

Dell PowerConnect W AirWave

Version 7.1

User Guide



Copyright

© 2010 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, and other registered marks are trademarks of Aruba Networks, Inc. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. Any other trademarks appearing in this manual are the property of their respective companies.

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

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.

Preface	11
Document Organization.....	11
Notice Icons.....	12
Contacting Support	12
Chapter 1 Introduction	13
AWMS—A Unified Wireless Network Command Center.....	13
AirWave Management Platform™.....	13
Dell PowerConnect W Configuration	14
VisualRF™.....	14
RAPIDS™.....	14
Master Console and Failover.....	15
Integrating AWMS into the Network and Organizational Hierarchy.....	15
Chapter 2 Installing AWMS	17
AWMS Hardware Requirements and Installation Media.....	17
Installing Linux CentOS 5 (Phase 1).....	17
Installing AWMS Software (Phase 2)	18
Getting Started.....	18
Step 1: Configuring Date and Time, Checking for Prior Installations	18
Date and Time.....	18
Previous AWMS Installations	19
Step 2: Installing AWMS Software, Including AWMS	19
Step 3: Checking the AWMS Installation	19
Step 4: Assigning an IP Address to the AWMS System	19
Step 5: Naming the AWMS Network Administration System	20
Step 6: Assigning a Host Name to the AWMS	20
Step 7: Changing the Default Root Password.....	21
Completing the Installation	21
Configuring and Mapping Port Usage for AWMS.....	21
AWMS Navigation Basics	22
Status Section.....	23
Navigation Section.....	23
Activity Section.....	25
Help Links in the GUI.....	26
Common List Settings	26
Buttons and Icons	27
Getting Started with AWMS	29
Completing Initial Login.....	29
Chapter 3 Configuring AWMS	31
Before You Begin.....	31
Formatting the Top Header	31
Customizing Columns in Lists	33
Resetting Pagination Records.....	34
Using the Pagination Widget.....	34

Using CSV Export for Lists and Reports.....	35
Defining Graph Display Preferences.....	35
Customizing the Overview Subtab Display.....	36
Customized Search	38
Setting Severe Alert Warning Behavior	38
Defining General AWMS Server Settings	39
What Next?.....	46
Defining AWMS Network Settings.....	47
What Next?.....	48
Creating AWMS Users	48
What Next?.....	50
Creating AWMS User Roles	50
What Next?.....	52
Enabling AWMS to Manage Your Devices	52
Configuring Communication Settings for Discovered Devices	53
Loading Device Firmware onto AWMS (Optional).....	58
Overview of the Device Setup > Upload Files Page	58
Loading Firmware Files to AWMS.....	59
Using Web Auth Bundles in AWMS.....	60
Configuring TACACS+ and RADIUS Authentication	62
Configuring TACACS+ Authentication	62
What Next?.....	63
Configuring RADIUS Authentication and Authorization	64
Integrating a RADIUS Accounting Server.....	65
What Next?.....	65
Configuring Cisco WLSE and WLSE Rogue Scanning.....	66
Introduction to Cisco WLSE.....	66
Configuring WLSE Initially in AWMS	66
Adding an ACS Server for WLSE	67
Enabling Rogue Alerts for Cisco WLSE	67
Configuring WLSE to Communicate with APs.....	67
Discovering Devices.....	67
Managing Devices	67
Inventory Reporting	68
Defining Access	68
Grouping	68
Configuring IOS APs for WDS Participation	68
WDS Participation.....	68
Primary or Secondary WDS	68
Configuring ACS for WDS Authentication.....	69
Configuring Cisco WLSE Rogue Scanning.....	69
What Next?.....	70
Configuring ACS Servers.....	71
What Next?.....	72
Integrating AWMS with an Existing Network Management Solution (NMS)	73
What Next?.....	74
Auditing PCI Compliance on the Network.....	74
Introduction to PCI Requirements	74
PCI Auditing in the AWMS Interface	75
Enabling or Disabling PCI Auditing.....	76
What Next?.....	77
Deploying WMS Offload.....	77
Overview of WMS Offload in AWMS	77
General Configuration Tasks Supporting WMS Offload in AWMS.....	78

	Additional Information Supporting WMS Offload	78
Chapter 4	Configuring and Using Device Groups in AWMS	79
	AWMS Group Overview	80
	Viewing All Defined Device Groups	81
	Editing Columns on the Groups > List Page and Additional Pages	82
	Configuring Basic Group Settings	83
	What Next?	90
	Configuring Group Security Settings	91
	Configuring Group SSIDs and VLANs	94
	Adding and Configuring Group AAA Servers	98
	Configuring Radio Settings for Device Groups	100
	An Overview of Cisco WLC Configuration	106
	Accessing Cisco WLC Configuration	106
	Navigating Cisco WLC Configuration	106
	Configuring WLANs for Cisco WLC Devices	107
	Defining and Configuring LWAPP AP Groups for Cisco Devices	109
	Viewing and Creating AP Groups	109
	Configuring Cisco Controller Settings	110
	Configuring Wireless Parameters for Cisco Controllers	110
	Configuring Security Parameters and Functions	110
	Configuring Management Settings for Cisco	111
	Configuring Group PTMP/WiMAX Settings	112
	Configuring Proxim Mesh Radio Settings	116
	Configuring Group MAC Access Control Lists	118
	Specifying Minimum Firmware Versions for APs in a Group	119
	Comparing Device Groups	120
	Deleting a Group	121
	Changing Multiple Group Configurations	121
	Modifying Multiple Devices	122
	Using Global Groups for Group Configuration	125
Chapter 5	Discovering, Adding, and Managing Devices	127
	Device Discovery Overview	127
	Discovering and Adding Devices	127
	SNMP/HTTP Scanning	128
	Adding Networks for SNMP/HTTP Scanning	128
	Adding Credentials for SNMP/HTTP Scanning	129
	Defining a SNMP/HTTP Scan Set	130
	Running a Scan Set	131
	What Next?	133
	Enabling Cisco Discovery Protocol (CDP)	134
	Assigning Devices to AWMS from APs/Devices > New Page	134
	Manually Adding Individual Devices	136
	Adding Devices with the Device Setup > Add Page	136
	Adding Multiple Devices from a CSV File	139
	Adding Universal Devices	140
	Assigning Devices to the Ignored Page	141
	Monitoring Devices	142
	Viewing Device Monitoring Statistics	142
	Understanding the APs/Devices > Monitor Pages for All Device Types	146
	Monitoring Data Specific to Wireless Devices	148

Monitoring Data Specific to Wired Devices (Routers and Switches).....	153
Understanding the APs/Devices > Interfaces Page.....	154
What Next?.....	155
Auditing Device Configuration	156
Using Device Folders (Optional)	157
Configuring and Managing Devices.....	158
Moving a Device from Monitor Only to Manage Read/Write Mode.....	158
Configuring AP Settings	159
Configuring Device Interfaces for Cisco Catalyst Switches.....	165
Configuring Cisco Router and Switch Interface Settings.....	169
Individual Device Support and Firmware Upgrades	169
Troubleshooting a Newly Discovered Device with Down Status	172

Chapter 6

Creating and Using Templates	175
Group Templates	175
Supported Device Templates	175
Template Variables	176
Viewing and Adding Templates	177
Configuring General Template Files and Variables	181
Configuring General Templates	181
IOS Configuration File Template:	182
Device Configuration File on APs/Devices > Audit Configuration Page	182
Using Template Syntax.....	183
Using Directives to Eliminate Reporting of Configuration Mismatches.....	183
Ignore_and_do_not_push Command	183
Push_and_exclude Command	183
Using Conditional Variables in Templates	184
Using Substitution Variables in Templates	184
Using AP-Specific Variables	185
Configuring Cisco IOS Templates.....	186
Applying Startup-config Files	186
WDS Settings in Templates	186
SCP Required Settings in Templates	187
Supporting Multiple Radio Types via a Single IOS Template	187
Configuring Single and Dual-Radio APs via a Single IOS Template	188
Configuring Cisco Catalyst Switch Templates.....	188
Configuring Symbol Controller / HP WESM Templates.....	188
Configuring a Global Template.....	191

Chapter 7

Using RAPIDS and Rogue Classification	195
Overview Tab	195
List.....	197
Viewing Ignored Rogue Devices	201
Using RAPIDS Workflow to Process Rogue Devices.....	201
RAPIDS Setup	202
Basic Configuration.....	202
Containment Options.....	203
Additional Settings	204
RAPIDS Rules.....	204
Controller Classification with WMS Offload	205
Device OUI Score	205
Rogue Device Threat Level.....	206
Viewing and Configuring RAPIDS Rules.....	206
Deleting or Editing a Rules.....	210
Recommended RAPIDS Rules.....	210

	Using RAPIDS Rules with Additional AWMS Functions	210
	Score Override	210
	Audit Log	212
	Additional Rogue Device Resources	212
	Additional Security-Related Topics	212
Chapter 8	Performing Daily Administration in AWMS	213
	Overview of Triggers and Alerts	213
	Viewing Triggers.....	213
	Creating New Triggers	214
	Setting Triggers for Devices.....	216
	Setting Triggers for Radios.....	218
	Setting Triggers for Discovery	220
	Setting Triggers for Users.....	221
	Setting Triggers for RADIUS Authentication Issues	222
	Setting Triggers for IDS Events.....	223
	Setting Triggers for AWMS Health	225
	Delivering Triggered Alerts.....	225
	Viewing Alerts.....	226
	Responding to Alerts.....	227
	Monitoring and Supporting WLAN Users.....	228
	Overview of the Users Pages	228
	Monitoring WLAN Users With the Users > Connected and Users > All Pages	229
	Supporting Guest WLAN Users With the Users > Guest Users Page	231
	Supporting Users on Thin AP Networks With the Users > Tags Page.....	233
	Evaluating and Diagnosing User Status and Issues.....	234
	Evaluating User Status with the Users > User Detail Page.....	234
	Using the Deauthenticate User Feature	235
	Evaluating User Status with the Users > Diagnostics Page	235
	Introduction and Overview of the Diagnostics Page	235
	Supporting AWMS Stations with the Master Console.....	239
	Adding a Managed AMP with the Master Console.....	239
	Monitoring and Supporting AWMS with the Home Pages.....	241
	Monitoring AWMS with the Home > Overview Page.....	241
	Viewing and Updating License Information with the Home > License Page	245
	Searching AWMS with the Home > Search Page	246
	Accessing AWMS Documentation with the Home > Documentation Page	247
	Configuring Your Own User Information with the Home > User Info Page	248
	Monitoring and Supporting AWMS with the System Pages.....	249
	Using the System > Status Page.....	251
	Using the System > Event Logs Page.....	252
	Using the System > Configuration Change Jobs Page	253
	Using the System > Performance Page.....	254
	Upgrading AWMS	256
	Upgrade Instructions	256
	Upgrading Without Internet Access	256
	Backing Up AWMS	256
	Overview of Backups.....	256
	Viewing and Downloading Backups	257
	Running Backup on Demand	257
	Restoring from a Backup.....	257
	AWMS Failover	258
	Navigation Section of AWMS Failover	258
	Adding Watched AWMS Stations	258

Chapter 9	Creating, Running, and Emailing Reports	261
	Overview of AWMS Reports.....	261
	Reports > Definitions Page Overview	261
	Reports > Generated Page Overview	263
	Using Daily Reports.....	264
	Viewing Generated Reports	264
	Using Custom Reports	265
	Using the Capacity Planning Report	266
	Using the Configuration Audit Report	267
	Using the Device Summary Report	268
	Using the Device Uptime Report.....	271
	Using the IDS Events Report	272
	Using the Inventory Report.....	273
	Using the Memory and CPU Usage Report.....	274
	Using the Network Usage Report.....	276
	Using the New Rogue Devices Report	277
	Using the New Users Report.....	280
	Using the PCI Compliance Report	281
	Using the Port Usage Report.....	282
	Using the RADIUS Authentication Issues Report	284
	Using the Rogue Containment Audit Report	284
	Using the User Session Report	285
	Defining Reports	289
	Emailing and Exporting Reports	292
	Emailing Reports in General Email Applications	292
	Emailing Reports to Smarthost.....	292
	Exporting Reports to XML or CSV	293
	Transferring Reports Using FTP	293
Chapter 10	Using the AWMS Helpdesk.....	295
	AWMS Helpdesk Overview	295
	Monitoring Incidents with Helpdesk	296
	Creating a New Incident with Helpdesk	297
	Creating New Snapshots or Incident Relationships.....	298
	Using the Helpdesk Tab with an Existing Remedy Server	299
Appendix A	Package Management for AWMS.....	303
	Yum for AWMS	303
Appendix B	Third-Party Security Integration for AWMS	305
	Bluesocket Integration	305
	Bluesocket Configuration	305
	ReefEdge Integration	305
	ReefEdge Configuration	306
	HP ProCurve 700wl Series Secure Access Controllers Integration	306
	Example Network Configuration	306
	HP ProCurve 700wl Series Configuration	306
Appendix C	Access Point Notes.....	309
	Resetting Cisco (VxWorks) Access Points.....	309
	Connecting to the AP	309
	Determining the Boot-Block Version	310
	Resetting the AP (for Boot-Block Versions from 1.02 to 11.06).....	310
	Resetting the AP (for Boot-Block Versions 11.07 and Higher).....	310

	Cisco IOS Dual Radio Template	311
	Speed Issues Related to Cisco IOS Firmware Upgrades.....	312
	AWMS Firmware Upgrade Process.....	312
Appendix D	Initiating a Support Connection.....	315
	Network Requirements.....	315
	Procedure	315
Appendix E	Cisco Clean Access Integration (Perfigo)	317
	Prerequisites for Integrating AWMS with Cisco Clean Access.....	317
	Adding AWMS as RADIUS Accounting Server.....	317
	Configuring Data in Accounting Packets	317
Appendix F	HP Insight Install Instructions for AWMS Servers	319
Appendix G	Installing AWMS on VMware ESX (3i v. 3.5)	321
	Creating a New Virtual Machine to Run AWMS.....	321
	Installing AWMS on the Virtual Machine.....	321
	AWMS Post-Installation Issues on VMware.....	322
Appendix H	Third-Party Copyright Information	323
	Packages	323
	Net::IP:.....	323
	Net-SNMP:	323
	Crypt::DES perl module (used by Net::SNMP):.....	326
	Perl-Net-IP:	327
	Berkeley DB 1.85:	327
	SWFObject v. 1.5:.....	328
	mod_auth_tacacs - TACACS+ authentication module:.....	328

This preface provides an overview of this guide, a list of all documentation available for AWMS 7.1, including contact information for Dell, and includes the following sections:

- “Document Organization” on page 11
- “Notice 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 Dell PowerConnect W AirWave Wireless Management Suite. This includes wide deployment of wireless access points (APs), device administration, rogue detection and classification, wireless controller devices, security, reports, and additional features of AWMS.

Table 1 Document Organization and Purposes

Chapter	Description
Chapter 1, “Introduction”	Introduces and presents the AirWave Wireless Management Suite, AWMS components, and general network functions.
Chapter 2, “Installing AWMS”	Describes system and network requirements, Linux OS installation, and AWMS installation.
Chapter 3, “Configuring AWMS”	Describes the primary and required configurations for startup and launch of AWMS, with frequently used optional configurations.
Chapter 4, “Configuring and Using Device Groups in AWMS”	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 the RAPIDS module of AWMS, and enhanced rogue classification supported in AWMS.
Chapter 8, “Performing Daily Administration in AWMS”	Describes common daily operations and tools in AWMS, to include general user administration, the use of triggers and alerts, network monitoring, and backups.
Chapter 9, “Creating, Running, and Emailing Reports”	Describes AWMS reports, scheduling and generation options, and distribution of reports from AWMS.
Chapter 10, “Using the AWMS Helpdesk”	Describes how to use the AWMS Helpdesk GUI and related functions.
Appendix A, “Package Management for AWMS”	Describes the Yum packaging management system, and provides advisories on alternative methods that may cause issues with AWMS.
Appendix B, “Third-Party Security Integration for AWMS”	Describes additional and optional security configurations in AWMS.
Appendix C, “Access Point Notes”	Provides guidelines and suggestions for Access Point devices in AWMS.

Table 1 Document Organization and Purposes

Chapter	Description
Appendix D, “Initiating a Support Connection”	Provides instructions about how to create and use a support connection between AWMS and AirWave Wireless Support.
Appendix E, “Cisco Clean Access Integration (Perfigo)”	Provides instructions for integrating Cisco Clean Access within AWMS.
Appendix F, “HP Insight Install Instructions for AWMS Servers”	Provides instructions for installing HP Insight on AWMS servers.
Appendix G, “Installing AWMS on VMware ESX (3i v. 3.5)”	Provides instructions for an alternative installation option on VMware ESX for AWMS.
Appendix H, “Third-Party Copyright Information”	Presents multiple copyright statements from multiple equipment vendors that interoperate with AWMS.
Index	Provides extensive citation of and links to document topics, with emphasis on the AWMS GUI and tasks relating to AWMS installation and operation.

Notice Icons

This document uses the following notice icons to emphasize advisories for certain actions, configurations, or concepts:



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



Caution: Indicates a risk of damage to your hardware or loss of data



Warning: Indicates a risk of personal injury or death.

Contacting Support

Table 2 Support Web Sites

Web Site	
• Main Site	www.dell.com
• Support Site	support.dell.com

Thank you for choosing the Dell PowerConnect W AirWave Wireless Management Suite, or AWMS. AWMS 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 the AirWave Wireless Management Suite. This chapter includes the following topics:

- “AWMS—A Unified Wireless Network Command Center” on page 13
- “AWMS Navigation Basics” on page 22
- “Integrating AWMS into the Network and Organizational Hierarchy” on page 15

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

AWMS—A Unified Wireless Network Command Center

AWMS 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, AWMS manages it all.

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

The components of the AirWave Wireless Management Suite are listed here, and detailed below:

- The Dell PowerConnect W AirWave Management Platform (AMP) wireless network management software, including the Dell PowerConnect W Configuration feature that supports global configuration of Dell PowerConnect W controllers.
- *VisualRF* location and RF mapping software module
- *RAPIDS* rogue access point detection software module
- **Master Console** and **Failover** tabs.

AirWave Management Platform™

The AirWave Management Platform (AMP) is the centerpiece of the Dell PowerConnect W AirWave wireless management solution, 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 wireless 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 and WiMAX network architecture
 - Multi-vendor support
 - Current and legacy hardware support

Dell PowerConnect W Configuration

AWMS supports global configuration of ArubaOS (AOS). AOS is the operating system, software suite, and application engine that operates Dell PowerConnect W mobility and centralizes control over the entire mobile environment. The AOS Wizards, the AOS command-line interface (CLI), and the AOS WebUI have been the primary means by which to configure and deploy AOS. For a complete description of AOS, refer to the *ArubaOS User Guide*.

AWMS consolidates ArubaOS configuration and pushes global Dell PowerConnect W configurations from within AWMS.

Two pages in AWMS support Dell PowerConnect W Configuration:

- **Device Setup > Dell PowerConnect W Configuration**
- **Groups > Dell PowerConnect W Config**

AWMS also introduces new settings and functionality on additional pages in support of Dell PowerConnect W Configuration. For additional information that includes a comprehensive inventory of all pages and settings that support Dell PowerConnect W Configuration, refer to the *Dell PowerConnect W AirWave Wireless Management Suite 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

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 AWMS 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. See [“Using Triggers and Alerts” on page 232](#).

Integrating AWMS into the Network and Organizational Hierarchy

AWMS generally resides in the NOC and communicates with various components of your WLAN infrastructure. In basic deployments, AWMS communicates solely with indoor wireless access points and WLAN controllers over the wired network. In more complex deployments AWMS seamlessly integrates and communicates with authentication servers, accounting servers, TACACS+ servers, routers, switches, network management servers, wireless IDS solutions, help systems, indoor wireless access points, mesh devices, and WiMAX devices.

AWMS has the flexibility to manage devices on local networks, remote networks, and networks using Network Address Translation (NAT). AWMS communicates over-the-air or over-the-wire utilizing a variety of protocols.

The power, performance, and usability of the AWMS solution become more apparent when considering the diverse components within a Wireless LAN. [Table 3](#) itemizes such network components, as an example.

Table 3 *Components of a Wireless LAN*

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	AWMS itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+	Used to authenticated AWMS administrative users
Routers/Switches	Provide AWMS with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR

Table 3 *Components of a Wireless LAN*

Component	Description
Rogue APs	Unauthorized APs not registered in the AWMS database of managed APs

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

Further flexibility and administrative power include the following benefits:

- 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 the AirWave Wireless Management Suite (AWMS), and includes the following topics:

- “AWMS Hardware Requirements and Installation Media” on page 17
- “Installing Linux CentOS 5 (Phase 1)” on page 17
- “Installing AWMS Software (Phase 2)” on page 18
- “Configuring and Mapping Port Usage for AWMS” on page 21
- “AWMS Navigation Basics” on page 22
- “Getting Started with AWMS” on page 29



Note: AWMS 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 AWMS, we recommend you perform a fresh installation of the earlier AWMS version, and then restore data from a pre-upgrade backup.

AWMS Hardware Requirements and Installation Media

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

AWMS hardware requirements vary by version. As additional features are added to AWMS, increased hardware resources become necessary. For the most recent hardware requirements, download the *Dell PowerConnect W Airwave Hardware Sizing Guide* from <http://support.dell.com/manuals>.

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 AWMS on the network management system.



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

1. Insert the AWMS installation CD-ROM into the drive and boot the server.
2. If this is a new installation of the AWMS software, type **install** and press **Enter**.



Note: When you press Enter, all existing data on the hard drive is erased.

To configure the partitions manually, type **expert** and press **Enter**.

The following message appears on the screen.

```
Welcome to AWMS Installer Phase I
```

```
- To install a new AMP, type install <ENTER>.
```

```
  WARNING: This will ERASE all data on your hard drive.
```

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

```
boot:
```

AWMS 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 AWMS, 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.

1. Allow the installation process to continue in automatic fashion. 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 automatically reboots and ejects the installation CD.

2. Remove the CD from the drive and store in a safe location.

Installing AWMS 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 **smp** kernel.
2. When the kernel is loaded, log into the server using the following credentials:
 - login = **root**
 - password = **admin**
3. Start the AWMS 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.*

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 a loss of graphical data, and you should avoid delayed configuration.

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

Previous AWMS Installations

The following message appears after date and time are set.

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

If a previous version of AWMS software is not discovered, the installation program automatically proceeds to [“Step 2: Installing AWMS Software, Including AWMS” 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 AWMS? This will erase AWMS's database. Reinstall (y/n)?
```

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



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

Step 2: Installing AWMS Software, Including AWMS

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

```
STEP 2: Installing AWMS 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 have the option of monitoring progress in more detail should you wish to do so:

- To view detailed output from the AWMS software installer, press **Alt-F9** or **Ctrl-Alt-F9**.
- Pressing **Alt-F1** or **Ctrl-Alt-F1** returns you to the main console.

Step 3: Checking the AWMS Installation

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

```
STEP 3: Checking AWMS installation
Database is up.
AWMS 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 AWMS System

While the AWMS primary network interface accepts a DHCP address initially during installation, *AWMS 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 AWMS's address

AWMS 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 AWMS's web interface, AWMS Setup --> Network Tab

1. Enter the network information.



Note: 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 AWMS Network Administration System

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

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

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

Step 6: Assigning a Host Name to the AWMS

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

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

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

```
Generating SSL certificate for < IP Address >
```

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

```
Enter AWMS's DNS name:
```

3. Type the AWMS 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:
```

1. 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. Aruba recommends keeping this password 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 AWMS upgrades and advanced troubleshooting. If you lose this password, contact Dell support for instructions on resetting it.

