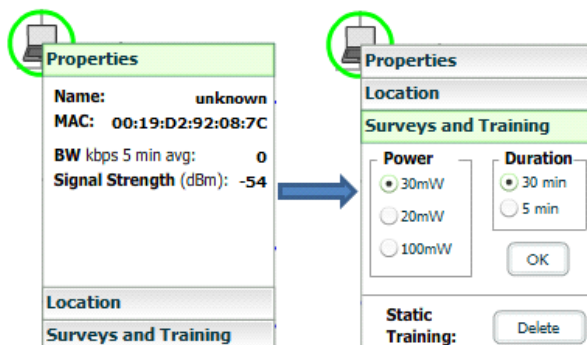
Key differentiators of AMP's client surveys are: (1) they take readings from the access points and not the client and (2) they take numerous samples. This produces a more accurate representation because signals obtained from the client's card (the signal level at which a client hears the AP) can vary from vendor to vendor.

The signal levels at which APs can hear a client are already normalized. Using multiple samples alleviates spikes or troughs that come from using a single sample.

To start a client survey, follow these steps:

1. Drag the client to the proper location.
2. Select the client to see the **Properties** pop-up menu, as shown in [Figure 206](#):

**Figure 206** *Client Surveys*



3. Select the **Surveys and Training** option.
4. Select the appropriate transmit power for the wireless client. Leave the default to **30mW** if you are unsure.
5. Select the **Duration** or the time that you want to sample the client's signal measurements. Longer durations will increase Path Loss accuracy and location accuracy.
6. Select **OK** to begin the survey.

To display survey locations, select the **Display** menu and select **Surveys**. Note the following information about this procedure:

- Ensure the client will remain in the same location for at least the duration of the survey.
- You should delete and resurvey an area or a floor plan after a remodel or significant interior movement.
- Surveys should be conducted during normal business hours to reflect normal RF activity on the floor.
- 11a clients automatically inherit the proper transmit power from the 11g configuration. Example: 30mW Pre-2006 laptops equate to 20mW for 11a clients.
- AMP dynamically assigns a transmit power to every client based on OUI as shown in [Table 144](#). This step increases the accuracy for surveys by allowing an override.

**Table 144** Auto-assigned Client Type and Transmit Power

Client Type	Transmit Power 11g
Pre-2006 Laptops	30 mW
Post -2006 Laptops	100 mW
SOHO WLAN Cards (D-Link, Net Gear, LINKSYS)	30 mW
RFID Tags	10 mW
PDA	20 mW
iPhone	20 mW
Desktop	100 mW
Cisco Cards	100 mW

## Adding Location Probability Regions

Location probability regions are optional regions that can be used to increase the accuracy of device location in VisualRF.

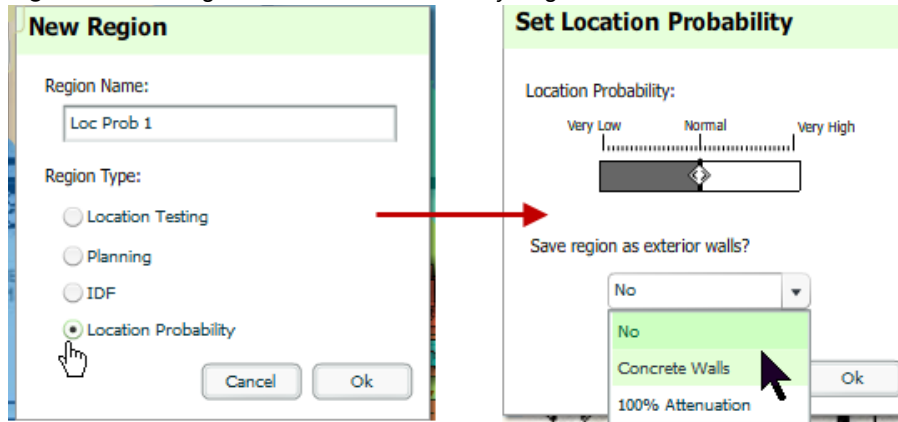
VisualRF calculates device locations based on probability. VisualRF determines the probability of a device being located in every grid cell and places the device where the probability is the highest.

Probability regions will add or remove up to 20% chance from the device location probability. They can be used to push users into regions where they are more likely to be located, like conference rooms and cubical farms, or they can be used to pull users out of regions where they are less likely to be like parking lots and courtyards.

To add a probability region to a floor plan, follow these steps:

1. Select the **Edit** menu and click the **Draw Region** option.
2. Outline the desired probability region. Double click to end the outline process.
3. Name the region, select a Region Type of **Location Probability** and select OK.
4. Move the location probability slider to the desired level, as shown on [Figure 207](#). **Very Low** will decrease the probability of a device being placed in that region by 20%. **Very High** will increase the probability of a device being placed in that region by 20%.

**Figure 207** Adding a New Location Probability Region



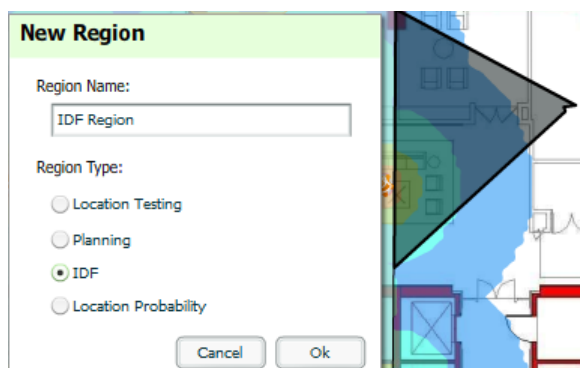
5. Optionally, you can save the location region as the exterior walls. 100% attenuation can be selected to force VisualRF to only place devices inside of the selected region. No device will ever be placed outside of the probability region when 100% attenuation is selected. 100% attenuation is only recommended for tall buildings where it is extremely unlikely that any user is located outside of the building. No heat map or attenuation grid is calculated for devices outside of the 100% attenuation region.

## Adding an IDF

To add an IDF to VisualRF, follow these steps:

1. In the **Edit** menu, select the **Draw Region** option.
2. Outline the desired IDF region. Double-click to end the outline process.
3. Name the region, select a Region Type of **IDF**, and select **OK**, as shown in [Figure 208](#).

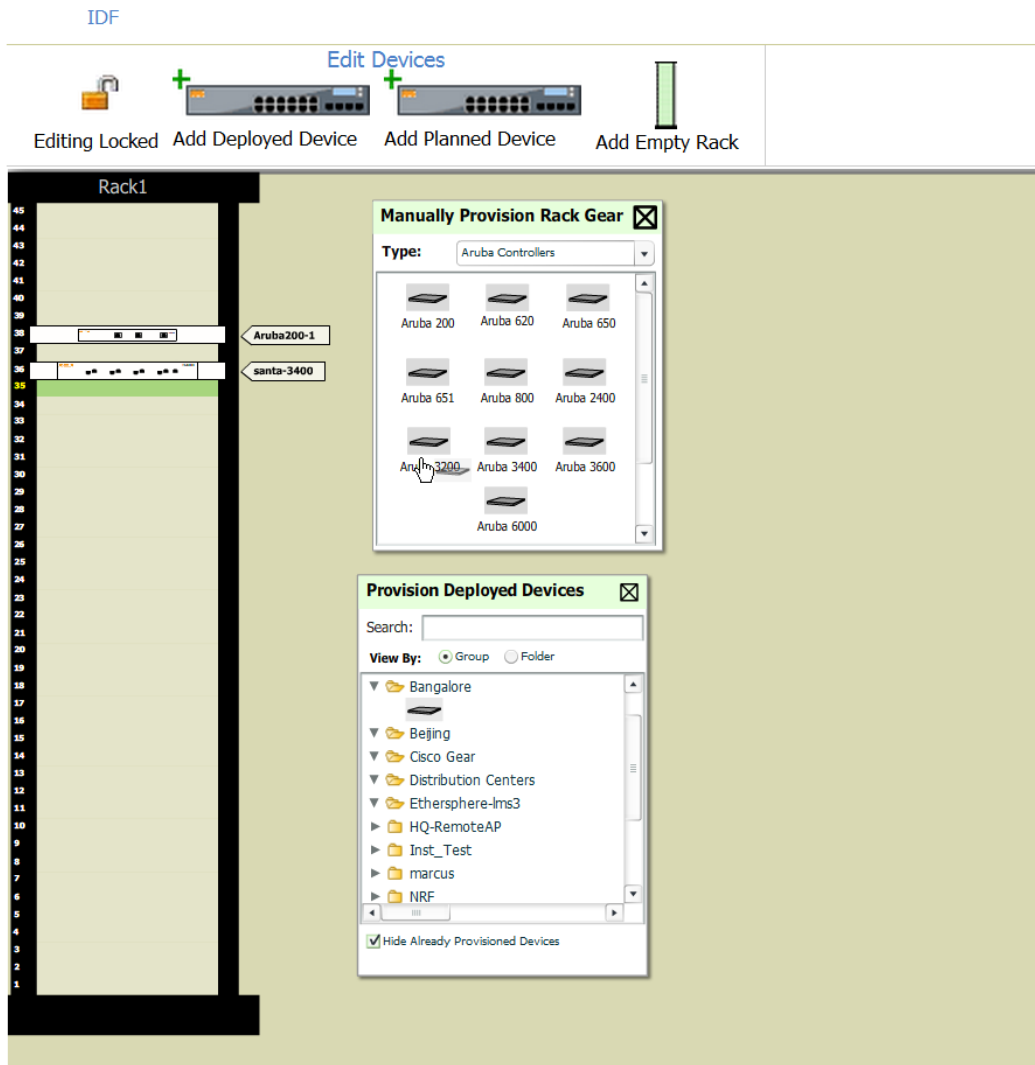
**Figure 208** Adding a new IDF Region



Now that the IDF is defined you will see a green IDF icon on your floor plan. Double click that icon to navigate into the IDF.

1. Add a rack to the IDF by selecting the **Add Empty Rack** icon and dragging it to the background.
2. To add a planned device, select the **Add Planned Device** icon to view the **Manually Provision Rack Gear** menu. Select the device type in the **Type** menu, and then find the device you want to add. Drag it into the rack at the appropriate location.
3. To add a wired device that is currently being monitored by AMP, select **Add Deployed Device**.
4. Locate the device to be added.
5. Drag the device to the appropriate location in the rack, as shown in [Figure 209](#).

**Figure 209** *Provisioning Devices*

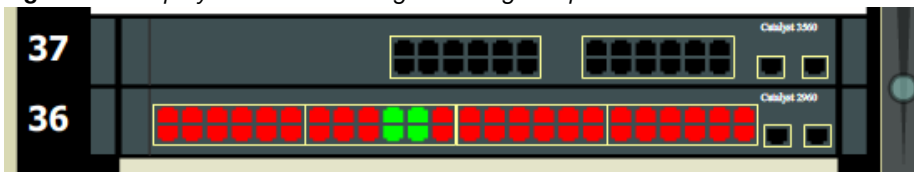


Wired devices that are added to an IDF are included in any BOM report covering that floor.

## Viewing Port Status on Deployed Switches

Deployed switches on a rack will display the port status as red (down) and green (up) interface icons, which corresponds with the operationally up devices on the **APs/Devices > Interfaces** list. Planned switches do not display these status indicators in VisualRF.

**Figure 210** *Deployed switch showing red and green port status icons*



## Fine-Tuning Location Service in VisualRF > Setup

There are several options on the **VisualRF > Setup** page which increase client location accuracy. All of these items will increase the processing requirements for the location service and could negatively impact the overall performance of AMP.