Completing the Installation

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

```
CONGRATULATIONS! AWMS is configured properly.  
To access AWMS 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/AWMS-install.log`.
- To access the AWMS GUI, enter the AWMS IP address in the address bar of any browser. The AWMS GUI then prompts for your license key. If you are entering a dedicated **Master Console** or **AWMS Failover** license, refer to [“Supporting AWMS Stations with the Master Console” on page 239](#) for additional information.

Configuring and Mapping Port Usage for AWMS

The following diagram itemizes the communication protocols and ports necessary for AWMS 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 AWMS Protocol and Port Chart

Port	Type	Protocol	Description	Dataflow Direction	Device Type
21	TCP	FTP	Configure devices and FW distribution	>	Legacy AP (Cisco 4800)
22	TCP	SSH	Configure devices	>	APs or controllers
22	TCP	SSH	Configure AWMS 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

Table 4 AWMS Protocol and Port Chart (Continued)

Port	Type	Protocol	Description	Dataflow Direction	Device Type
25	TCP	SMTP	Support email (optional)	>	AirWave support email server
49	UDP	TACACS	AWMS Administrative Authentication	>	Cisco TACACS+
53	UDP	DNS	DNS lookup from AWMS	>	DNS Server
69	UDP	TFTP	Transfer configuration files or FW	<	APs or controllers
80	TCP	HTTP	Configure devices	>	Legacy APs
80	TCP	HTTP	Firmware upgrades	<	Colubris devices
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 AWMS	>	NMS
443	TCP	HTTPS	Web management	<	Laptop or workstation
443	TCP	HTTPS	WLSE polling	>	WLSE
443	TCP	VTUN	Support connection (optional)	>	AirWave support home office
1701	TCP	HTTPS	AP and rogue discovery	>	WLSE
1741	TCP	HTTP	WLSE polling	>	WLSE
1813	UDP	RADIUS	Retrieve client authentication info	<	Accounting Server
1813	UDP	RADIUS	Retrieve client authentication info	<	AP or controllers
1813	UDP	RADIUS	Outbound from AWMS to a RADIUS server for AWMS administrator authentication	>	RADIUS server
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

AWMS Navigation Basics

Every AWMS page contains three basic sections, as follows:

- Status Section
- Navigation Section
- Activity Section

The AWMS pages also contain **Help** links with GUI-specific help information and certain standard action buttons. illustrates these sections.

Status Section

The **Status** section provides a snapshot view of overall WLAN performance and provides direct links for immediate access to key system components. The Status section remains at the top of all pages in the AWMS and RAPIDS modules. AWMS 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 248](#).

The table below describes these elements in further detail.

Table 5 Status Section Components of the AWMS Graphical User Interface (GUI)

Field	Description
New Devices	The number of wireless APs or wireless LAN controllers that have been discovered by AWMS but not yet managed by network administrators. When you click this link, AWMS directs you to a page that displays a detailed list of devices awaiting authorization.
Up (Wired, Wireless, and combined)	The number of managed, authorized devices that are currently responding to AWMS requests. When you click this link, AWMS will direct you to a page that displays a detailed list of all Up devices.
Down (Wired, Wireless, and combined)	The number of managed, authorized devices that are not currently responding to AWMS SNMP requests. When you click this link, AWMS will direct you to a page that displays a detailed list of all "Down" devices.
Mismatched	The total number of Mismatched devices. A device is considered mismatched when the desired configuration in AWMS does not match the actual device configuration read from the device.
Rogue	The number of devices that have been classified by the RAPIDS rules engine above the threshold defined on the Home > User Info page.
Users	The number of wireless users currently associated to the wireless network via all the APs managed by AWMS. When you click this link, AWMS directs you to a page that contains a list of users that are associated.
Alerts	Displays the number of non-acknowledged AWMS alerts generated by user-configured triggers. When you click this link, AWMS directs you to a page containing a detailed list of active alerts.
Severe Alerts (conditional)	When triggers are given a severity of Critical , they generate Severe Alerts . When a Severe Alert exists, a new component appears at the right of the Status field in bold red font. Only users configured on the Home > User Info 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. However, unlike Alerts, the Severe Alerts section is hidden if there are no Severe Alerts.
Device Types to Include in Header Stats	You can support statistics for any combination of the following device types: <ul style="list-style-type: none">● Autonomous APs● Controllers● Routers/Switches● Thin APs● Universal Devices Refer to “Configuring Your Own User Information with the Home > User Info Page” on page 248 .
Search	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 of all the APs as well as the client MAC, VPN user, LAN IP, VPN IP fields.

Navigation Section

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

Table 6 Components and Sub-Menus of the AWMS Navigation Screen

Main Tab	Description	Sub-Menus
Home	<p>The Home pages provide basic AWMS information including system name, host name, IP address, current time, running time, and software version.</p> <p>The Home page also provides a central point for network status information and monitoring tools, giving graphical display of network activity.</p> <p>The Home > Overview page provides links to many of the most frequent tools in AWMS.</p> <p>For additional information, refer to “Monitoring and Supporting AWMS with the Home Pages” on page 241.</p>	<ul style="list-style-type: none"> ● Overview ● Search ● Documentation ● License ● User Info
Helpdesk	<p>The Helpdesk pages provide an interface for support and diagnostic tools. For additional information refer to Chapter 10, “Using the AWMS Helpdesk” on page 295.</p>	<ul style="list-style-type: none"> ● Incidents ● Setup
Groups	<p>The Groups pages provide information on the logical "groups" of devices that have been established for efficient monitoring and configuration. For additional information, see Chapter 4, “Configuring and Using Device Groups in AWMS” on page 79.</p> <p>NOTE: Some of the focused sub-menus will not appear for all groups. Focused sub-menus are visible based on the device type field on the Groups > Basic page. This sub-menu is the first page to appear when adding or editing groups.</p> <p>NOTE: 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"> ● List ● Focused Sub-Menus <ul style="list-style-type: none"> ■ Monitor ■ Basic ■ Templates ■ Security ■ SSIDs ■ AAA Servers ■ Radio ■ Dell PowerConnect W Config ■ Cisco WLC Config ■ PTMP/WiMAX ■ Proxim Mesh ■ Colubris ■ MAC ACL ■ Firmware ■ Compare (Master Console Only)
APs/Devices	<p>The APs/Devices 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 AWMS. One chapter to emphasize the APs/Devices pages is Chapter 5, “Discovering, Adding, and Managing Devices” on page 127.</p> <p>NOTE: When specified, device-level settings override the default Group-level settings.</p>	<ul style="list-style-type: none"> ● List ● New ● Up ● Down ● Mismatched ● Ignored ● Focused Sub-Menus <ul style="list-style-type: none"> ■ Manage ■ Audit ■ Compliance ■ Interfaces ■ Containment Status
Users	<p>The Users pages provide detailed information about all client devices and users currently associated to the WLAN. For additional information, refer to “Monitoring and Supporting WLAN Users” on page 228.</p>	<ul style="list-style-type: none"> ● Connected ● All ● Guest Users ● User Detail ● Diagnostics ● Tags

Table 6 Components and Sub-Menus of the AWMS Navigation Screen (Continued)

Main Tab	Description	Sub-Menus
Reports	The Reports pages list all the standard and custom reports generated by AWMS. AWMS supports 13 reports in the AWMS module. For additional information, refer to Chapter 9, “Creating, Running, and Emailing Reports” on page 261 .	<ul style="list-style-type: none"> ● Generated ● Definition ● Focused Sub-Menus ● Details
System	The System page provides information about AWMS operation and administration, including overall system status, the job scheduler, trigger/alert administration, and so forth. For additional information, refer to “Monitoring and Supporting AWMS with the System Pages” on page 249 .	<ul style="list-style-type: none"> ● Status ● Event Log ● Triggers ● Alerts ● Configuration Change Jobs ● Firmware Upgrade Jobs ● Performance
Device Setup	The Device Setup 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 “Enabling AWMS to Manage Your Devices” on page 52 .	<ul style="list-style-type: none"> ● Discover ● Add ● Communication ● Aruba Configuration ● Upload Files
AMP Setup	The AMP Setup pages provide all information relating to the configuration of AWMS itself and its connection to your network. This page entails several processes, configurations, or tools in AWMS. For additional information, start with Chapter 3, “Configuring AWMS” on page 31 . NOTE: The AMP Setup pages may not be visible, depending on the role and license set in AWMS.	<ul style="list-style-type: none"> ● General ● Network ● Users ● Roles ● Authentication ● WLSE ● ACS ● NMS ● RADIUS Accounting ● PCI Compliance
RAPIDS	The RAPIDS 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 Chapter 7, “Using RAPIDS and Rogue Classification” on page 195 . NOTE: The RAPIDS pages may not be visible, depending on the role and license set in AWMS.	<ul style="list-style-type: none"> ● Overview ● Rogue APs ● Setup ● Rules ● Score Override ● Audit Log
VisualRF	VisualRF pages provide graphical access to floor plans, client location, and RF visualization for floors, buildings, and campuses that host your network. For additional information, refer to the <i>VisualRF User Guide</i> . NOTE: VisualRF may not be visible, depending on the role and license set in AWMS.	<ul style="list-style-type: none"> ● Overview ● Floor Plans ● Campus/Building ● Setup ● Import



Note: 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 AWMS view.

Activity Section

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

Help Links in the GUI

The [Help](#) link is available on every page within AWMS. When clicked, this launches a PDF document with information describing the AWMS page that is currently displayed.



Note: [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 AWMS have some common options. All lists are paginated with a configurable number of items per page, as shown in [Figure 1](#).

Figure 1 Example of **Common List Settings** Configurable Attributes

Username	Role	MAC Address	AP/Device	Location	SSID
-	-	00:22:FA:BA:B7:62	CiscoIOS1100-12.3(2)	-	muirtest1200
-	-	00:24:2C:05:BB:C3	CiscoIOS1100-12.3(2)	-	muirtest1200
-	-	00:1C:B3:05:44:1E	RoamAbout AP	-	RoamAbout Default Network Nam
-	-	00:23:12:DF:D8:F5	CiscoIOS1100-12.3(2)	-	muirtest1200
-	-	00:22:41:0C:40:39	ag-2100	-	-

20 records per page of 5 Users Page 1 of 1 Choose Columns
1-5 of 5 Users Page 1 of 1

Clicking on the left most down arrow allows you to set how many rows appear on one page of the list. The next down arrow is used to jump to a specific page in the list. Clicking it will bring up a drop down menu that allows you to select the exact page you would like to view, as shown in [Figure 2](#).

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

Username	Role	MAC Address	AP/Device	Location	SSID
-	-	00:22:FA:BA:B7:62	Cisco	-	muirtest1200
-	-	00:24:2C:05:BB:C3	Cisco	-	muirtest1200
-	-	00:1C:B3:05:44:1E	Roam	-	RoamAbout Default Network Name 0
-	-	00:23:12:DF:D8:F5	Cisco	-	muirtest1200
-	-	00:22:41:0C:40:39	ag-2	-	-

20 records per page of 5 Users Page 1 of 1 Choose Columns
1-5 of 5 Users Page 1 of 1

Alert Summary at 10/30/2009 2:19 PM

Type	Last 2 Hours
Incidents	0
Alerts	0
RADIUS Authentication Issues	0

Save | Cancel

- Username ↑↓
- Role ↑↓
- MAC Address ↑↓
- AP/Device ↑↓
- Location ↑↓
- SSID ↑↓
- VLAN ↑↓
- AP Radio ↑↓
- Connection Mode ↑↓
- Ch BW ↑↓
- Association Time ↑↓
- Duration ↑↓
- LAN IP Address ↑↓
- LAN Hostname ↑↓
- Guest User ↑↓
- VPN IP Address ↑↓
- VPN Hostname ↑↓

The **Choose Columns** option allows you to configure the columns that are presented in the list and the order in which they are presented. To disable a column simply uncheck the checkbox. To reorder the columns, click and drag a specific row to the appropriate new position. When you are satisfied with the enabled columns and their order, click on the save button.

These settings are user specific. To reset them to the defaults click the **Reset List Preferences** button on the Home > User Info page.

Buttons and Icons

Standard buttons and icons are used consistently from screen to screen throughout the AWMS user pages and GUI, as itemized in the following table:

Table 7 Standard Buttons and Icons of the AWMS User Page





























Buttons and Icons	Appearance ^a	Description
Acknowledge		Acknowledges and clears an AWMS alert.
Add		Adds the object to both AWMS' database and the onscreen display list.
Add Folder		Adds a new folder to hierarchically organize APs.
Alert		Indicates an alert.
Apply		Applies all "saved" configuration changes to devices on the WLAN.
Attach		Attaches a snapshot of an AWMS screen to a Helpdesk incident.
Audit		Reads device configuration, compare to desired, and update status.
Bandwidth		Displays current bandwidth for group.
Choose		Chooses a new Helpdesk incident to be the Current Incident.
Create		Creates a new Helpdesk incident.
Customize		Ignores selected settings when calculating the configuration status.
Delete		Deletes an object from AWMS' database.
Down		Indicates down devices and radios.
Drag and Drop		Dragging and dropping objects with this icon changes the sequence of items in relation to each other. Refer to "Using RAPIDS and Rogue Classification" on page 195 as one example of drag-and-drop.
Duplicate		Duplicates or makes a copy of the configuration of an AWMS object.
Edit		Edits the object properties.
Email		Links to email reports.
Filter		Filters rogue list by score and/or ad hoc status.
Google Earth		Views device's location in Google Earth (requires plug-in).
Manage		Manages the object properties.

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

Buttons and Icons	Appearance ^a	Description
Mismatched		Indicates mismatched device configuration, in which the most recent configuration in AWMS and the current configuration on a device are mismatched.
Monitor		Indicates an access point is in "monitor only" mode.
Ignore		Ignores specific device(s) - devices selected with check boxes.
Import		Updates a Group's desired settings to match current settings.
New Devices		Indicates new access points and devices.
Poll Now		Polls device (or controller) immediately, override group polling settings.
Preview		Displays a preview of changes applicable to multiple groups.
Print		Prints the report.
Reboot		Reboots devices or AWMS.
Refresh		Refreshes the display of flash graphs when settings have changed.
Relate		Relates an AP, Group or Client to a Helpdesk incident.
Replace Hardware		Confers configuration and history of one AP to a replacement device.
Revert		Returns all configurable data on the screen to its original status.
Rogue		Indicates a rogue access point.
Run		Runs a new user-defined report.
Save		Saves the information on the page in the AWMS database.
Save & Apply		Saves changes to AWMS' database and apply all changes to devices.
Scan		Scans for devices and rogues using selected networks.
Schedule		Schedules a window for reports, device changes, or maintenance.
Search		Searches AWMS for the specified name, MAC or IP address.
Set Time Range		Sets the time range for flash graphs to the range specified with the time-range bar.
Up		Indicates access points which are in the up status.
Update Firmware		Applies a new firmware image to an AP/device.
User		Indicates a user.
View Graph in New Window		Displays flash graphs in a new window.
VisualRF		Links to VisualRF - real time visualization.
XML		Links to export XHTML versions of reports.

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

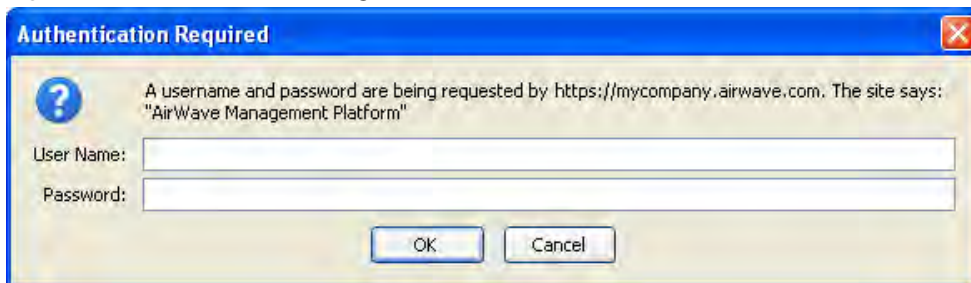
Getting Started with AWMS

This topic describes how to perform an initial launch of the AWMS network management solution. This topic requires successful completion of installation, as described earlier in this chapter. This topic prepares the administrator for wider deployment and device support and operations once initial startup is complete.

Completing Initial Login

Use your browser to navigate to the static IP address assigned to the internal page of the AWMS. Once your session launches, the **Authentication Dialog Box** appears as shown in [Figure 3](#).

Figure 3 Authentication Dialog Box



Perform these steps to complete the initial login.

1. Enter User name **admin**
2. Enter Password **admin**
3. Click **OK**

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

Note: AWMS pages are protected via SSL.



Aruba recommends changing the default login and password on the **AMP Setup > Users** page. Refer to the procedure [“Creating AWMS User Roles”](#) on [page 50](#) for additional information.

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

- [“Formatting the Top Header” on page 31](#)
- [“Customizing Columns in Lists” on page 33](#)
- [“Resetting Pagination Records” on page 34](#)
- [“Using the Pagination Widget” on page 34](#)
- [“Using CSV Export for Lists and Reports” on page 35](#)
- [“Defining Graph Display Preferences” on page 35](#)
- [“Customizing the Overview Subtab Display” on page 36](#)
- [“Setting Severe Alert Warning Behavior” on page 38](#)
- [“Defining General AWMS Server Settings” on page 39](#)
- [“Defining AWMS Network Settings” on page 47](#)
- [“Creating AWMS Users” on page 48](#)
- [“Creating AWMS User Roles” on page 50](#)
- [“Enabling AWMS to Manage Your Devices” on page 52](#)
- [“Configuring TACACS+ and RADIUS Authentication” on page 62](#)
- [“Configuring Cisco WLSE and WLSE Rogue Scanning” on page 66](#)
- [“Configuring ACS Servers” on page 71](#)
- [“Integrating AWMS with an Existing Network Management Solution \(NMS\)” on page 73](#)
- [“Auditing PCI Compliance on the Network” on page 74](#)
- [“Deploying WMS Offload” on page 77](#)



Note: Additional configurations of multiple types are available after basic configuration is complete, as shown in this chapter.

Before You Begin

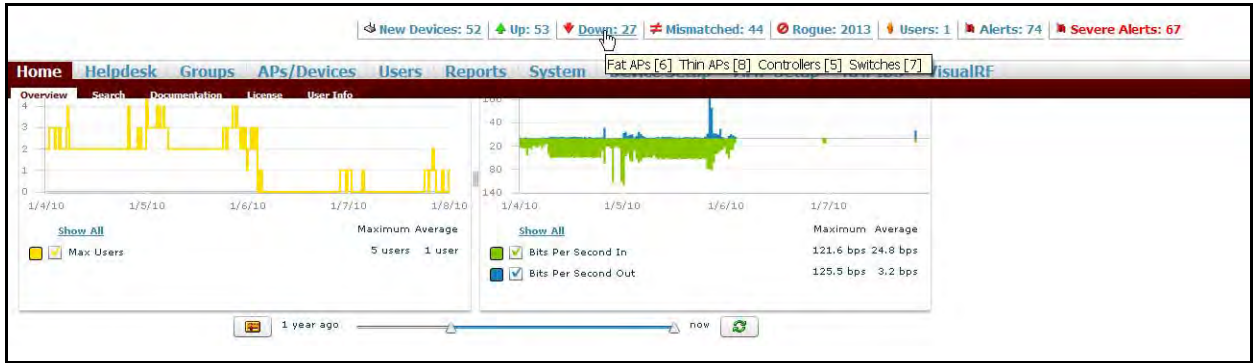
Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document. Dell support remains available to you for any phase of AWMS installation.

Formatting the Top Header

The AWMS interface centers around a horizontal row of tabs corresponding to high level components, with nested subtabs pertaining to relevant information and features within that component. Above the component tabs reside a row of statistics hyperlinks representing many commonly used subtabs. These hyperlinks provide two things: an ability to view certain key statistics by mousing over, such as number and type of **Down** devices (Fat APs, switches for example), and a short cut to certain frequently viewed subtabs. Clicking the Down hyperlink is the same as clicking **APs/Devices > Down**, to use the same example.

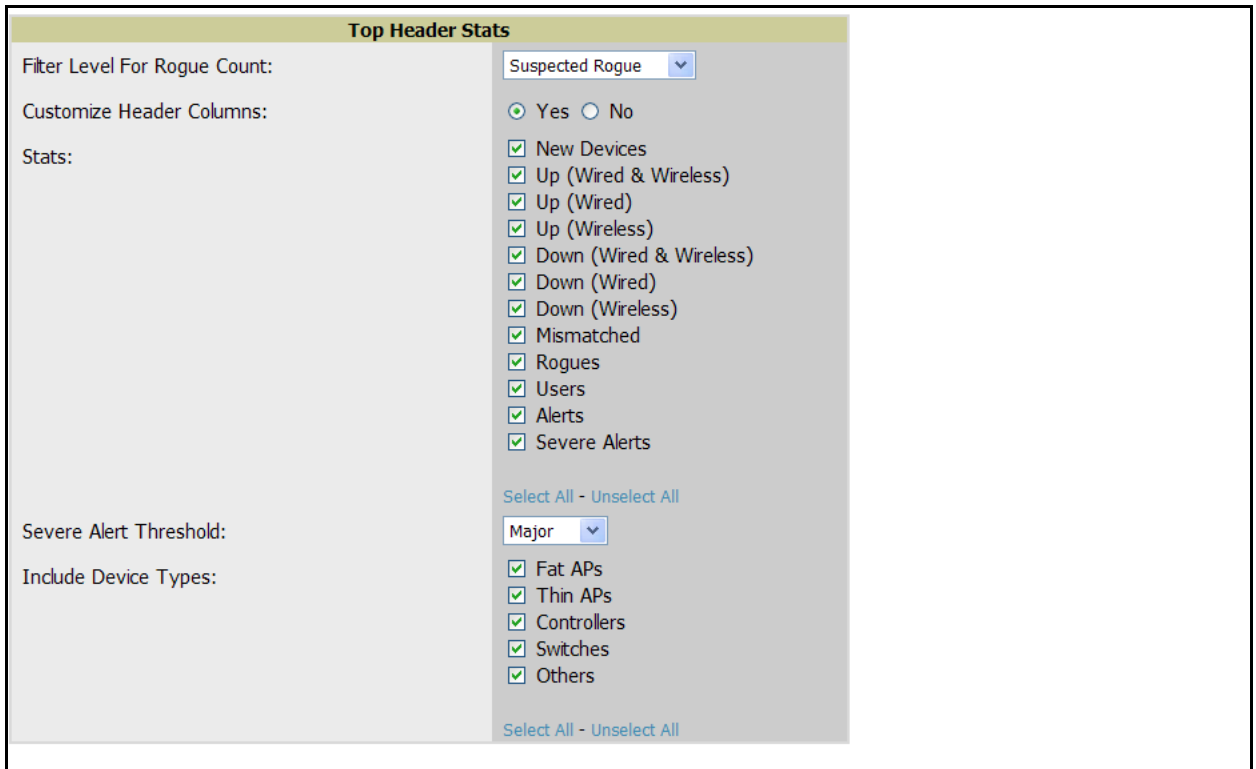
Figure 4 illustrates the navigation bar. For more details on hyperlinks, tabs and submenus, see “AWMS Navigation Basics” on page 22.

Figure 4 Navigation Bar Displaying Home Subtabs and Down Device Statistics



You can control which **Top Header Stats** links appear across the entire product from the **AMP Setup > General** page, as described in “Defining General AWMS Server Settings” on page 39. Top Header Stats hyperlinks can also be customized for individuals, according to individual user roles from the **Home > User Info** page by clicking the **Yes** radio button in the **Top Header Stats** pane. There you can select which statistics are displayed for what device types, and override choices made from the **AMP Setup** page. All possible display options are shown in Figure 5, and these fields are described in detail in “Monitoring and Supporting AWMS with the Home Pages” on page 241.

Figure 5 Top Header Stats Display Options



You can also set the severity level of critical alerts displayed for a given user role. For details including a description of what constitutes a severe alert, see “Setting Severe Alert Warning Behavior” on page 38.

Customizing Columns in Lists

You can determine which columns are displayed in any AWMS table by selecting or deselecting its checkbox from the dropdown list made visible by clicking **Choose Columns** as shown in [Figure 6](#). Using the up/down arrows to the right of each column title, you can change the order in which the column heads appear with the upper most column in the dropdown list correlating to the left most column in the table. As shown in [Figure 6](#), Username if it remains checked will appear as the left most column, Role will appear to the right of that, and so on.

Figure 6 *Choose Columns Dropdown List*

Type	Last 2 Hours
Incidents	0
Alerts	0
RADIUS Authentication Issues	0

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 the **Yes** radio button in the **Customize Header Columns** field, as also appears in [Figure 5](#). This exposes the **Choose Columns for Roles** dropdown menu in all tables shown in [Figure 7](#). The right hand column shows the user roles already customized, if any, for your particular production environment. The left hand column allows you to establish left to right columns and order them using the up and down arrows alongside the column head entries. The column heads and user roles displayed are set to their defaults, but can always be customized further, as needed.

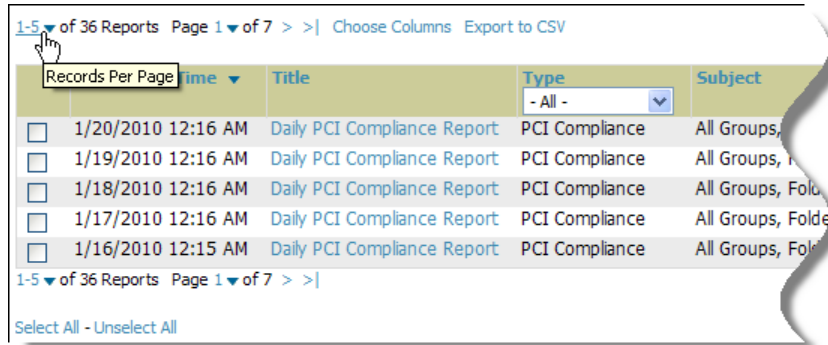
Figure 7 *Table With Choose Columns for Roles Menu Selected*

(kbps)	Uptime	Configuration	Device Group
	27 days 3 hrs 46 mins	Good	-
	1 day 4 hrs 58 mins	Error	-
	23 hrs 34 mins	Error	-

Resetting Pagination Records

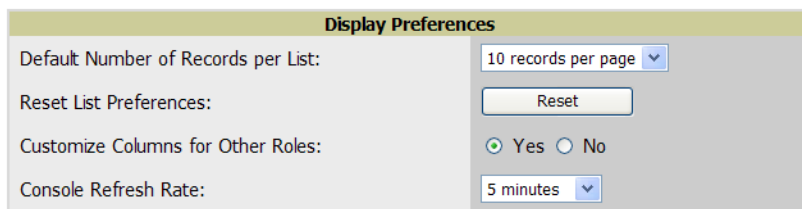
You can control how many records appear in any list individually by clicking the link with **Records Per Page** mouseover text at the top left of each table, as shown in [Figure 8](#). AWMS stores each list's pagination preferences so once you have customized the table (by choosing **Custom** from the **Records Per Page** dropdown menu and entering 5), each time you return to the **Generated Reports** list, it will always show just 5 records at a time, as in this example.

Figure 8 *Records Per Page Drop Down Menu*



If for some reason you would like to reset all AMP list **Records Per Page** preferences, you can select **Reset** in the **Display Preferences** pane of the **Home > User Info** page. The **Display Preferences** pane is shown in [Figure 9](#).

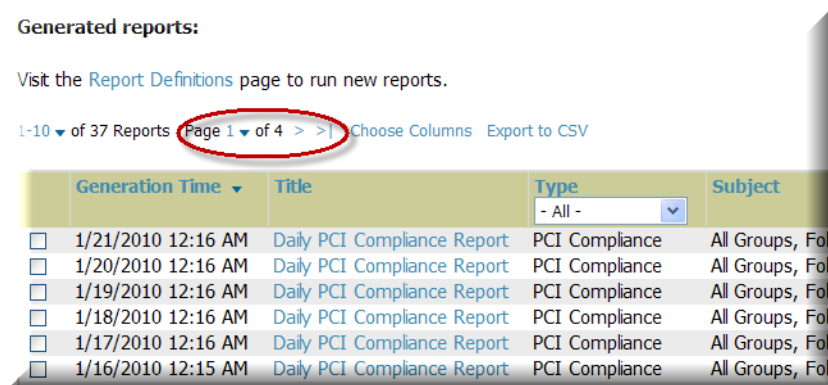
Figure 9 *Display Preferences Pane*



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*



As you mouse over it, you will see **Jump to Page**. Click the down arrow next to where it says **Page 1**, and a dropdown list appears with all the page numbers listed for that table. From here, you can jump to any portion of the table. You can browse the pages of any list table using the right pointing arrows on the outermost sides of the

pagination widget. Using the mouseover text as a guide, you can to jump to the next or previous and first or last pages of the table.

Using CSV Export for Lists and Reports

Wherever you see an **Export to CSV** setting above a list, you can export the data shown into a CSV file that you can open as a Microsoft Excel spreadsheet or in any text editor. All vertical and horizontal columns appearing in the table will also appear in the exported data file. See [Figure 11](#) for an example of a list with the **Export to CSV** option selected.

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

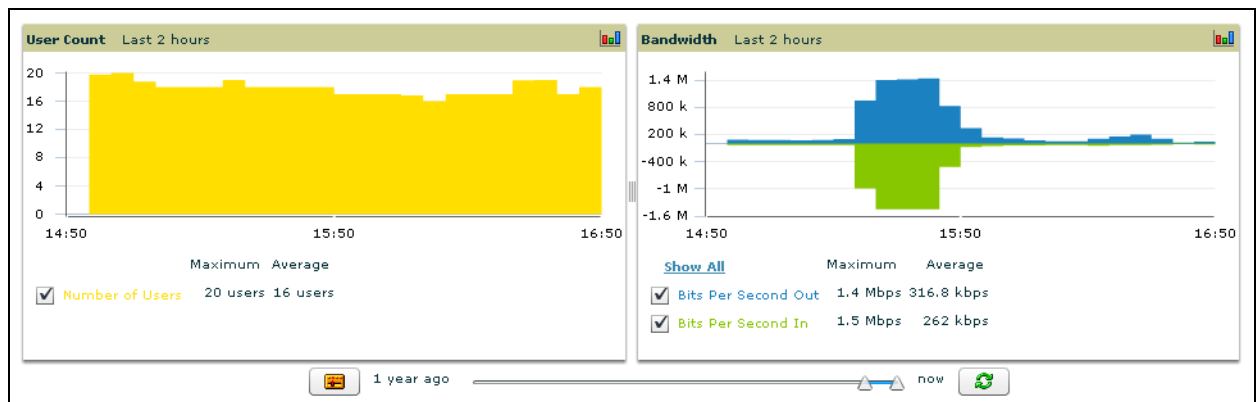
Device	Status	Uptime	Configuration	Group
Aruba3600-Master	Up	5 hrs 8 mins	Mismatched	Access Points
Aruba3600-Local	Up	10 days 23 hrs 7 mins	Mismatched	Access Points
Alcatel-Lucent-4308	Up	4 days 23 hrs 41 mins	Error	Access Points
ap-Cisco3	Up	4 days 22 hrs 53 mins	Error	Access Points
cisco3560	Up	5 days 4 hrs 17 mins	Error	Access Points
Aruba3200-RN	Up	47 days 7 hrs 20 mins	Error	Access Points
Enterprise AP	Up	4 days 22 hrs 30 mins	Mismatched	Access Points
Aruba2400	Down	-	Mismatched	Access Points
Mos Eisley aka Roamabout 3000	Down	-	Mismatched	Access Points
Intel PRO/Wireless LAN	Down	-	Mismatched	Access Points
Hirschmann	Down	-	Error	Access Points
Aruba200-Master-realy	Up	46 days 20 hrs 5 mins	Error	Access Points
Aruba800-FIPS	Up	4 days 23 hrs 38 mins	Mismatched	Access Points
Cisco-3750-2	Up	5 days 4 hrs 46 mins	Error	Access Points
something-witty	Down	-	Error	Access Points

AWMS also enables CSV exporting of all report types. For more information, see [“Using Custom Reports”](#) on page 265.

Defining Graph Display Preferences

Many of the graphs in AWMS are flash-based, which allows you change graph attributes, as shown in [Figure 12](#).

Figure 12 Flash Graphs on the **Home Overview** Page



This flash-enabled GUI allows for custom settings and adjustments, and the following examples illustrate some changes you can make or functions that are supported:

- 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.

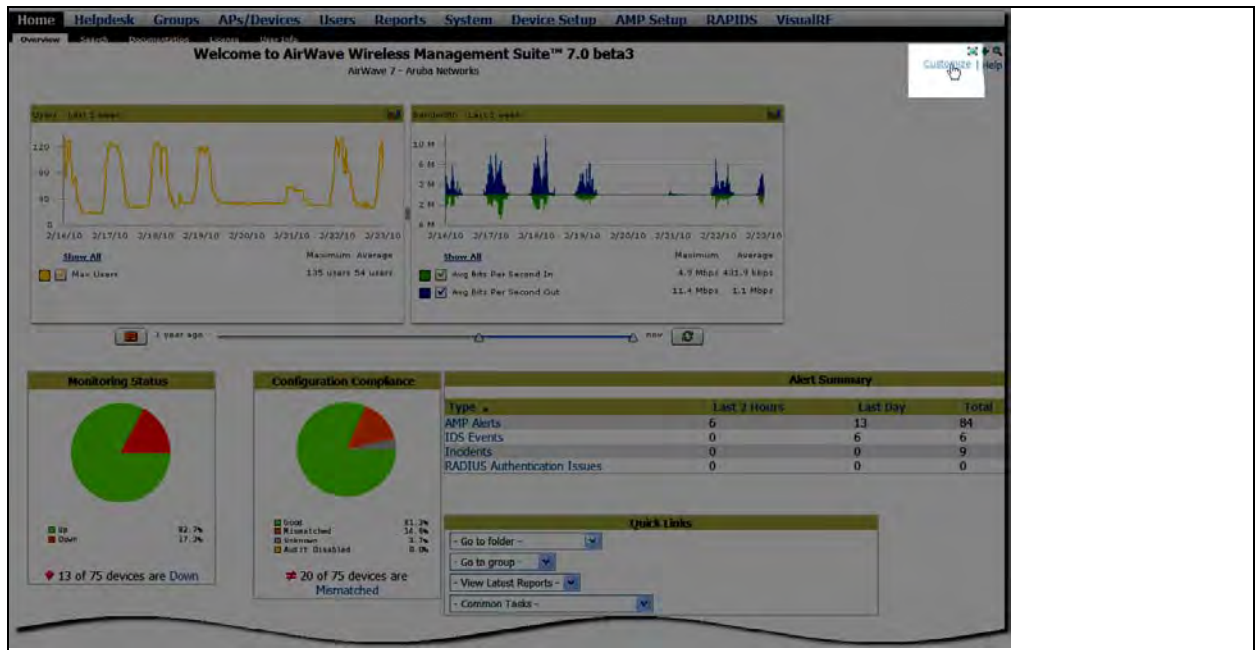
- The **Show All** link displays all of the available checkboxes supporting the flash graphs.
- Once a change to the slider bars or to the display boxes has been made, the same change can be applied to all other flash graphs with an **apply** button (appears on mouse-over only).
- For non-flash graphs, click the graph to open a popup window that shows historical data.

A non-flash version of the AWMS user page is available if desired; instead of flash it uses the RRD graphs that were used in AWMS through the 5.3 Version. Contact Dell support for more information on activating this feature in the AWMS database.

Customizing the Overview Subtab Display

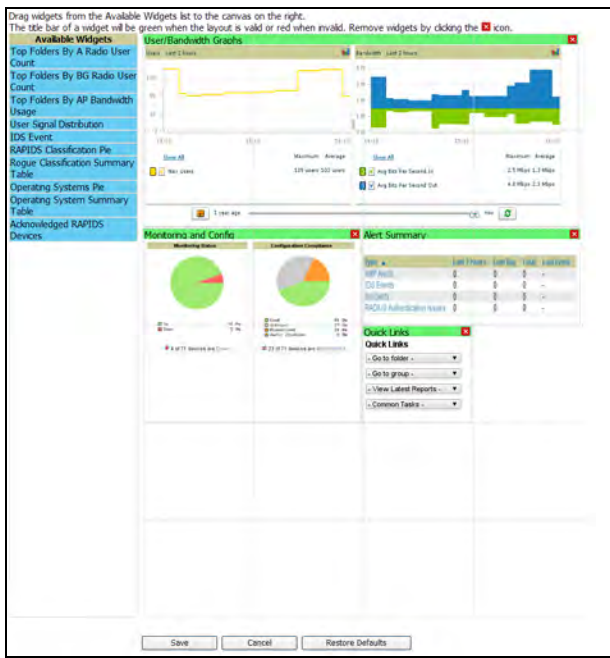
You can rearrange or remove widgets appearing on the **Home > Overview** dashboard by clicking **Customize** to the right of this window, as shown in [Figure 13](#).

Figure 13 *Customize Button on the Home Overview Page*



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

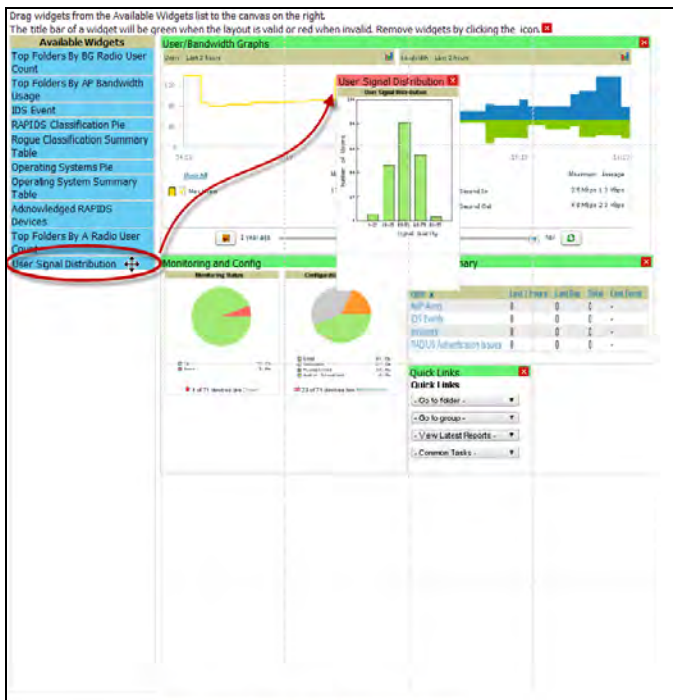
Figure 14 *Customize Overview Page*



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

Drag the widgets you want to appear on the **Overview** dashboard across to the gridlines and arrange them in the right pane, 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, as shown in [Figure 15](#).

Figure 15 *Example of Improper Widget Placement*

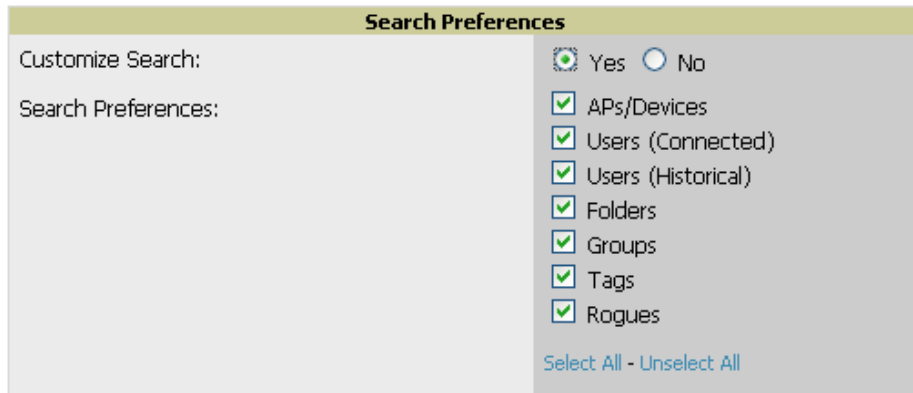


Green widgets are those that are properly placed and set to appear when you click **Save**. Widgets that remain in the left pane will not appear (although they can be returned at a later time, or reinstated by clicking **Restore Defaults**).

Customized Search

You can customize search results to display only desired categories of matches on the Home > User Info page. Navigate to the Search Preferences box and toggle the Customize Search option to “Yes”; then select or unselect categories of results and save your changes. By default customize search is turned off and all boxes are selected. When you enter a search string into the search box in the upper right-hand corner of any AMP page only results in the selected categories will be returned.

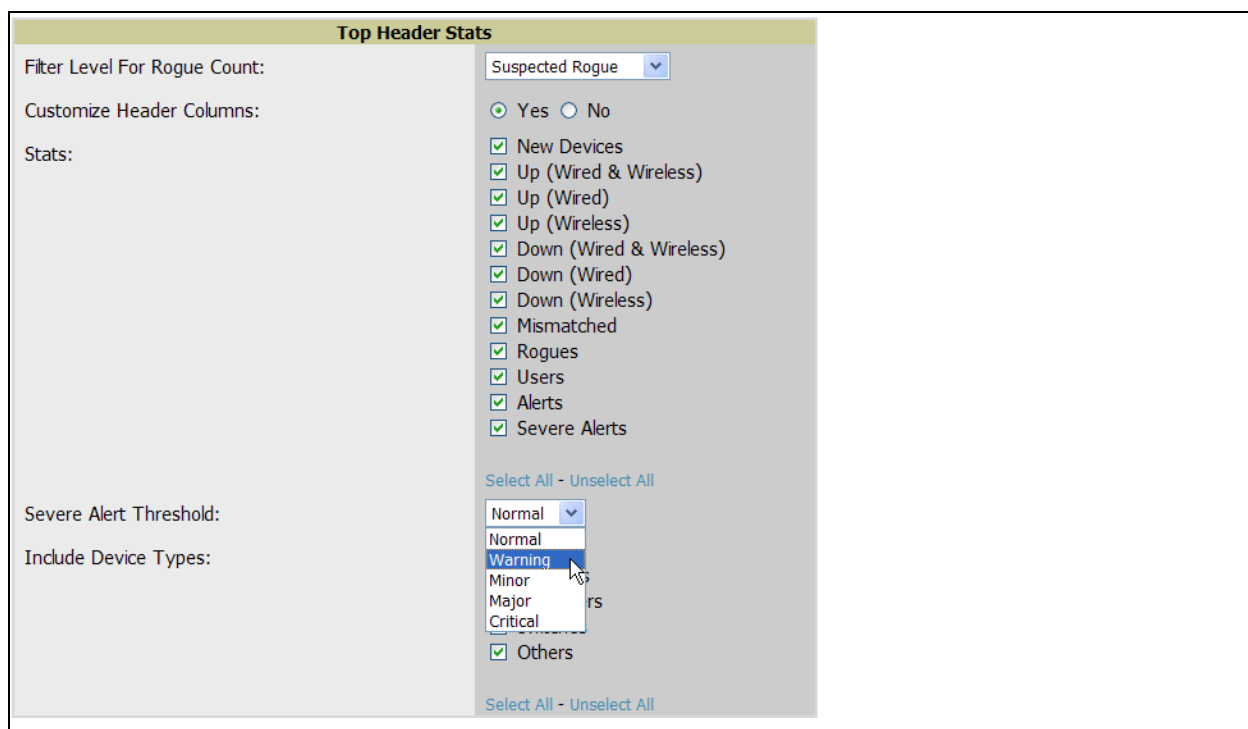
Figure 16 Customized Search Preferences



Setting Severe Alert Warning Behavior

You can control the alert levels users can see on the Alerts statistics hyperlink from the Home > User Info page. These settings will apply unless and until other users change settings for themselves. When a trigger is assigned a severity of Critical, it generates a severe alert. When a severe alert exists, a new component appears at the right of the Status field in bold red font. Only users configured on the Home > User Info page to be enabled to view critical alerts can see severe alerts. The Severe Alert Threshold dropdown menu, located in the Top Header Stats pane of the Home > User Info page, with all options displayed is shown in Figure 17.

Figure 17 Severe Alert Threshold Dropdown Menu



Defining General AWMS Server Settings

This section describes all pages accessed from the **AWMS 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 AWMS is to specify the general settings for the AWMS server. [Figure 18](#) illustrates the **AMP Setup > General** page:

Figure 18 AMP Setup > General Page Illustration

General	
System Name:	AirWave 7
Automatically monitor/manage new devices:	No
Default Group:	Aruba HQ
Device Configuration Audit Interval:	Daily
Automatically repair misconfigured devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send debugging messages to AirWave Wireless:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Nightly Maintenance Time (00:00 - 23:59):	20:15
AMP User Authorization Lifetime (0-240 min):	180
Check for software updates from AirWave Wireless: Periodically check the AirWave Wireless 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
Top Header	
Stats:	<input checked="" type="checkbox"/> New Devices <input 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 type="checkbox"/> Down (Wired) <input type="checkbox"/> Down (Wireless) <input checked="" type="checkbox"/> Mismatched <input checked="" type="checkbox"/> Rogues <input checked="" type="checkbox"/> Users <input checked="" type="checkbox"/> Alerts Select All - Unselect All <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
Include device types:	
Display	
Use fully qualified domain names: Cisco IOS/Aruba/Alcatel-Lucent only	<input type="radio"/> Yes <input checked="" type="radio"/> No
Show vendor-specific device settings for:	All devices
Look up wireless user hostnames:	<input checked="" type="radio"/> Yes <input type="radio"/> No
DNS Hostname Lifetime:	24 hours
Device Troubleshooting Hint: Displayed along with the 'Down' reason if a device's upstream device is up.	
Device Configuration	
Guest User Configuration:	Enabled for devices in Manage (Read/Write)
Allow WMS offload configuration in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow disconnecting users while in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Keep unreferenced Aruba configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No
External Logging	
Syslog Server:	10.51.51.51
Syslog Port:	514
Include event log messages:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Event log facility:	local3
Include audit log messages:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Audit log facility:	local1
	Send Test Message
Historical Data Retention	
Inactive User Data (2-1500 days):	1500
User Association History (2-550 days):	30
Tag History (2-550 days):	14
Rogue AP Discovery Events (2-550 days): Cannot be smaller than the 'Delete Rogues not detected for' window (14) configured on the RAPIDS Setup page.	30
Reports (2-550 days):	14
Automatically acknowledge alerts (0-550 days, zero disables):	1
Acknowledged Alerts (2-550 days):	2
Traps from managed devices (0-550 days, zero disables):	2
Archived Device Configurations (1-100):	10
Guest Users (0-550 days, zero disables):	30
Closed Helpdesk Incidents (0-550 days, zero disables):	30
Inactive SSIDs (0-550 days, zero disables):	3
Inactive Interfaces (0-550 days, zero disables):	425
Interface Status History (0-550 days, zero disables):	425
Firmware Upgrade Defaults	
Allow firmware upgrades in monitor-only mode:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Simultaneous Jobs (1-20):	3
Simultaneous Devices Per Job (1-1000):	3
Failures before stopping (0-20, zero disables):	1
Additional AMP Services	
Enable FTP server: required to manage Cisco WLC and Aironet 4800 APs; optional for FTP upgrades on supported devices.	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable RTLS collector: Aruba/Alcatel-Lucent only	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use embedded mail server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Send Test Email
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Performance	
Monitoring Processes (1-4):	4
Maximum number of configuration processes (1-20):	4
Maximum number of audit processes (1-20):	4
Verbose logging of SNMP configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No
SNMP rate limiting for monitored devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
RAPIDS Processing Priority: When AWMS is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (e.g. client connections and bandwidth) is not adversely impacted.	Low
The default priority is Low. You can also tune your system performance by changing group poll periods.	
	Save Revert

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

1. Browse to the AMP Setup > General page, locate the General area, and enter the information described in Table 8:

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

Setting	Default	Description
System Name	AWMS	Defines your name for the AWMS server, with a maximum limit of 20 alphanumeric characters.
Automatically Monitor/Manage New Devices	No	<p>Launches a drop-down menu that specifies the behavior AWMS should follow when it discovers a new device. Devices are placed in the default group which is defined in the next field.</p> <ul style="list-style-type: none"> When devices are in Monitor Only mode, AWMS 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. When devices are in Manage Read/Write mode, AWMS 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 Managed Read/Write mode will overwrite the configuration with the desired configuration in AWMS, and should only be used when you are certain AWMS has the correct configuration. This can be risky, and generally, devices should be placed in Monitor Only mode as the default.
Default Group	NA	Sets the device group that this AWMS 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 Groups > List page to appear in this drop-down menu. For additional information, refer to Chapter 4, "Configuring and Using Device Groups in AWMS" on page 79 .
Device Configuration Audit Interval	Daily	<p>If enabled, this setting defines the interval of AWMS queries, in which each device compares actual device settings to the Group configuration policies stored in the AWMS database. If the settings do not match, the AP is flagged as mismatched and AWMS sends an alert via email, log, or SNMP.</p> <p>Aruba recommends enabling this feature with a frequency of Daily or more frequently to ensure that your AP configurations comply with your established policies.</p>
Automatically Repair Misconfigured Devices	Disabled	If enabled, this setting automatically reconfigures the settings on the device when the device is in Manage mode and AWMS detects a variance between actual device settings and the Group configuration policy in the AWMS database.
Send Debugging Messages to Aruba	Enabled	If enabled, AWMS automatically emails any system errors to the Dell Support Center to assist in debugging.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the time of day AWMS should perform daily maintenance. During maintenance, AWMS cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
AWMS User Authorization Lifetime (0-240 min)	120	Sets the amount of time, in minutes, that an AWMS user session lasts before the user must authenticate when a new browser window is opened. Setting the lifetime to 0 requires the user to log in every time a new browser window is opened.