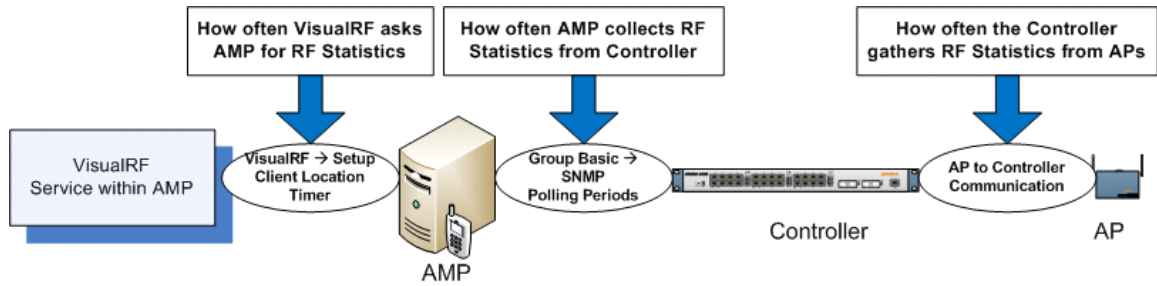


- **Grid Size** - decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy. You can right-click on a floor plan within a building view and change this setting.
- **Dynamic Attenuation** - enabling dynamic attenuation (which is on by default) instructs the location service to sample the current RF environment and to dynamically adjust Path Loss.

## Configuring Infrastructure

Ensure that the hardware is configured to retrieve the RF information and that it provides this information on a timely basis. There are three unique timing mechanisms which impact location accuracy: how often the infrastructure collects and correlates RF statistics in their MIB, how often the AMP queries those MIB entries, and how often VisualRF service queries AMP for this RF information.

**Figure 211** Timing Factors Impacting Location Accuracy



These best practices are recommended when configuring hardware infrastructure:

- For legacy autonomous APs, ensure on the **Group > Radio** page that **Rogue Scanning** is enabled and the interval is accurate, as shown in Figure 212:

**Figure 212** Group Rogue Scanning Configuration

- For thin APs, ensure that the controllers are configured to gather RF information from the thin APs frequently.
- For Cisco LWAPP, navigate to **Groups > Cisco WLC Config** page in AMP. Navigate the tree control to the **Wireless** section, and for each PHY navigate to **RRM > General** section.

**Figure 213** WLC RRM Configuration in AMP

Profile Thresholds for Traps	
Interference (0-100%):	10
Clients (1-75):	12
Noise (-127 to 0 dBm):	-70
Coverage (3-50 dBm):	12
Utilization (0-100%):	80
Data Rate (1-1000 Kbps):	1000

Noise/Interference/Rogue Monitoring Channels	
Monitoring Channels:	Country Channels

Monitor Intervals	
Signal Measurement (60-3600 sec):	300
Noise Measurement (60-3600 sec):	300
Load Measurement (60-3600 sec):	300
Coverage Measurement (60-3600 sec):	300

- Review the values in the **Monitor Intervals** section. These should be configured to a recommended setting of **180** for better accuracy.

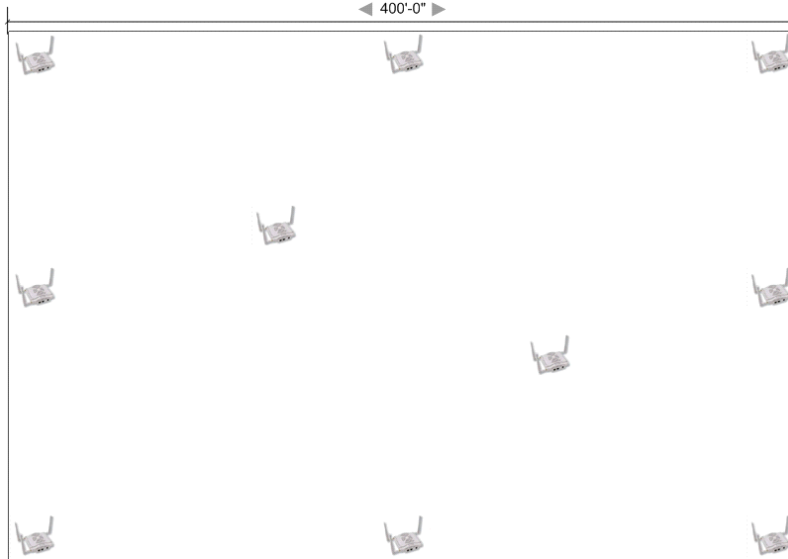
## Deploying APs for Client Location Accuracy

Deploying access points for client location accuracy can be different than deploying access points for capacity. Follow these guidelines for best results:

- Ensure that at least 3 radios can hear each client devices at -85 dBm or below
- Ensure that you deploy an access point approximately every 3,500 square feet.
- For square or rectangular floor plans ensure access points are deployed on the exterior walls of each floor with access points in the middle as well.

Refer to [Figure 214](#) for an example.

**Figure 214** Rectangular Floor Plan AP Deployment



## Using QuickView to Assess RF Environments

QuickView has four distinct views or entry points: client view, access point view, floor plan view, and network, campus, and building view.

This section contains the following corresponding topics:

- “Viewing a Wireless User's RF Environment” on page 276
- “Viewing an AP's Wireless RF Environment” on page 278
- “Viewing a Floor Plan's RF Environment” on page 279
- “Viewing a Network, Campus, Building's RF Environment” on page 280

### Viewing a Wireless User's RF Environment

1. Navigate to **Users > List** in AMP.
2. Click the link under the **Location** column for the user of interest, as shown in [Figure 215](#). A QuickView window of that location opens and indicates the client with a Username label, as shown in [Figure 216](#):

**Figure 215** Link to user's thumbnail (the Location column)

Username	Location ▼
ARUBANETWORKS\mgalvin	APAC SE TR > BLDG! > Floor 2
umahindra	APAC SE TR > BLDG! > Floor 2
dkurose	APAC SE TR > BLDG! > Floor 1
jzelnosky	-

**Figure 216** QuickView of the selected device



You can also access this information from the **Clients > Client Detail** page by selecting the QuickView thumbnail, located next to the **Current Association** section of this page as shown in Figure 217:

**Figure 217** QuickView thumbnail in **Clients > Client Detail**

Current Association			
Username:	dkurose	AP/Device:	1394
Role:	employee	Controller:	ethersphere-1322
Signal Quality:	-	Group:	1322 Test Controller
Association Time:	3/24/2011 2:26 PM	Folder:	Top > Sunnyvale HQ > 1322 Test controller
Duration:	4 mins	Device Location:	-
Connection Mode:	802.11n (2.4GHz)	Radio:	802.11bgn
Bandwidth:	-	Channel Bandwidth:	HT20
SSID:	ethersphere-voip	VLAN:	66
LAN IP Address:	0.0.0.0	LAN Hostname:	-
VPN IP Address:	-	VPN Hostname:	-
Auth Type:	WPA2 (EAP-PEAP)	Auth Time:	4 mins
Session:	APC	Session Mode:	Test/Control

Location: APAC SE TR > BLDG! > Floor 1 (Floor 1)

Enlarge |

Last Placed: 3/24/2011 2:26 PM

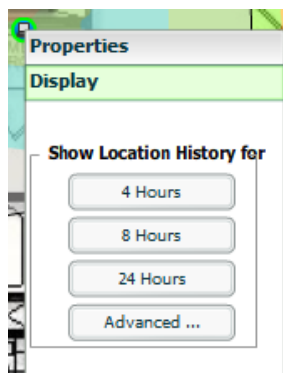
This view is focused on the wireless user enabling you quick resolution of a user's issues and therefore disables most RF objects by default.

- Users - only the user in focus is displayed
- APs - only the access point in which the focus client is associated with is displayed
- Radios - the heatmap represents only the radio to which the client in focus is associated
- Rogues - all rogues are off
- Client/Rogue Surveys - all surveys are off
- Walls - all walls are displayed
- Lines - client to AP of association
- Labels - all labels are disabled

## Tracking Location History

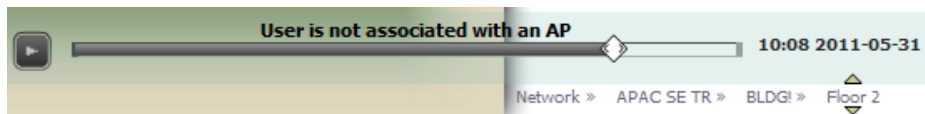
Select a client icon in the Floor Plan and select **Display** from the pop-up menu shown in Figure 218:

**Figure 218** Show Location History



A location history player, illustrated in Figure 219, appears at the bottom of the QuickView window.

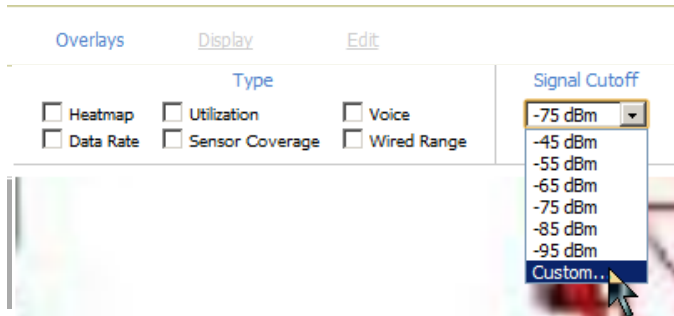
**Figure 219** Location History Player



## Checking Signal Strength to Client Location

1. On a Floor Plan, locate the **Signal Cutoff** menu.
2. Select the desired signal level to display, as shown in [Figure 220](#). The heatmap updates immediately.

**Figure 220** Signal Cutoff dBm Dropdown Menu

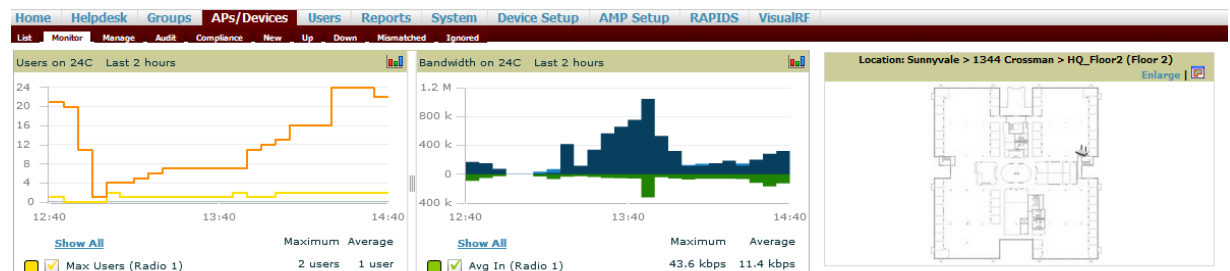


## Viewing an AP's Wireless RF Environment

To view an access point's RF environment from **APs/Devices > Monitor** page:

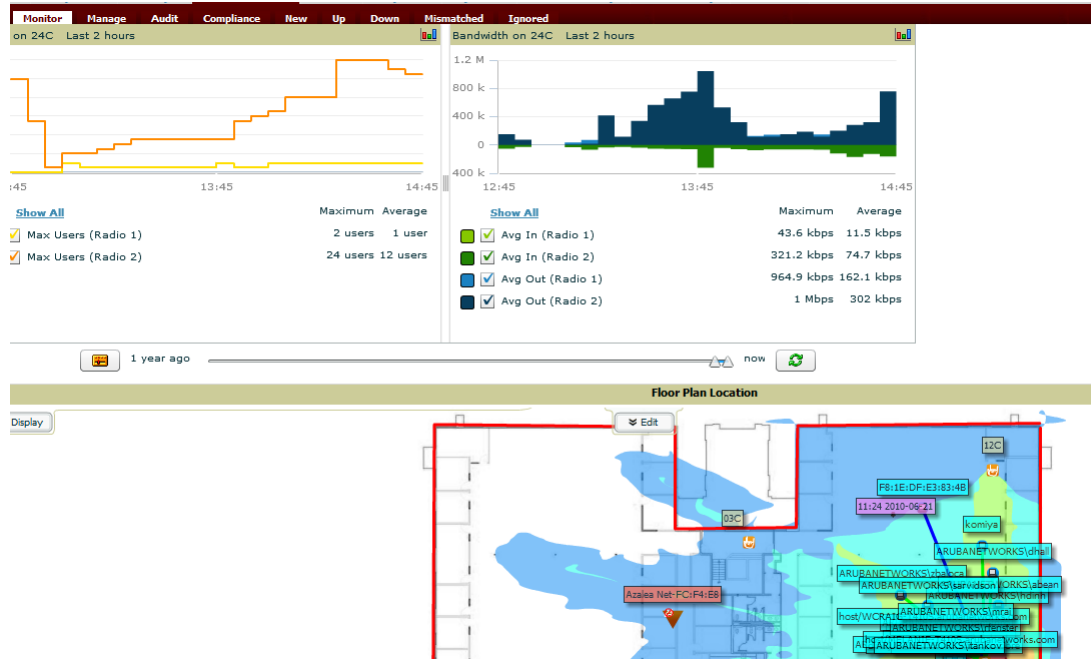
1. Select a device of interest from **APs/Devices > List**, or any other AMP page that lists your APs. The **APs/Devices > Monitor** page opens.
2. Click on the QuickView thumbnail showing the location of the AP, shown on the right side of [Figure 221](#):

**Figure 221** QuickView Thumbnail in **APs/Devices > Monitor** page for an AP



A fully interactive QuickView display opens below the thumbnail on the same page (not in a new window), as shown in [Figure 222](#):

**Figure 222** Full QuickView in **APs/Devices > Monitor** page for an AP (partial view)



This view is focused on enabling quick resolution of AP issues and therefore disables many RF objects by default as follows:

- Users - only users associated with radios within access point of focus are displayed
- APs - only the access point in focus is displayed
- Radios - the heatmap represents all radios within the access point of focus
- Rogues - all rogues are **off**
- Client/Rogue Surveys - all surveys are **off**
- Walls - all walls on displayed
- Lines - client to AP of association are displayed
- Labels - all labels are disabled

## Viewing a Floor Plan's RF Environment

View a floor plan's RF environment from **VisualRF > Floor Plans** page. This page has a fixed sorting filter of **Campus > Building > Floor number**.

**Figure 223** Floor Plans List View

Add New Floor Plan

11-14 of 14 Floor Plans | < < Page 3 of 3 | Choose columns | Export CSV

Campus	Building	Floor	Name	Size	Grid Cell Size	# of APs	# of Radios	# of Users	# of Rogues	File Size	Original Floor Plan
<input type="checkbox"/>	Default Campus	Default Building	2.0 Floor 2.0	277 x 123 ft	5.0 ft	0	0	0	0	16 KIB	<a href="#">Download</a>
<input type="checkbox"/>	Default Campus	Default Building	3.0 Floor 3	288 x 192 ft	5.0 ft	0	0	0	0	300 KIB	<a href="#">Download</a>
<input type="checkbox"/>	Default Campus	Default Building	4.0 Floor 4	526 x 381 ft	10.0 ft	0	0	0	0	592 KIB	<a href="#">Download</a>
<input type="checkbox"/>	Default Campus	Default Building	5.0 Atrium	400 x 215 ft	7.0 ft	4	6	3	0	1 MIB	<a href="#">Download</a>

11-14 of 14 Floor Plans | < < Page 3 of 3

Select All - Unselect All

Delete

The **VisualRF > Floor Plans** page provides a snapshot of how VisualRF is performing, as described in [Table 145](#):

**Table 145** *Floor Plans list columns*

Field	Description
Campus	Campus associated to the floor.
Building	Building associated to the floor.
Floor	Floor number. The decimal place can be used for mezzanine levels.
Name	Optional name of a floor. (If the name is not changed, it displays the name as Floor [Number] by default.)
Size	The height and width in feet of the floor plan, including white space.
Grid Cell Size	The size of the grid cells, in feet.
# of APs	The number of access points on the floor.
# of Radios	The number of radios associated with access points on the floor
# of Users	The number of wireless users associated with access points on the floor.  <b>NOTE:</b> Locating users consumes significant VisualRF resources. A floor with hundreds or thousands of clients can take a long time to process.
# of Rogues	The number of rogue devices heard by access points on the floor. This number reflects the filters configured on the VisualRF > Setup. This means that while APs on the floor might hear more rogue devices, they are being filtered because of weak signal, they haven't been heard recently, or they are ad-hoc.
File Size	The floor plan background or image reported, in kilobytes. The larger the file, the longer it will take to render in the canvas.
Original Floor Plan	A link to download the original image background file.


## Viewing a Network, Campus, Building's RF Environment

To view floors from a geographical perspective:

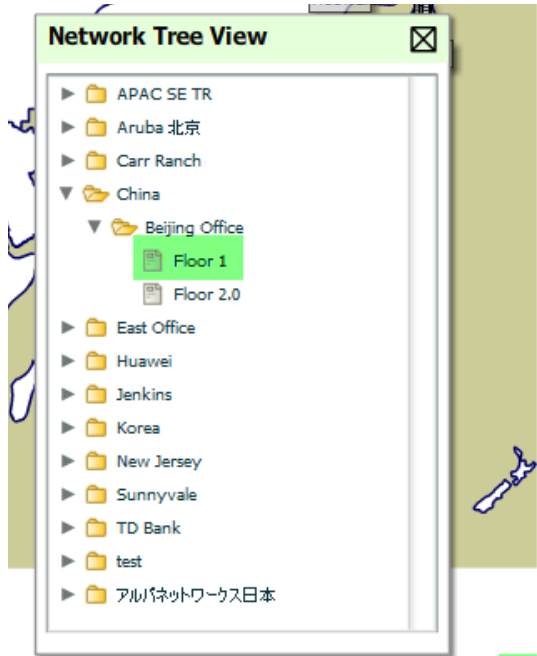
1. Navigate to the **VisualRF > Floor Plans** page.
2. Click on each network, campus, or building successively to drill down further until you reach the floor plan. This navigation provides information in each view as follows:
  - Network View - contains all campuses within your WLAN
  - Campus View - all buildings within a campus
  - Building View - all floors within a building
  - Floor Plan View - all devices access points, clients, and rogues within the floor

## Viewing Campuses, Buildings, or Floors from a Tree View

As an alternative to using QuickView, you can use the Tree View to view floors from a hierarchical tree, as follows:

1. Navigate to the **VisualRF > Floor Plans** page.
2. Select the **Tree** icon () at the top right of any view. The **Network Tree View** window, shown in [Figure 224](#), appears on the screen.

**Figure 224** Network Tree View - Floor highlighted



3. Use the arrows to drill down into the folders to select the Campus, Building, or Floor. Select the folder or floor plan icon to open the view you have selected. The Network Tree View window will remain on the screen until you close it.



If you prefer not to use background maps for your campus or building placements, click a background and select **Auto-Arrange** to move the campuses, buildings from their placements into an alphabetically-sorted list.

## Planning and Provisioning

VisualRF provides the capability to plan campuses, buildings, floors, and access points prior to the actual access point deployment. The following procedure describes the workflow:

- “Creating a New Campus” on page 281
- “Creating a New Building in a Campus” on page 282
- “Importing a Floor Plan” on page 284
- “Editing a Floor Plan Image” on page 284
- “Provisioning Existing Access Points onto the Floor Plan” on page 287
- “Automatically Provisioning APs onto a Floor Plan” on page 288
- “Tweaking a Planning Region” on page 289
- “Printing a Bill of Materials Report” on page 290

### Creating a New Campus

Floors are associated with a building and buildings are associated with a campus. In order to create a new floor, you must first create a campus and building.

To create and place your campus, follow these steps:

1. Navigate to **VisualRF > Floor Plans**.
2. Select the **Add Campus** button, located above the floor plan on the top left. The **Create New Campus** window, illustrated in Figure 225, appears.



3. Enter the following campus information:

- **Name** of the campus
- **Client Transmit Power** - used in auto placement of access points onto floors within this campus. The range is 30mW to 100mW.
- **Desired Speed** (mbps)- used in auto placement of access points onto floors within this campus. The range is 6 to 200 mbps.



---

Buildings and floors inherit transmit power and speed from the campus.

---

**Figure 225** *Create New Campus window*

The image shows a 'Create New Campus' dialog box. It has a title bar with the text 'Create New Campus'. Inside the dialog, there are three input fields: 'Name' with the value 'East', 'Client Transmit Power' with a dropdown menu showing '30mW', and 'Desired Speed (mbps)' with a dropdown menu showing '36 mbps'. At the bottom of the dialog are two buttons: 'Cancel' and 'OK'.

4. Select **OK** to save. You will see a new Campus icon appear on the campus canvas.
5. Add appropriate network geographical background or upload a personalized image by right-clicking on the background.
  - Set Map - allows you to browse with the included maps.
  - Auto Arrange Campuses - arranges the campus in alphabetical order across the background.
6. Drag the new Campus icon to the appropriate location on the map background.



---

QuickView automatically saves background map images, campus locations, building locations, and building types

---

## Creating a New Building in a Campus

1. Select the newly created Campus icon from the previous step. When the blank campus area opens, select the **Add New Building** icon.
2. When the New Building window appears, enter the following information:

**Table 146** *New Building Fields and Descriptions*

Field	Description
<b>Name</b>	Name of the building; located on an existing campus.
<b>Campus</b>	Lists all campuses configured on your AMP.
<b>Longitude &amp; Latitude</b>	These fields are used to represent a building on Google Earth.
<b>Distance between floors</b>	The normal distance between floors in the building. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently utilized by AirWave.

**Table 146** *New Building Fields and Descriptions (Continued)*

Field	Description
<b>Attenuation between floors</b>	Enter the attenuation loss in decibels between floors. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently utilized by AirWave.
<b>Client Transmit Power</b>	This value is used when auto-provisioning access points onto a floor plan.
<b>Desired Speed</b>	Speed will determine the new access points when auto-provisioning.
<b>Address</b>	Building or Campus address (optional)

**Figure 226** *Create New Building Window*

3. Select **OK** to save. A new Building icon will appear in the middle of the canvas.
4. Drag the Building icon to the appropriate location on the map background.




---

QuickView automatically saves background map images, campus locations, building locations, and building types.

---

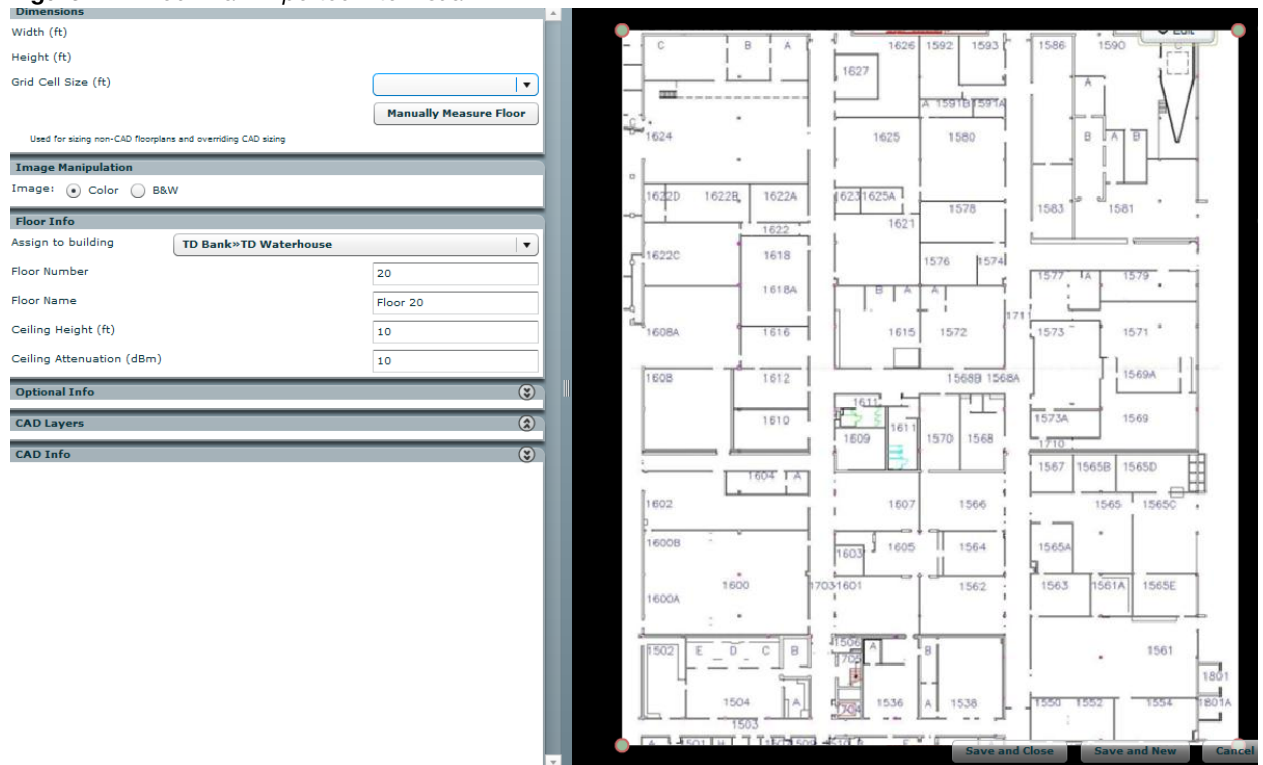
5. Add appropriate geographical background or upload a personalized image by right-clicking on the background.
  - Set Map - allows you to browse with the included maps.
  - Custom - launches the image upload wizard documented in [“Importing a Floor Plan” on page 284](#).
6. To change building types, right-click the Building icon.
7. Select proper building type.
8. Select the newly created Building icon from the previous step. You are redirected to a blank canvas without a background. You are now ready to import your floor plan.