Check Updates from Aruba	Yes	Enables AWMS to check automatically for multiple update types. Check daily for AWMS updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct internet connection via AWMS .

2. Select the **Top Header Stats** by checking the corresponding check box. The selected options will be displayed at the top of GUI. For more detailed information about each option, refer to [Table 5 on page 23](#).
3. On the **AMP Setup > General** page, locate the **Display Options** section and adjust settings as required. The **Display Options** section configures which **Group** tabs and options appear by default in new device groups.



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

[Table 9](#) describes the settings and default values in this section.

Table 9 *AMP Setup > General > Display Options Fields and Default Values*

Setting	Default	Description
Use Fully Qualified Domain Names	No	Sets AWMS 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.
Show Vendor-Specific Device Settings For	All Devices	Displays a drop-down menu that determines which Group 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"> • All Device—When selected, AWMS displays all Group tabs and setting options. • Only Devices on this AMP—When selected, AWMS hides all options and tabs that do not apply to the APs and devices currently on AWMS. • Selected device type—When selected, a new field appears listing many device types. This option allows you to specify the device types for which AWMS displays group settings. You can override this setting at the individual group level.
Look Up Wireless User Hostnames	Yes	Enables AWMS to look up automatically the DNS for new user hostnames. This setting can be turned off to troubleshoot performance issues.
DNS Hostname Lifetime	24 hours	Defines the length of time, in hours, for which a DNS server hostname remains valid on AWMS , after which AWMS refreshes DNS lookup. Select a time duration from the drop-down menu. Options are as follows: <ul style="list-style-type: none"> • 1 hour • 2 hours • 4 hours • 12 hours • 24 hours
AP Troubleshooting Hint	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.

4. On the **AMP Setup > General** page, locate the **Configuration Options** section and adjust settings as required. The settings in this field configure whether certain changes can be pushed to devices in **Monitor Only** mode. [Table 10](#) describes the settings and default values of this section.

Table 10 *AMP Setup > General > Configuration Options Section Fields and Default Values*

Setting	Default	Description
Guest User Configuration	Disabled	Enables or prevents guest users to/from pushing configurations to devices. Options are Disabled (default), Enabled for Devices in Manage (Read/Write) , Enabled for all Devices .

Table 10 AMP Setup > General > Configuration Options Section Fields and Default Values

Setting	Default	Description
Allow WMS offload configuration in monitor-only mode	No	When Yes is selected, you can enable the Dell PowerConnect W WMS offload feature on the Groups > Basic page for WLAN switches in Monitor Only mode. Enabling WMS offload does not cause a controller to reboot. This option is supported only for Aruba Networks and Dell PowerConnect W devices.
Desire all global Aruba Configuration	No	Allows AWMS to retain unused Dell PowerConnect W OS configuration profiles. You can define profiles on a WLAN switch but it is not necessary to reference them from a virtual AP configuration or other component of Dell PowerConnect W Configuration. Normally AWMS deletes unreferenced profiles, but this setting retains them when enabled with Yes . NOTE: If this setting is enabled with Yes , then all profiles are pushed to all controllers. In this case, you cannot have different configurations for different controllers.

- On the AMP Setup > General page, locate the **External Logging** section and adjust settings as required. Use this section to configure AWMS to send audit and system events to an external syslog server. [Table 11](#) describes these settings and default values.

Table 11 AMP Setup > General > External Syslog Section Fields and Default Values

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

- On the AMP Setup > General page, locate the **Historical Data Retention** section and specify the number of days you wish to keep client session records and rogue discovery events. [Table 12](#) describes the settings and default values of this section. Many settings can be set to have no expiration date, such that the information will remain in the AWMS indefinitely, as noted.

Table 12 AMP Setup > General > Historical Data Retention Fields and Default Values

Setting	Default	Description
Inactive User Data (2-1500 days)	60	Defines the number of days AWMS stores basic information about inactive users. Aruba recommends a shorter setting of 60 days for customers with high user turnover such as hotels or convention centers. The longer you store inactive user data, the more hard disk space you require.
User Association History (2-550 days)	14	Defines the number of days AWMS stores client session records. The longer you store client session records, the more hard disk space you require.
Tag History (2-550 days)	14	Sets the number of days AWMS retains location history for Wi-Fi tags.

Table 12 AMP Setup > General > Historical Data Retention Fields and Default Values (Continued)

Setting	Default	Description
Rogue AP Discovery Events (2-550 days)	14	Defines the number of days AWMS stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.
Reports (2-550 days)	60	Defines the number of days AWMS stores Reports. Large numbers of reports, over 1000, can cause the Reports > List page to be slow to respond.
Automatically Acknowledged Alerts (0-550 days, zero disables)	14	Defines automatically acknowledged alerts as the number of days AWMS 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 AWMS database.
Acknowledged Alerts (2-550 days)	60	Defines the number of days AWMS retains information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the System > Alerts page to be slow to respond.
Traps from managed devices (0-550 days, zero disables)	14	Defines the number of days AWMS retains information about SNMP traps from Managed Devices. Setting this value to 0 disables this function, and the trap information will never expire or be deleted from the AWMS database.
Archived Device Configurations (1-100)	10	Sets the number of archived configurations to retain for each device.
Guest Users (0-550 days, zero disables)	30	Sets the number of days that AWMS is to support any guest user. Setting this value to 0 disables this function, and guest users will never expire or be deleted from the AWMS database.
Closed Helpdesk Incidents (0-550 days, zero disables)	30	Sets the number of days that AWMS is to retain records of closed Helpdesk incidents once closed. Setting this value to 0 disables this function, and Helpdesk information will never expire or be deleted from the AWMS database.
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days AWMS retains historical information after AWMS last saw a client on a specific SSID. Setting this value to 0 disables this function, and inactive SSIDs will never expire or be deleted from the AWMS database.
Inactive Interfaces (0-550 days, zero disables)	425	Sets the number of days AWMS retains inactive interface information after the interface has been removed or deleted from the device. Setting this value to 0 disables this function, and inactive interface information will never expire or be deleted from the AWMS database.
Interface Status History (0-550 days, zero disables)	425	Sets the number of days AWMS retains historical information on interface status. Setting this value to 0 disables this function.

- On the AMP Setup > General page, locate the **Default Firmware Upgrade Options** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for AWMS. [Table 13](#) describes the settings and default values of this section.

Table 13 AMP Setup > General > Default Firmware Upgrade Options Fields and Default Values

Setting	Default	Description
Allow Firmware upgrades in Monitor Only mode	No	If yes is selected, AWMS upgrades the firmware for APs in Monitor Only mode. When AWMS upgrades the firmware in this mode, the desired configuration are not be pushed to AWMS . Only the firmware is applied. The firmware upgrade may result in configuration changes. AWMS does not correct those changes when the AP is in Monitor Only mode.
Simultaneous Jobs (1-20)	20	Defines the number of jobs AWMS runs at the same time. A job can include multiple APs.

Table 13 AMP Setup > General > Default Firmware Upgrade Options Fields and Default Values

Setting	Default	Description
Simultaneous Devices per Job (1-1000)	20	Defines the number of devices that can be in the process of upgrading at the same time. AWMS 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.
Failures Before Stopping (0-20)	1	Sets the default number of upgrade failures before AWMS pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to 0 disables this function.

- On the AMP Setup > General page, locate the Additional AMP Services section, and adjust settings as required. Table 14 describes the settings and default values of this section.

Table 14 AMP Setup > General > Additional AMP Services Fields and Default Values

Setting	Default	Description
Enable FTP Server	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.
Enable RTLS Collector	No	Enables or disables the RTLS Collector, which is used to allow AOS controllers to send RTLS packets to VisualRF. 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 and Aruba devices. With selection of Yes , the following additional fields appear: <ul style="list-style-type: none"> RTLS Port—Specify the port for the RTLS server. RTLS Username—Enter the user name supported by the RTLS server. RTLS Password—Enter the RTLS server password.
Use Embedded Mail Server	Yes	Enables or disables the embedded mail server that is included with AWMS . This field supports a Send Test Email button for testing server functionality. Clicking this button prompts you with a To and From field in which you must enter valid email addresses, and a button to send a test email.
Process User Roaming Traps from Cisco WLC	Yes	AMP now parses client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.
Enable AMON data collection	Yes	Allows AMP to collect enhanced data from Aruba devices on certain firmware versions; see the Aruba Best Practices Guide for more details.

- On the AMP Setup > General page, locate the Performance Tuning section. Performance tuning is unlikely to be necessary for many AWMS implementations, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Dell support if you think you might need to change any of these settings. Table 15 describes the settings and default values of this section.

Table 15 AMP Setup > General > Performance Tuning Fields and Default Values

Setting	Default	Description
Monitoring Processes	Based on the number of cores for your server	Optional setting configures the throughput of monitoring data. Increasing this setting allows AWMS to process more data per second, but it can take resources away from other AWMS processes. Please contact Dell support if you think you might need to increase this setting for your network.

Table 15 AMP Setup > General > Performance Tuning Fields and Default Values (Continued)

Setting	Default	Description
Maximum Number of Configuration Processes	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. Please contact Dell support if you think you might need to increase this setting for your network.
Maximum Number of Audit Processes	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 Dell support if you are considering increasing this setting for your network.
Verbose Logging of SNMP Configuration	No	Enables or disables logging detailed records of SNMP configuration information.
SNMP Rate Limiting for Monitored Devices	No	Enables or disables a maximum bandwidth consumption threshold for each port for monitored devices. This setting prevents unnecessary SNMP traffic from compromising device performance. Aruba recommends enabling this setting when monitoring Aruba controllers.
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to AWMS as a whole. When AWMS 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) are not adversely impacted. The default priority is Low . You can also tune your system performance by changing group poll periods.

10. Click Save when the **General Server** settings are complete and whenever making subsequent changes.

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Defining AWMS Network Settings

The next step in configuring AWMS is to confirm the AMP network settings. Define these settings by navigating to the AMP Setup > Network page. [Figure 19](#) illustrates the contents of this page.

Figure 19 AMP Setup > Network Page Illustration

Perform the following steps to define the AWMS 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 16](#) describes the settings and default values.

Table 16 Primary and Secondary Network Interface Fields and Default Values

Setting	Default	Description
IP Address	None	Sets the IP address of the AWMS network interface. This address must be static IP address.
Hostname	None	Sets the DNS name assigned to the AWMS server.
Subnet Mask	None	Sets the subnet mask for the AWMS primary network interface.
Gateway	None	Sets the default gateway for the AWMS network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the AWMS network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the AWMS network interface.
Secondary Network Interface	No	Select Yes 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 AWMS and your network reference NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.

Note: Specifying NTP servers is optional. NTP servers synchronize the time on the AWMS server, not on individual access points. Secondary network interface options may include multiple telnet terminal configurations, DHCP/BOOTP auto-configuration, time zone offsets, daylight savings time, and NTP addressing modes such as unicast, broadcast, and multicast. Secondary NTP information is only supported on AWMS that have multiple interfaces.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between AWMS and the NTP servers creates an entry in the event log. [Table 17](#) describes the settings and default values in more detail.

Table 17 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 Network Time Protocol server.
Secondary	ntp2.yourdomain.com	Sets the IP address or DNS name for the secondary Network Time Protocol 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.



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

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

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Creating AWMS Users

AWMS installs with only one AMP user—the administrator or *admin* user. The admin user has these parameters authorizations within AWMS:

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

For each general user that you add, you define a Username, Password and a Role. You use the username and password when logging into AWMS. It is helpful to use unique and meaningful user names as they are recorded in the log files when you or other users make changes in AWMS.



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

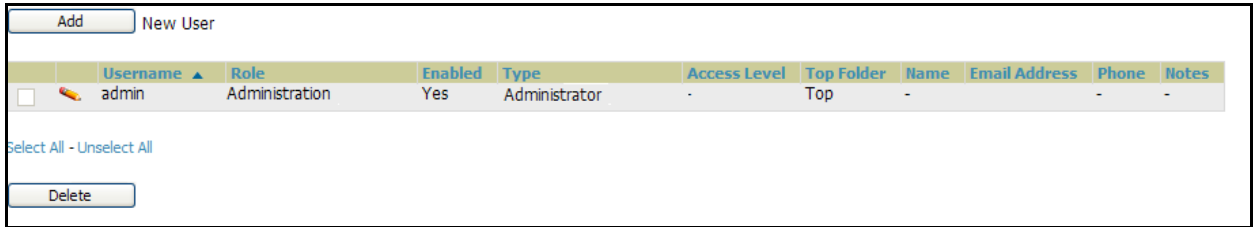
The user role defines the user type, access level, and the top folder for that user. User roles are defined on the **AMP Setup > Roles** page. Refer to the next procedure in this chapter for additional information, [“Creating AWMS User Roles” on page 50](#).

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 AWMS users of any privilege level. You must be an admin user to complete these steps.

1. Navigate to the **AMP Setup > Users** page. This page displays all users currently configured in AWMS. [Figure 20](#) illustrates the contents and layout of this page.

Figure 20 AMP Setup > Users Page Illustration



2. Click **Add** to create a new user, click the pencil icon to edit an existing user, or select a user and click **Delete** to remove that user from AWMS. When you click **Add** or the edit icon, the **Add User** page appears, illustrated in [Figure 21](#).

Figure 21 AMP Setup > Users > Add/Edit User Page Illustration

3. Enter or edit the settings on this page. [Table 18](#) describes these settings in additional detail.

Table 18 AMP Setup > User > Add/Edit User Fields and Default Values

Setting	Default	Description
Username	None	Sets the username as an alphanumeric string. The Username is used when logging in to AWMS and appears in AWMS log files.
Role	None	Specifies the User Role that defines the Top viewable folder, type and access level of the user specified in the previous field. The admin user defines user roles on the AMP Setup > Roles page, and each user in the system is assigned to a role.
Password	None	Sets the password for the user being created or edited. Enter an alphanumeric string without spaces, and enter the password again in the Confirm Password field. Because the default user's password is identical to the name, Aruba strongly recommends that you change this password. Aruba strongly recommends that you immediately change the default AWMS " admin " password for admin users.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.
Email Address	None	Allows you to specify a specific email address that will propagate throughout many additional pages in AWMS for that user, including reports, triggers, and alerts.
Phone	None	Allows you to enter an optional phone number for the user.
Notes	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.

- Click **Add** to create the new user, click **Save** to retain changes to an existing user, or click **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 additional AWMS pages and functions relevant to that user.

Note: AWMS 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 AWMS deployment, such as help desk or IT staff.



In prior AWMS versions, user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now 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.

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Creating AWMS User Roles

The **AMP Setup > Roles** page defines the viewable devices, the operations that can be performed on devices, and general AWMS access. **VisualRF** uses the same user roles as defined for AWMS—users can see floor plans that contain an AP to which they have access in AWMS, 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. When a new role is added to AWMS, **VisualRF** must be restarted for the new user to be enabled. Refer to the *VisualRF User Guide* 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 AWMS deployment. In prior AWMS releases, AWMS user roles could only be assigned to a single top folder (such as "West Coast" or "European Stores"). 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**:

- Navigate to the **AMP Setup > Roles** page. This page displays all roles currently configured in AWMS. [Figure 22](#) illustrates the contents and layout of this page.

Figure 22 AMP Setup > Roles Page Illustration

		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

- Click **Add** to create a new role, click the pencil icon to edit an existing role, or select a role and click **Delete** to remove that role from AWMS. When you click **Add** or the edit icon, the **Add Role** page appears, illustrated in [Figure 23](#).

Figure 23 AMP Setup > Roles > Add/Edit Role Page Illustration

3. Enter or edit the settings on this page. [Table 18](#) 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 AWMS. [Table 19](#) describes the settings and default values of this section.

Table 19 AMP Setup > Roles > Add/Edit Roles Fields and Default Values

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. Aruba recommends that the role name give an indication of the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AWMS.
Type	AP/Device Manager	Defines the type of role. AWMS supports the following role types: <ul style="list-style-type: none"> ● AMP Administrator—The AWMS Administrator has full access to AWMS and all of the devices. The administrator can view and edit all settings and all APs in AWMS. Only the AWMS Administrator can create new Users or access the AMP Setup page. ● AP/Device Manager—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. ● Aruba Management Client—Defines the AWMS user. The user information defined in AMC must match the user with the Aruba Management Client type. ● Guest Access Sponsor—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.

Table 19 AMP Setup > Roles > Add/Edit Roles Fields and Default Values (Continued)

Setting	Default	Description
AP/Device Access Level	None	<p>Defines the privileges the role has over the viewable APs. AWMS supports three privilege levels, as follows:</p> <ul style="list-style-type: none"> ● Manage (Read/Write)—Manage users have read/write access to the viewable devices and Groups. They can change all AWMS settings for the devices and Groups they can view. ● Audit (Read Only)—Audit users have read only access to the viewable devices and Groups. Audit users have access to the APs/Devices > Audit page, which may contain sensitive information including AP passwords. ● Monitor (Read Only)—Monitor users have read-only access to devices and groups. Monitor users cannot view the APs/Devices > Audit page which may contain sensitive information, including AP passwords. Monitor-only users also have read-only access to VisualRF.
Top Folder	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>NOTE: AWMS 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 <i>a subset of accounts or sites</i> within a single AWMS deployment, such as help desk or IT staff.</p> <p>Prior to Version 6.3, AWMS user roles could be assigned only to a single top folder, such as "West Coast" or "European Stores", for example. User roles can now 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>
RAPIDS	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"> ● None—Cannot view the RAPIDS tab or any Rogue APs. ● Read Only—The user can view the RAPIDS pages but cannot make any changes to rogue APs or perform OS scans. ● Read/Write—The user may ignore, delete, override scores and perform OS scans.
Helpdesk	No	Sets the role to support helpdesk users, with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network.
Enable Adobe Flash	Yes	<p>Enables the Adobe Flash application for all users who are assigned this role. Adobe Flash supports dynamic graphics on the Home > Overview page, VisualRF, Quickview functions, and additional AWMS pages.</p> <p>NOTE: This field is only visible if a specific flag is set in the AWMS database. By default this option is hidden and flash is enabled for all users.</p>
Guest User Preferences	Allow accounts with no expiration	AMP Administrators can configure AP/Device Manager roles with read/write access to allow guest user accounts with no expiration, allow a sponsor to change the sponsorship name, and print a custom message with the guest user badge.

What Next?

- Navigate to additional tabs in the AMP Setup section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Enabling AWMS to Manage Your Devices

Once AWMS is installed and active on the network, the next task is to define the basic settings that allow AWMS 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 Airespace/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 AWMS \(Optional\)](#)
 - [Overview of the Device Setup > Upload Files Page](#)
 - [Loading Firmware Files to AWMS](#)
 - 📄 [Overview of the Device Setup > Upload Files Page](#)
 - 📄 [Loading Firmware Files to AWMS](#)
 - 📄 [Using Web Auth Bundles in AWMS](#)

Configuring Communication Settings for Discovered Devices

To configure AWMS 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 24](#).

Figure 24 Device Setup > Communication Page Illustration

Default Credentials	
The credentials below are used to communicate with devices that are discovered by OV3600 (regardless of the credentials used for discovery). Changing these credentials does not affect APs that are already being managed or are already in the <i>New Devices</i> list.	
3Com	Edit View
3Com 8750	Edit View
Alcatel-Lucent	Edit View
Apple AirPort Graphite Base Station	Edit View
Aruba	Edit View
Avaya	Edit View
BelAir	Edit View
Cisco Aironet 4800	Edit View
Cisco IOS	Edit View
Cisco Switch	Edit View
Cisco VxWorks	Edit View
Cisco WLC	Edit View
Colubris	Edit View
Compaq WL400	Edit View
Custom Device	Edit View
Enterasys	Edit View
Enterasys RoamAbout AP2000	Edit View
Enterasys RoamAbout AP3000/AP4102	Edit View
Enterasys RoamAbout R2	Edit View
Foundry	Edit View
Funkwerk Artem W-1000	Edit View
HP	Edit View
HP ProCurve 420	Edit View
HP ProCurve 520WL	Edit View
HP ProCurve 530	Edit View
HP Wireless Service Module	Edit View
Hirschmann	Edit View
Intel	Edit View
Intermec	Edit View
Juniper NetScreen 5GT	Edit View
LANCOM	Edit View
Lucent/ORINOCO	Edit View
Meru	Edit View
Motorola	Edit View
NEC	Edit View
Nomadix	Edit View
Nortel	Edit View
Proxim MP.11	Edit View
Proxim WIMAX	Edit View
Router/Switch	Edit View
Siemens Scalance W788 PRO	Edit View
Symbol	Edit View
Symbol Wireless Switch	Edit View
Systimax AirSpeed AP542	Edit View
Teklogix	Edit View
Trapeze	Edit View
Tropos	Edit View
Universal Network Device	Edit View
Vivato	Edit View

SNMPv3 Informs	
SNMPv3 User	
Username:	<input type="text"/>
Auth Protocol:	SHA <input type="button" value="v"/>
Auth Passphrase:	<input type="text"/>
Confirm Auth Passphrase:	<input type="text"/>
Priv Protocol:	DES <input type="button" value="v"/>
Priv Passphrase:	<input type="text"/>
Confirm Priv Passphrase:	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	
Telnet/SSH Settings	
Telnet/SSH Timeout (3-120 sec):	<input type="text" value="10"/>
HTTP Discovery Settings	
HTTP Timeout (3-120 sec):	<input type="text" value="5"/>
ICMP Settings	
Attempt to ping devices that were unreachable via SNMP:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Colubris Administration Options	
<input checked="" type="radio"/> Do not modify security/HTTPS settings <input type="radio"/> Replace existing user with specified user	
Cisco Aironet VxWorks User Creation Options	
<input checked="" type="radio"/> Do not modify security/SNMP settings <input type="radio"/> Create and use a specified user	
Symbol 4131/Intel 2011B, Cisco Aironet IOS and Nomadix AG2000w SNMP Initialization	
<small>Upon authorization into read-write manage mode, OV3600 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.</small>	
<input checked="" type="radio"/> Do not modify SNMP settings <input type="radio"/> Enable read-write SNMP	
<input type="button" value="Save"/> <input type="button" value="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.



Note: Community strings and shared secrets must have read-write access for AWMS to configure the devices. Without read-write access, AWMS 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** area, and enter or revise the following information. [Table 20](#) lists the settings and default values.

Table 20 *Device Setup > Communication > SNMP Settings Fields and Default Values*

Setting	Default	Description
SNMP Timeout	3	Sets the time, in seconds, that AWMS waits for a response from a device after sending an SNMP request.
SNMP Retries	3	Sets the number of times AWMS tries to poll a device when it does not receive a response within the SNMP Timeout period. If AWMS does not receive an SNMP response from the device after the specified number of retries, AWMS classifies that device as Down.

3. On the **Device Setup > Communication** page, locate the **SNMP v3 Informs** section. Click **Add New SNMP v3 User** button to reveal an **SNMP v3 User** configuration section. AMP users will need to configure all v3 users that are configured on the controller; SNMP traps will be restarted when users are changed or added to the controller.
 - **Username** - Username of the SNMP v3 user as configured on the controller. There is no default username.
 - **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. There is no default passphrase.
 - **Priv Protocol** - Can be DES or AES. The default setting is DES.
4. On the **Device Setup > Communication** page, locate the **Telnet/SSH Settings** section, and complete or adjust the default value for the field in this section. [Table 21](#) lists the setting and default value.

Table 21 *Telnet/SSH Settings Fields and Default Values*

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

5. On the **Device Setup > Communication** page, locate the **HTTP Discovery Settings** section. Complete or revise the default values for the settings in this section. [Table 22](#) lists these settings and default values.

Table 22 *HTTP Discovery Settings Fields and Default Values*

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

- On the **Device Setup > Communication** page, locate the **ICMP Settings** section. Complete the settings or revise the default values as required. [Table 23](#) itemizes the setting and default value of this section.

Table 23 Device Setup > Communication > ICMP Settings Fields and Default Values

Setting	Default	Description
Attempt to ping down devices	Yes	<p>Enables a function that applies when an AP is unreachable over SNMP.</p> <ul style="list-style-type: none"> When Yes is selected, this option has AWMS attempt to ping the AP device. Select No 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. <p>NOTE: If ICMP is disabled on the network, select No to avoid the performance penalty caused by numerous ping requests.</p>

- On the **Device Setup > Communication** page, locate the **Colubris Administration Options** section. You only need to provide this information if you use Colubris APs on your network. Select one of the options listed. [Figure 25](#) illustrates this section and [Table 24](#) explains related fields.

Figure 25 Device Setup > Communication > Colubris Administration Options Section Illustration

Table 24 Colubris Administration Options Fields and Default Values

Setting	Default	Description
Do not modify security/HTTPS settings	N/A	Enables AWMS to use only an existing user account on the AP. This user account must have all permissions set. The user accounts are defined in the Colubris Username/Password section in the Default Secrets area.
Replace existing user with specified user	Disabled	When enabled, this setting allows you to define a new Colubris username and password on each Colubris AP.
New Colubris Username and Password	N/A	Specifies the username and password to be used only if the option Replace existing user with specified user is selected.

- On the **Device Setup > Communication** page, locate the **Cisco Aironet VxWorks User Creation Options** section. You only need to provide this information if you use VxWorks-based Cisco APs on your network, as follows:
 - Aironet 340
 - Aironet 350
 - Aironet 1200

Select one of the three options listed. [Table 25](#) describes the settings and default values of this section.

Table 25 Cisco Aironet VxWorks User Creation Options Fields and Default Values

Setting	Default	Description
Do Not Modify Security/SNMP Settings	N/A	Enables AWMS using only an existing user account on the AP, as defined in the Cisco VxWorks Username/Password section in the Default Secrets area. This user account must have all permissions set.
Create and Use Specified User	N/A	Enables AWMS to create a new user account, specified below, on each AP, with all permissions enabled.

9. On the Device Setup > Communication page, locate the Symbol 4131/Intel 2011b and Cisco Aironet IOS SNMP Initialization area. You only need to provide this information if you use Symbol 4131, Intel 2011b, or Cisco Aironet IOS access points. Select one of the options listed. [Table 26](#) describes the settings and default values.

Table 26 Device Setup > Communications Fields and Default Values

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

Loading Device Firmware onto AWMS (Optional)

Overview of the Device Setup > Upload Files Page

AWMS 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 AWMS for distribution to devices via the **Device Setup > Upload Files** page.

Figure 26 illustrates the **Upload Files** page, which lists all firmware files on AWMS 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 AWMS on this **Upload File** page appear as options in the drop-down menus on the **Group > Firmware** page and on individual **AP/Device > Manage** pages. These firmware files can be applied automatically to devices through AWMS.
- Use the **AMP Setup** page to configure AWMS-wide default firmware options.

Figure 26 *Device Setup > Upload Files Page Illustration*

Type	Owner Role	Description	Server Protocol	Use Group File Server	Firmware Filename	Firmware Version
Aruba 3xxx	AMP Administration	Aruba OS version 3.3.2.10 for Aruba 3xxx	TFTP	Disabled	ArubaOS_MMC_3_3_2_10_20355_0.bin	3.3.2.10
Avaya AP-3	AMP Administration	-	TFTP	Disabled	AV_AP3_bin_0	2.3.3
Avaya AP-3	AMP Administration	-	TFTP	Disabled	AV_AP3_R245_bin_0	2.4.5
Avaya AP-3	AMP Administration	-	TFTP	Disabled	AV_AP3_2_1_0_bin_0	2.1.0
Avaya AP-3	AMP Administration	-	TFTP	Disabled	OR_AP2K_bin_0.bin	2.4.4

Firmware MDS Checksum	Firmware File Size	HTML Filename	HTML Version	HTML MDS Checksum	HTML File Size	Desired Firmware File for Specified Group
662ee818feb4bbcd279ec9c7b3cccdad	31,616,820 bytes	-	-	-	-	-
fc965b9c3cd8191d51deeb31000a9e39	1,485,568 bytes	-	-	-	-	-
6ff4d266dbd76e787ad5c6c7a0211b16	1,780,992 bytes	-	-	-	-	Acme Corporation, Global Corporate PC
cd72cd99de90550cee1f41adede0c365	3,681,741 bytes	-	-	-	-	-
fs9bd897f9415a37ce1419b2a817639c	1,781,760 bytes	-	-	-	-	-

Table 27 below itemizes the contents, settings, and default values for the **Upload Files** page.

Table 27 *Device Setup > Upload Files Fields and Default Values*

Setting	Default	Description
Type	None	Displays a drop-down list of the primary AP makes and models that AWMS supports with automated firmware distribution.
Owner Role	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.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server.
Use Group File Server	None	Displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to AWMS and to be transferred to an AP when the file is used in an upgrade.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.

Table 27 Device Setup > Upload Files Fields and Default Values (Continued)

Setting	Default	Description
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to AWMS. The MD5 checksum is used to verify that the file was uploaded to AWMS without issue. The checksum should match the checksum of the file before it was uploaded.
Firmware File Size	None	Displays the size of the firmware file in bytes.
HTML Filename	None	Supporting HTML, displays the name of the file that was uploaded to AWMS and to be transferred to an AP when the file is used in an upgrade.
HTML Version	None	Supporting HTML, displays the version of HTML used for file transfer.
HTML MD5 Checksum	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to AWMS. The MD5 checksum is used to verify that the file was uploaded to AWMS without issue. The checksum should match the checksum of the file before it was uploaded.
HTML File Size	None	Supporting HTML, displays the size of the file in bytes.
Desired Firmware File for Specified Groups	None	The firmware file is set as the desired firmware version on the Groups > Firmware Files 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 AWMS

Perform the following steps to load a device firmware file onto AWMS.

1. Browse to the **Device Setup > Upload Files** page.
2. From the **Upload Files** page, click the **Add** button. The **Add Firmware File** dialog box appears. [Figure 27](#) illustrates this page.

Figure 27 Device Setup > Upload Files > Add New Firmware Page Illustration

3. Click the **Supported Firmware Versions and Features** link to view a list of supported firmware versions.




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

4. Enter the appropriate information and click the **Add** button. The file uploads to AWMS and once complete, this file appears on the **Device Setup > Upload Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **AP/Device > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. [Table 28](#) itemizes the settings of this page.

Table 28 Supported Firmware Versions and Features Fields and Default Values

Setting	Default	Description
Type	None	Indicates the firmware file is used with the specified type. If you select an IOS device from the Type drop-down menu, you have the option of choosing a server protocol of TFTP or FTP. If you choose FTP you may 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.
Firmware Version	None	Provides a user-configurable field to specify the firmware version number.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware)	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 File Server IP Address and the Firmware Filename .
Use an external firmware file server	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 Groups > Firmware page. Complete the Firmware File Server IP Address field. NOTE: 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, AWMS uses an anonymous user for file upload.
Use Group File Server	Disabled (not selected)	If you opt to use an external firmware file server, this additional option appears. This setting instructs AWMS to use the server that is associated with the group instead of defining a server.
TFTP Server IP	None	Provides the IP address of the External TFTP Server (like SolarWinds) that is used for the firmware upgrade. This option displays when the user selects Use a Different TFTP server option.
Firmware Filename	None	Enter the filename of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. Click the Browse button to locate the appropriate Intel or Symbol HTML firmware file on your network.

 **Note:** Additional fields may appear for multiple device types. AWMS 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 AWMS for the firmware to be distributed successfully via AWMS.

- Click **Add** to import the firmware file.
- To delete a firmware file that has already been uploaded to AWMS, return to the **File Upload** page, select the checkbox for the firmware file and click **Delete**.

 **Note:** 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 AWMS

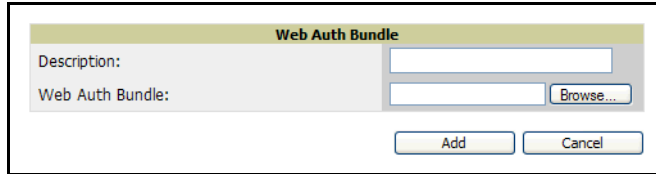
Web authentication bundles are configuration files that support Cisco Airespace/WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco Airespace/WLC devices.

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

1. Navigate to the **Device Setup > Upload Files** page. This page displays any existing Web Auth bundles that are currently configured in AWMS, and allows you to add or delete Web Auth bundles.
2. Scroll to the bottom of the page. Click **Add New Web Auth Bundle** to create a new Web Auth bundle, or click 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 clicking **Delete**.

When you add or edit a Web Auth bundle, the **Web Auth Bundle** page appears, as illustrated in [Figure 28](#).

Figure 28 Add Web Auth Bundle Page Illustration



The screenshot shows a form titled "Web Auth Bundle". It contains two text input fields: "Description:" and "Web Auth Bundle:". The "Web Auth Bundle:" field has a "Browse..." button next to it. At the bottom of the form, there are two buttons: "Add" and "Cancel".

3. Enter a descriptive label in the description field. This is the label by which you identify and track Web Auth bundles on the **Device Setup > Upload Files** page once they are present in AWMS.
4. Enter the path and filename of the Web Auth configuration file in the **Web Auth Bundle** field. Click **Browse** to locate the file with the browsing method, as required.
5. Click **Add** to complete the Web Auth bundle creation, or click **Save** if replacing a previous Web Auth configuration file, or click **Cancel** to abort the Web Auth integration.
6. The **Device Setup > Upload files** page displays your changes.

For additional information and a case study that illustrates the use of Web Auth bundles with Cisco Airespace/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

Configuring TACACS+ and RADIUS Authentication

As an optional configuration, you can set AWMS to use an external user database to simplify password management for AWMS administrators and users. This section contains the following procedures:

- [Configuring TACACS+ Authentication](#)
- [Configuring RADIUS Authentication and Authorization](#)
- [Integrating a RADIUS Accounting Server](#)

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 AWMS users, and does not affect APs or users logging into APs. Perform these steps to configure TACACS+ authentication:

1. Navigate to the **AMP Setup > Authentication** page. This page displays current status of TACACS+. [Figure 29](#) illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in AWMS.

Figure 29 AMP Setup > Authentication Page Illustration

The screenshot displays two configuration sections: TACACS+ Configuration and RADIUS Configuration. Each section has a header and a set of fields. In the TACACS+ section, 'Enable TACACS+ Authentication and Authorization' is set to 'Yes'. The 'Primary Server Hostname/IP Address' is 'tacacs.aire.com', 'Primary Server Port' is '49', and 'Primary Server Secret' and 'Confirm Primary Server Secret' are both masked with dots. The 'Secondary Server Hostname/IP Address' is empty, 'Secondary Server Port' is '49', and 'Secondary Server Secret' and 'Confirm Secondary Server Secret' are empty. The RADIUS section has 'Enable RADIUS Authentication and Authorization' set to 'Yes'. The 'Primary Server Hostname/IP Address' is '10.200.200.200', 'Primary Server Port' is '1645', and 'Primary Server Secret' and 'Confirm Primary Server Secret' are both masked with dots. The 'Secondary Server Hostname/IP Address' is empty, 'Secondary Server Port' is '1812', and 'Secondary Server Secret' and 'Confirm Secondary Server Secret' are empty.

2. Click **No** to disable or **Yes** to enable TACACS+ authentication. If you click **Yes**, several new fields appear. Complete the fields described in [Table 29](#).

Table 29 AMP Setup > Authentication Fields and Default Values

Field	Default	Description
Primary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the primary TACACS+ server.
Primary Server Port	1812	Enter the port for the primary TACACS+ server.
Primary Server Secret	N/A	Specify the primary shared secret for the primary TACACS+ server, and confirm in the Confirm field.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary TACACS+ server.

Table 29 AMP Setup > Authentication Fields and Default Values (Continued)

Field	Default	Description
Secondary Server Port	1812	Enter the port for the secondary TACACS+ server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary TACACS+ server.

3. Click **Save** to retain these configurations, and continue with additional steps.
 4. To configure Cisco ACS to work with AWMS, 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.
 - Click **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, AWMS does not need to know usernames.
6. AWMS also needs to be configured as an AAA client.
 - On the **Network Configuration** page, click **Add Entry** to add an AAA client.
 - Enter the IP address of AWMS as the **AAA Client IP Address**.
 - The secret should be the same value that was entered on the **AMP Setup > TACACS+** page.
 7. Select **TACACS+ (Cisco IOS)** in the **Authenticate Using** drop down menu and click **submit + restart**.



Note: AWMS 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 AWMS server. The only recommended user is the backup administrator, in the event that the TACAS+ server goes down.

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS 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:

1. Navigate to the **AMP Setup > Authentication** page. This page displays current status of RADIUS. [Figure 30](#) illustrates this page when neither TACACS+ nor RADIUS authentication is enabled in AWMS.

Figure 30 AMP Setup > Authentication Page Illustration

The screenshot shows two configuration sections: TACACS+ Configuration and RADIUS Configuration. Each section has a radio button to enable or disable authentication and authorization, followed by input fields for primary and secondary server details.

TACACS+ Configuration	
Enable TACACS+ Authentication and Authorization:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Primary Server Hostname/IP Address:	<input type="text" value="tacacs.aire.com"/>
Primary Server Port:	<input type="text" value="49"/>
Primary Server Secret:	<input type="password" value="....."/>
Confirm Primary Server Secret:	<input type="password" value="....."/>
Secondary Server Hostname/IP Address:	<input type="text"/>
Secondary Server Port:	<input type="text" value="49"/>
Secondary Server Secret:	<input type="password"/>
Confirm Secondary Server Secret:	<input type="password"/>

RADIUS Configuration	
Enable RADIUS Authentication and Authorization:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Primary Server Hostname/IP Address:	<input type="text" value="10.200.200.200"/>
Primary Server Port:	<input type="text" value="1645"/>
Primary Server Secret:	<input type="password" value="....."/>
Confirm Primary Server Secret:	<input type="password" value="....."/>
Secondary Server Hostname/IP Address:	<input type="text"/>
Secondary Server Port:	<input type="text" value="1812"/>
Secondary Server Secret:	<input type="password"/>
Confirm Secondary Server Secret:	<input type="password"/>

2. Click **No** to disable or **Yes** to enable TACACS+ nor RADIUS authentication. If you click **Yes**, several new fields appear. Complete the fields described in [Table 30](#).

Table 30 AMP Setup > Authentication Fields and Default Values

Field	Default	Description
Primary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the primary RADIUS server.
Primary Server Port	49	Enter the TCP port for the primary RADIUS server.
Primary Server Secret	N/A	Specify the primary shared secret for the primary RADIUS server, and confirm in the Confirm field.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
Secondary Server Port	49	Enter the TCP port for the secondary RADIUS server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary RADIUS server.

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

Integrating a RADIUS Accounting Server



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

As an optional configuration, AWMS supports RADIUS server accounting. Use the **AMP Setup > RADIUS Accounting** page enables this configuration. This capability is not required for basic AWMS operation, but can increase the user-friendliness of AWMS administration in large networks. [Figure 31](#) illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable AWMS to receive accounting records from a separate RADIUS server. [Figure 31](#) illustrates the display of RADIUS accounting clients already configured, and [Figure 32](#) illustrates the Add RADIUS Accounting Client page.

Figure 31 AMP Setup > RADIUS Accounting Page Illustration

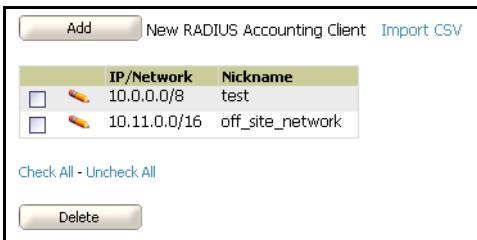


Figure 32 AMP Setup > RADIUS > Add RADIUS Accounting Client Page Illustration

1. To specify the RADIUS authentication server or network, browse to the **AMP Setup > RADIUS Accounting** page and click **Add**, illustrated in [Figure 32](#), and provide the information described in [Table 31](#).

Table 31 AMP Setup > Radius Accounting Fields and Default Values

Setting	Default	Description
Nickname	None	Sets a user-defined name for the authentication server.
IP/Network	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).
(Confirm) Shared Secret	None	Sets the Shared Secret that is used to establish communication between AWMS and the RADIUS authentication server.

2. Click **Add**.

What Next?

- For additional information about configuring WLAN Gateways or WLAN controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to [“Third-Party Security Integration for AWMS” on page 305](#).

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Configuring Cisco WLSE and WLSE Rogue Scanning

The Cisco Wireless LAN Solution Engine (WLSE) includes rogue scanning functions that AWMS 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 AWMS](#)
- [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 AWMS to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. [Table 32](#) describes these components.

Table 32 Cisco SWAN Architecture Components

SWAN Component	Requirements
WDS (Wireless Domain Services)	<ul style="list-style-type: none"> • WDS Name • Primary and backup IP address for WDS devices (IOS AP or WLSM) • WDS Credentials APs within WDS Group <p>NOTE: 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>
WLSE (Wireless LAN Solution Engine)	<ul style="list-style-type: none"> • IP Address • Login
ACS (Access Control Server)	<ul style="list-style-type: none"> • IP Address • Login
APs	<ul style="list-style-type: none"> • APs within WDS Group

Configuring WLSE Initially in AWMS

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

- [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

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

Enabling Rogue Alerts for Cisco WLSE

1. Navigate to the **Faults > Network Wide Settings > Rogue AP Detection** page.
2. Select the **Enable** toggle.
3. Click **Apply**.

Additional information about rogue device detection is available in [“Configuring Cisco WLSE Rogue Scanning” on page 69](#).

Configuring WLSE to Communicate with APs

1. Navigate 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. Navigate 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.



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

Use these pages to make such configurations:

1. Navigate 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. AWMS 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 AWMS' CDP, SNMP scanning, and HTTP scanning discovery for Cisco IOS access points. Perform these steps for inventory reporting.

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

Defining Access

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

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

Grouping

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

1. Navigate 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.



Note: 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. Navigate to the **Wireless Services > AP** page.
3. Click **Enable participation in SWAN Infrastructure**.
4. Click **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. Navigate 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. Navigate to the **Security > Server Manager** page.
5. Enter the **IP address** and **Shared Secret** for the ACS server.
6. Click the **Apply** button.
7. Navigate to the **Wireless Services > WDS > Server Group** page.
8. Enter the WDS Group of AP.
9. Select the ACS server in the **Priority 1** drop-down menu.
10. Click the **Apply** button.

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. Navigate to the **System Configuration > ACS Certificate Setup** page.
3. Install a New Certificate by clicking the **Install New Certificate** button, or skip to the next step if the certificate was previously installed.
4. Click the **User Setup** button in the left frame.
5. Enter the **Username** that will be used to authenticate into the WDS and click **Add/Edit** button.
6. Enter the **Password** that will be used to authenticate into the WDS and click the **Submit** button.
7. Navigate 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 click the **Submit** button.

For additional and more general information about ACS, refer to [“Configuring ACS Servers” on page 71](#).

Configuring Cisco WLSE Rogue Scanning

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

[Figure 33](#) illustrates and itemizes the AWMS settings for communication that is enabled between AWMS and WLSE.

Figure 33 *AMP Setup > WLSE > Add WLSE Page Illustration*

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

- To add a Cisco WLSE server to AWMS, navigate to the **AMP Setup > WLSE** page and click **Add**. Complete the fields in this page. [Table 33](#) describes the settings and default values.

Table 33 AMP Setup > WLSE Fields and Default Values

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

- After you have completed all fields, click the **Save** button. AWMS 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 > Rogue** page.

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Configuring ACS Servers

This is an optional configuration. The **AMP Setup > ACS** page allows AWMS to poll one or more Cisco ACS servers for wireless username information. When you specify an ACS server, AWMS gathers information about your networks wireless users. Refer to the [“Configuring TACACS+ and RADIUS Authentication” on page 62](#) section if you want to use your ACS server to manage your AWMS users.

Perform these steps to configure ACS servers:

1. Navigate to the **AMP Setup > ACS** page. This page displays current ACS information, as illustrated in [Figure 34](#).

Figure 34 AMP Setup > ACS Page Illustration

The screenshot shows the 'AMP Setup > ACS' page. At the top, there is an 'Add' button and the text 'New ACS Server'. Below this, it says 'Enter one or more Cisco ACS servers to be polled for wireless username information.' There is a pagination indicator '1-1 of 1 ACS Servers Page 1 of 1'. A table with the following columns is displayed: Hostname/IP Address, Protocol, Port, Username, Polling Period, Last Contacted, and Errors. The table contains one entry: Hostname/IP Address: 10.1.11.1, Protocol: HTTP, Port: 2002, Username: stuff, Polling Period: 10 minutes, Last Contacted: 5/14/2009 6:37 AM. Below the table, there is a 'Select All - Unselect All' link and a 'Delete' button.

2. Click **Add** to create a new ACS server, or click a pencil icon to edit an existing server. To delete an ACS server, select that server and click **Delete**. When clicking **Add** or edit, the **Details** page appears, as illustrated in [Figure 35](#).

Figure 35 AMP Setup > ACS > Add/Edit Details Page Illustration

The screenshot shows the 'ACS Server' details page. It has a title bar 'ACS Server'. The fields are: Hostname/IP Address (text input), Protocol (dropdown menu with 'HTTP' selected), Port (text input with '2002'), Username (text input), Password (text input), Confirm Password (text input), and Polling Period (dropdown menu with '10 minutes' selected). At the bottom, there are 'Add' and 'Cancel' buttons.

3. Complete the settings on the **AMP Setup > ACS > Add/Edit Details** page. [Table 34](#) describes these fields:

Table 34 AMP Setup > ACS > Add/Edit Details Fields and Default Values

Field	Default	Description
IP/Hostname	None	Sets the DNS name or the IP address of the ACS Server.
Protocol	HTTP	Launches a drop-down menu specifying the protocol AWMS uses when it polls the ACS server.
Port	2002	Sets the port through which AWMS communicates with the ACS. AWMS generally communicates via SNMP traps on port 162.
Username	None	Sets the Username of the account AWMS uses to poll the ACS server.
Password	None	Sets the password of the account AWMS uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently AWMS polls the ACS server for username information.

4. Click **Add** to finish creating the new ACS server, or click **Save** to finish editing an existing ACS server.
5. The ACS server must have logging enabled for passed authentications. To configure your ACS server to log the required information, you must 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, click the **Logging** link.
 - Under **Enable Logging**, click the **CSV Passed Authentications** link. The default logging options function and support AWMS. These include the two columns AWMS requires: **User-Name** and **Caller-ID**.

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Integrating AWMS with an Existing Network Management Solution (NMS)

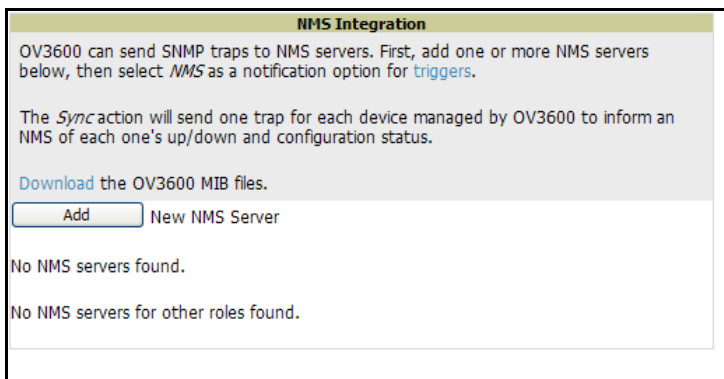
This is an optional configuration. The **AMP Setup > NMS** configuration page allows AWMS to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

- AWMS can forward WLAN-related SNMP traps to the NMS, or AWMS can send SNMPv1 or SNMPv2 traps to the NMS.
- AWMS 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 Dell support.

Perform these steps to configure NMS support in AWMS:

1. Navigate to the **AMP Setup > NMS** page, illustrated in [Figure 36](#).

Figure 36 AMP Setup > NMS Integration Page Illustration



NMS Integration

OV3600 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 OV3600 to inform an NMS of each one's up/down and configuration status.

[Download the OV3600 MIB files.](#)

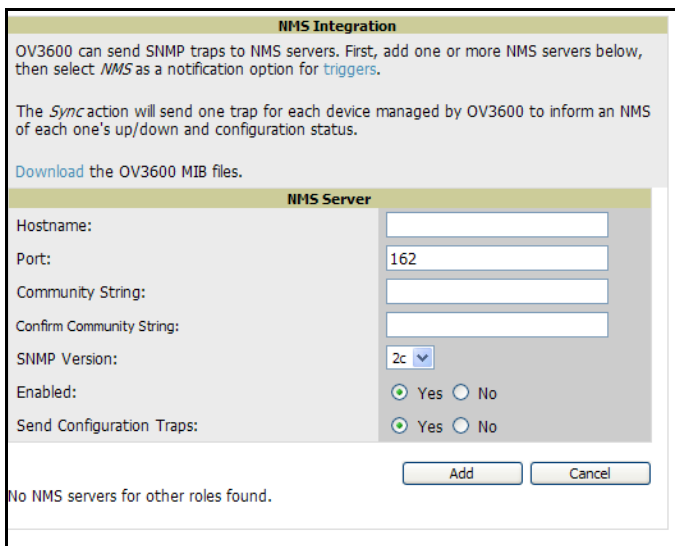
New NMS Server

No NMS servers found.

No NMS servers for other roles found.

2. Click **Add** to integrate a new NMS server, or click the pencil icon to edit an existing NMS server. Provide the information described in [Table 35](#):

Figure 37 AMP Setup > NMS Integration Add/Edit Page Illustration



NMS Integration

OV3600 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 OV3600 to inform an NMS of each one's up/down and configuration status.

[Download the OV3600 MIB files.](#)

NMS Server

Hostname:

Port:

Community String:

Confirm Community String:

SNMP Version:

Enabled: Yes No

Send Configuration Traps: Yes No

No NMS servers for other roles found.

Table 35 AMP Setup > NMS Integration Add/Edit Fields and Default Values

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

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

What Next?

- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Auditing PCI Compliance on the Network

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

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

Introduction to PCI Requirements

AWMS 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. AWMS 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

PCI Auditing in the AWMS Interface

PCI Auditing in AWMS 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 76](#).
- The **Reports > Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See [“Reports > Definitions Page Overview” on page 261](#).
- 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 click. Refer to [“Reports > Generated Page Overview” on page 263](#).
- 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 76](#).
- The **PCI Compliance Report** offers additional information. Refer to [“Using the PCI Compliance Report” on page 281](#). 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.

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

Table 36 *PCI Requirements and Support in AWMS*

PCI Requirement	Description
1.1	<p>Monitoring configuration standards for network firewall devices</p> <p>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.</p> <p>When Disabled: When this PCI requirement is disabled in AWMS, firewall router and device configurations are not checked for PCI compliance in firewall configuration, and Pass or Fail status is not reported nor monitored.</p>
1.2.3	<p>Monitoring firewall installation between any wireless networks and the cardholder data environment</p> <p>When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall.</p> <p>When Disabled: When this PCI requirement is disabled in AWMS, firewall router and device installation are not checked for PCI compliance.</p>
2.1	<p>Monitoring the presence of vendor-supplied default security settings</p> <p>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 AWMS to communicate with the device are on a list of forbidden default credentials. The list includes common vendor default passwords, for example.</p> <p>When Disabled: When this PCI requirement is disabled in AWMS, device passwords and other vendor default settings are not checked for PCI compliance.</p>

Table 36 PCI Requirements and Support in AWMS







PCI Requirement	Description
2.1.1	<p>Changing vendor-supplied defaults for wireless environments</p> <p>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 AWMS establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance.</p> <p>When Disabled: When this PCI requirement is disabled in AWMS, then network devices are not checked for forbidden information and PCI Compliance is not established.</p>
4.1.1	<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: When this PCI monitoring function is disabled in AWMS, then AWMS cannot establish a pass or fail status with regard to PCI encryption requirements on the network.</p>
11.4	<p>Using intrusion-detection or intrusion-prevention systems to monitor all traffic</p> <p>When Enabled: AWMS 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: When this function is disabled, then AWMS does not monitor the presence of PCI-compliant intrusion detection or prevention systems, nor can it report Pass or Fail status with regard to IDS events.</p>

Enabling or Disabling PCI Auditing

Perform these steps to verify status and to enable or disable AWMS support for PCI 1.2 requirements. Enabling one or all PCI standards on AWMS enables real-time information and generated reports that advise on Pass or Fail status. The PCI auditing supported in AWMS is reported in [Table 36](#).

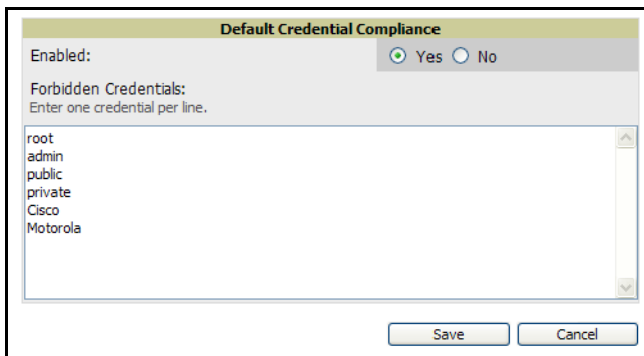
1. To determine what PCI Compliance standards are enabled or disabled on AWMS, navigate to the AMP Setup > PCI Compliance page, illustrated in [Figure 38](#).

Figure 38 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 AWMS, click the pencil icon next to the compliance category you wish to change. 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 AWMS. [Figure 39](#) illustrates one example.

Figure 39 Default Credential Compliance for PCI Requirements



4. Click **Save** to retain the settings. The **PCI Compliance** page should reflect changes on the next viewing.
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. Navigate to the **APs/Devices > List** page, click a specific device, and the **Monitor** page for that device displays. The **Monitor** page displays a **Compliance** page in the menu bar.
 - b. Click the **Compliance** page to view complete PCI compliance auditing for that specific device.

What Next?

- For additional information about configuring WLAN Gateways or WLAN controllers such as BlueSocket, ReefEdge, or ProCurve wireless gateways, refer to [“Third-Party Security Integration for AWMS” on page 305](#).
- Navigate to additional tabs in the **AMP Setup** section to continue additional setup configurations.
- *Complete the required configurations in this chapter prior to proceeding to ensuing chapters of this document.* Dell support remains available to you for any phase of AWMS installation.

Deploying WMS Offload

Overview of WMS Offload in AWMS

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

- ArubaOS Version 2.5.4 or later
- AWMS Version 6.0 or later

The *Dell PowerConnect W 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 AWMS graphical user interface (GUI) allows users to access and use the Dell PowerConnect W WMS functionality.

In AWMS Version 6.1 and Version 6.2, WMS Offload is the ability to offload the WMS server data and GUI functions into AWMS. WMS master controllers provide this data so that AWMS can support rigorous network monitoring capabilities. Additional support for WMS Offload continues with newer versions of AWMS.

General Configuration Tasks Supporting WMS Offload in AWMS

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


1. Configure WLAN switches for optimal AWMS monitoring.
 - Disable debugging.
 - Ensure AWMS server is a trap receiver host.
 - Ensure proper traps are enabled.
2. Configure AWMS to optimally monitor the Dell PowerConnect W infrastructure.
 - Enable WMS offload.
 - Configure SNMP communication.
 - Create a proper policy for monitoring Dell PowerConnect W infrastructure.
 - Discover the infrastructure.
3. Configure device classification.
 - Set up rogue classification.
 - Set up rogue classification override.
 - Establish user classification override devices.
4. Deploy Dell PowerConnect W-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:
 - MMS
 - AOS
 - RF Plan
6. Use RTLS for increasing location accuracy (optional).
 - Enable RTLS service on the AWMS server.
 - Enable RTLS on Dell PowerConnect W Infrastructure.

Additional Information Supporting WMS Offload

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

This chapter describes the deployment of device groups within AWMS. The section below describes the pages or focused sub-menus available on the Groups tab. Note that the available sub-menus can vary significantly from one device group to another—one or more sub-menus 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.

- **List**—This page is the default page in the **Groups** section of AWMS. This page lists all groups currently configured in AWMS and provides the foundation for all group-level configurations. See [“Viewing All Defined Device Groups” on page 81](#). In the case of WLAN switches and configuration, refer also to the *Aruba Configuration Guide*.
- **Monitor**—This page displays user and bandwidth 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 device-level activity in a given group. Several procedures in this chapter cite the **Groups > Monitor** page.

 **Note:** The **Incidents** portion of the **Alert Summary** table only increments the counter for incidents that are open and associated to an AP. The incidents are based on the Top folder on the **Groups > Monitor** page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in this **Alert Summary**. To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.

- **Basic**—This sub-menu page appears when you create a new group with the **Add** button on the **Groups > List** page. Once you define a group name, AWMS displays the **Basic** page from which you configure many group-level settings. This page remains available for any device group configured in AWMS. Refer to [“Configuring Basic Group Settings” on page 83](#).
- **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, Enterasys, HP, Hirschmann, LANCOM, Nomadix, 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 175](#).
- **Security**—This page defines general security settings for device groups, to include TACACS+, RADIUS, encryption, and additional security settings on devices. Refer to [“Configuring Group Security Settings” on page 91](#).
- **SSIDs**—This page sets SSIDs, VLANs, and related parameters in device groups. Refer to [“Configuring Group SSIDs and VLANs” on page 94](#).
- **AAA Servers**—This page configures authentication, authorization, and accounting settings in support of TACACS+ and RADIUS servers for device groups. Refer to [“Adding and Configuring Group AAA Servers” on page 98](#).
- **Radio**—This page defines general 802.11 radio settings for device groups. Refer to [“Configuring Radio Settings for Device Groups” on page 100](#).
- **Dell PowerConnect W Configuration**—This page manages Dell PowerConnect W Device Groups, AP Overrides, and other profiles specific to Dell PowerConnect W devices on the network. Use this page in combination with the **Device Setup > Dell PowerConnect W Configuration** page. For additional information, refer to the *Dell PowerConnect W 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 [“Configuring Cisco Controller Settings” on page 110](#).

- **PTMP/WiMAX**—This page defines settings specific to Proxim MP devices when present. Refer to [“Configuring Group PTMP/WiMAX Settings” on page 112](#).
- **Proxim Mesh**—This page defines mesh AP settings specific to Proxim devices when present. Refer to [“Configuring Proxim Mesh Radio Settings” on page 116](#).
- **MAC ACL**—This page defines MAC-specific settings that apply to Proxim, Cisco Vxworks, Symbol, Intel and Procurve520 devices when present. Refer to [“Configuring Group MAC Access Control Lists” on page 118](#).
- **Firmware**—This page manages firmware files for many devices. [“Specifying Minimum Firmware Versions for APs in a Group” on page 119](#).
- **Compare**—This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, click **Compare Two Groups**, select the two groups from the drop-down menus, then click **Compare**. The **Compare** page allows you to edit any line-item configuration for either of the two groups you compare. [“Comparing Device Groups” on page 120](#).

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

- [“Deleting a Group” on page 121](#)
- [“Changing Multiple Group Configurations” on page 121](#)
- [“Modifying Multiple Devices” on page 122](#)
- [“Using Global Groups for Group Configuration” on page 125](#)

AWMS Group Overview

Enterprise APs, controllers, routers, and switches are complex devices with 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. AWMS addresses this challenge by automating the processes of device configuration and compliance auditing. At the core of this approach is the concept of groups, with the following functions and benefits:

- AWMS allows certain settings to be managed efficiently at a "Group level" while others are managed at an "individual device level."
- AWMS 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 variable appropriate for your business needs.
- Devices within a group may be from different vendors or hardware models—the core requirement and benefit of this approach is that 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.

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

With AWMS, you can create as many different groups as required. AWMS users usually establish groups that range in size from five to 100 wireless devices.

Group configuration can be enhanced with the AWMS *Global Groups* feature; this feature allows you to create global groups with master configurations that are pushed to individual subscriber groups. More information is available in page 125 as well as the section on the [“Supporting AWMS Stations with the Master Console” on page 239](#).

Viewing All Defined Device Groups

To display a list of all groups that have been defined in AWMS, browse to the **Groups > List** page, illustrated in [Figure 40](#). [Table 37](#) describes the contents and functions of this page.

Figure 40 *Groups > List Page Illustration*

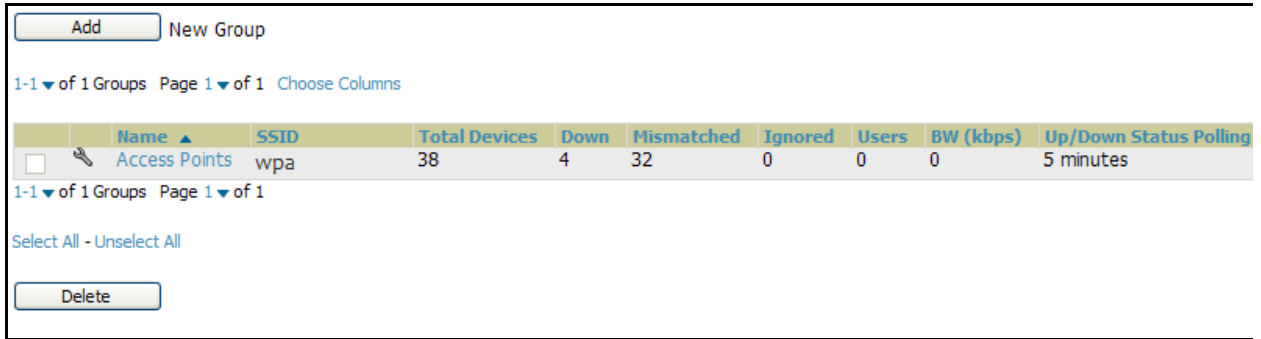


Table 37 *Groups > List Page Fields and Default Values*

Column	Description
Add New Group	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 “Configuring Basic Group Settings” on page 83 .
Manage (wrench icon)	The wrench icon for any existing group provides a hyperlink to the Groups > Basic configuration page to begin editing Group configuration settings for that group.
Name	Displays a user-defined name that 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).
Is Global Group	Identifies whether or not the group has been identified as a global group that can be used to configure subscriber groups. Global groups cannot contain APs and are visible by users of any role.
Global Group	Displays the global group to which the group is subscribed, if any.
SSID	Column represents the Service Set Identifier (SSID) assigned to all devices within the group.
Total Devices	Column represents the total number of devices contained in the group, including APs, wireless controllers and routers or switches.
Down	Column represents 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, AWMS classifies the device as down.
Mismatched	Column represents the number of access points or wireless controllers within the group that are in a mismatched state.
Ignored	Column displays the number of ignored devices in that group.