## Importing a Floor Plan

The following steps show how to import a floor plan background image file.

1. In **VisualRF > Floor Plans**, click the **Add Floorplan** icon (displays when viewing a Building) or use the **Add** button above the floor plan list at the bottom of the page.
2. Select **Choose File** to locate a floor plan image file from your hard drive.
3. In VisualRF, select **Upload**. This opens the image file along with VisualRF planning tools on the left side.

**Figure 227** Floor Plan Imported into VisualRF



- If the floor plan does not require cropping, sizing, or layer control, then click **Save and Close** to begin provisioning APs or **Save and New** to upload a new floor plan.
- If the floor plan does require cropping, sizing, or layer control, then proceed to the next procedure.

## Editing a Floor Plan Image

There are many ways to edit a floor plan that you have uploaded, as explained in the following topics:

- “Cropping the Floor Plan Image” on page 284
- “Sizing a Non-CAD Floor Plan” on page 285
- “Removing Color from a Floor Plan Image” on page 285
- “Assigning Campus, Building and Floor Numbers” on page 286
- “Assigning Optional Planner, Owner, or Installer Information for the Floor Plan” on page 286
- “Controlling the Layers in the Uploaded Floor Plan (CAD only)” on page 286
- “Error Checking of CAD Images” on page 286
- “Last Steps in Editing an Uploaded Image” on page 287

## Cropping the Floor Plan Image

Use the cropping handles (red circles) to remove extra white space around the floor plan. VisualRF will calculate an attenuation grid for the entire map including white space. Reducing the white space on a floor

plan will increase location accuracy and decrease the load on the server. A good rule of thumb would be about ½ inch white space, if possible, on all sides.

VisualRF dissects each floor plan into a grid consisting of cells specified in this setting. The Core Thread service calculates the path loss for every radio to every cell on the floor plan.

By default the importation wizard allocates 2,500 grid cells to each site based on dimensions. If you have a site that is 250 ft. by 100 ft, the Floor Plan importation wizard would calculate the grid cell size at 10 feet.  $250 \text{ ft.} \times 100 \text{ ft.} = 25,000 \text{ ft.}$   $25,000 \text{ ft.} / 2,500 \text{ ft.} = 10 \text{ ft.}$



Decreasing the grid cell size will increase accuracy, but it also increase CPU consumption by the floor caching threads and the location caching threads. Check the System ' Performance page to ensure your server is functioning properly when you make a change to this setting.

Other items worth noting:

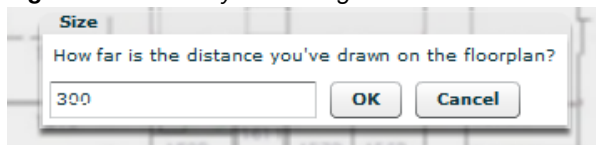
- If this is a CAD file, then the Floor Plan creation wizard will automatically inherit height and width from the drawing.
- If this is a non-CAD file, then the height and width is zero.
- CAD files are converted to a JPG with a resolution of 4096 horizontal pixels at 100% quality prior to cropping. If you crop, then you will lose clarity.
- CAD files may not exceed 10 MB.
- Metric CAD files are supported.
- Importing GIF files for floor plans will result in blank QuickView thumbnails.

### Sizing a Non-CAD Floor Plan

You should not have to resize a CAD drawing unless you see nonsensical dimensions. To resize a non-CAD image if you already know the dimensions, follow these steps:

1. Select the **Manually Measure Floor** button in the **Dimensions** section. The pointer changes to a cross-hair icon.
2. Locate two points within the floor plan that you know the distance. Most door jams (door openings) are 3 feet.
3. Select and hold to establish the first point and drag your mouse to the second point and release.
4. A distance dialogue box appears. Enter the proper length in feet, as shown in [Figure 228](#).

**Figure 228** *Manually Measuring a Floor Plan*



5. Select **OK**.

Floor plans can be resized in VisualRF after they have been uploaded. Within VisualRF you will also be able to zoom in on a room or doorway to increase the accuracy of your sizing.

### Removing Color from a Floor Plan Image

To remove color, locate the **Image Manipulation** section and select **B&W** in the **Image** field.

## Assigning Campus, Building and Floor Numbers

Locate the **Floor Info** Section and assign the following information, as detailed in [Table 147](#) and illustrated in [Figure 229](#):

**Table 147** Assigning numbers

Setting	Default	Description
Building drop-down	N/A	Use this drop-down to associate the floor with a building which associate it to a Campus as well.
Floor Number	0.0	The floor number. You can enter negative numbers for basements. <b>NOTE:</b> Each floor plan within a building must have a unique floor number.
Floor Name	Floor [Number]	A descriptive name for the floor. It inherits the floor number as a name if nothing is entered.
Ceiling Height	10	Specifies the height from the floor to the ceiling. This will default to the ceiling height for the building, but you can override here if needed for atria or basements.
Ceiling Attenuation	20	Specifies the attenuation characteristics in dB of the ceiling or the floor above.

**Figure 229** Entering Floor Info for the Uploaded Floor Plan Image

The screenshot shows a web form titled "Floor Info". It contains the following fields:

- Assign to building:** A dropdown menu with "New Jersey»N" selected.
- Floor Number:** A text input field containing the value "4".
- Floor Name:** A text input field containing the value "Floor 4".
- Ceiling Height (ft):** A text input field containing the value "10".
- Ceiling Attenuation (dBm):** A text input field containing the value "10".

## Assigning Optional Planner, Owner, or Installer Information for the Floor Plan

Locate the **Optional Information** section and enter the following information in [Table 148](#):

**Table 148** Optional Information for the Floor Plan

Setting	Default	Description
Owner	N/A	The owner of the floor (used in diagnostics and alerts).
Planner	N/A	The person in charge of planning the RF layout for the floor.
Installer	N/A	The person in charge of installing RF equipment for the floor.

## Controlling the Layers in the Uploaded Floor Plan (CAD only)

Follow these steps for CAD images:

1. Find the CAD Layers section on the page.
2. Unselect the layers which are not required. There is slight delay because each request makes a round trip to the server.

## Error Checking of CAD Images

VisualRF will check for errors in your uploaded CAD image. You can view any issues as follows:

1. Locate the **CAD Info** section, as shown in [Figure 230](#).
2. Review the CAD version, units of measurement, and raw width and height numbers.

**Figure 230** Checking for CAD errors

CAD Info	
Name	Value
FUW Version	3.03
Source File	fwcpk-3.dwg
File Type	DWG
Version	2004
Layout	Model

## Last Steps in Editing an Uploaded Image

Click the **Save and Close** button to begin provisioning APs or **Save and New** to upload another floor plan. After clicking **Save and Close**, you are redirected back into QuickView where you can provision APs, IDF's, and wired infrastructure.

## Provisioning Existing Access Points onto the Floor Plan

To provision existing AP in your network onto the floor plan you just uploaded, follow these steps:

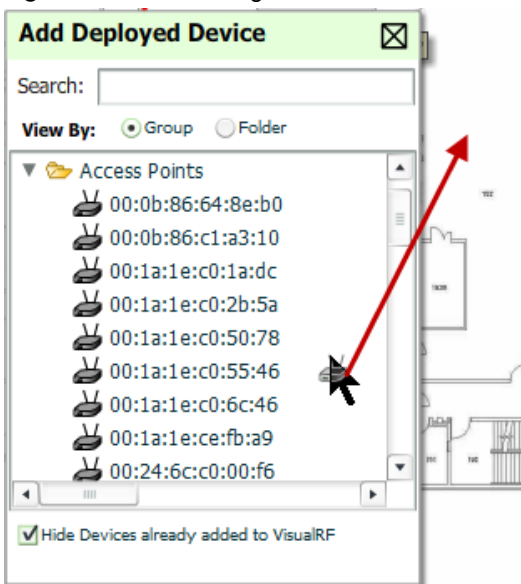
1. Navigate to **VisualRF > Floor Plans**.
2. Select the floor plan you have uploaded using the floor number or name links in the list.
3. Select the **Add Deployed Device** icon in the **Edit** menu. A pop-up window list of devices in your AMP appears, as shown on 4..
4. Select whether to navigate by Group or by Folder in the **View By** field.



Alternatively, you can use the **Search** field.

5. Expand the Group or Folder containing the access points which need to be provisioned on this floor plan. Note that by default, devices that have already been added to VisualRF are hidden. To show them, clear the "Hide Devices already added to VisualRF" checkbox at the bottom of the list.
6. Click and drag an AP to its proper location on the floor, as shown in [Figure 231](#):

**Figure 231** Provisioning APs onto the Floor Plan



- Once all APs are provisioned on the floor plan, select **Save** (floppy disk icon) in the top right of the QuickView window.



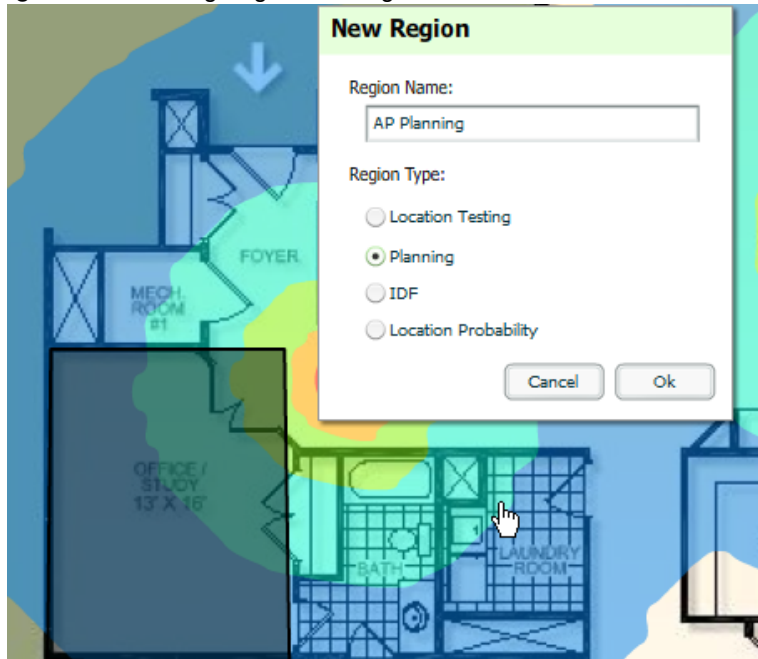
The floor is submitted to one of the core threads to recalculate path loss and then to one of the location caching threads to recalculate client locations. All changes may not be visible on a refresh until this process complete.

## Automatically Provisioning APs onto a Floor Plan

To automatically provision your access points onto your floor plan:

- Select **Draw Region** from the **Edit** menu. A new provisioning popup appears as shown in 4. with a crosshair pointer.