Users	Column represents the number of mobile users associated with all access points within the group. To avoid double counting of users, users 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 users.
BW (kbps)	Column represents a running average of the sum of bytes in and bytes out for the managed radio page.

Table 37 *Groups > List Page Fields and Default Values (Continued)*

Column	Description
Up/Down Status Polling Period	Column represents the time between Up/Down SNMP polling periods for each device in the group. Detailed SNMP polling period information is available on the Groups > Basic configuration page. Note that by default, most polling intervals do not match the up/down period.
Duplicate	Column represents a hyperlink, and the link creates a new group with the name Copy of <Group Name> with the same group configuration.



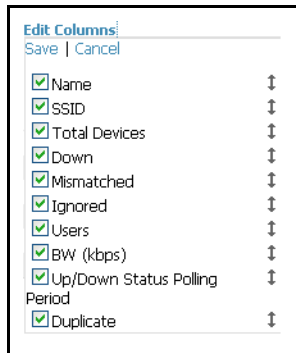
Note: When you first configure AWMS, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to [“Configuring Basic Group Settings” on page 83](#).

Editing Columns on the Groups > List Page and Additional Pages

Perform the following steps to edit the columns that appear on the **Groups > List** page. All additional list and reports pages in AWMS Version 7.0 and later allow you to edit the presence and sequence of columns in this manner:

1. Above the list or report, click **Edit Columns**. The supported columns appear in a popup window, as illustrated in [Figure 41](#):

Figure 41 *Edit Columns Illustration for the Groups > List Page*



2. To remove one or more columns from the **Groups > List** page, click to remove the check mark from the associated checkbox.
3. To change the sequence in which columns appear on the **Groups > List** page, place your cursor over the drag-and-drop icon, left click, move the column to the new position, and release.
4. Click **Save** to retain your settings. The **Groups > List** page displays your changes.

The following pages include columns able to be edited for data display:

- **Home > Search** (results)
- **Helpdesk > Incidents**
- **Groups > List**
- **Groups > Monitor**
- **Groups > Cisco WLC Config**
- **APs/Devices > List**
- **APs/Devices > New**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**

- APs/Devices > Ignored
- Users > Connected
- Users > All
- Users > Guest Users
- Users > Tags
- Reports > Generated
- Reports > Definitions (defining report setup)
- Device Setup > Discover
- Device Setup > Aruba Configuration (and several additional pages in this section)
- AMP Setup > NMS
- AMP Setup > RADIUS Accounting
- RAPIDS > Rogue APs
- RAPIDS > Score Override

Configuring Basic Group Settings

The first default device group that AWMS 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. Navigate to the **Groups > List** page. Existing device groups appear on this page.
2. To create a new group, click **Add**. Enter a group name and click **Add**. The **Group > Basic** page appears.
 To edit an existing device group, click the **manage** (wrench) icon next to the group. The **Group > Basic** page appears. If you hover your cursor over an existing group's **manage** (wrench) icon, a popup menu appears after a moment, and allows you to click **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, or **Radio** to edit those pages as desired.

[Figure 42](#) illustrates the **Groups > Basic** page. Page content differs according to the devices that a group contains. This page may change over time as you add or remove devices from the group.

Figure 42 Groups > Basic Page Illustration

Group: San Francisco

Basic	
Name:	San Francisco
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	United States
Timezone: For scheduling group configuration changes	OV3600 system time
Allow One-to-One NAT:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Audit Configuration on Devices:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Global Groups	
Is 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 type="radio"/> Yes <input checked="" type="radio"/> No
User Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	5 minutes
Device Bandwidth Polling Period:	10 minutes
802.11 Counters Polling Period:	15 minutes
Rogue AP and Device Location Data Polling Period:	30 minutes
CDP Neighbor Data Polling Period:	30 minutes
Notes	
Notes:	
Group Display Options	
Show device settings for:	Only devices on this OV3600
Selected Device Types:	3Com 8750, Alcatel-Lucent, Aruba, Cisco IOS, Cisco VxWorks, Cisco WLC, Enterasys RoamAbout AP3000/AP4102, HP ProCurve 420, HP ProCurve 530, Nomadix, Proxim, Proxim MP.11, Symbol, Symbol Wireless Switch, Trapeze
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/VxWorks	
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
Track Usernames on Cisco Aironet VxWorks APs: Configures devices to send SNMP traps to OV3600	<input type="radio"/> Yes <input checked="" type="radio"/> No
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:	80
Country Code:	United States
HP ProCurve	
SNMP Version:	2c
Symbol/Intel	
SNMP Version:	2c
Symbol/Intel Client Inactivity Timeout (3-600 min):	3
Symbol Controller CLI Communication: WS5100 and RFS7000 only	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Web Config Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Aruba/Alcatel-Lucent	
SNMP Version:	2c
Offload Aruba/Alcatel-Lucent WMS Database:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alcatel-Lucent GUI Config:	<input checked="" type="radio"/> Yes <input type="radio"/> No
3Com/Enterasys/Nortel/Trapeze	
SNMP Version:	2c
Routers and Switches	
Read ARP Table:	4 hours
Read CDP Table for Device Discovery:	4 hours
Read Bridge Forwarding Table:	4 hours
Interface Polling Period:	5 minutes

3. Define the settings in the **Basic** and **Global Group** sections. [Table 38](#) describes several typical settings and default values of this **Basic** section.

Table 38 Basic and Global Group Fields and Default Values

Setting	Default	Description
Name	Defined when first adding the group	Displays or changes the group name. As desired, use this field to set the user-definable name to uniquely identify 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).
Missed SNMP Poll Threshold	1	Sets the number of Up/Down SNMP polls that must be missed before AWMS considers a device to be down. The number of SNMP retries and the SNMP timeout of a poll can be set on the Device Setup > Communication page.
Regulatory Domain	United States	Sets the regulatory domain in AWMS, limiting the selectable channels for APs in the group.
Timezone	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.
Allow One-to-One NAT for Groups	No	Allows AWMS to talk to the devices on a different IP address than the one configured on the device. NOTE: If enabled, the LAN IP Address listed on the AP/Devices > Manage configuration page under the Settings area is different than the IP Address under the Device Communication area.
Audit Configuration on Devices	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.
Global Groups	No	When enabled, this field allows you to define the device group to be a global group. Refer also to "Using Global Groups for Group Configuration" on page 125.

- Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. [Table 39](#) describes the SNMP polling settings.

Table 39 SNMP Polling Period Fields and Default Values

Setting	Default	Description
Up/Down Status Polling Period	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 Device Setup > Communication configuration page. Aruba recommends an initial polling interval of 5 minutes for most networks.
Override Polling Period for Other Services	No	Radio button enables or disables overriding the base SNMP Polling Period. If you select Yes for this field, then the other settings in the SNMP Polling Periods section are activated, and you can override default values.
User Data Polling Period	5 minutes	Sets time between SNMP polls for User Data for devices in the group.
Thin AP Discovery Polling Period	5 minutes	Sets time between SNMP polls for Thin AP Device Discovery. Controllers are the only devices affected by this polling interval.
Device-to-Device link Polling Period	5 minutes	Sets time between SNMP polls for Device-to-Device link polling. Mesh APs are the only devices affected by this polling interval.
Device Bandwidth Polling Period	5 minutes	Sets the interval at which AWMS polls for the bandwidth being used by a device.
802.11 Counters Polling Period	5 minutes	Sets time between SNMP polls for 802.11 Counter information.
Rogue AP and Device Location Data Polling Period	5 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.

Table 39 SNMP Polling Period Fields and Default Values (Continued)

Setting	Default	Description
CDP Neighbor Data Polling Period	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.
- To configure which options and tabs are visible for the group, complete the settings in the **Group Display Options** section. [Table 40](#) describes the settings and default values.

Table 40 Group Display Options Fields and Default Values

Setting	Default	Description
Show device settings for:	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"> All Devices—AWMS displays all Group tabs and setting options. Only Devices in this group—AWMS 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 perform a Save and Apply action on the group. Only Devices on this AMP—AWMS hides all options and tabs that do not apply to the APs and devices currently on AWMS. Use system defaults—Use the default settings defined on the AWMS configuration page Selected device types—Allows the user to specify the device types for which AWMS displays Group settings.
Selected Device Types	Disabled	If you chose to display selected device types, then this option appears, allowing you to select the device types for which AWMS displays group settings. Click Select devices in this group for a quick way to display only devices in the current group being configured.

- 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 41](#) describes the settings and default values.

Table 41 Automatic Static IP Assignment Fields and Default Values

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

- To configure Spanning Tree Protocol on WLSE devices and Proxim APs, locate the Spanning Tree Protocol section on the **Groups > Basic** configuration page. Adjust these settings as required. [Table 42](#) describes the settings and default values.

Table 42 Spanning Tree Protocol Fields and Default Values

Setting	Default	Description
Spanning Tree Protocol	No	Enables or disables Spanning Tree Protocol on WLSE devices and Proxim APs.
Bridge Priority	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.
Bridge Maximum Age	20	Sets the maximum time, in seconds, that the device stores protocol information. The supported range is from 6 to 40.
Bridge Hello Time	2	Sets the time, in seconds, between Hello message broadcasts.
Bridge Forward Delay	15	Sets the time, in seconds, that the port spends in listening and learning mode if the spanning tree has changed.

- To configure NTP settings locate the **NTP** section and adjust these settings as required. [Table 43](#) describes the settings and default values.

Table 43 NTP Fields and Default Values

Setting	Default	Description
NTP Server #1,2,3	None	Sets the IP address of the NTP server that is to be configured on the AP.
UTC Time Zone	0	Sets the hour offset from UTC time to local time for the AP. Times displayed in AWMS graphs and logs use the time set on the AWMS server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim and HP ProCurve 420 sections of the Groups > Basic configuration page.

- To configure settings specific to Cisco IOS/VxWorks, locate the **Cisco IOS/VxWorks** section and adjust these settings as required. [Table 44](#) describes the settings and default values.

Table 44 Cisco IOS/VxWorks Fields and Default Values

Setting	Default	Description
Cisco IOS SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.
Cisco IOS CLI Communication	Telnet	Sets the protocol AWMS uses to communicate with Cisco IOS devices. Selecting SSH uses the secure shell for command line page (CLI) communication. Selecting Telnet sends the data in clear text via Telnet.
Cisco IOS Config File Communication	TFTP	Sets the protocol AWMS uses to communicate with Cisco IOS devices. Selecting SCP uses the secure copy protocol for file transfers. Selecting TFTP will use the insecure trivial file transfer protocol. The SCP login and password should be entered in the Telnet username and password fields.
Track Usernames on Cisco Aironet VxWorks APs	No	Configures VxWorks APs to send SNMP packets to AWMS.

11. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section and adjust these settings as required. [Table 45](#) describes the settings and default values.

Table 45 Cisco WLC Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to WLC controllers.
CLI Communication	Telnet	Sets the protocol AWMS uses to communicate with Cisco IOS devices. Selecting SSH uses the secure shell for command line page (CLI) communication. Selecting Telnet sends the data in clear text via Telnet.



Note: When configuring Cisco WLC controllers, refer also to [“Configuring Wireless Parameters for Cisco Controllers” on page 110.](#)

12. To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section and adjust these settings as required. [Table 46](#) describes the settings and default values.

Table 46 Proxim/Avaya Fields and Default Values

Setting	Default	Description
SNMP Version	1	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.
Enable DNS Client	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 Yes for this setting, additional DNS fields display.
Primary DNS server	Blank	Sets the IP address of the Primary DNS server.
Secondary DNS server	Blank	Sets the IP address of the Secondary DNS server.
Default DNS domains	Blank	Sets the default DNS domain used by the AP.
HTTP Server Port	80	AWMS sets this port as the HTTP server port on all Proxim APs in the group.
Country Code	United States	Configures AWMS to derive its time settings based on the country of location, as specified in this field.

13. To configure HP ProCurve 420 specific settings, locate the **HP ProCurve 420** section and adjust these settings as required. [Table 47](#) describes the settings and default values.

Table 47 HP ProCurve 420 Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.
ProCurve XL/ZWeSM CLI Communication	Telnet	Sets the protocol AWMS uses to communicate with ProCurve XLWeSM devices. Selecting SSH will use the secure shell for command line page (CLI) communication. Selecting telnet will send the data in clear text via telnet.

Table 47 HP ProCurve 420 Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.



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

- To configure Symbol or Intel-specific settings, locate the **Symbol/Intel** section and adjust these settings as required. [Table 48](#) describes the settings and default values of this section.

Table 48 Symbol/Intel Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the device.
Symbol/Intel Client Inactivity Timeout (3-600 min)	3	Sets the minutes of inactivity after which a client associated to an Intel or Symbol AP will be considered "inactive." A lower value typically provides a more accurate representation of current WLAN usage. NOTE: For other APs, AWMS has more precise methods to determine when inactive clients are no longer associated to an AP.
Symbol Controller CLI Communication	Telnet	Select which connection type is to support the command-line interface (CLI) connection. The options are Telnet and secure shell (SSH). This is supported for WS5100 and RFS7000 devices only.
Web Config Interface	Yes	Enables or disables the http/https configuration page for the Symbol 4131 and Intel 2011 devices.

- To configure settings specific to Dell PowerConnect W, locate the **Dell PowerConnect W** section and adjust these settings as required. [Table 49](#) describes the settings and default values of this section.

Table 49 Dell PowerConnect W Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.
Offload Dell PowerConnect W WMS database	No	Configures commands previously documented in the <i>Dell PowerConnect W AirWave Best Practices Guide</i> . See the current <i>Best Practices</i> guide for more information about this feature. When enabled, this feature allows AWMS to display historical information for WLAN switches. Changing the setting to Yes 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 Allow WMS Offload setting on the AWMS configuration page is changed to Yes .
Dell PowerConnect W GUI Config	Yes	Enables or disables AWMS support for the Dell PowerConnect W configuration interface. This setting relates to the Device Setup > Dell PowerConnect W Configuration page and all related operations. For additional information, refer to the <i>Dell PowerConnect W Configuration Guide</i> .

16. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/Trapeze** section and adjust these settings as required. [Table 50](#) describes the settings and default values of this section.

Table 50 3Com/Enterasys/Nortel/Trapeze Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate to the AP.

17. To configure support for routers and switches in the Access Points group, locate the **Routers and Switches** section and adjust these settings as required. This section defines the frequency in which all devices in the Access Points group poll for IP routing information. This can be disabled entirely as desired. [Table 51](#) describes the settings and default values of this section.

Table 51 Routers and Switches Fields and Default Values

Setting	Default	Description
Read ARP Table	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.
Read CDP Table for Device Discovery	4 hours	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.
Read Bridge Forwarding Table	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.
Interface Polling Period	5 minutes	Sets the frequency in which network interfaces are polled. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 15 seconds to 12 hours.

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.

Table 52 Universal Devices, Routers and Switches Fields and Default Values

Setting	Default	Description
SNMP Version	2c	Drop-down menu specifies the version of SNMP used by AWMS to communicate with universal devices on the network.

19. Click **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 Access Points group. **Save** is a good option if you intend to make additional device changes in the Access Points group, and wish to wait until all configurations are complete before you push all configurations at one time.

Click **Save and Apply** to save and push these configurations to devices immediately in the Access Points group, or click **Revert** to return to the most recently saved settings.

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 AWMS functions.

Configuring Group Security Settings

The **Groups > Security** page allows you to set security policies for APs in a device group. Perform these steps.

1. Select the device group for which to define security settings from the **Groups > List** page.
2. Select the **Groups > Security** page. Some controls on this page interact with additional AWMS pages. [Figure 43](#) illustrates this page and [Table 53](#) explains the fields and default values.

Figure 43 *Groups > Security Page Illustration*

The screenshot shows the configuration page for a device group's security settings. It is organized into several sections:

- VLANs Section:**
 - VLAN Tagging and Multiple SSIDs:** Radio buttons for Enabled and Disabled.
 - Management VLAN ID (0-4094, Untagged):** A text box containing "Untagged".
 - Permit RADIUS-Assigned Dynamic VLANs:** Radio buttons for Yes and No.
 - VLAN ID Format:** Radio buttons for ASCII and Hex.
 - Ethernet Untagged VLAN ID (1-4094):** A text box containing "1".
- General Section:**
 - Create Closed Network:** Radio buttons for Yes and No.
 - Block All Inter-Client Communication:** Radio buttons for Yes and No.
- EAP Options Section:**
 - WEP Key Rotation Interval (0-10000000 sec):** A text box containing "300".
 - Session Key Refresh Rate (0-1440 min):** A text box containing "0".
 - Session Timeout (0-65535 sec):** A text box containing "0".
 - Cisco TKIP:** Radio buttons for Yes and No.
 - Cisco MIC:** Radio buttons for MMH and Disabled.
- RADIUS Authentication Servers Section:**
 - RADIUS Authentication Server #1-4:** Four dropdown menus, each set to "Select".
 - Authentication Profile Name:** A text box containing "Proxim Only".
 - Authentication Profile Index:** A text box containing "1".
- RADIUS Accounting Servers Section:**
 - RADIUS Accounting Server #1-4:** Four dropdown menus, each set to "Select".
 - Accounting Profile Name:** A text box containing "Proxim Only".
 - Accounting Profile Index:** A text box containing "3".
- MAC Address Authentication Section:**
 - MAC Address Authentication:** Radio buttons for Yes and No.
 - MAC Address Format:** A dropdown menu set to "Single Dash".
 - Authorization Lifetime (900-43200 sec):** A text box containing "1800".
 - Primary RADIUS Server Reattempt Period (0-120 min):** A text box containing "0".

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

Table 53 *Groups > Security Page Fields and Default Values*

Setting	Default	Description
VLANs Section		
VLAN Tagging and Multiple SSIDs	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 Groups > SSIDs page. Refer to “Configuring Group SSIDs and VLANs” on page 94 .
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in AWMS. This setting is supported only for the following devices: <ul style="list-style-type: none"> ● Proxim AP-600, AP-700, AP-2000, AP-4000 ● Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8 ● ProCurve520WL; ProCurve420 ● Enterasys AP3000

Table 53 Groups > Security Page Fields and Default Values (Continued)

Setting	Default	Description
Permit RADIUS-Assigned Dynamic VLANs	No	This setting enables dynamic VLANs to be assigned by the RADIUS server. This setting is supported only for HP ProCurve 420.
VLAN ID Format	Hex	This setting defines the naming convention for VLANs to be supported in AWMS. The supported naming formats are ASCII and Hexadecimal.
Ethernet Untagged VLAN ID (1-4094)	1	This field defines the VLAN that will use untagged Ethernet. The VLAN must be a number between 1 and 4094, and defines the untagged VLAN ID for the RoamAbout AP3000.
General Section		
Create Closed Network	No	If enabled, the APs in the Group do not broadcast their SSIDs. NOTE: Aruba recommends creating a closed network to make it more difficult for intruders to detect your wireless network.
Block All Inter-client Communication	No	If enabled, this setting blocks client devices associated with an AP from communicating with other client devices on the wireless network. NOTE: This option may also be identified as PSPF (Publicly Secure Packet Forwarding), which can be useful for enhanced security on public wireless networks.
EAP Options Section		
WEP Key Rotation Interval	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.
Session Key Refresh Rate	0	Sets the frequency at which the general session key is refreshed in the device group being configured. The supported range is from 1 to 40 minutes. This setting is supported only for HP ProCurve 420.
Session Timeout	0	Sets the time at which the session times out for the device group being configured. The supported range is from 0 to 65,535 seconds. This setting is supported only for HP ProCurve 420.
Cisco TKIP	No	Sets the device group to use the Cisco Temporal Key Integrity Protocol (TKIP). If enabled, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. NOTE: TKIP can only be enabled when EAP-based security is used.
Cisco MIC	Disabled	Sets the device group to use the Cisco Message Integrity Check (MIC). Selecting MMH encryption enables this function. If enabled, Message Integrity Check (MIC) adds several bytes per packet to make it more difficult to tamper with the packets.
RADIUS Authentication Servers Section		
RADIUS Authentication Server #1 - #4	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.
Authentication Profile Name	AMP-Defined Server #1	For Proxim devices only, this field sets the name of the authentication profile to be supported in this device group.
Authentication Profile Index	1	For Proxim devices only, this field sets the name of the authentication profile index to be supported in this device group.
RADIUS Accounting Servers Section		
RADIUS Accounting Server #1 - #4	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.

Table 53 Groups > Security Page Fields and Default Values (Continued)

Setting	Default	Description
Authentication Profile Name	Accounting	For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group.
Authentication Profile Index	3	For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group.
MAC Address Authentication Section		
MAC Address Authentication	No	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
MAC Address Format	Single Dash	Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: <ul style="list-style-type: none"> ■ Dash Delimited: xx-xx-xx-xx-xx-xx (default) ■ Colon Delimited: xx:xx:xx:xx:xx:xx ■ Single-Dash: xxxxxx-xxxxxx ■ No Delimiter: xxxxxxxxxxxx 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, ProCurve 420 v2.1.0 and higher.
Authorization Lifetime	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.
Primary RADIUS Server Reattempt Period	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. Click **Save** to retain these Security configurations for the group, click **Save and Apply** to retain and push these configurations, or click **Revert** to return to the last saved security settings for this group.
4. Continue with additional security-related procedures in this document for additional TACACS+, 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.



Note: 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*

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

New SSID/VLAN

	SSID	VLAN ID	Name	Encryption Mode	First Radio		Second Radio		Native VLAN
					Enabled	Primary	Enabled	Primary	
<input type="checkbox"/>	stores	11	-	No Encryption	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	distribution	1	-	No Encryption	<input type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/>	corp	51	-	No Encryption	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>

Select All - Unselect All



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



Note: Multiple VLANs and SSIDs are supported only on Cisco access points.

1. Navigate to the **Groups > List** page and select the group for which to define SSIDs/VLANs by clicking the group name. Alternatively, click **Add** to create a new group, define a group name. In either case, the **Groups > Monitor** page appears.
2. Select the **Groups > SSIDs** configuration page. [Table 54](#) describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 54 *Groups > SSIDs Fields and Descriptions*

Field	
SSID	Displays the SSID associated with the VLAN.
VLAN ID	Identifies the number of the primary VLAN SSID on which encrypted or unencrypted packets can pass between the AP and the switch.
Name	Displays the name of the VLAN.
Encryption Mode	Displays the encryption on the VLAN.
First or Second Radio Enabled	Checkbox enables the VLAN, SSID and Encryption Mode on the radio control.

Table 54 Groups > SSIDs Fields and Descriptions

Field	
First or Second Radio Primary	Specifies which VLAN to be used as the primary VLAN. A primary VLAN is required. NOTE: If you create an Open network (see Create Closed Network below) in which the APs broadcast an SSID, the Primary SSID is the one that is broadcast.
Native VLAN	Selects this VLAN to be the native VLAN. Native VLANs are untagged and typically used for management traffic only. AWMS requires a Native VLAN to be set. Some AP types do not require a native VLAN. For those APs, you need to create a dummy VLAN, disable it on both radio controls and ensure that it has the highest VLAN ID.

- Click **Add** to create a new SSID or VLAN, or click 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 55](#).

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

- 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 55](#) describes the settings and default values.

Table 55 Groups > SSIDs > SSID/VLAN Section Fields and Default Values

Setting	Default	Description
Specify Interface Name	Yes	Enables or disables an interface name for the VLAN interface. <ul style="list-style-type: none"> Selecting No for this option displays the Enable VLAN Tagging option.
Interface	None	Sets the interface to support the SSID/VLAN combination.
SSID	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.

Table 55 *Groups > SSIDs > SSID/VLAN Section Fields and Default Values (Continued)*

Setting	Default	Description
Name	None	Sets a user-definable name associated with SSID/VLAN combination.
VLAN ID	None	Indicates the number of the VLAN designated as the Native VLAN , typically for management purposes
Service Priority (Cisco VxWorks only)	None	Identifies the delivery priority which packets receive on the VLAN/SSID (VxWorks only).
Maximum Allowed Associations (0-2007)	255	Indicates the maximum number of mobile users which can associate with the specified VLAN/SSID. NOTE: 0 means unlimited for Cisco and none for Colubris.
Broadcast SSID (Proxim 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 Create Closed Network setting on the Groups> Security configuration page. Proxim devices support a maximum of four SSIDs. NOTE: This option should be enabled to ensure support of legacy users.
Partial Closed System (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.
Unique Beacon (Proxim only)	No	For Proxim only, if more than one SSID is enabled, this option enables them to be sent in separate beacons.
Block All Inter-client Communication	Yes	For Colubris only, 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 56](#) describes the settings and default values.

Table 56 *Groups > SSIDs > Encryption Section Fields and Default Values*

Setting	Default	Description
Encryption Mode	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"> • Optional WEP—Wired Equivalent Privacy, not PCI compliant as of 2010 • Require WEP—Wired Equivalent Privacy, not PCI compliant as of 2010 • Require 802.1x—This encryption type is based on the WEP algorithm. • Require Leap—Lightweight Extensible Authentication Protocol • 802.1x+WEP—Combines the two encryption types shown • LEAP+WEP—Combines the two encryption types shown • Static CKIP—Cisco Key Integrity Protocol • WPA—Wi-Fi Protected Access protocol • WPA/PSK—Combines WPA with Pre-Shared Key encryption • WPA2—Wi-Fi Protected Access 2 encryption • WPA2/PSK—Combines the two encryption methods shown

6. Locate the EAP Options area on the Groups > SSIDS page, and complete the settings. [Table 57](#) describes the settings and default values.

Table 57 Groups > SSIDs > EAP Options Section Fields and Default Values

Setting	Default	Description
WEP Key Rotation Interval (seconds)	120	Time (in seconds) between WEP key rotation on the AP.
Cisco TKIP	No	If enabled, Cisco Temporal Key Integrity Protocol (TKIP) provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. NOTE: TKIP can only be enabled when EAP-based security is used.
Cisco MIC	Disabled	If enabled, Cisco Message Integrity Check (MIC) adds several bytes per packet to make it more difficult to tamper with the packets.

7. Locate the **RADIUS Authentication Servers** area on the **Groups > SSIDS** configuration page and define the settings. [Table 58](#) describes the settings and default values.

Table 58 Groups > SSIDs > RADIUS Authentication Servers Fields and Default Values

Setting	Default	Description
RADIUS Authentication Server 1-3 (Colubris, ProCurve420, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the Group > RADIUS configuration page. These RADIUS servers dictate how wireless clients authenticate onto the network.
Authentication Profile Name (Proxim Only)	None	Sets the Authentication Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Authentication Profile Index (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

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



Note: You may need to return to the **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 59](#) describes the settings and default values.

Table 59 Groups > SSIDs > Radius Accounting Servers Fields and Default Values

Setting	Default	Description
RADIUS Accounting Server 1-3 (Proxim Only)	None	Pull-down menu selects RADIUS Accounting servers previously entered on the Group > RADIUS configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets for this SSID/VLAN.
Accounting Profile Name (Proxim Only)	None	Sets the Accounting Profile Name for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.
Accounting Profile Index (Proxim Only)	None	Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8 and HP ProCurve 520WL APs.

- Click **Save** to retain these **Security** configurations for the group, click **Save and Apply** to retain and push these configurations, or click **Revert** to return to the last saved security settings for this group.
- Continue with additional security-related procedures in this document for additional TACACS+, RADIUS, and SSID settings for device groups, as required.

Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Group > AAA Servers** page. TACACS+ servers are configured as a part of Cisco WLC configuration. In that case, refer to “[Configuring Security Parameters and Functions](#)” on page 110.

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.



Note: TACACS+ servers are configurable only for Cisco WLC devices. Refer to “[Configuring Wireless Parameters for Cisco Controllers](#)” on page 110.

- Navigate to the **Groups > List** page and select the group for which to define AAA servers by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
- Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. [Figure 46](#) and [Figure 47](#) illustrate this page for AAA RADIUS Servers:

Figure 46 *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, click the **Add New RADIUS Server** button or click the corresponding pencil icon to edit an existing server. [Table 60](#) describes the settings and default values of the **Add/Edit** page.

Figure 47 *Adding a RADIUS Server Page Illustration*

RADIUS Server

Hostname/IP Address:
Not all devices support hostnames.

Secret:

Confirm Secret:

Authentication: Yes No

Authentication Port: 1812

Accounting: Yes No

Accounting Port: 1813

Timeout (0-86400):

Max Retries (0-20):

Table 60 Adding a RADIUS Server Fields and Default Values

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

4. Click **Add** to complete the creation of the RADIUS server, or click **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.

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



Note: AWMS first checks its own database prior to checking the RADIUS server database.

5. To make additional RADIUS configurations for device groups, use the **Groups > Security** page, and refer to [“Configuring Group Security Settings” on page 91](#).

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.



Note: 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. Navigate to the **Groups > List** page and select the group for which to define radio settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Navigate to the **Groups > Radio** page. [Figure 48](#) illustrates this page.

Figure 48 *Groups > Radio Page Illustration*

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="button" value="Required"/> 2.0: <input type="button" value="Required"/> 5.5: <input type="button" value="Optional"/> 11.0: <input type="button" value="Optional"/>
Frag Threshold Enabled:	<input type="radio"/> Yes <input checked="" type="radio"/> No
RTS/CTS Threshold Enabled:	<input type="radio"/> Yes <input checked="" type="radio"/> No
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="102"/>
DTIM Period (1-255):	<input type="text" value="3"/>
Ethernet Encapsulation:	<input type="radio"/> 802.1H <input checked="" type="radio"/> RFC1042
Radio Preamble:	<input checked="" type="radio"/> Long <input type="radio"/> Short
Cisco VxWorks	
Use Aironet Extensions:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Lost Ethernet Action:	<input type="button" value="Repeater Mode"/>
Lost Ethernet Timeout (1-10000 sec):	<input type="text" value="2"/>
Upgrade Radio Firmware When AP Firmware Is Upgraded (Require use of radio firmware x.xx):	<input checked="" type="radio"/> Yes <input type="radio"/> No
Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5, 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="button" value="Large"/>
802.11g Operational Mode:	<input type="button" value="802.11b + 802.11g"/>
802.11abg Operational Mode:	<input type="button" value="802.11b + 802.11g"/>
802.11b Transmit Rate:	<input type="button" value="Auto Fallback"/>
802.11g Transmit Rate:	<input type="button" value="Auto Fallback"/>
802.11a Transmit Rate:	<input type="button" 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="button" value="20"/>
802.11a/4.9GHz Public Safety Operational Mode:	<input type="button" value="802.11a"/>
Colubris	
Rogue Scanning:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Rogue Scanning Interval (10-600 sec):	<input type="text" value="600"/>
Automatic Channel Interval:	<input type="button" value="12 Hours"/>
First Radio:	
Operational Mode:	<input type="button" value="802.11b only"/>
Multicast Data Rate:	<input type="button" value="1 Mbps"/>
Second Radio: CN330 Only	
Operational Mode:	<input type="button" value="802.11b only"/>
Multicast Data Rate:	<input type="button" value="1 Mbps"/>
Symbol	
Rogue Scanning:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Rogue Scanning Interval (5-480 min):	<input type="text" value="240"/>
Enterasys R2	
Operational Mode:	<input type="button" value="802.11b + 802.11g"/>
<input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Rever"/>	

3. Locate the **Radio Settings** area and adjust these settings as required. [Table 61](#) describes the settings and default values.

Table 61 *Groups > Radio Fields and Default Values*

Setting	Default	Description
Allow Automatic Channel Select (2.4, 5 GHz and 4.9GHz)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and automatically select its optimal RF channel based on observed signal strength from other radios. NOTE: If you enable this feature, AWMS automatically reboots the APs in the group when the change is implemented.
802.11b Data Rates (Mb/sec)	Required: <ul style="list-style-type: none"> ● 1.0 ● 2.0 Optional: <ul style="list-style-type: none"> ● 5.5 ● 11.0 	Displays pull-down menus for various data rates for transmitting data. NOTE: 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"> ● Required—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 yes on Cisco devices.) ● Optional—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of basic on Cisco devices.) ● Not Used—The AP does not transmit data at the specified data rate. (Corresponds to a setting of no on Cisco devices.)
Frag Threshold Enabled	No	If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, Aruba recommends leaving this option disabled.
Threshold Value	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower Fragmentation Threshold setting might be required if there is a great deal of radio interference.
RTS/CTS Threshold Enabled	No	If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, Aruba recommends leaving this option disabled.
RTS/CTS Threshold Value	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.
RTS/CTS Maximum Retries	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 1 to 128 .
Maximum Data Retries	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet.
Beacon Period (19-5000 Kµsec)	100	Time between beacons (in kilo microseconds).
DTIM Period (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.
Ethernet Encapsulation	RFC1042	This setting selects either the RFC1042 or 802.1h Ethernet encapsulation standard for use by the group.
Radio Preamble	Long	This setting determines whether the APs uses a short or long 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. NOTE: 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.



Note: 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 HP ProCurve 420 settings exclusively, locate the **HP ProCurve 420** section and adjust these settings as required. [Table 62](#) describes the settings and default values.

Table 62 HP ProCurve 420 Fields and Default Values

Setting	Default	Description
Slot Time	Auto	Short-slot-time mechanism, if used on a pure 802.11g deployment, improves WLAN throughput by reducing wait time for transmitter to assure clear channel assessment.
Multicast Data Rate	5.5Mbps	Sets the maximum data rate of the multicast data packets.
Rogue Scanning	Enabled	If enabled the 420 APs in the group will scan for rogues.
Rogue Scanning Interval (15-10080 min)	720	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. NOTE: This setting only applies to Periodic scans.
Rogue Scanning Duration (50-1000 msec)	350	Specifies the amount of time, in milliseconds, the AP should spend performing the rogue scan. If the duration is set too high users may start to experience connectivity issues. NOTE: This setting only applies to periodic scans.
Rogue Scan Type	Periodic	Specifies the Rogue Scanning mode. When set to Dedicated , users are unable to associate to the AP.

- To configure the HP ProCurve 240, Enterasys AP 3000 and AP 4102 Operational Mode and Max Station Data Rate, locate the **HP ProCurve 240, Enterasys AP 3000 and AP 4102** section of the **Proprietary Settings** area, and define the settings. [Table 63](#) describes the settings and default values of this page.

Table 63 HP ProCurve 240, Enterasys AP 3000 and AP 4102 Fields and Default Values

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Sets the radio operational mode for all of the ProCurve 420s, Enterasys 3000s and 4102sin the group to either b only, g only, or b + g.
Max Station Data Rate	54 Mbps	The maximum data rate at which a user can connect to the AP.

- To configure settings specific to Enterasys AP3000 and Enterasys AP4102, locate the **Enterasys AP3000 and Enterasys AP4102** section of the **Proprietary Settings** area, and define the settings. [Table 64](#) describes the settings and default values of this page.

Table 64 Enterasys AP3000 and Enterasys AP4102 > Proprietary Settings Fields and Default Values

Setting	Default	Description
802.11a Multicast Data Rate	6 Mbps	Drop-down menu that specifies the a radio multicast data rate.
802.11b/g Multicast Data Rate	5.5 Mbps	Drop-down menu that specifies the b/g multicast data rate.
Rogue Scanning	Enabled	If enabled AP 3000s and 4102s in the group with firmware 3.1.20 or newer will passively scan for rogue access points at the specified interval for the specified amount of time. This rogue scan will not break users' association to the network.
Rogue Scan Interval (30-10080 min)	720	Specifies the time, in minutes, between rogue scans.
Rogue Scan Duration (200-1000 msec)	350	Specifies the amount of time, in milliseconds, the AP listens to rogues before returning to normal operation.

- To configure radio settings for Cisco VxWorks devices in the group, locate the **Groups > VxWorks** section and adjust these settings as required. [Table 65](#) describes the settings and default values of this page.

Table 65 Groups > VxWorks Proprietary Settings Fields and Default Values

Setting	Default	Description
Use Aironet Extensions	Yes	When enabled, this option allows Cisco devices to provide functionality not supported by 802.11 IEEE standards, including the following: <ul style="list-style-type: none"> ● Load balancing—Allows the access point to direct Aironet clients to the optimum access point. ● Message Integrity Check (MIC)—Protects against bit-flip attacks. ● Temporal Key Integrity Protocol (TKIP)—Key hashing algorithm that protects against IV attacks.
Lost Ethernet Action	Repeater Mode	Pull-down menu that specifies the action to take when the Lost Ethernet Timeout threshold is exceeded: <ul style="list-style-type: none"> ● No Action—No action taken by the AP. ● Repeater Mode—The AP converts to a repeater, disassociating all its clients while the backbone is unavailable. If the AP can communicate with another root AP on the same SSID, its clients will be able to re-associate and connect to the backbone. If the AP cannot communicate with another root AP, clients are not allowed to re-associate. ● Disable Radio—The AP disassociates its clients and disables the radio until it can establish communication with the backbone. ● Restrict SSID—The AP disassociates all clients and then allows clients to re-associate with current SSID.
Lost Ethernet Timeout (1-1000 secs)	2	Specifies the time (in seconds) the AP waits prior to taking action when its backbone connectivity is down. Actions are defined in the Lost Ethernet Action field.
Upgrade Radio Firmware When AP Firmware Is Upgraded	Yes	If enabled, this setting mandates that the radio firmware be upgraded to a firmware version compatible with the current version of AP firmware.

- 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 66](#) describes the settings and default values.

Table 66 Groups > LWAPP APs, Proprietary Settings Fields and Default Values

Setting	Default	Description
Load Balancing	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. NOTE: This feature is only available when two 802.11b wireless cards are used in an AP-2000.
Interference Robustness	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.
Distance Between APs	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.
802.11g Operational Mode	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.
802.11abg Operational Mode	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.
802.11b Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11g Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11a Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
Rogue Scanning	Yes	If enabled, any ORiNOCO, or Avaya access points 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. NOTE: This feature can affect the data performance of the access point.
Rogue Scan Interval	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.

10. To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. [Table 67](#) describes the settings and default values.

Table 67 Proxim 4900, Proprietary Settings Fields and Default Values

Setting	Default	Description
4.9GHz Public Safety Channel Bandwidth	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.
802.11a/4.9GHz Public Safety Operational Mode	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.

11. To configure Colubris-only settings in this device group, locate the **Colubris** section and define the required fields. [Table 68](#) describes the settings and default values.

Table 68 Colubris-only Fields and Default Values

Setting	Default	Description
Rogue Scanning	Yes	If enabled, Colubris access points 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.
Rogue Scanning Interval (10-600 secs)	600	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.
Automatic Channel Interval	12 Hours	Sets the frequency by which APs monitor radio channels for availability and activity.
First Radio	802.11b only 1 Mbps	Sets the operational mode and multicast data rate for the first Colubris radio.
Second Radio (CN330 only)	802.11b only 1 Mbps	Sets the operational mode and multicast data rate for the second Colubris radio, supported only for the Colubris CN330.

12. To configure Symbol-only settings, locate the **Symbol** section and define the required fields. [Table 69](#) describes the settings and default values.

Table 69 Symbol-only Fields and Default Values

Setting	Default	Description
Rogue Scanning	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.
Rogue Scanning Interval (5-480 min)	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.

13. To configure Enterasys R2 settings, locate the **Enterasys R2** section and define the required fields. [Table 69](#) describes the settings and default values.

Table 70 Enterasys Section Fields and Default Values

Setting	Default	Description
Operational Mode	802.11b + 802.11g	Drop-down menu defines the 802.11 settings to support with the Enterasys radio devices in this group. Supported options are as follows: <ul style="list-style-type: none"> ● 802.11a only ● 802.11b only ● 802.11g only ● 802.11b + 802.11g

14. Click **Save** when radio configurations as described above are complete, or click **Save and Apply** to retain changes and push them to network devices. Click **Revert** to return to the last saved changes.

An Overview of Cisco WLC 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 HP Procurve 420s, 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

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

1. Navigate to the **Groups > List** page and select a group that has been defined to support Cisco devices. Click the group name, or the Manage (wrench) icon, and the **Cisco WLC Config** option appears in the navigation pane at the top.
2. Navigate to the **Groups > List** page and create a new group to support Cisco devices with these steps:
 - Click **Add** from the **Groups > List** page to create a new group, enter a group name, and click **Add**.
 - Once AWMS prompts you with the **Groups > Basic** page, ensure that you enable device specific settings for Cisco WLC.
 - Once you click **Save** or **Save and Apply**, then the **Groups > Cisco WLC Config** sub-menu 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 49](#) and [Figure 50](#) illustrate this navigation pane.

Figure 49 *Groups > Cisco WLC Config* page illustration, contracted view

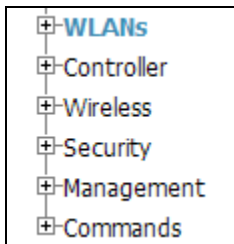
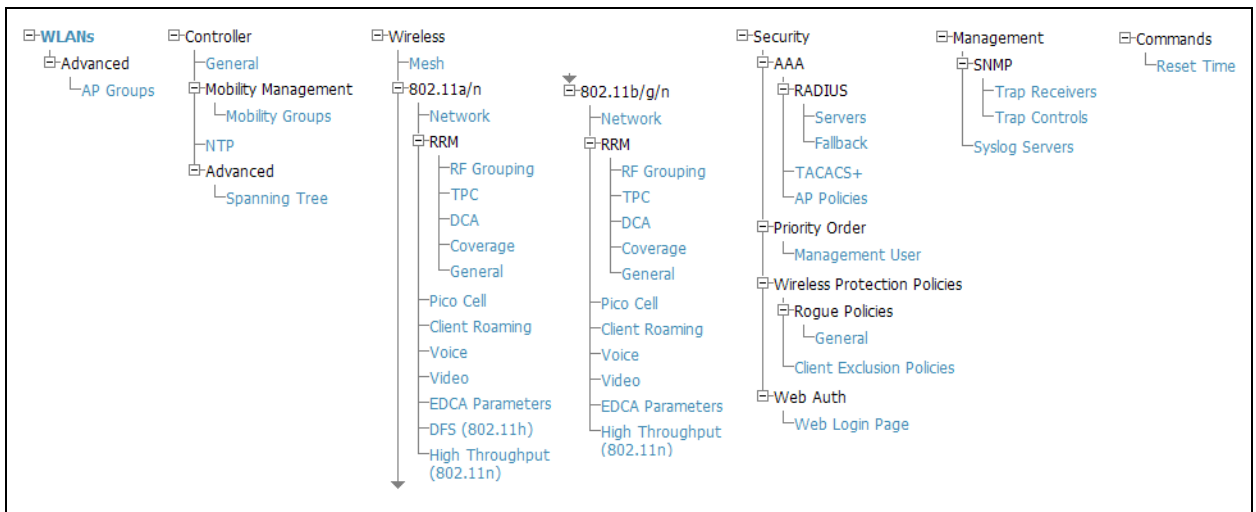


Figure 50 *Groups > Cisco WLC Config* page illustration, expanded view



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. Navigate to the **Groups > Cisco WLC Config** page, and click **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 51](#) 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 51 *Groups > Cisco WLC Config > WLANS page illustration*

The screenshot shows the Cisco WLC Config page for the 'Cisco Gear' group. The 'WLANs' section is active, displaying a list of 10 WLANs. The table below summarizes the data shown in the screenshot:

Profile	SSID	Admin Status	Encryption Mode	Radius Profile
5500 8021x	5500 8021x	Yes	Require 802.1X	All
5500 CKIP	5500 CKIP lab la la	Yes	Static CKIP	All
5500 guest	5500 guest_bundle	Yes	No Encryption	All
5500 wep short ascii 3	5500 wep short ascii 3	Yes	No Encryption	All
5500 WPA PSK	5500 WPA PSK	Yes	WPA2/PSK	All
5500 WPA2 PSK	5500 WPA2 PSK	Yes	WPA2/PSK	All
5500 WPA2 WEB	5500 WPA2 WEB	Yes	No Encryption	All
5500 WPA2C RADIUS	5500 WPA2C RADIUS	Yes	WPA2	All
5500-wpa-psk-hex	5500-wpa-psk-hex	Yes	WPA/PSK	All
5500-wpa2-psk-hex	5500-wpa2-psk-hex	Yes	WPA2/PSK	All

3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either click the **Add New SSID/VLAN** button, or click 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.



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

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

Group: cisco-ios,airespace and switches

General Security QoS Advanced

General

Profile:

SSID:

Admin Status: Yes No

Specify Interface Name: Yes No

Interface: 5500_guest_interface

Radio Policy: All

Broadcast SSID: Yes No

Add Cancel

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

General Security QoS Advanced

Security

Encryption Mode: No Encryption

Web Policy: Disabled

AAA Servers

RADIUS Authentication Server #1: Select

RADIUS Authentication Server #2: Select

RADIUS Authentication Server #3: Select

RADIUS Accounting Server #1: Select

RADIUS Accounting Server #2: Select

RADIUS Accounting Server #3: Select

Figure 54 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > QoS Tab Illustration*

Group: cisco-ios,airespace and switches

General Security QoS Advanced

QoS

Quality of Service: Silver (best effort)

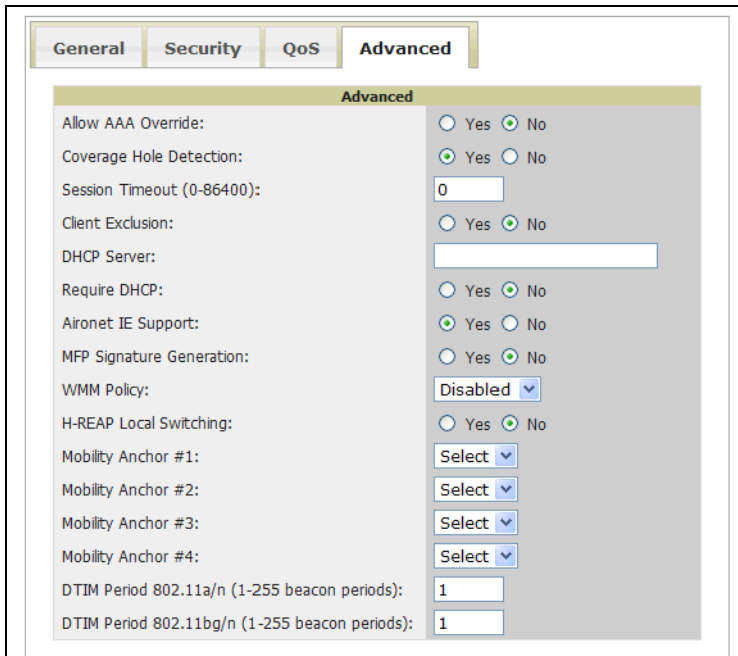
Platinum (voice)

Gold (video)

Silver (best effort)

Bronze (background)

Figure 55 *Groups > Cisco WLC Config > WLANs > Add New SSID/VLAN > Advanced Tab Illustration*



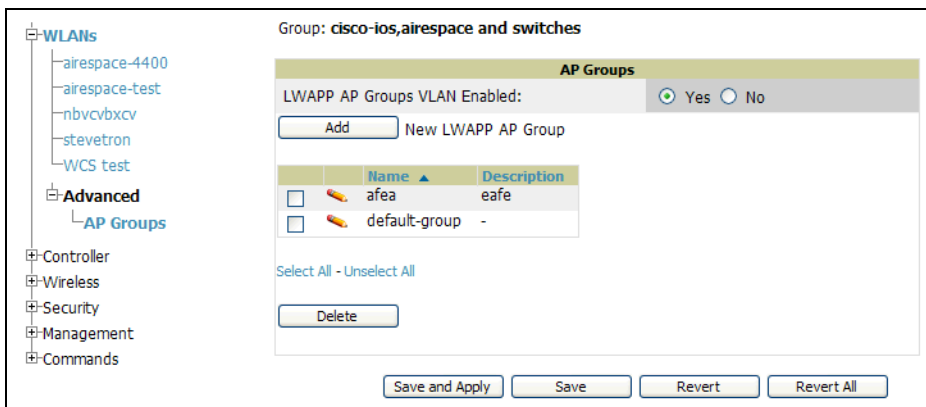
Defining and Configuring LWAPP AP Groups for Cisco Devices

The Groups > Cisco WLC Config > WLANs > Advanced > AP Groups page allows the user 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 AP Groups

1. Navigate to the Groups > Cisco WLC Config page, and click WLANs > Advanced > AP Groups in the navigation pane at left. This page displays the configured LWAPP APs. [Figure 56](#) illustrates this page.

Figure 56 *Groups > Cisco WLC Config > WLANS > Advanced > AP Groups Page Illustration*



2. To add a new LWAPP AP group, click **Yes** in the **AP Groups** section. Additional controls appear.
3. Click the **Add** button to create a new LWAPP AP group. To edit an existing LWAPP AP group, click 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. Click **Save and Apply** to push these settings to the Cisco WLC controllers immediately, or click **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, Cisco mobility groups to be supported on Cisco controllers, Network Transfer Protocol (NTP), and Spanning Tree Protocol settings.

Navigate to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in [Figure 57](#).

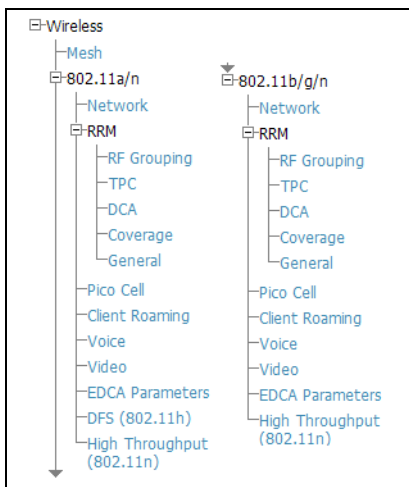
Figure 57 *Groups > Cisco WLC Config > Controller Navigation*



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 58](#).

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



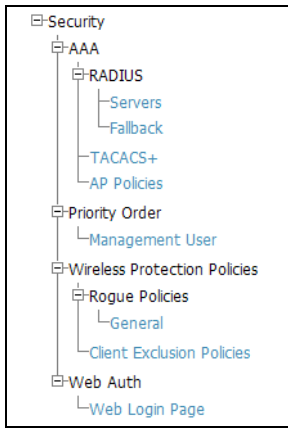
Configuring Security Parameters and Functions

AWMS 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 59](#) illustrates these components and this navigation:

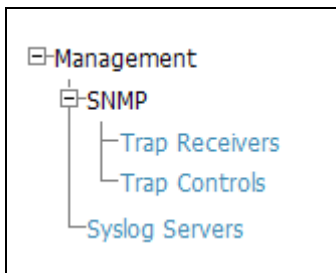
Figure 59 *Groups > Cisco WLC Config > Security Navigation Illustration*



Configuring Management Settings for Cisco

AWMS allows you to configure of SNMP and Syslog Server settings for Cisco WLC controllers. Users should be able to 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, navigate to the **Groups > Cisco WLC Config > Management** page, illustrated in [Figure 60](#).

Figure 60 *Groups > Cisco WLC Config > Management Navigation Illustration*



Configuring Group PTMP/WiMAX Settings

The **Groups > PTMP/WiMAX** configuration page configures Point-to-Multipoint and WiMAX settings 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.

Packet identification rules (PIR) are used to identify traffic types. Service flow classes define the priority given to traffic. Subscriber Station classes link traffic types (PIRs) with service flow classes to fully define how packets should be handled.

Perform the following steps to configure these functions.

1. Navigate to the **Groups > List** page and select the group for which to define PTMP/WiMAX settings by clicking the group name. Alternatively, click **Add** from the **Groups > List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Click the PTMP/WiMAX tab in the AWMS navigation menu. [Figure 61](#) illustrates this page.

Figure 61 *Groups > PTMP/WiMAX Page Illustration*

3. Define the settings on this page. [Table 71](#) describes the settings and default values.

Table 71 *Groups > PTMP/WiMAX Fields and Default Values*

Setting	Default	Description
Proxim MP.16 Section		
3.5GHz WiMAX Channel Bandwidth	3.5GHz	Sets the frequency used by the WiMAX devices in the group.
BSID	00:00:00:00:00:00	Defines the BSID used by the subscriber stations in the group. To define the BSID for a base station, refer to its APS/Devices > Manage configuration page.
Configure Packet Identification Rules	N/A	This link takes you to the list of packet identification rules for the group being configured. You can select rules to apply and add new rules, then return to the Group WiMAX page.
Configure Service Flow Classes	N/A	This link takes you to the list of service flow classes for the group being configured. You can select service flow classes to apply and add new classes, then return to the Group WiMAX page.
Configuration Subscriber Station Classes	N/A	This link takes you to the list of subscriber station classes. You can select subscriber station classes to apply and add new classes, then return to the Group WiMAX page.
Proxim MP.16 Section		
802.11a Radio Channel	58	Selects the channel used for 802.11a radios by the devices in this group.

Table 71 Groups > PTMP/WiMAX Fields and Default Values

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

- To configure packet identification rules, click the **Configure packet identification rules** link on the **Groups > PTMP/Wimax** configuration page and define the settings as required. Packet identification rules are used to define which packets match a subscriber station class. [Figure 62](#) illustrates this page and [Table 72](#) describes the settings and default values.

Figure 62 Groups > PTMP/WiMAX Configuring Packet Identification Rules Page Illustration

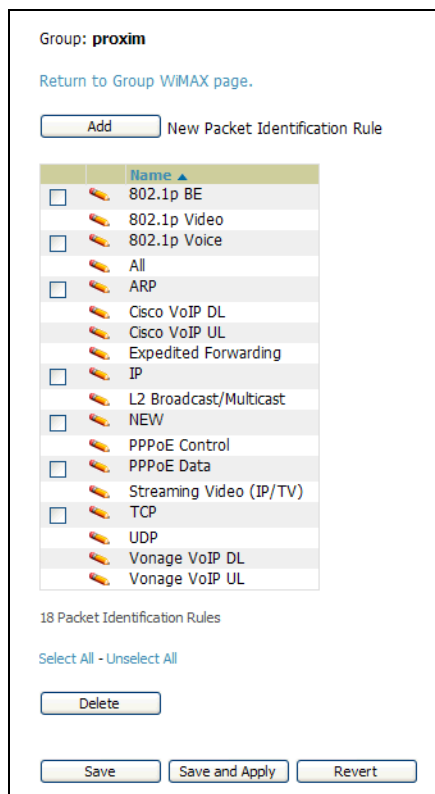


Table 72 PTMP/WiMAX Configuring Packet Identification Rules Fields and Default Values

Setting	Default	Description
Name	None	Text field defines a name for the PIR. The name should be meaningful and descriptive. The name is used to define the subscriber station class.
Use IP TOS	No	Identifies packets based on IP Type-of-Service for the PIR.
Minimum TOS Value (positive integer)	0	Specifies the minimum TOS used to identify packets.
Maximum TOS Value (positive integer)	0	Specifies the maximum TOS used to identify packets

Table 72 PTMP/WiMAX Configuring Packet Identification Rules Fields and Default Values

Setting	Default	Description
Mask (positive integer)	0	Specifies the TOS mask used to identify packets.
Use Ethernet Type	No	Identifies packets based on Ethernet type settings.
Ethernet Type	DIX SNAP	Drop-down menu specifies the Ethernet types used to identify a packet.
Ethernet Value (positive integer)	0	Identifies packets that have a specific ethernet value.
Ethernet Priority	No	Identifies packets based on Ethernet Priority settings.
Ethernet Priority Minimum (0-7)	None	Identifies packets that meet a minimum priority.
Ethernet Priority Maximum (0-7)	0	Identifies packets that meet a maximum priority.
Use VLAN ID	No	Identifies packets based on the VLAN ID.
VLAN ID (positive integer)	0	Specifies the VLAN that will be used to identify packets.
Use Source IP Address	No	Identifies packets based on source IP address.
Source IP address	None	Defines the source IP addresses that will be used to identify packets.
Use Destination IP Address	No	Identifies packets based on destination IP address.
Destination IP Address	None	Defines the destination IP addresses that will be used to determine identify packets.
Use IP Protocol	No	Identifies packets based on IP protocol.
IP Protocol (0-255)	None	Identifies packets that have a specific IP Protocol value.
Use Source MAC Address	No	Identifies packets based on Source MAC address.
Source MAC Address	None	Defines that packets from this MAC address match this PIR.
Use Destination MAC Address	No	Identifies packets based on Destination MAC address
Destination MAC Address	None	Defines that packets to this destination MAC address match this PIR.

- To configure service flow classes, click the **Configure service flow classes** link on the **Groups > PTMP/Wimax** configuration page, and define the settings. Service flow classes are used to describe how the device handles traffic. [Figure 63](#) illustrates this page and [Table 73](#) describes settings and default values.

Figure 63 PTMP/WiMAX Configuring Service Flow Classes Page Illustration

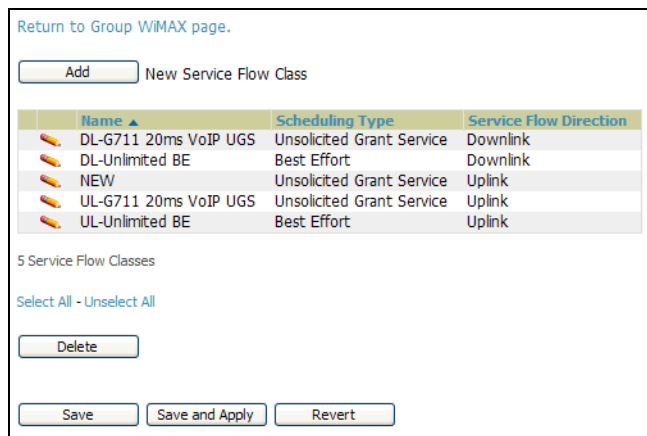


Table 73 Groups > PTMP/WiMAX Configure Service Flow Classes Fields and Default Values

Setting	Default	Description
Name	None	Text field defines the name of the Service Flow Class. The name should be meaningful and descriptive. The name is used to define the subscriber station class.
Scheduling Type	Best Effort	Drop-down menu specifies the scheduling priority for the Service Flow Class. There are two options as follows: <ul style="list-style-type: none"> • Best Effort—Maximum sustained data rate and traffic priority • Unsolicited Grant Service—Maximum sustained data rate, maximum latency and tolerable jitter.
Service Flow Direction	Uplink	Defines the direction of the service.
Maximum Sustained Data Rate (in Kbps)	0	Sets the maximum sustained data rate for this service class. The base station does not allow the data rate to exceed this value.
Traffic Priority (0-7)	7	Sets the priority of the traffic from 0 - 7 with 7 getting the highest priority.

- To configure subscriber station classes, click the **Configure subscriber station classes** link on the **Groups > PTMP/Wimax** configuration page. Subscriber station classes link packet identification rules and service flow classes. [Figure 64](#) illustrates this page and [Table 74](#) describes the settings and default values.

Figure 64 Groups > PTMP/WiMAX Configuring Subscriber Station Classes Page Illustration

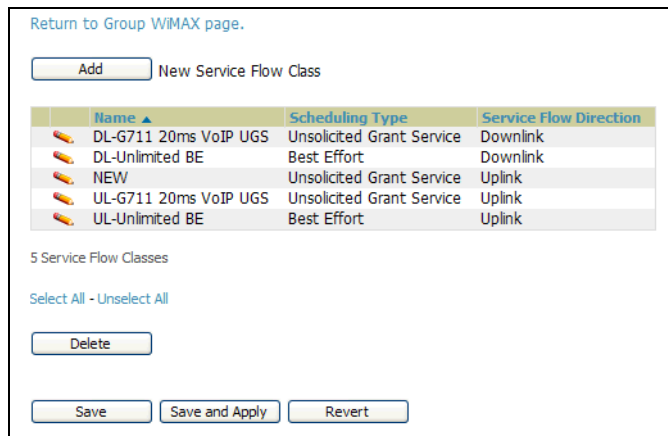


Table 74 Groups > PTMP/WiMAX Configuring Subscriber Station Classes Fields and Default Values

Setting	Default	Description
Name	None	Text field that defines the name of the Subscriber Station Class. The name should be meaningful and descriptive.
VLAN Mode	Transparent	Defines the VLAN mode.
Service Flows	None	Checkbox field that defines the service flow classes that apply to this Subscriber Station Class.
Packet Identification Rules	None	Define the priority for all of the packet identification rules.

- Click **Save and Apply** when configurations are complete and to push this configuration to controllers, or click **Save** to retain these settings prior to pushing to controllers at a later time.

Configuring Proxim Mesh Radio Settings

1. Navigate to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. [Figure 65](#) illustrates this page. [Table 74](#) and [Table 76](#) describe the settings and default values.

Figure 65 *Groups > Proxim Mesh Page Illustration*

The screenshot shows the configuration page for Proxim Mesh. It is divided into three main sections: General, Security, and Mesh Cost Matrix. The General section includes settings 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 (No). The Mesh Cost Matrix section includes settings 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, there are buttons for Save, Save and Apply, and Revert.

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

Table 75 *Groups > Mesh Radio Settings > General Fields and Default Values*

Setting	Default	Description
Mesh Radio	4.9/5Ghz	Drop-down selects the radio that acts as the backhaul to the network.
Max Number of Mesh Links	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.
Neighbor RSSI Smoothing	16	Specifies the number of beacons to wait before switching to a new link.
Roaming Threshold	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.
De-auth Client when Uplink is down	Yes	With Yes selected, clients have authentication removed (are deauthenticated) if the uplink is lost.

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

Table 76 *Groups > Mesh Radio Settings > Security Fields and Default Values*

Setting	Default	Description
SSID	None	Sets the SSID used by the Mesh Radio to connect to the mesh network.
Enable AES	No	Enable or Disable AES encryption.

3. The **Mesh Count 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 77](#) describes these settings and default values.

Table 77 *Groups > Mesh Radio Settings > Mesh Count Matrix Fields and Default Values*

Setting	Default	Description
Hop Factor	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.
Maximum Hops to Portal	4	Set the maximum number of hops for the AP to reach the Portal AP.
RSSI Factor	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.
Minimum RSSI Cutoff	10	Specifies the minimum RSSI needed to become a mesh neighbor.
Medium Occupancy Factor	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.
Current Medium Occupancy Weight	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. Click **Save** when configurations are complete to retain these settings. Click **Save and Apply** to retain these settings and push them to devices in the group. Click **Revert** to cancel out of these changes and return to the most recently saved changes.

Configuring Group MAC Access Control Lists

This configuration is optional. If you use Symbol 4121/4131, Intel 2011/2011b, Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP-3/4/5/6/7/8, or ProCurve 520WL wireless access points, AWMS 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.



Note: If **User MAC ACL** is enabled for Cisco VxWorks, AWMS does not disable this feature on the AP; but the MAC list entered is not populated on the AP. The individual MAC addresses must be entered manually on the AP. If you have APs from other vendors in the Group, the ACL restrictions do not apply to those APs.

Perform the following steps to use the MAC ACL function.

1. Browse to the **Groups > MAC ACL** configuration page. [Figure 66](#) illustrates this configuration page.

Figure 66 *Groups > MAC ACL Page Illustration*

The screenshot shows a web-based configuration interface for a group named 'proxim'. At the top, it says 'Group: proxim' and 'These settings apply to Proxim, Cisco Vxworks, Symbol, Intel and Procurve520 devices.' Below this is a section titled 'MAC ACL'. It contains a 'Use MAC ACL:' label with a dropdown menu currently set to 'Yes'. Below that is an 'Authorized MAC Addresses:' label with a text input field. A note below the input field states 'This list will not be set on Cisco VxWorks APs.' At the bottom of the form are three buttons: 'Save', 'Save and Apply', and 'Revert'.

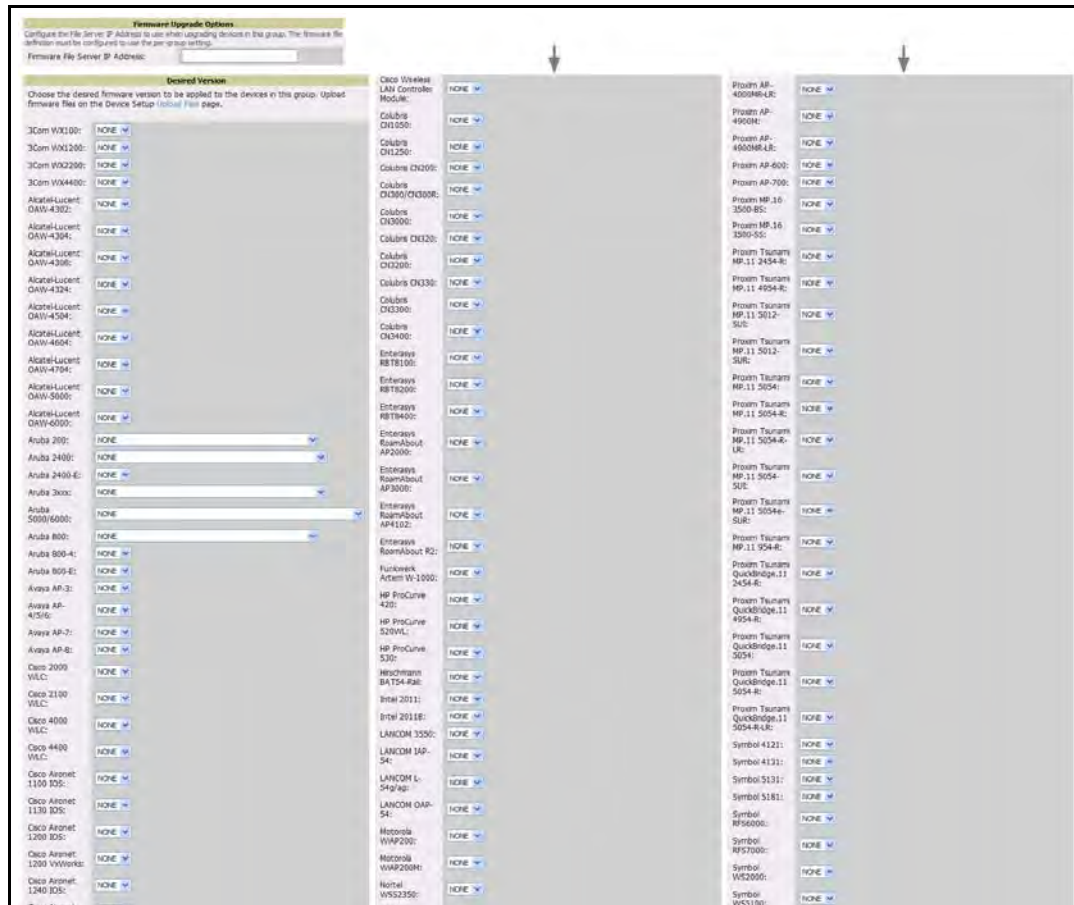
2. Select **Yes** on the **Use MAC ACL** drop-down menu. Enter all authorized MAC addresses, separated by white spaces.
3. Click **Save** when configurations are complete to retain these settings. Click **Save and Apply** to retain these settings and push them to devices in the group. Click **Revert** to cancel out of these changes and return to the most recently saved changes.

Specifying Minimum Firmware Versions for APs in a Group

This configuration is optional. AWMS 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, AWMS automatically upgrades all eligible APs. When you add APs into the group in the future, you will be able to upgrade APs in manual fashion. 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 67](#) illustrates this page.

Figure 67 Groups > Firmware Page Illustration (Partial View)



2. For each device type in the group, use the pull-down menu to specify the minimum acceptable firmware version. If no firmware versions are listed, you must browse to the **Device Setup > Firmware** configuration page to upload the firmware files to AWMS.
3. Click **Upgrade** to apply firmware preferences to devices in the group. Refer to the firmware upgrade help under **APs/Devices > Manage** configuration page for detailed help on Firmware job options.
4. Click **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 > Firmware** 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 AWMS 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 AWMS is set to **Automatically Monitor/Manage New Devices** on the AWMS configuration page.
7. Browse to the **Groups > List** configuration page. See [Figure 41](#) for the **Groups > List** configuration page.

- 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 AWMS, each with saved configurations. Perform the following steps to compare two existing device groups:

- From the **Groups > List** page, click **Compare two groups**. Two drop-down menus appear.
- Select the two groups to compare to each other in the drop-down menus, and click **Compare**. The **Compare** page appears, displaying some or many configuration categories. [Figure 68](#) illustrates this page.

Figure 68 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
SNMP Trap Receiver #1 IP:	(empty string)	→	10.51.2.37
SNMP Trap Receiver #1 Name:	(empty string)	→	gauss
SNMP Trap Receiver #2 IP:	(empty string)	→	10.51.2.5
SNMP Trap Receiver #2 Name:	(empty string)	→	joule
SNMP Trap Receiver #3 IP:	(empty string)	→	10.51.2.15
SNMP Trap Receiver #3 Name:	(empty string)	→	mole
SNMP Version:	2c	→	1
SSH Version:	v1	→	v2
Show device settings for:	Only devices on this AMP	→	All devices
Spanning Tree Protocol:	No	→	Yes
Thin AP Discovery Polling Period:	15 minutes	→	30 minutes
User Data Polling Period:	5 minutes	→	10 minutes

- 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, click **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
 - Click **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 clicking **Edit** in the corresponding column heading. The appropriate configuration page appears.
- If you make and save changes to either or both groups, navigate back to the **Groups > List** page and click **Compare two groups**. Select the same two groups again for updated information.
- Additional topics in this document or in the *Aruba Configuration Guide* 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 AWMS 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. AWMS does not permit you to delete the current default Group.
3. Ensure there are no devices in the Group you wish to delete. AWMS 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. Select the checkbox and click **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. Click 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 navigate 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, or click **Save and Apply** to save and push configurations.
4. When all changes for the group are complete click the **Save and Apply** button. [Figure 69](#) illustrates the confirmation message that appears.

Figure 69 Configuration Change Confirmation

Confirm changes:

Group "Access Points"

Allow One-to-One NAT: No Yes

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.

Current time: December 20, 2007 2:45 pm PST

Start Date/Time:

5. AWMS 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** —This button applies the changes immediately to access points within the group. If you wish to edit multiple groups you must use the Preview button.

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



Note: To completely nullify the change request, click **Revert** on one of the group configuration pages after you have clicked **Cancel**.

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

Modifying Multiple Devices

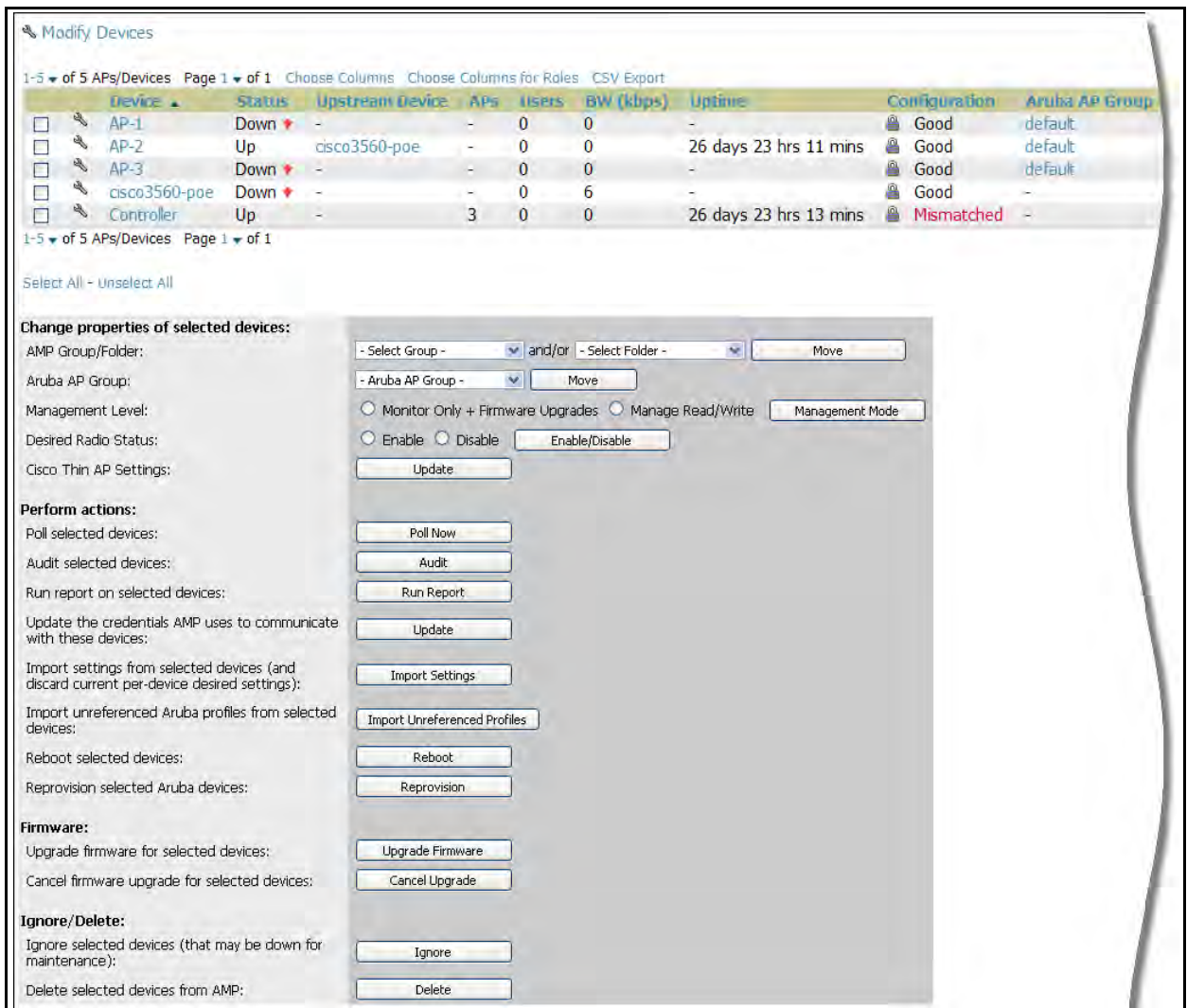
AWMS provides a very powerful utility that modifies all APs or a subset of access points unrelated to the typical AWMS group construct. This utility provides the ability to delete simultaneously multiple devices, migrate multiple devices to another group and/or folder, update credentials and optimize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

1. To modify multiple devices, navigate to one of the following pages:
 - **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

2. Click **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. [Figure 70](#) illustrates this page.

Figure 70 Modify Multiple Devices Section Illustration



3. Select one or more devices that are to share the configurations. Click inside the checkbox for each device to modify.
4. In the Modify Multiple Devices section, click 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, AWMS is able to optimize channel selection for APs. Select the APs to optimize and AWMS minimizes the channel interference while giving channel priority to the most heavily used APs. [Table 78](#) describes these action and controls.