**Figure 232** Planning Region Drawing and Selection Illustration



- Draw your polygon as follows:
  - Left-click to initiate the process. The tool will automatically shade in your provisioning area.
  - Complete the polygon by double-clicking.
- Once you have finished drawing the region, enter a name for the region and select a Region Type of **Planning**. Then select **OK**.
- Enter the following information into the **Autoprovision APs** window as described in Table 149 and illustrated in Figure 233:

**Table 149** Fields in the Autoprovision APs Window

Field	Description
<b>Device Selection</b>	
<b>AP Type</b>	The type of AP used in this planning region.
<b>Radio Section</b>	
<b>Phy</b>	Whether they PHY is set to 11n or no radio.
<b>Xmit</b>	Transmit power of the APs.
<b>Gain</b>	Gain of the APs.
<b>EIRP</b>	EIRP of the APs.



**Table 149** *Fields in the Autoprovision APs Window (Continued)*

Field	Description
<b>Environment</b>	A range from 1-4 that best describes whether the environment is related to an office space, cubicles, offices, or concrete. Decimal points are allowed.
<b>Plan By Section</b>	
<b>Coverage</b>	Plan Coverage by Speed or Signal.
<b>Location</b>	Plan for location accuracy. This mode will result in additional APs placed near the edge of the region to aid in location calculation.
<b>Number of APs</b>	Number of APs to place in the planning region.
<b>Client Info Section</b>	
<b>Enable</b>	Whether to enable planning by user capacity.
<b>Total clients in region</b>	Set the anticipated number of clients that will be stationed in a region.
<b>Max clients per radio</b>	The maximum number of clients supported by each radio.
<b>Other Section</b>	
<b>Plan Sensors</b>	Whether to plan sensors into the region.
<b>Save Region as Walls</b>	Whether to save the edges of the planning region as walls.
<b>Update Environment and Data Rate</b>	Whether to update the environment and data rate in case of changes.

**Figure 233** *Autoprovision APs Window Illustration*

The screenshot shows the 'Autoprovision APs' window with the following sections:

- Device Selection:** AP Type is set to 'Aruba AP 105(n)'.
- Plan By:** Radio button for 'Speed' is selected, with a dropdown set to '300 mbps'. A 'Coverage' dropdown is also visible.
- Radio Section:**
  - Radio 1:** Phy is '11n 2.4 GHz', Xmit is '12 dBm', Gain is '2.5', and EIRP is '14.5 dBm'.
  - Radio 2:** Phy is '11n 5 GHz', Xmit is '12 dBm', Gain is '4', and EIRP is '16 dBm'.
- Client Info:**
  - 'Total clients in region' is set to '20'.
  - 'Max clients per radio' is set to '3'.
  - 'Enable' checkbox is checked.
- Environment:** A slider bar is shown with labels 'Open Space', 'Cubicles', 'Offices', and 'Concrete'. The value is set to '3.5'.
- Other:**
  - 'Plan Sensors' and 'Save Region as Walls' are unchecked.
  - 'Update Environment and Data Rate' checkbox is checked.

At the bottom are 'Cancel' and 'Ok' buttons.

5. When you're finished selecting the desired options, select **OK**.

## Tweaking a Planning Region

If the planning layout does not meet your expectations, you can edit by right-clicking within the region to see the following options:

- **Delete Planned APs in the Region** - deletes only provisioned APs in the region
- **Reprovision APs** - remove all planned APs inside this region and prompts for new information to replan the region

- **Delete the Region** - deletes the region and all planned APs
- **Edit the region** - change the name of the region
- **Copy the Region to floors above** - will copy the region and auto plan for floors above.




---

The starting floor will add one to the highest floor in the building and the ending floor defaults to 10 more than the starting floor.

---

To replicate a floor plan, follow these steps:

1. Navigate back to the Building view by clicking on the navigation tags in the bottom-right corner of the window.
2. Right-click the floor and select **Duplicate**.
3. Enter the following information:
  - Starting and ending floors
  - Select the toggles to copy walls, regions, data rates (speeds), and AP placement




---

The starting floor will add one to the highest floor in the building and the ending floor defaults to 10 more than the starting floor.

---

4. Select **OK** to save your changes.
5. Manually refresh page and you are redirected to the **VisualRF > Floor Plan** page. The Building view will reflect the new floors.




---

You should see all replicate floors with matching number of access points.

---

## Auto-Matching Planned Devices

You can right-click a campus, building, or network icon and select the **Auto-Match Planned Devices** option to efficiently match planned APs to managed APs. If you select this option for a campus, then all planned APs in that campus are checked. If used on a building, then all the APs in that building are checked. If used on a floor, then all APs on that floor are checked.

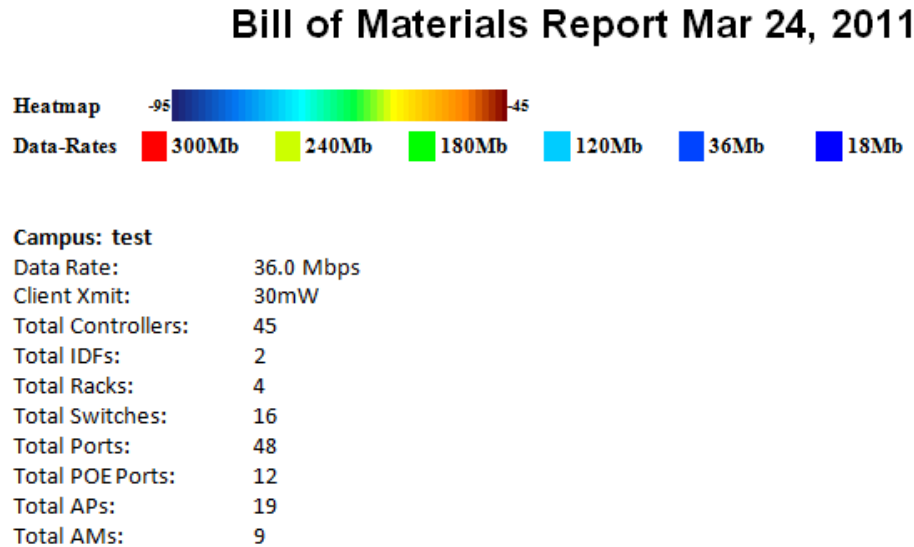
Planned devices first attempt to auto-match on MAC address, and then by name. The VisualRF MAC address checks against all of the LAN MAC addresses of a deployed AP.

## Printing a Bill of Materials Report

You can generate a Bill of Materials (BOM) Report from within VisualRF in Word format. Follow these steps:

1. Navigate back to the Network view.
2. Right select Campus icon and select **Show Bill of Materials**. A generating report popup appears.
3. Select options such as heatmap, speed, sensor coverage, wired range, and summary.
4. Select **OK**. A BOM report appears in Microsoft Word as illustrated in [Figure 234](#):

Figure 234 Bill of Materials Report Illustration



## Importing and Exporting in VisualRF

### Exporting a campus

To export a campus from VisualRF so you can import it into another AMP, follow these steps:

1. Navigate back to the **Network** view.
2. Right-click the **Campus** icon.
3. Select **Export**. An object selection window appears.
4. Select the objects to export and select **Export**. A File Download window appears.
5. Select **Save** and save the zipped file to your local hard drive for importation to another AMP.

At this point, you are ready to deploy a production AMP and manage devices by importing your exported campus and matching the access points to your plan.

### Importing from CAD

The Floor Plan Upload Wizard (FUW) should inherit all pertinent information from your CAD file if you follow this procedure:

1. Determine UNITS - all modern CAD versions (2001 and newer) support UNITS
2. Determine MEASURE - Legacy CAD versions (2000 and older) used a Imperial or Metric system.
  - If UNITS are 0 or undefined, then the standard dictates defaulting to MEASURE value
  - If MEASURE is 0 or undefined, then the standard dictates defaulting to English and inches
3. Find MODEL VIEW - If the drawing contains multiple views the FUW will default to the Model view
4. Determine Bounding Box - FUW will encompass all lines and symbols on the drawing and create a bounding box which is generally smaller than entire drawing. It is based on the UNITS or MEASUREMENT above.
5. Convert to JPG - FUW will convert the bounding box area to a JPG file with a resolution of 4096 horizontal pixels at 100% quality.
6. Start Web UI of FUW Step #1 - This is the cropping step.

This and all subsequent steps use the converted JPG file. The greater the floor plan dimensions, the less clarity the background image provides.

## Batch Importing CAD Files

This process provides the ability to automatically upload many CAD files and auto provision existing walls and access points, and contains the following topics:

- “Requirements” on page 292
- “Pre Processing Steps” on page 292
- “Upload Processing Steps” on page 292
- “Post Processing Steps” on page 293
- “Sample Upload Instruction XML File” on page 293
- “Common Importation Problems” on page 293

### Requirements

- Operating System: Client machine must be Windows XP, Windows Vista, or Windows 7
- Flash: Version 9 or later

### Pre Processing Steps

1. Increase Memory Allocation in **VisualRF > Setup** as follows:
  - 25 floors or less - 512 MB
  - 25 to 75 floors - 1 GB
  - More than 75 floors - 1.5 GB
2. Massage the output data.
3. Increase the **Location Caching Timer** to 1 hour so that VisualRF does not overload the server calculating client locations while calculating path loss and process floor plan images.

### Upload Processing Steps

1. Create CAD XML files which contain drawing filename, dimensions and optional information like device manufacture and model, device coordinates, wall coordinates and building material. This step is usually performed by your facilities or CAD department. The output of AutoCAD will not be properly formed XML, so you may need to massage the output data.
2. Copy all CAD drawings and corresponding XML files into a single directory on Windows machine. All files must be in a single directory.
3. Compress all files into a single \*.zip file.
4. Open your browser and navigate to your AMP: [https://<AMP\\_NAME>/visualrf/site\\_batch](https://<AMP_NAME>/visualrf/site_batch).
5. Select **Browse** to launch the File Explorer Window.
6. Select the zip file containing the upload instructions and click the **Open** button. The File Explorer Window will disappear you will return to the Batch Floor Upload Wizard.
7. Select **Next**.
8. The application validates the following information
  - Well-formed XML
  - All drawing files are accessible
  - All APs are present
  - All Building and Campuses are present
9. If there are any errors, none of the floor plans are created.

## Post Processing Steps

1. Decrease the Location Caching Timer to previous value.
2. Review the **VisualRF > Floor Plans** page to ensure server is keeping up.

## Sample Upload Instruction XML File

```
<?xml version='1.0' encoding='ISO-8859-1'?>
<visualrf:site_batch xmlns:visualrf='http://www.example.com'
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  version='1' origin='lower-left'>
  <floor name='T-0607' number='21' building-id='218'>
    <image filename='T-0607_WLS_02.dwg' />
    <access-points>
      <access-point id=29648 x=177.51 y=293.15 />
      <access-point id=29678 x=312.78 y=293.63 />
      <access-point id=29748 x=259.15 y=432.62 />
    </access-points>
    <walls>
      <wall type=4 x1=135.94 y1=159.43 x2=135.94 y2=453.16 />
      <wall type=4 x1=135.04 y1=453.16 x2=439.83 y2=453.16 />
      <wall type=4 x1=439.83 y1=453.16 x2=439.83 y2=418.16 />
    </walls>
  </floor>
  <floor name='T-0068' number='22' building-id='218'>
    <image filename='T-0068_WLS_01.dwg' />
  </floor>
  <floor name='Test JPG' number='23' building-id='218' width='523.34' height='231.34'>
    <image filename='Flwst IT_dwg.jpg' />
  </floor>
</visualrf:site_batch>
```

## Common Importation Problems

- Improper or undefined UNITS or MEASURE
- Text embedded into the Model view which causes an inconsistent bounding box
- Large dimensions which cause grainy resolution upon zoom
- Legacy CAD versions prior to Release 15 or AutoCAD 2000.

## Importing from an Aruba Controller

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into an Aruba controller.