Table 78 Modify Multiple Devices Section Fields and Default Values

Action	Description
Set Group/Folder	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.

Table 78 Modify Multiple Devices Section Fields and Default Values

Action	Description
Move to Dell PowerConnect W AP Group	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.
Desired Radio Status	Enables or disables the radios on the selected device. Does <i>not</i> apply Cisco IOS APs.
Update Cisco Thin AP Settings	Bulk configuration for per-thin AP settings, previously configured on the Group LWAPP AP tab can be performed from Modify Devices on the APs/Devices List page. Make changes to LWAPP AP groups, including the option that was under Modify Devices, is now available here.
Poll now	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 AWMS server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired AWMS configuration. The audit action updates the Configuration Status.
Run report on selected devices	Takes you to the Reports > Definitions page where you can define or run a custom report for selected devices. For more details and a procedure, see "Using Custom Reports" on page 265 .
Update the credentials AMP uses to communicate with these devices	Update. changes the credentials AWMS uses to communicate with the device. It does <i>not</i> change the credentials on the AP.
Import settings from selected devices (and discard current pre-device desired settings)	Audit updates a number of the AP specific settings AWMS initially read off of the AP including channel, power, antenna settings and SSL certifications. AWMS recommends using this setting if APs have been updated outside of AWMS. Most settings on the APs/Devices Manage configuration page are set to the values currently read off of the devices.
Reboot selected devices	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
Reprovision selected Dell PowerConnect W devices	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.
Upgrade firmware for selected devices	Upgrades firmware for the selected devices. Refer to the firmware upgrade help under APs/Devices > Manage configuration page for detailed help on Firmware job options.
Cancel firmware upgrade for selected devices	Cancels any firmware upgrades that are scheduled or in progress for the selected APs.
Ignore selected devices	Ignores selected APs, preventing AWMS from generating any alerts or including the AP in an up/down count. The device's history is preserved but it will not be polled. Ignored devices can be seen and taken out of ignore status by navigating to the New Devices configuration page and clicking the View Ignored Devices link at the bottom.
Delete selected devices from AMP	Removes the selected APs from AWMS. 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 AWMS global groups feature, first navigate to the **Groups > List** configuration page. Click the **Add** button to add a new group, or click the name of the group to edit settings for an existing group. Click the **Duplicate** icon 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 71](#) illustrates this configuration page.

Figure 71 *Groups > List Page Illustration*

	Name	SSID	Total Devices	Down	Mismatched	Ignored	Users	BW (kbps)	Up/Down Status	Polling Period	Duplicate
<input type="checkbox"/>	Access Points	wpa	38	4	32	0	0	0	5 minutes		
<input type="checkbox"/>	San Francisco	-	0	0	0	0	0	0	5 minutes		

- To set a group as a global group, navigate 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 check box next to fields on the **Basic**, **Security**, **SSIDs**, **AAA Servers**, **Radio**, **Cisco WLC Config**, **LWAPP APs**, **PTMP/WiMAX**, **Proxim Mesh** and **MAC ACL** tabs. [Figure 72](#) illustrates this configuration page.

Figure 72 *Groups > Basic Page for a Global Group*

Selecting a checkbox allows groups using global groups to override the corresponding setting.

Basic	Cisco IOS/VxWorks
Name: test	Cisco IOS SNMP Version: 2c
<input type="checkbox"/> Missed SNMP Poll Threshold (1-100): 1	<input type="checkbox"/> Cisco IOS CLI Communication: <input checked="" type="radio"/> Telnet <input type="radio"/> SSH
<input type="checkbox"/> Regulatory Domain: United States	<input type="checkbox"/> Cisco IOS Config File Communication: <input checked="" type="radio"/> TFTP <input type="radio"/> SCP
<input type="checkbox"/> Timezone: AMP system time	<input type="checkbox"/> Track Usernames on Cisco Aironet VxWorks: <input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="checkbox"/> Allow One-to-One NAT: <input checked="" type="radio"/> Yes <input type="radio"/> No	APs: <input type="checkbox"/> Configures devices to send SNMP traps to AMP

- 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 (navigate to the **Groups > SSIDs** configuration page and click the **Add** button). Global templates are also configurable as part of global groups; see [“Creating and Using Templates” on page 175](#) for more information.
- Once global groups have been configured, groups may be created or configured to subscribe to a particular global group. Navigate to the **Group > 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 click **Save and Apply** to push the configuration from the global group to the subscriber group. [Figure 73](#) illustrates this page.

Figure 73 *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: globalgroupMC (SSID: -)
globalgroupMC (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.
- In the example below, the field **Name** was overridden with the checkbox in the global group, so it can be configured for each subscriber group. The other four fields in the **Basic** section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can be altered only on the global group.

Figure 74 *Groups > Basic > Managed* Illustration for a Subscriber Group

Basic

Name: new_group

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: United States

Timezone: OV3600 system time
For scheduling group configuration changes

Allow One-to-One NAT: Yes No

Audit Configuration on Devices: Yes No

- 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 AWMS Stations with the Master Console” on page 239](#).

This chapter describes how to add, configure and monitor devices, both wired and wireless, and contains the following sections, corresponding to features of the AMP Device Setup tab:

- [“Device Discovery Overview” on page 127](#)
- [“Discovering and Adding Devices” on page 127](#)
- [“Monitoring Devices” on page 142](#)
- [“Configuring and Managing Devices” on page 158](#)
- [“Troubleshooting a Newly Discovered Device with Down Status” on page 172](#)

Device Discovery Overview

Once you have deployed AWMS on the network, the next step is to discover all existing APs connected to your network. AWMS has added the ability to discover and provision Cisco edge switches, and the ability to discover and monitor HP ProCurve and NetGear edge switches. You can gather statistics and generate reports displaying wired port usage, and error counting. Individual interface monitoring and configuration has also been added.

AWMS allows device discovery in the following ways, all of which are described in this chapter:

- **SNMP/HTTP scanning**—This is the primary method for AWMS to discover devices on your network, and this discovery method contains four specific procedures. The interface that configures this discovery method is the **Device Setup > Discovery** page. See [“SNMP/HTTP Scanning” on page 128](#).
- **Cisco Discovery Protocol (CDP)**—AWMS enhances support for CDP by discovering a device’s CDP neighbors. See [“Enabling Cisco Discovery Protocol \(CDP\)” on page 134](#).
- **Manual device entry**—This method of discovery applies when the devices are already on your network. The **admin** user adds devices manually with known device information. See the following section for information and procedures:
 - [“Assigning Devices to AWMS from APs/Devices > New Page” on page 134](#)
 - [“Manually Adding Individual Devices” on page 136](#)
 - [“Adding Multiple Devices from a CSV File” on page 139](#)
 - [“Adding Universal Devices” on page 140](#)
- **Controller-driven device discovery**—Thin APs will automatically be added to the network when you add their controller to AWMS.

Discovering and Adding Devices

Devices are prepared for discovery in the ways described in the previous section. This section describes the following topics:

- [SNMP/HTTP Scanning](#)
- [Enabling Cisco Discovery Protocol \(CDP\)](#)
- [Assigning Devices to AWMS from APs/Devices > New Page](#)
- [Manually Adding Individual Devices](#)

SNMP/HTTP Scanning

SNMP/HTTP scanning is the primary method for discovering devices on your network, including the discovery of rogue devices. Enable this scanning method from the **Device Setup > Discover** page.

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 SNMP/HTTP Scanning](#)—explains how to define network credentials for scanning. Credentials must be defined before using them in scan sets.
- [Defining a SNMP/HTTP 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.

Figure 75 illustrates the **Device Setup > Discover** page.

Figure 75 *Device Setup > Discover Page Illustration*

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.

red devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

Sets Page 1 of 1 [Choose Columns](#)

Network	Credentials	Total Devices Found	New Devices Found	Total Rogues Found	New Rogues Found	Start	Stop
.051.1.0	admin, default, private, public	8	8	1	0	8/26/2009 11:59 AM	8/26/2009 12:01 PM
.051.3.0	admin, default, private, public	30	30	0	0	8/26/2009 11:59 AM	8/26/2009 12:03 PM

Sets Page 1 of 1

Select All

Refresh this page for updated results.

[Filtering Options](#)

Networks

1 Networks Page 1 of 1 [Choose Columns](#)

Name	Network	Subnet Mask
10.51.1.0	10.51.1.0	255.255.255.0
10.51.3.0	10.51.3.0	255.255.255.0

1 Networks Page 1 of 1

Select All

Credentials

New Scan Credential

	Name	Type	Username
<input type="checkbox"/>	admin	HTTP	admin
<input type="checkbox"/>	default	HTTP	default
<input type="checkbox"/>	private	SNMPv1	-
<input type="checkbox"/>	public	SNMPv1	-

4 Scan Credentials

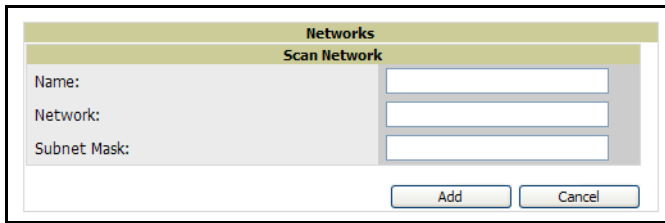
[Select All - Unselect All](#)

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. Navigate to the **Device Setup > Discover** page, and locate the **Networks** section.
2. In the **Networks** section, click **Add New Scan Network**. The **Scan Network** page appears, as shown in [Figure 76](#). Alternatively, you can edit an existing scan network by clicking the corresponding pencil icon. The **New/Edit Networks** page also appears in this instance.

Figure 76 *Device Setup > Discover > New Network Section Illustration*



The screenshot shows a web form titled "Networks" with a sub-section "Scan Network". It contains three text input fields labeled "Name:", "Network:", and "Subnet Mask:". At the bottom of the form are two buttons: "Add" and "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 AWMS supports is 255.255.0.0.
6. Click **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.

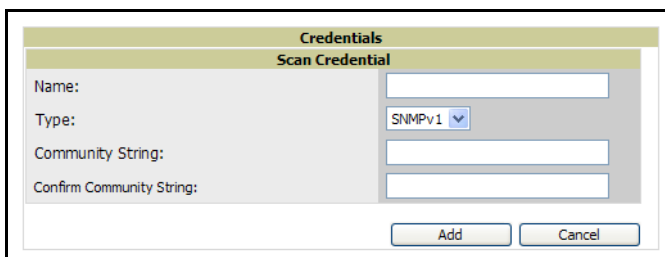
Adding Credentials for SNMP/HTTP Scanning

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, click **Add New Scan Credential**. [Figure 77](#) illustrates this page.

Figure 77 *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*



The screenshot shows a web form titled "Credentials" with a sub-section "Scan Credential". It contains four input fields: "Name:", "Type:" (a dropdown menu with "SNMPv1" selected), "Community String:", and "Confirm Community String:". At the bottom of the form are two buttons: "Add" and "Cancel".

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, we advise that you perform scans using SNMP for device discovery, but the following are considerations you should factor in to 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.

- 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 AWMS only uses it for discovering APs. To bring APs under management, AWMS uses the credentials supplied in the **Device Setup > SNMP** page.



Note: AWMS automatically appends the type of scan (SNMP or HTTP) to the Label.

- Click **Add**. The **Device Setup > Discover** page displays the new scan credential or credentials just created or edited.
- Repeat these steps to add as many credentials as you require.
- Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure titled “[Defining a SNMP/HTTP Scan Set](#)” on page 130.

Defining a SNMP/HTTP 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.

- Locate the **Scan Set** area at the top of the **Device Setup > Discover** page. [Figure 75](#), shown previously, illustrates this page. The **Scan Set** pane is illustrated in [Figure 78](#).

Figure 78 *Device Setup > Discover > Scan Sets Section Illustration*

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. If you have configured scan credentials for the selected networks, the scan set will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

n Sets Page 1 of 1

Network	Credentials	Total Devices Found	New Devices Found	Total Rogues Found	New Rogues Found	Start	Stop
.51.1.0	Default HTTP, private, public	7	0	0	0	5/5/2009 4:29 AM	5/5/2009 4:30 AM
.51.2.0	private, public	0	0	0	0	2/25/2009 1:46 PM	2/25/2009 1:50 PM
.51.3.0	Aruba AP's, Cisco, Cisco IOS APs, public	31	3	0	0	3/26/2009 2:31 PM	3/26/2009 2:35 PM
.51.5.0	private, public	6	0	0	0	1/9/2009 4:22 PM	1/9/2009 4:24 PM
remy's Lab	Cisco, public	0	0	0	0	3/27/2009 4:34 PM	3/27/2009 4:34 PM
Test Net 1	private, public	-	-	-	-	-	-
Test Net 2	private, public	-	-	-	-	-	-

Refresh this page for updated results.

Filtering Options

- Click **Add New Scan Set**, and the **Scan Set** section displays. Below the **Scan Set** section, the **Networks** and **Credentials** sections display all scan components configured so far. If you wish to create a new network, or new scanning credentials, you can click **Add** in either of these fields to create new components prior to creating a scan set. [Figure 79](#) illustrates the **Add New Scan Set** page.

Figure 79 Device Setup > Discover > Add New Scan Set Page 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.

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

Scan Set

Network: 10.51.3.0

Credentials:

- admin (HTTP)
- default (HTTP)
- private (SNMPv1)
- public (SNMPv1)

[Select All - Unselect All](#)

Networks

New Scan Network

1-2 of 2 Scan Networks Page 1 of 1 [Choose Columns](#)

	Name	Network	Subnet Mask
<input type="checkbox"/>	10.51.1.0	10.51.1.0	255.255.255.0
<input type="checkbox"/>	10.51.3.0	10.51.3.0	255.255.255.0

1-2 of 2 Scan Networks Page 1 of 1

[Select All - Unselect All](#)

Credentials

New Scan Credential

	Name	Type	Username
<input type="checkbox"/>	admin	HTTP	admin
<input type="checkbox"/>	default	HTTP	default
<input type="checkbox"/>	private	SNMPv1	-
<input type="checkbox"/>	public	SNMPv1	-

4 Scan Credentials

[Select All - Unselect All](#)

3. Select the **Network(s)** to be scanned and the **Credential(s)** to be used. You may select as many networks and credentials as you would like. AWMS defines a unique scan for each **Network-Credential** combination.
4. Click the **Add** button to create the selected scans. The newly defined scans appear in a list at the top of the **Device Setup > Discover** page.
5. To edit an existing scan, click the **pencil** icon next to the scan on the **Device Setup > Discover** page.
6. When ready, proceed to the next task, [“Running a Scan Set” on page 131](#).

Note: Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer access points, most D-Link, Linksys, 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 access points. Wireless scans and the Aruba Management Client discover these rogues without any special changes.

Running a Scan Set

Once a scan has been defined on the **Device Setup > Discover** page, AWMS can now scan for devices. Perform these steps.

1. Browse to the **Device Setup > Discover** page and locate the **Discovery Execution** area at the top of the page. This section lists all scan sets that have been defined so far. [Figure 80](#) illustrates this page.

Figure 80 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 [Com](#)

Note: Discovered devices will use the default credentials configured on the [Communication](#) page, *not* the credentials defined below for scanning.

New Scan Set

1-10 ▼ of 10 Scan Sets Page 1 ▼ of 1

	Network ▲	Credentials	Total APs Found	New APs Found	Total Rogues Found	New Rogues Found	Start	Stop
<input type="checkbox"/>	10.51.51.51	Default HTTP, private, public	1	0	0	0	2/27/2009 3:17 AM	2/27/2009
<input type="checkbox"/>	10.52.52.52	private, public	0	0	0	0	2/25/2009 1:46 PM	2/25/2009
<input type="checkbox"/>	10.53.53.53	private, public	22	0	0	0	2/27/2009 5:04 PM	2/27/2009
<input type="checkbox"/>	10.51.50.50	private, public	6	0	0	0	1/9/2009 4:22 PM	1/9/2009
<input type="checkbox"/>	10.90.90.90	private, public	0	0	0	0	1/9/2009 3:47 PM	1/9/2009

Select All - Unselect All

Refresh this page for updated results.

2. Check the box next to the scan(s) that you would like to execute.
3. Click **Scan** to execute the selected scans, and the scan immediately begins. The **Stop** column reads **In Progress**.
4. For future scans, click **Show Scheduling Options** and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, click the **Refresh** button in your browser to refresh the page and view the results of the scan you have just run. When the **Start** and **Stop** columns display date and time information, and no longer display **In progress**, the scan is available to display the results.
6. Click the Pencil icon for the scan you have just run to display the results. [Table 79](#) describes the scan results and related information.

Table 79 Device Setup > Discover > Discovery Execution Fields

Column	Description
Network	Displays the network to be scanned.
Credentials	Displays the credentials used in the scan.
Total APs Found	Displays the total number of APs detected during the scan that AWMS can configure and monitor. Total includes both APs that are currently being managed by AWMS as well as newly discovered APs that are not yet being managed.
New APs Found	Displays the number of newly discovered APs that are not yet being managed by AWMS but are available.
Total Rogues Found	Displays the total number of APs detected during the scan that AWMS could not configure or monitor. Total includes both APs that have been discovered in earlier scans as well as newly discovered APs from the most recent scan.
New Rogues Found	Displays the number of rogue APs discovered on the most recent scan.
Start	Displays the date and time the most recent scan was started.
Stop	Displays the date and time the scan most recently completed.
Scheduled	Displays the scheduled date and time for scans that are scheduled to be run.

7. Navigate to the **APs/Devices > New page** to see a full list of the newly discovered devices that the scan detected. [Figure 81](#) illustrates this page.

Figure 81 APs/Devices > New Page Illustration

To discover more devices, visit the [Discover](#) page.

1-35 ▼ of 35 APs/Devices Page 1 ▼ of 1 Choose Columns

<input type="checkbox"/>	Device	Controller	Type	IP Address	LAN MAC Address	Discovered ▼
<input type="checkbox"/>	Intel PRO/Wireless LAN	-	Intel 2011B	10.51.1.60	00:03:47:15:EA:53	11/2/2009 12:08 PM
<input type="checkbox"/>	R014-00861	-	Colubris CN3200	10.51.1.105	00:03:52:01:63:9C	11/2/2009 12:07 PM
<input type="checkbox"/>	RADIO4	RFS7000	Symbol AP 100	-	00:A0:F8:56:8B:40	10/30/2009 1:06 PM
<input type="checkbox"/>	AP0014.6940.8f22	Cisco_40:7c:83	Cisco Aironet 1240 LWAPP	10.51.1.94	00:14:69:40:8F:22	10/29/2009 9:20 PM
<input type="checkbox"/>	00:24:6c:c0:80:0f	Aruba3600-US	Intel 2011B	10.51.1.214	00:24:6C:C0:80:0F	10/29/2009 9:07 AM
<input type="checkbox"/>	AP1	Cisco_40:7c:83	Cisco Aironet 1250 LWAPP	10.51.1.98	00:1D:45:91:14:1A	10/16/2009 4:15 PM
<input type="checkbox"/>	AP-2	meru	Meru AP 150	-	00:0C:E6:00:DF:B6	10/13/2009 11:17 AM
<input type="checkbox"/>	AP-8	meru	Meru AP 201	-	00:12:F2:39:5D:A7	10/13/2009 11:17 AM
<input type="checkbox"/>	AP-3	meru	Intel 2011B	-	00:0C:E6:03:33:65	10/13/2009 11:17 AM
<input type="checkbox"/>	AP-7	meru	Meru AP 201	-	00:12:F2:39:57:AF	10/13/2009 11:17 AM
<input type="checkbox"/>	AP-4	meru	Meru AP 100	-	00:0C:E6:00:0B:0D	10/13/2009 11:17 AM
<input type="checkbox"/>	RADIO8	RFS7000	Symbol AP 100	-	00:A0:F8:56:8A:CD	10/12/2009 9:52 AM
<input type="checkbox"/>	AP-5	meru	Meru AP 320	-	00:0C:E6:05:01:6A	10/10/2009 12:07 PM
<input type="checkbox"/>	AP 124 - Trouble with capital T	Aruba2400	Alcatel-Lucent AP	10.51.5.17	00:1A:1E:C0:2B:34	10/9/2009 9:47 AM
<input type="checkbox"/>	Radio envy	Aruba2400	Intel 2011B	10.51.3.250	00:08:86:C7:07:EF	10/9/2009 9:47 AM
<input type="checkbox"/>	00:1a:1e:c6:d5:d2	Aruba800-FIPS	Alcatel-Lucent AP	10.51.1.232	00:1A:1E:C6:D5:D2	10/9/2009 9:46 AM
<input type="checkbox"/>	mesh-portal-C2:2e:4a	Aruba2400	Aruba AP 65	10.51.4.211	00:1A:1E:C2:2E:4A	10/9/2009 9:46 AM
<input type="checkbox"/>	Alcatel Lucent	-	Aruba Controller	10.51.5.31	-	10/9/2009 9:45 AM
<input type="checkbox"/>	00:1a:1e:c0:55:46	Aruba200	Intel 2011B	10.51.5.44	00:1A:1E:C0:55:46	10/9/2009 9:45 AM
<input type="checkbox"/>	00:1a:1e:c0:2b:3e	Alcatel-Lucent-4308	Alcatel-Lucent AP 124	10.51.1.248	00:1A:1E:C0:2B:3E	10/9/2009 9:45 AM
<input type="checkbox"/>	AP1	Cisco_40:7c:83	Cisco Aironet 1250 LWAPP	10.51.1.247	00:1D:45:91:14:42	10/9/2009 9:45 AM
<input type="checkbox"/>	AP0022.bd19.5f2b	Cisco_40:7c:83	Cisco Aironet 1140 LWAPP	10.51.1.142	00:22:BD:19:5F:2B	10/9/2009 9:45 AM
<input type="checkbox"/>	AP0018.19bd.a082	Cisco_40:7c:83	Cisco Aironet 1200 LWAPP	10.51.4.3	00:18:19:BD:A0:82	10/9/2009 9:45 AM
<input type="checkbox"/>	Talsker	Aruba200	Alcatel-Lucent AP	10.51.9.106	00:1A:1E:C6:D5:C2	10/9/2009 9:44 AM
<input type="checkbox"/>	Talsker	Aruba200	Aruba AP 105	10.51.9.105	00:24:6C:C0:00:F6	10/9/2009 9:44 AM
<input type="checkbox"/>	ap-Not set	Aruba-800-2X	Alcatel-Lucent AP	10.51.6.95	00:08:86:C7:9D:36	10/9/2009 9:43 AM
<input type="checkbox"/>	ap-Not set	Aruba-800-2X	Aruba AP 70	10.51.1.252	00:08:86:CE:E1:8C	10/9/2009 9:43 AM
<input type="checkbox"/>	ap-Not set	Aruba-800-2X	Alcatel-Lucent AP	10.51.8.114	00:08:86:C0:99:BC	10/9/2009 9:43 AM
<input type="checkbox"/>	ap-1.1.1	Aruba-800-2X	Aruba AP 65	10.51.5.2	00:1A:1E:C2:2E:F0	10/9/2009 9:43 AM
<input type="checkbox"/>	ap:78	Aruba3600-Local	Alcatel-Lucent AP	10.51.5.18	00:1A:1E:C0:50:78	10/9/2009 9:43 AM
<input type="checkbox"/>	3600 AP124	Aruba3600-Local	Aruba AP 124	10.51.5.19	00:1A:1E:C0:00:EC	10/9/2009 9:43 AM
<input type="checkbox"/>	Alcatel-Lucent AP	-	Aruba Controller	10.51.5.117	-	10/9/2009 9:43 AM
<input type="checkbox"/>	RADIO 4_4	WS2000_Controller	Symbol AP 100	-	00:A0:F8:56:8A:7D	10/9/2009 9:43 AM
<input type="checkbox"/>	brand new shiny name	Aruba-3400	Alcatel-Lucent AP	10.51.5.7	00:1A:1E:C2:2E:AE	10/9/2009 9:42 AM
<input type="checkbox"/>	00:1a:1e:c0:1a:dc	Aruba-3400	Aruba AP 125	10.51.1.215	00:1A:1E:C0:1A:DC	10/9/2009 9:42 AM

1-35 ▼ of 35 APs/Devices Page 1 ▼ of 1

Select All - Unselect All

View Ignored Devices

Group:

Folder:

Aruba AP Group:

LWAPP AP Group:

Monitor Only + Firmware Upgrades

Manage Read/Write

What Next?

- To assign one or more devices to a group, see [“Assigning Devices to AWMS from APs/Devices > New Page” on page 134.](#)
- To delete a device altogether from AWMS, select the corresponding check box for each device, and click **Delete.**
- Aruba and some Cisco devices can also be added to an Aruba AP Group or an LWAPP AP Group when they are authorized.

Enabling Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual switch or router on the **Groups > List** page. AWMS requires read-only access to a router or switch for all subnets that contain wired or wireless devices. As AWMS adds each router or switch, AWMS pings that device and initiates a connection using SNMP with the specified community string. This verifies that the proper IP address and community string have been provided.

Assigning Devices to AWMS from APs/Devices > New Page

Once you have discovered devices on your network, you must add these devices to a group. To configure a new group, refer to [“Configuring and Using Device Groups in AWMS” on page 79](#). When you add a device to a group, you must specify whether the device is to be placed in **Manage read/write** or **Monitor only** mode.

If you place the device in **Manage read/write** mode, AWMS compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy.

If you place the device in **Monitor read only** mode, AWMS 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.

Aruba recommends putting devices in **Monitor only** mode when they are added to a newly established 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, and the device vendor, model, MAC Address, IP Address, and the date/time of discovery. [Figure 82](#) illustrates this page.

Figure 82 APs/Devices > New

To discover more devices, visit the [Discover](#) page.

1-35 of 35 APs/Devices Page 1 of 1 Choose Columns

Device	Controller	Type	IP Address	LAN MAC Address	Discovered
<input type="checkbox"/> Intel PRO/Wireless LAN	-	Intel 2011B	10.51.1.60	00:03:47:15:EA:53	11/2/2009 12:08 PM
<input type="checkbox"/> R014-00861	-	Colubris CN3200	10.51.1.105	00:03:52:01:63:9C	11/2/2009 12:07 PM
<input type="checkbox"/> RADIO4	RFS7000	Symbol AP 100	-	00:A0:F8:56:8B:40	10/30/2009 1:06 PM
<input type="checkbox"/> AP0014.6940.8f22	Cisco_40:7c:83	Cisco Aironet 1240 LWAPP	10.51.1.94	00:14:69:40:8F:22	10/29/2009 9:20 PM
<input type="checkbox"/> 00:24:6c:c0:80:0f	Aruba3600-US	Intel 2011B	10.51.1.214	00:24:6C:C0:80:0F	10/29/2009 9:07 AM
<input type="checkbox"/> AP1	Cisco_40:7c:83	Cisco Aironet 1250 LWAPP	10.51.1.98	00:1D:45:91:14:1A	10/16/2009 4:15 PM
<input type="checkbox"/> AP-2	meru	Meru AP 150	-	00:0C:E6:00:DF:B6	10/13/2009 11:17 AM
<input type="checkbox"/> AP-8	meru	Meru AP 201	-	00:12:F2:39:5D:A7	10/13/2009 11:17 AM
<input type="checkbox"/> AP-3	meru	Intel 2011B	-	00:0C:E6:03:33:65	10/13/2009 11:17 AM
<input type="checkbox"/> AP-7	meru	Meru AP 201	-	00:12:F2:39:57:AF	10/13/2009 11:17 AM
<input type="checkbox"/> AP-4	meru	Meru AP 100	-	00:0C:E6:00:0B:0D	10/13/2009 11:17 AM
<input type="checkbox"/> RADIO8	RFS7000	Symbol AP 100	-	00:A0:F8:56:8A:CD	10/12/2009 9:52 AM
<input type="checkbox"/> AP-5	meru	Meru AP 320	-	00:0C:E6:05:01:6A	10/10/2009 12:07 PM
<input type="checkbox"/> AP 124 - Trouble with capital T	Aruba2400	Alcatel-Lucent AP	10.51.5.17	00:1A:1E:C0:2B:34	10/9/2009 9:47 AM
<input type="checkbox"/> Radio envy	Aruba2400	Intel 2011B	10.51.3.250	00:08:86:C7:07:EF	10/9/2009 9:47 AM
<input type="checkbox"/> 00:1a:1e:c6:d5:d2	Aruba800-FIPS	Alcatel-Lucent AP	10.51.1.232	00:1A:1E:C6:D5:D2	10/9/2009 9:46 AM
<input type="checkbox"/> mesh-portal-c2:2e:4a	Aruba2400	Aruba AP 65	10.51.4.211	00:1A:1E:C2:2E:4A	10/9/2009 9:46 AM
<input type="checkbox"/> Alcatel Lucent	-	Aruba Controller	10.51.5.31	-	10/9/2009 9:45 AM
<input type="checkbox"/> 00:1a:1e:c0:55:46	Aruba200	Intel 2011B	10.51.5.44	00:1A:1E:C0:55:46	10/9/2009 9:45 AM
<input type="checkbox"/> 00:1a:1e:c0:2b:3e	Alcatel-Lucent-4308	Alcatel-Lucent AP 124	10.51.1.248	00:1A:1E:C0:2B:3E	10/9/2009 9:45 AM
<input type="checkbox"/> AP1	Cisco_40:7c:83	Cisco Aironet 1250 LWAPP	10.51.1.247	00:1D:45:91:14:42	10/9/2009 9:45 AM
<input type="checkbox"/> AP0022.bd19.5f2b	Cisco_40:7c:83	Cisco Aironet 1140 LWAPP	10.51.1.142	00:22:BD:19:5F:2B	10/9/2009 9:45 AM
<input type="checkbox"/> AP0018.19bd.a082	Cisco_40:7c:83	Cisco Aironet 1200 LWAPP	10.51.4.3	00:18:19:BD:A0:82	10/9/2009 9:45 AM
<input type="checkbox"/> Talisker	Aruba200	Alcatel-Lucent AP	10.51.9.106	00:1A:1E:C6:D5:C2	10/9/2009 9:44 AM
<input type="checkbox"/> Talisker	Aruba200	Aruba AP 105	10.51.9.105	00:24:6C:C0:00:F6	10/9/2009 9:44 AM
<input type="checkbox"/> ap-Not set	Aruba-800-2X	Alcatel-Lucent AP	10.51.6.95	00:08:86:C7:9D:36	10/9/2009 9:43 AM
<input type="checkbox"/> ap-Not set	Aruba-800-2X	Aruba AP 70	10.51.1.252	00:08:86:CE:E1:8C	10/9/2009 9:43 AM
<input type="checkbox"/> ap-Not set	Aruba-800-2X	Alcatel-Lucent AP	10.51.8.114	00:08:86:C0:99:BC	10/9/2009 9:43 AM
<input type="checkbox"/> ap-1.1.1	Aruba-800-2X	Aruba AP 65	10.51.5.2	00:1A:1E:C2:2E:F0	10/9/2009 9:43 AM
<input type="checkbox"/> ap:78	Aruba3600-Local	Alcatel-Lucent AP	10.51.5.18	00:1A:1E:C0:50:78	10/9/2009 9:43 AM
<input type="checkbox"/> 3600 AP124	Aruba3600-Local	Aruba AP 124	10.51.5.19	00:1A:1E:C0:00:EC	10/9/2009 9:43 AM
<input type="checkbox"/> Alcatel-Lucent AP	-	Aruba Controller	10.51.5.117	-	10/9/2009 9:43 AM
<input type="checkbox"/> RADIO 4_4	WS2000_Controller	Symbol AP 100	-	00:A0:F8:56:8A:7D	10/9/2009 9:43 AM
<input type="checkbox"/> brand new shiny name	Aruba-3400	Alcatel-Lucent AP	10.51.5.7	00:1A:1E:C2:2E:AE	10/9/2009 9:42 AM
<input type="checkbox"/> 00:1a:1e:c0:1a:dc	Aruba-3400	Aruba AP 125	10.51.1.215	00:1A:1E:C0:1A:DC	10/9/2009 9:42 AM

1-35 of 35 APs/Devices Page 1 of 1

Select All - Unselect All

View Ignored Devices

Group:

Folder:

Aruba AP Group:

LWAPP AP Group:

Monitor Only + Firmware Upgrades

Manage Read/Write

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). Note that 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 click the **Add** button.

At this point you can navigate 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 AWMS, go to [step 4](#).



Note: If you select **Manage Select Devices**, AWMS automatically overwrites existing device settings with the specified Group settings. Aruba strongly recommends placing newly discovered devices in Monitor mode 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 click either **Ignore Selected Devices** or **Delete Selected Devices**. 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 AWMS in a subsequent scan.

Manually Adding Individual Devices

Some deployment situations may require that you manually add devices to AWMS. 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 AWMS 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 controllers and/or APs, and AWMS automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to AWMS:

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 83](#) illustrates this page.

Figure 83 *Device Setup > Add Page Illustration*

Select the type of device to add:

3Com 8750 [v] [Add] Import Devices via CSV

- 3Com 8750
- 3Com WX100
- 3Com WX1200
- 3Com WX2200
- 3Com WX4400
- APC**
- APC PDU
- Alcatel-Lucent**
- Alcatel-Lucent OAW
- Apple**
- Apple AirPort Graphite Base Station
- Aruba**
- Aruba Controller
- Avaya**
- Avaya AP-3
- Avaya AP-4/5/6
- Avaya AP-7
- Avaya AP-8
- BelAir**
- BelAir 200
- Cisco**
- Cisco Aironet 4800
- Cisco Aironet 340 VxWorks
- Cisco Aironet 350 VxWorks
- Cisco Aironet 1200 VxWorks
- Cisco Catalyst
- Cisco IOS AP
- Cisco WLC
- Colubris**
- Colubris CN200

2. Click **Add**, and the **Device Communications** and **Location** sections appear, illustrated in [Figure 84](#).

Figure 84 *Device Setup > Add > Device Communications and Location Page Illustration*

3. Complete these **Communications** and **Location** settings for the new device. [Table 80](#) further describes the contents of this page. Note that 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 80 *Device Communications and Location Fields and Default Values*

Setting	Default	Description
Name	None	User-configurable name for the AP (maximum of 20 characters).
IP Address (Required)	None	IP address of the device Ethernet page. If One-to-One NAT is enabled, AMP communicates with the AP on a different address (the IP address defined in the Device Communication area).
SNMP Port	161	Port AWMS uses to communicate with the AP using SNMP.
Community String (Confirm)	Taken from the Device Setup > Communication page	Community string used to communicate with the AP. NOTE: The Community String should have RW (Read-Write) capability.
SNMPv3 Username	Taken from the Device Setup > Communication page	Provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. AWMS initially uses this username and password combination to control the Cisco AP. AWMS creates a user-specified account with which to manage the AP if the User Creation Options are set to Create and user Specified as User. NOTE: 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.
Auth Password (Confirm)		

Table 80 Device Communications and Location Fields and Default Values

Setting	Default	Description
Privacy Password (Confirm)	Taken from the Device Setup > Communication page	SNMPv3 privacy password.
SNMPv3 Auth Protocol	Taken from the Device Setup > Communication page	Drop-down menu that allows you to enable the SNMPv3 authentication protocol to the device being added.
SNMPv3 Privacy Protocol	Taken from the Device Setup > Communication page	Drop-down menu that allows you to enable SNMPv3 privacy protocol to the device being added.
Telnet/SSH Username & Password (Confirm)	Taken from the Device Setup > Communication page	Telnet username and password for existing Cisco IOS APs. AWMS uses the Telnet username/password combination to manage the AP and to enable SNMP if desired. NOTE: New, out-of-the-box Cisco IOS-based APs typically have SNMP disabled with a default telnet username of Cisco and default password of Cisco . This value is required for management of any existing Cisco IOS-based APs.
Enable Password (Confirm)	Taken from the Device Setup > Communication page	Password that allows AWMS to enter enable mode on the AP.
HTTP Username & Password	Taken from the Device Setup > Communication page	HTTP password used to manage the AP initially, and to enable SNMP if desired. NOTE: Enter Intel if you are supporting new, out-of-the-box Intel APs.
Auth Password	Taken from the Device Setup > Communication page	SNMPv3 authentication password. NOTE: SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AWMS currently only supports authentication and encryption.
Privacy Password	Taken from the Device Setup > Communication page	SNMPv3 privacy password. NOTE: SNMPv3 supports three security levels: (1) no authentication and no encryption, (2) authentication and no encryption, and (3) authentication and encryption. AWMS currently only supports authentication and encryption.

- In the **Location** field, select the appropriate group and folder for the device. Refer to [Table 81](#).

Table 81 Device Setup > Communications > Add > Location Section Fields and Default Values

Setting	Default	AP Type	Description
Group	Default Group	All	This is a drop-down menu used to assign the AP to a Group .
Folder	Top	All	This is drop-down menu used to assign the AP to a Folder .

- 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 [“Assigning Devices to AWMS from APs/Devices > New Page”](#) on page 134.



Note: If you select **Manage read/write**, AWMS overwrites existing device settings with the **Group** settings. Aruba recommends placing newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings.

- Click **Add** to finish adding the devices to the network.

Adding Multiple Devices from a CSV File

Adding devices in bulk from a CSV file to AWMS is another option for adding all device types. Here you also have the option of specifying vendor name only, and AWMS will automatically determine the correct type while bringing up the device. Note that if your CSV file includes make and model information, AWMS 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 shown in illustrated in [Figure 85](#).

Figure 85 *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, navigate to the **Device Setup > Add** page.
2. Click **Import Devices via CSV**. The **CSV Upload** page displays, as illustrated in [Figure 86](#).

Figure 86 Device Setup > Add > Import Devices via CSV Page Illustration

Upload a list of devices

Location

Group: new group (SSID: -) ▾

Folder: Top ▾

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,
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,
10.70.36.172,public,Cisco-WLC-4012-3,Cisco 4000 WLC,
10.46.111.48,,
```