## Pre-Conversion Checklist

Prior to importing floor plans, ensure that VisualRF's memory allocation is sufficient for the anticipated number of floor plans.

To change the memory allocation, navigate to the **VisualRF > Setup** page and configure the memory allocation accordingly. Memory allocation should equal .5 GB for 1-75 floor plans, 1 GB for 76-250 floor plans, 1.5 GB for 251-500 floor plans, and 2 GB for 501-1,000 floor plans.



Importing a large number of floor plans can impact performance of the AMP server. VisualRF must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. This can cause the **VisualRF > Floor Plans** page to be unresponsive.

## Process on Controller

1. On the controller's UI, navigate to the **Plan > Building List** page.
2. Select the buildings to be exported and select **Export**.
3. When the dialog box appears, make sure that you have included all images and select **Save to a file**.

## Process on AMP

1. Navigate to **VisualRF > Import**.
2. Select the **Import floor plans from an Aruba Controller** link.
3. Select the **Begin Importing Floor Plans** link.
4. When prompted for input file, use the file saved from the controller process.

## VisualRF Location APIs

VisualRF provides the following location APIs:

**Site Inventory:** `https://[amp_host]/visualrf/site.xml?site_id=...`

- You can find the `site_id` from the Floor Plan List query defined on the XML API page
- This interface provides floor details including access points, walls, regions, surveys, etc.
- The corresponding example XML and schema are attached in `visualrf_site_inventory.*`

**Device Location:** `https://[amp_host]/visualrf/location.xml?mac=...`

- Provide the radio MAC of the client to locate.
- The corresponding site where the user was placed is provided along with the dimensions
- If a client is heard on multiple floors, it will only be placed on the floor that contains the AP it is associated with.

## Sample Device Location Response

```
<visualrf:device_location version="1" xmlns:visualrf="www.example.com">
  <device mac="00:13:02:C2:39:28" name="Peter"
    site_id="4f674301-4b47-4ac6-8417-4eba3f7df3a6"
    site_name="NewYork">
    <site-width>124.51</site-width>
    <site-height>161.14</site-height>
    <x>82.50</x>
    <y>37.50</y>
  </device>
</visualrf:device_location>
```

## Sample Site Inventory Response

```
<amp:amp_site_inventory version="1"
  xmlns:amp=http://www.example.com
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <site id="b45e7a49-23b5-4db0-891a-2e60bff90d2c" version="677">
    <name>Remax</name>
    <uom>ft</uom>
    <width>314.45</width> <height>425.88</height>
    <property name="site_owner" value="" format="" />
    <property name="name" value="Remax" format="" />
    <property name="installer" value="" format="" />
    <property name="planner" value="" format="" />
    <image type="background">
      <filename>/var/example/snapshot/b45e7a49-23-2e6d2c.677/background.jpg</filename>
      <relative-url>/snapshot/b423b5-4db0-891a2e0d2c.677/background.jpg</relative-url>
      <pixel-width>1151</pixel-width>
      <pixel-height>1557</pixel-height>
    </image>
    <image type="thumbnail">
      <filename>/var/example/snapshot/b45e7a49891af90d2c.677/thumb.jpg</filename>
      <relative-url>/snapshot/b45e7a49-23b5-4db0-891a2c.677/thumb.jpg</relative-url>
      <pixel-width>230</pixel-width>
      <pixel-height>311</pixel-height>
    </image>
    <ap id="12615" name="AP-4000M-1">
      <x>118.97</x> <y>130.38</y>
      <total-bandwidth>0</total-bandwidth>
      <total-clients>0</total-clients>
```

```

<status>down</status>
<uptime>0.0</uptime>
<radio index="1" phy="g" mac="00:20:A6:5A:63:66" beamwidth="0.0"
  gain="1.5" antenna="" orientation="0.0" mount="Ceiling" valid="false">
  <discovering-radio id="11276" index="1" dBm="-85" />
  <discovering-radio id="11828" index="1" dBm="-93" />
</radio>
</ap>
</site>
</amp:amp_site_inventory>

```

## About VisualRF Plan

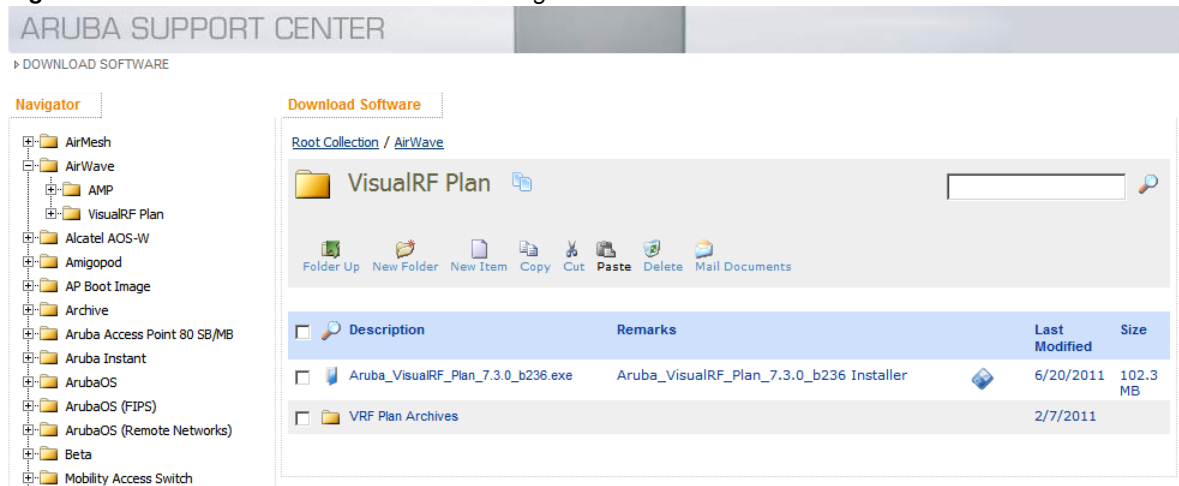
### Overview

VisualRF Plan is a standalone Windows client that can be used for planning sites that do not yet use the AirWave service on the Web. You can use VisualRF Plan to do basic planning procedures like adding a floor plan, provisioning APs, and generating a Bill of Materials (BOM) report.

VisualRF Plan is free to use for anyone with an Aruba support account. No license is required.

The client can be downloaded from the Aruba Support Center at <http://support.arubanetworks.com>. At the Support site, select the Download Software Link, which will display a tree view of Aruba software. Select the AirWave directory, and then the VisualRF Plan sub directory. The figure below shows the page that displays.

**Figure 235** VisualRF Plan Download Location Page Illustration



The latest version of the VisualRF Plan client will display in this folder – earlier versions are located under the VisualRF Plan Archives subdirectory. Select the.exe file you want to download.

After VisualRF Plan has finished downloading, launch the installer.

### Minimum requirements

Must be installed on a Windows machine with the following minimum specifications:

- 250MB Hard drive storage space
- 2GB RAM
- 2.0 GHz dual-core CPU



If installing VisualRF Plan on a VMWare virtual machine hosted by a Mac computer, you must disable **Folder Sharing**.



## Installation

To install VisualRF Plan after you have downloaded it from the Aruba support site:

1. The installer will prompt you for the location of the data directory. You must have access to the directory you choose for the installation.
2. Choose a directory for auto-backup. The default is user directory.
3. Follow the rest of the instructions on your installation screen.

## Differences between VisualRF Plan and VisualRF online

**Table 150** *VisualRF Plan vs. VisualRF Online*

Feature	VisualRF	VisualRF Plan
Hardware sizing		<b>X</b>
Installation required		<b>X</b>
How to plan a site	X	<b>X</b>
Navigation	X	<b>X</b>
Track users	X	
Track interferers	X	
VisualRF APIs	X	
Location accuracy	X	
QuickView preferences	X	
Resource utilization	X	
Add external walls	X	<b>X</b>
Client surveys	X	
IDF	X	<b>X</b>
View deployed switches	X	
View signal strength	X	
Planning and provisioning	X	<b>X</b>
Import and Export	X	<b>X</b>

This appendix describes the Aruba Instant access point and Virtual Controller system introduced by Aruba Networks in March 2011, and how to integrate this system with AMP 7.2.2 and later. The appendix contains the following topics:

- “Overview of Aruba Instant” on page 297
- “Using Aruba Instant with AMP” on page 297
- “Workflow of the Aruba Instant and AMP Integration Process” on page 298
- “AMP Pages with Instant-Specific Features” on page 301
- “Other Available Features” on page 302
- “Known Issues of the Aruba Instant integration with AirWave” on page 302

### Overview of Aruba Instant

Aruba Instant is a system of up to 16 access points (IAP-92, IAP-93, or IAP-105) per Layer 2 subnet. Aruba Instant IAPs are controlled by a single IAP that serves a dual role as a primary Virtual Controller, eliminating the need for dedicated controller hardware. This system can be deployed through a simplified setup process appropriate for smaller organizations, or for multiple geographically-dispersed locations without an on-site administrator.

Only the first IAP/Virtual Controller you add to the network must be configured; the subsequent IAPs will all inherit the necessary configuration information from the Virtual Controller. Aruba Instant continually monitors the network to determine which IAP should function as the Virtual Controller at any time, and the Virtual Controller will move from IAP to IAP as necessary without impacting network performance.

The Virtual Controller technology in Aruba Instant is capable of IAP auto discovery, 802.1X authentication, role- and device-based policy enforcement, rogue detection, and Adaptive Radio Management (ARM).

### Using Aruba Instant with AMP

AMP has added centralized network management support for Aruba Instant in version 7.2.2.

With a distributed deployment where multiple locations each have an Aruba Instant Virtual Controller and IAPs, AMP serves as a centralized management console. AMP provides all functionality for normal WLAN deployments including long-term trend reporting, PCI compliance, configuration auditing, role-based administration, location services, RF visualization, and many other features.

Integrating Aruba Instant systems into AMP is unique from the setup of any other device class due to the following considerations:

- **Discovery:** AMP does not discover Aruba Instant devices via scanning (SNMP or HTTP) the network. Each Aruba Instant deployment will automatically check-in to the AMP configured within the IAP's user interface. The first Virtual Controller for an organization will automatically appear as a new device in AMP. Subsequent IAPs are discovered via the Virtual Controller, just like standard controller/thin AP deployments.
- **Auto-provisioning:** The first authorized Virtual Controller requires manual authorization into AMP via shared secret to ensure security. Along with the shared secret, the Virtual Controller sends an Organization String which automatically initializes and organizes the IAPs in AMP. Unlike the

traditional infrastructure of a physical controller and thin APs, Aruba Instant automates many tedious steps of developing a complex hierarchical structure of folders, config groups, templates, admin users, and admin roles for Aruba Instant.

- **Communication via HTTPS:** Because Aruba Instant devices may be deployed behind NAT-enabled firewalls, Virtual Controllers "push" data to AMP via HTTPS. AMP initiates no connections to Aruba Instant devices via SNMP, TFTP, SSH, and the like. This enables quick remote setup without having to modify firewall rules.
- **Virtual controller listed as separate device:** The Virtual Controller is listed as an additional device, even though it is part of the existing set of IAPs. If you have 10 physical IAPs, AMP will list 10 Aruba Instant IAPs and one Aruba Instant Virtual Controller. You can identify the IAP acting as the Virtual Controller by their identical LAN MAC addresses in **APs/Devices > List** pages, Device Inventory reports, and any other AMP pages that list your network devices.

Refer to the *Aruba Instant Data Sheet* for full operational and regulatory specifications, hardware capabilities, antenna plots, and radio details.

## Workflow of the Aruba Instant and AMP Integration Process

The following is a sample setup workflow around a common Aruba Instant use case.

### Setting up Aruba Instant Hardware

See the *Aruba Instant Quick Start Guide*, the *Aruba Instant Professional Installation Guide*, the *IAP-105 Wireless Access Point Installation Guide*, and the *IAP-92 and IAP-93 Wireless Access Point Installation Guide* for information on setting up the hardware and configuring the network.

### Required Personnel

For each remote location, an on-site installer is required to physically mount the IAPs, connect to the Aruba Instant SSID, configure the WLAN, configure the names of the IAPs, and enter the information in the first IAP's user interface that will enable communication with the AMP.

An AMP administrator sends an Organization String and Shared Secret key along with AMP's IP address to the on-site installer. The AMP admin later validates the first Virtual Controller's Organization String and its Shared Secret when it appears in the **APs/Devices > New** list. The administrator also enables user roles to administer the Aruba Instant systems, makes any other changes in AMP as necessary.

### Creating your Organization String

The Organization String is a set of colon-separated strings created by the AMP administrator to accurately represent the deployment of each Aruba Instant system. This string is entered into the Aruba Instant UI by the on-site installer.

The format of the Organization String is "Org:subfolder1:subfolder2..." and so on, up to 31 characters long. "Org," the top-level string, is generally the name of your organization and is used to automatically generate the following (if not already present) in AMP:

- AMP Role: "Org Admin" (initially disabled)
- AMP User: "Org Admin" (assigned to the role "Org Admin")
- Folder: "Org" (under the Top folder in AMP)
- Configuration Group: "Org"

Additional strings in the Organization String are used to create a hierarchy of subfolders under the folder named "Org":

- subfolder1 would be a folder under the "Org" folder

- subfolder2 would be a folder under subfolder1

To create your Organization String, consider the plan of how your Aruba Instant IAPs are to be physically distributed. As a best practice, the Organization String should mirror your company's geographical or internal reporting structure. For example, if you plan to deploy Aruba Instant in four stores in two different cities for Acme Corporation, your Organization Strings might look like these:

- Acme:New York:Times Square Store
- Acme:New York:Queens Store
- Acme:San Francisco:Sunset Store
- Acme:San Francisco:SOMA Store

## The Shared Secret Key

The Shared Secret key is used by the administrator to manually authorize the first Virtual Controller for an organization that appears in the **APs/Devices > New** page in AMP. Any string is acceptable.



**NOTE:** Always ensure the protection of your organization's shared secret. Knowledge of this shared secret, the organization string, and communication protocol could allow a rogue device to masquerade as an Aruba Instant device.

At this point, the admin in our example should send the Organization String, Shared Secret key, and AMP IP address to the on-site installers setting up Aruba Instant hardware inside the storefronts.

## Entering the Organization String and AirWave Information into the IAP

For the initial IAP/Virtual Controller set up in each location, the on-site installer logs in to the first IAP's web interface via the Aruba Instant configuration SSID, and navigates to **Settings > AirWave**. The installer then enters the correct Organization String, the AMP IP address, and the Shared Secret key, as shown in [Figure 236](#).

**Figure 236** Aruba Instant UI: Settings > AirWave

## Receiving the Aruba Instant Virtual Controller as a New Device in AMP

After the installer enters this information in the Aruba Instant user interface, the device will immediately attempt to contact your AirWave server. Within a few minutes, the **New Devices** link at the top of the AMP UI will increase by one - that first IAP is added as an Aruba Instant Virtual Controller in the **APs/Devices > New** page, as shown in Figure 237.

**Figure 237** New Instant Virtual Controller on **APs/Devices > New** Page Illustration

ARUBA networks

New Devices: 1 Up: 84 Down: 18 Mismatched: 69 Rogue: 1294 Users: 3 Alerts: 0

Home Helpdesk Groups **APs/Devices** Users Reports System Device Setup AMP Setup

List New Up Down Mismatched Ignored

To discover more devices, visit the [Discover](#) page.

1-1 of 1 APs/Devices Page 1 of 1 Choose Columns CSV Export

Device	Type	IP Address	LAN MAC Address	Discovered
Instant Karma	Aruba Instant Virtual Controller	-	-	3/7/2011 8:55 PM

1-1 of 1 APs/Devices Page 1 of 1

Select All - Unselect All

## Verifying the Shared Secret and Adding the Device

When an Aruba Instant device appears in the **APs/Devices > New** page, the admin user should mouse over the value under the **Type** column to verify the device's Shared Secret with AMP, as shown in Figure 238.

**Figure 238** Mouseover the Aruba Instant Type to Indicate Shared Secret

1-1 of 1 APs/Devices Page 1 of 1 Choose Columns CSV Export

Device	Type	IP Address	LAN MAC Address	Discovered
Instant Karma	Aruba Instant Virtual Controller	-	-	3/7/2011 8:55 PM

1-1 of 1 APs/Devices Page 1 of 1

Shared Secret: airwave

If the incoming Shared Secret matches the one you created, select **Add**, then **Save and Apply** in the confirmation page.



NOTE

**NOTE:** With an Organization specified, you do not have to select any Group or Folder from the drop-down menus on the **APs/Devices > New** page. In fact, if you do change the Group/Folder drop-down menus, all Organization-specified Virtual Controllers will ignore these values and will use the folder/group values from the Organization String instead. If you select **Add** for some non-Aruba-Instant devices as well as some Organization-specified Virtual Controllers, the drop-down menus will apply to the non-IAPs but not the Virtual Controllers. If you have any Virtual Controllers with no Organization specified the first time they communicate with AMP, then they will be placed in the Folder/Group drop-box values you have selected.

AMP parses the information from the Organization String and auto-creates the following in its own interface:

- a new User Role (disabled by default for security reasons) named "Acme Admin"
- a new User named "Acme Admin" with a password equal to the Virtual Controller's Shared Secret
- a new configuration group called "Acme"
- a new folder just under the Top folder called "Acme"
- two subfolders: "New York" and "San Francisco" from subfolder2
- two subfolders under New York: "Times Square Store" and "Queens Store" from subfolder3
- two subfolders under San Francisco: "Sunset Store" and "SOMA Store" from subfolder3

## Remaining Manual Admin Tasks in AMP

The Admin will then complete the following tasks in AMP:

1. Enable the newly created Admin User Role in **AMP Setup > Roles**, as shown in [Figure 239](#).

**Figure 239** Enable Admin User Role in **AMP Setup > Roles**

The screenshot shows the 'AMP Setup' tab selected in the top navigation bar. Below it, the 'Roles' sub-tab is active. The 'Role' configuration form is displayed with the following fields and values:

Role	
Name:	Acme Admin
Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Type:	AP/Device Manager
AP/Device Access Level:	Manage (Read/Write)
Top Folder:	Acme
RAPIDS:	Read Only
VisualRF:	Read/Write
Helpdesk:	<input type="radio"/> Yes <input checked="" type="radio"/> No

2. In **Groups > Template** for the newly created Acme group, verify the first Virtual Controller's auto-created template.



**NOTE:** The auto-created template is most useful if the first Virtual Controller for the top-level Organization String is fully configured on-site *before* it is pointed at AMP in the Virtual Controller's UI.

3. Evaluate, approve, or ignore incoming Virtual Controllers with a different top level Organization String and/or Shared Secret in the **APs/Devices > New** list. Subsequent IAPs are auto-authorized if they have an Organization/Shared Secret key that matches the Shared Secret key of any existing authorized Virtual Controller in the top-level Organization String.
4. Set the initial Virtual Controller to **Manage Read/Write** mode and push the good configuration to the subsequent IAPs.
5. Set up AMP users to have access to specific folders, if desired.

## AMP Pages with Instant-Specific Features

The following is a summary of AMP pages affected by Aruba Instant support:

### APs/Devices > New

When an Aruba Instant device appears in the **APs/Devices > New** page, an admin user can mouse over the value on the **Type** column to display the device's Shared Secret with AMP.

### APs/Devices > List

The Virtual Controller is listed as an additional device, even though it is part of the existing set of IAPs. You can identify the IAP acting as the Virtual Controller by their identical LAN MAC addresses.

### Clients > Client Detail

Once IAPs are serving clients, the IAPs can use user-agent strings to extract operating systems and device descriptions of its clients, and then populate the Device Description and Device OS fields in **Clients > Client Detail**.

### APs/Devices > Audit

Aruba Instant configuration fetching can be performed in **APs/Devices > Audit**. The running configuration is stored on the IAP and verified by the template.

## APs/Devices > Monitor > Radio Statistics

The Radio Statistics page for Aruba Instant devices displays CPU Utilization, Channel Utilization, Bandwidth, Power, and MAC/Phy Error statistics.

### RAPIDS

Since Aruba Instant does not support mitigation or high-level rogue reporting, it does not synchronize classification. All rogue devices are reported and stored in the AMP for evaluation based on high-level rule sets.

Aruba Instant currently does not match wireless BSSIDs to local MAC addresses within an IAP's ARP table.

Aruba Instant does not currently support IDS event notification.

### Reports

Aruba Instant Virtual Controllers appear as a separate device in the Device Inventory Report and most other reports that list devices.



---

**NOTE:** AMP does not provide a Device Uptime report for Aruba Instant devices.

---

## Other Available Features

### Firmware Image Management

AMP pushes firmware to the Aruba Instant Virtual Controller, and the Virtual Controller pushes the firmware to the rest of its IAPs. When using AMP to manage IAPs, you can upgrade the firmware by loading the firmware onto AMP and then scheduling an upgrade from AMP.

### Intrusion Detection System

AMP automatically detects rogue IAPs irrespective of their location in the network. It prevents authorized IAPs from being detected as rogue IAPs, and tracks and correlates the IDS events to provide a comprehensive picture of your network's security.

## Known Issues of the Aruba Instant integration with AirWave

If the Organization String configured on the Aruba Instant device is different than what is statically written in the template, AMP will overwrite the configured Organization String to match the template.



## Numerics

802.11 counters ..... 76, 125, 126, 196

## A

AAA servers ..... 71, 81

access points  
    adding with CSV file ..... 114

ACLs, see groups

ACS  
    integrating ..... 64  
    servers ..... 64

Active BSSIDs ..... 128

Adaptive Radio Management ..... 124

admin role ..... 46

Air Monitor ..... 69

Alert Summary table ..... 118, 194

alerts  
    viewing ..... 194  
    warning behavior, setting ..... 34

AMON data collection ..... 42

AMP Alerts ..... 195

Antenna Diversity ..... 139

AP Interface Polling Period ..... 125

AP/Device Manager role ..... 46

APs  
    enabling automatic discovery ..... 111

ARM ..... 124, 126, 127, 147

ARM Events table ..... 127

Aruba GUI Config ..... 140

Aruba Instant ..... 297–302

Aruba Overrides ..... 150

Association History table ..... 206

audit  
    configuring intervals ..... 36  
    device configuration ..... 133  
    PCI Compliance ..... 66

Audit (Read Only) ..... 48

Auto Detect Upstream Device setting ..... 138

Automatic Authorization ..... 36, 81, 109

Automatically monitor/manage new devices ..... 36

## B

backups ..... 223  
    restoring from a backup ..... 223  
    running on demand ..... 223  
    using Failover ..... 224

browsers, supported ..... 17

## C

CDP, enabling for device discovery ..... 111

Channel Busy Threshold ..... 37

Choose Columns link ..... 30

Cipher ..... 123

Cisco  
    ACS ..... 50  
    Catalyst ..... 71, 151, 162  
    configuring IOS templates ..... 157, 160  
    Dynamic AP Management in AMP ..... 141  
    IOS ..... 51, 62, 71, 78, 137, 151, 160  
    safe flag in firmware upgrade ..... 145  
    Wireless Domain Services ..... 60  
    WLC ..... 59, 71, 78  
    WLSE ..... 59, 269

Cisco Discovery Protocol  
    see CDP ..... 111

Client Transmit Power, see VisualRF ..... 260

comparing device groups ..... 100

configuration change jobs, viewing ..... 215

configuration change jobs, viewing ..... 136

Configuration Compliance chart ..... 210

Connected Users table ..... 132

Containment, managing rogue AP ..... 171

CSV File, adding multiple devices with ..... 114

Current Association ..... 206

## D

dashboard  
    customizing display ..... 32

date and time

configuring .....	18
Deauthenticate Client .....	206
Detected Interfering Devices .....	128
Device Events .....	40
Device OUI score .....	173
Device Troubleshooting Hint .....	38
Device Type Setup .....	59
devices .....	107
adding manually .....	112
communication settings .....	54
discovering, managing, and troubleshooting ...	107
folders .....	134
importing via CSV .....	115
individual support and firmware upgrades .....	144
modifying .....	103
status .....	137
troubleshooting a newly discovered device .....	146
verifying .....	117, 133
DHCP, using .....	140
discovery	
automatic AP .....	111
Discovery Events table .....	180
Disk Space charts .....	219
DNS Hostname Lifetime .....	38

## E

editing interfaces .....	131
Error fetching existing configuration .....	146
Expand folders to show all APs .....	117
external logging .....	39

## F

Failover .....	14, 220, 224
Firefox .....	17
firewall, configuring .....	21
firmware	
MD5 Checksum .....	56
specifying minimum versions for APs .....	99
uploading .....	56, 58
firmware upgrade jobs, viewing .....	215
firmware upgrades in monitor-only mode .....	41
Folders .....	134
FTP Server, enabling .....	41
fully qualified domain names .....	38

## G

getting started with AirWave .....	28
Global Aruba Configuration .....	148
Global Groups	
with Master Console .....	222
global templates .....	165
Google Chrome .....	17
Google Earth .....	27, 120, 138, 282
Groups .....	71–106
groups	
changing multiple group configurations .....	102
comparing .....	100
configuring and using .....	71
configuring basic group settings .....	74
configuring group AAA servers .....	81
configuring group SSIDs and VLANs .....	84
configuring group templates .....	151
configuring radio settings .....	88
configuring security settings .....	82
deleting .....	101
deleting a group .....	101
global groups .....	72, 105
MAC ACLs .....	99
overview .....	72
radio settings .....	88
security .....	82
viewing .....	72
Guest Access Sponsor role .....	47
Guest User Configuration .....	38
Guest Users .....	40

## H

hardware requirements .....	17
Heatmap, see VisualRF	
Historical Data Retention .....	40
host name	
assigning host name .....	20
HP ProCurve .....	79, 81, 151
HTTP Timeout .....	55

## I

IAP, see Aruba Instant	
ICMP settings .....	55
IDS Events .....	195
Incidents .....	195
Interface Monitoring page .....	132
Interfering Devices .....	40

Internet Explorer .....	17
IP address	
adding and assigning .....	19
iPhone .....	221

## L

Licenses .....	120
Linux CentOS 5	
installing .....	18
localization .....	28
Logging out of AirWave .....	225
Login message, configuring .....	49
logs	
ARM Events .....	127
async_logger .....	185
audit .....	39
config_pusher .....	185
error_log .....	185
syslog .....	39

## M

MAC/Phy errors .....	126
Maintenance windows .....	81, 104, 141
Manage (Read/Write) .....	48
Managed AMPs	
adding .....	221
Master Console .....	14, 220
Public Portal .....	220
Master Console and Failover .....	14
Mesh	
Aruba AirMesh .....	122, 123, 264
device-to-device link polling .....	76
gateway .....	120
in VisualRF .....	263
mode .....	120
monitoring .....	128
Proxim .....	98
Mesh Links table .....	123
message-of-the-day .....	49
Modify Devices link .....	133
Monitor (Read Only) .....	48
monitoring	
mesh devices .....	128
wired devices .....	130
wireless devices .....	118

## N

navigation .....	22
------------------	----

understanding the UI .....	29
Network integration with AMP .....	15
network settings	
defining .....	43
Nightly Maintenance Time setting .....	36
NMS .....	65, 66
non-UTF8 characters .....	38
NTP .....	78

## O

Open controller web UI link .....	206
Organization String, see Aruba Instant	
OUI .....	173

## P

pagination records	
setting, resetting .....	31
pagination widget, using .....	31
password	
changing default root .....	20
PCI Compliance	
Default Credential Compliance .....	69
PCI Requirements .....	67
Physical Interfaces table .....	131
planned maintenance mode .....	135, 137
Poll Now button .....	119
product overview	
configuring date and time .....	18
defining a scan .....	109
executing a scan .....	110
navigating .....	22
protocols and ports .....	21
Proxim 4900M .....	91
Proxim/Avaya .....	79

## Q

Quick Links .....	206, 210
-------------------	----------

## R

Radio Enabled option .....	140
Radio Role field .....	149
radio settings	
configuring for groups .....	88
radio statistics .....	124–128
Radio table .....	121

RADIUS .....	81
authentication .....	49
configuring authentication and authorization .....	51
integrating .....	52
RADIUS Authentication Issues .....	195
Radius/ARM/IDS Events retention .....	40
RAPIDS .....	25, 167
audit log .....	181
enabling .....	39
overview .....	14
score override .....	180
setup .....	169
viewing ignored rogues .....	180
Recent Events table .....	124
Replace Hardware button .....	146
reports .....	227
Aruba License .....	232
Capacity Planning .....	232
Client Session .....	250
Configuration Audit .....	234
creating, running, and emailing .....	227
custom .....	230
defining custom reports .....	252
Device Summary .....	235
Device Uptime .....	237, 302
emailing and exporting .....	255
IDS Events .....	239
Inventory .....	239
Memory and CPU Utilization .....	241
Network Usage .....	241
New Clients .....	245
New Rogue Devices .....	242
RADIUS Authentication Issues .....	246
RF Health Report .....	247
Rogue Clients .....	249
Rogue Containment Audit .....	250
transferring with FTP .....	256
restoring from backup .....	223
RF Health Report .....	247
RFprotect license .....	147
Rogue AP Discovery Events .....	40
Rogue Association History table .....	206
rogue classification .....	167
Rogue Client Associations table .....	179
rogue clients .....	179, 193, 249
rogue scanning	
enabling in Groups > Radio .....	91, 275
root password, changing .....	20
routers and switches .....	130
adding with a CSV file .....	114
RTLS Collector .....	41

Run a command menu .....	206
--------------------------	-----

## S

scan credentials .....	109
scan sets .....	109
scanning	
defining credentials .....	108
security	
auditing PCI compliance .....	66
configuring ACS servers .....	64
configuring group security settings .....	82
configuring group SSIDs and VLANs .....	84
configuring RADIUS .....	49
configuring TACACS+ .....	49
integrating NMS .....	65
RAPIDS and rogue classification .....	167
using triggers and alerts .....	183
servers	
specifying general settings .....	35
Severe Alert .....	34
Shared Secret key .....	299
Signal Cutoff .....	260, 278
Signal Quality .....	123
single sign-on .....	48, 49, 120
Smarthost .....	255
SNMP	
Fetcher .....	218
polling period .....	76
Port .....	113
Rate Limiting for Monitored Devices .....	42
read-write .....	55
timeout setting .....	54
Trap .....	146
v3 Informs .....	55
Software updates .....	36
SOTI MobiControl .....	207
spectrum analysis .....	147
SSIDs .....	84
inactive .....	40
SSL Certificates .....	140
static IPs, assigning .....	77
Static Routes .....	44
switches	
virtual interfaces .....	142
Symbol .....	79, 91, 151
Syslog .....	39, 185
system status, viewing .....	184

## T

TACACS+ .....	50, 81
configuring authentication .....	49
integrating .....	49
Telnet/SSH Timeout .....	55
templates.....	152
adding .....	154, 165
configuring a global template .....	165
configuring Cisco IOS templates .....	160
configuring for groups .....	151
global template variables .....	165
variables.....	165
Top Header Stats .....	29
Transmit Power Level.....	139
trap types .....	127
Trapeze.....	151
triggers .....	186–194

## U

UI	
understanding the navigation bar .....	29
Unexpected LAN MAC Address.....	146
Universal devices,adding .....	115
user account, configuring.....	214
User Data Polling Period .....	125
User Idle Timeout .....	49
user interface	
AMP Setup > Device Type Setup .....	59
AMP Setup > General .....	35
AMP Setup > MDM Server .....	208
AMP Setup > Network .....	43
AMP Setup > NMS.....	65, 66
AMP Setup > Roles.....	44, 46
AMP Setup > Users .....	44, 45
APs/Devices > Audit36, 112, 120, 133, 134, 135, 157	
APs/Devices > Ignored .....	116
APs/Devices > Interfaces.....	131, 132, 142
APs/Devices > List.....	117
APs/Devices > New .....	112, 116, 299
buttons and icons .....	26
Clients > Clients Detail.....	208
Clients > Connected .....	196, 197
Clients > Diagnostics .....	207
Clients > Guest Users .....	200
Clients > Tags .....	202
Clients > User Detail .....	206
Configuration Change Confirmation .....	102
Device Setup > Add.....	112, 115
Device Setup > Communication .....	54, 55, 56
Device Setup > Discover .....	108, 109, 110
Device Setup > Firmware Files .....	56

flash graphs .....	32, 33, 34
Group SNMP Polling Period .....	76
Groups > Aruba Config .....	71
Groups > Basic.....	75, 76, 77, 78, 79, 81, 106
Groups > Cisco WLC Config .....	92
Groups > Firmware.....	100
Groups > List .....	73
Groups > MAC ACL.....	99
Groups > Proxim Mesh .....	98
Groups > PTMP .....	97
Groups > Radio .....	89
Groups > Security .....	82
Groups > SSIDs.....	84
Groups > Templates.....	152, 154, 165, 166
Help .....	26
Home .....	209
Home > License .....	211
Home > Managed AMPs .....	221
Home > Overview .....	209
Home > Search.....	211, 212
Home > User Info .....	34, 213
Home Overview .....	32, 33, 34
Master Console .....	220
Master Console > Groups > Basic .....	222
Master Console > Groups > Basic, Managed ..	222
Master Console > Manage AMPs, IP/Hostname	221
page sections	
Activity section.....	25
Navigation section .....	24
Status section .....	22
Radio Statistics .....	124
RAPIDS > Audit Log .....	181
RAPIDS > List.....	176
RAPIDS > Rogue APs (Detail), Score Override	181
RAPIDS > Score Override .....	180
RAPIDS > Setup .....	169
Reports > Definitions .....	229, 252
Reports > Generated > Port Usage.....	246
System.....	183
System > Alerts .....	40, 195
System > Backups .....	223
System > Configuration Change Jobs .....	136, 215
System > Event Logs .....	186
System > Events Log .....	124
System > Firmware Upgrade Jobs.....	215
System > Performance.....	216
System > Status .....	184
System > Syslog and Traps .....	185
System > Trigger Detail .....	188
System > Triggers .....	187
View AP Credentials .....	147

user roles	
creating.....	46
users	
creating.....	44

## V

vendor-specific device settings .....	38
View Device Credentials link .....	146
Virtual controller, see Aruba Instant	
VisualRF .....	14, 25
adding exterior walls.....	270
APIs.....	294
Auto-Arrange feature .....	281
Auto-Match Planned Devices .....	290
autoprovisioning .....	288
checking signal strength .....	278
client surveys .....	271
Client Transmit Power.....	260
Data Set menu .....	260
Device Types .....	261
Display Menu .....	261
Edit Menu.....	262
editing a floor plan image .....	284
Enabling .....	39, 259
Floors .....	260
Frequencies .....	261
icons .....	259
IDF.....	273
importing a floor plan .....	284
Importing and Exporting .....	291
Interferers.....	261
location history.....	277
location probability regions.....	272
Location Service .....	269
location training .....	270
Mesh .....	261
Mesh View.....	259, 263
Navigation .....	259
Network View .....	260
New building .....	282
New Campus .....	281
Overlays .....	260
Overview .....	257
Planning and Provisioning .....	281
Preferences.....	268
printing a BOM.....	290
provisioning existing APs.....	287
QuickView .....	123, 259
Removing color .....	285
Sensors .....	261
Setup page .....	264
Terminology .....	258
Tree view.....	280
View a floor plan RF environment .....	279
Viewing a wireless user.....	276
VisualRF Plan .....	295
Wired Range .....	260
VLANs.....	84
Voice overlay .....	260

## W

Watched AMPs .....	224
WDS Role.....	140
Web Auth bundles .....	53, 58
wired devices	
monitoring .....	130
Wired Interfaces table .....	121