3. Select a group and folder into which to import the list of devices.
4. Click the **Browse...** button and navigate to the CSV list file.
5. Click **Upload** to add the list of devices into AWMS. The AWMS user interface provides additional instructions, supporting links, and examples of CSV file contents.

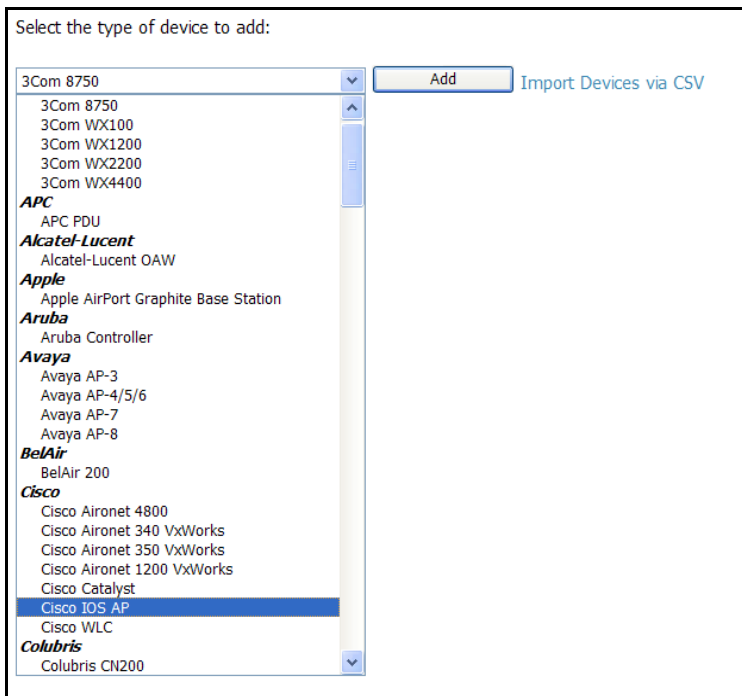
Adding Universal Devices

AWMS get basic monitoring information from any device including switches, routers and access points whether or not they are supported devices. Entering SNMP credentials is optional. If no SNMP credentials are entered, AWMS 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 AWMS 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 these steps to add universal devices to AWMS.

1. Browse to the AWMS **Device Setup > Add** page and select the device vendor name for the wired or wireless device you are adding. [Figure 87](#) illustrates this page.

Figure 87 Device Setup > Add Page Illustration



2. Click **Add**. Large numbers of Universal Network Devices can be added from a CSV file by clicking the **Import Devices via CSV** link.
3. Enter the name, IP address and read-only SNMP community string for the device.
4. Select the appropriate group and folder.
5. Click **Add**. All universal devices are added in **Monitor Only** mode.

AWMS 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 the device's interfaces on the **APs/Devices > Manage** page.

By clicking the pencil icon next to an interface, you can assign it to be non-monitored or monitored as Interface 1 or 2. AWMS collects this information and displays it on the **APs/Devices > Monitor** interface. AWMS supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. AWMS also monitors sysUptime.

Assigning Devices to the Ignored Page

There are two ways a device can be assigned to the **Ignored** page: from the **APs/Devices > New** page, or from the **APs/Devices > Manage** 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**.

- If you choose to ignore devices, they are not be displayed in the **APs/Devices > New** list if they are discovered in subsequent scans.
- If you choose to delete the device, it will be listed on the **APs/Devices > New** list if discovered by AWMS in a subsequent scan.

This procedure provides additional guidelines about using the **APs/Devices > Ignored** page. Perform these steps to further process or return an ignored device to a managed status.

1. To view all devices that are ignored, navigate to the **APs/Devices > Ignored** page, illustrated in [Figure 88](#).

Figure 88 APs/Devices > Ignored Page Illustration

1-20 of 78 Ignored APs/Devices Page 1 of 4 > >							
	Device	Controller	Type	IP Address	LAN MAC Address	Discovered	
<input type="checkbox"/>	hex-wiredclient	-	Cisco Aironet 1200 IOS	172.23.56.143	-	4/22/2009 12:06 PM	
<input type="checkbox"/>	00:1a:1e:c3:30:b8	Aruba800	Alcatel-Lucent AP 65	10.51.1.86	00:1A:1E:C3:30:B8	4/17/2009 12:02 PM	
<input type="checkbox"/>	00:0b:86:c1:a0:88	Aruba-3400	Aruba AP 65	10.51.6.115	00:0B:86:C1:A0:88	4/15/2009 11:09 AM	
<input type="checkbox"/>	00:1a:1e:c0:55:46	Aruba200	Aruba AP 125	10.51.1.51	00:1A:1E:C0:55:46	4/8/2009 4:02 PM	
<input type="checkbox"/>	00:1a:1e:c0:00:ec	aruba-3600-2	Aruba AP 124	10.51.1.55	00:1A:1E:C0:00:EC	4/7/2009 6:04 PM	
<input type="checkbox"/>	1.1.3	Aruba800	Alcatel-Lucent AP 65	10.51.1.3	00:0B:86:C0:99:BC	4/3/2009 5:44 PM	
<input type="checkbox"/>	00:1a:1e:c3:30:d4	Aruba200	Aruba AP 65-WB	10.51.1.52	00:1A:1E:C3:30:D4	4/3/2009 2:41 PM	
<input type="checkbox"/>	hp-530-3	-	HP ProCurve 530	10.51.3.218	00:14:C2:A5:08:B7	3/26/2009 2:32 PM	
<input type="checkbox"/>	00:1a:1e:c9:b2:5a	alpha-master-1	Aruba AP 125	10.3.18.239	00:1A:1E:C9:B2:5A	3/26/2009 2:08 PM	
<input type="checkbox"/>	00:1a:1e:c9:4f:4e	alpha-master-1	Aruba AP 125	10.3.18.240	00:1A:1E:C9:4F:4E	3/26/2009 1:38 PM	
<input type="checkbox"/>	Aruba650	-	Aruba Controller	10.3.18.3	-	3/26/2009 12:43 PM	
<input type="checkbox"/>	00:1a:1e:c9:b6:be	alpha-master-1	Aruba AP 125	10.3.18.245	00:1A:1E:C9:B6:BE	3/26/2009 11:08 AM	
<input type="checkbox"/>	00:1a:1e:c9:4e:f6	alpha-master-1	Aruba AP 125	10.3.18.247	00:1A:1E:C9:4E:F6	3/26/2009 11:08 AM	
<input type="checkbox"/>	00:0b:86:cc:cb:0a	ethersphere-lms3	Aruba AP 65	10.13.11.186	00:0B:86:CC:CB:0A	3/24/2009 9:34 PM	
<input type="checkbox"/>		-	Aruba Controller	10.3.18.38	-	3/24/2009 4:29 PM	
<input type="checkbox"/>	00:1a:1e:c9:9f:14	alpha-master-1	Aruba AP 125	10.3.18.248	00:1A:1E:C9:9F:14	3/24/2009 8:01 AM	
<input type="checkbox"/>	alpha-651-qaarea	-	Aruba Controller	10.3.18.107	-	3/23/2009 4:03 PM	
<input type="checkbox"/>	10.168.11.217	-	Aruba Controller	10.3.18.32	-	3/20/2009 5:56 PM	
<input type="checkbox"/>	alpha-local-dolcetto	-	Aruba Controller	10.3.18.10	-	3/19/2009 5:29 PM	
<input type="checkbox"/>	Symbol Access Point	-	Symbol 4131	10.51.3.67	00:A0:F8:4C:F3:18	3/9/2009 10:25 PM	

Select All - Unselect All

View New Devices

Group: Aruba HQ (SSID: aruba-ap, wpa)

Folder: Top

Monitor Only + Firmware Upgrades

Manage Read/Write

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 the device with the corresponding checkbox, and adjust group, folder, monitor, and manage settings as desired.
 3. Click **Add** to add the device to AWMS, so that it appears on the APs/Devices New list.

Monitoring Devices

This section discusses various device monitoring options and includes the following sections:

- [Viewing Device Monitoring Statistics](#)
- [Auditing Device Configuration](#)

Viewing Device Monitoring Statistics

You can view many useful device monitoring statistics as an aggregate, and individual from the APs/Devices > List page.

1. Browse to the APs/Devices > List page, which lists all devices that are managed or monitored by AWMS. Using the drop-down menu at the top of the Activity Area, you can determine whether to view all devices or only the devices from a specified folder. A lock icon in the Configuration column indicates that the device is in Monitor only mode. Figure 89 illustrates this page.

Figure 89 APs/Devices > List (partial split view accounts for horizontal scrolling)

Folder: **Top (38 Devices)** Expand folders to show all APs/Devices Go to folder: Top (38 Devices)

Total Devices: 38 Up: 34 Down: 4 Mismatched: 32 Users: 0 Avg/Device: 0 Bandwidth: 0 kbps

Users for folder Top Last 2 hours

Bandwidth for folder Top Last 2 hours

1-10 of 38 APs/Devices Page 1 of 4 > | Choose Columns

Device	Status	Upstream Device	APs	Users	BW (kbps)	Uptime	Configuration	Group	Controller	SSID
(id: 9)	Up	-	0	0	0	131 days 23 hrs 22 mins	Good	Access Points	-	-
3Com Access Point	Down	-	-	0	0	-	Unknown	Access Points	-	-
AaaS Test Customer	Down	-	0	0	0	-	Good	Access Points	-	-
ag-2100	Up	-	-	0	0	2 days 2 hrs 58 mins	Verifying	Access Points	-	-
Alcatel-Lucent-4308	Up	-	0	0	0	10 days 19 hrs 51 mins	Good	Access Points	-	-
ap	Up	-	-	0	0	74 days 21 hrs 46 mins	Verifying	Access Points	-	-
AP340-425e23	Down	-	-	0	0	-	Good	Access Points	-	-
ap-Cisco3	Up	-	-	0	0	97 days 1 hr 33 mins	Verifying	Access Points	-	-
Aruba200	Up	-	0	0	0	15 days 4 hrs 10 mins	Good	Access Points	-	-
Aruba200	Up	-	0	0	0	3 days 23 hrs 42 mins	Verifying	Access Points	-	-

1-10 of 38 APs/Devices Page 1 of 4 > |

Select All - Unselect All

Change properties of selected devices:

Group/Folder: - Select Group - and/or - Select Folder - Move

AP Group: - AP Group - Move

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

Desired Radio Status: Enable Disable Enable/Disable Update

Cisco Thin AP Settings: Update

Perform actions:

Audit selected devices: Audit

Run report on selected devices: Run Report

Update the credentials AMP uses to communicate with these devices: Update

Import settings from selected devices (and discard current per-device desired settings): Import Settings

Reboot selected devices: Reboot

Reprovision selected Aruba devices: Reprovision

Firmware:

Upgrade firmware for selected devices: Upgrade Firmware

Cancel firmware upgrade for selected devices: Cancel Upgrade

Ignore/Delete:

Ignore selected devices (that may be down for maintenance): Ignore

Delete selected devices from AMP: Delete

Alert Summary at 2/9/2010 1:21 PM

Type	Last 2 Hours	Last Day	Total	Last Event
Alerts	7	9	10	2/9/2010 11:58 AM
IDS Events	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

2. Verify that the devices you added are now appearing in the devices list with a Status of **Up**.



Note: Immediately after you have added the device to a group, notice the device **Status** change to **Down** while AWMS brings up the device and fetches the configuration from the device to compare it to the group settings. The device **Status** will change to **Up** when verification is complete.

The same section also appears on the **Groups > Monitor** page, and is hyperlinked from a controller's monitoring interface.

3. Navigate to the **Alert Summary** section of the **APs/Devices > List** page. The **Alert Summary** section 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 follows:
 - AMP Alerts
 - IDS Events
 - Incidents
 - RADIUS Authentication Issues



Note: The **Alerts Summary** table is also a feature of the **Home > Overview** page, and has the same links in that location.

Figure 90 *APs/Devices > List > Alert Summary Section Illustration*

Alert Summary at 3/4/2009 10:36 AM				
Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP/OV3600 Alerts	0	0	0	-
IDS Events	11	387	704	3/4/2009 10:30 AM
Incidents	0	0	2	2/27/2009 12:18 PM
RADIUS Authentication Issues	10	79	274	3/4/2009 10:28 AM

4. You can view details and incidents by clicking the specific **Alert Type**. The alert types and detailed information available for each are as follows:
 - **AMP Alerts**—Clicking this link takes you to the **AMP Alerts Summary** page, which cites detailed information for the current AMP Alerts. [Figure 91](#) illustrates this page.

Figure 91 APs/Devices > List > AMP Alerts

Summary

Alerts for devices in folder [Top](#) and subfolders | [Return to APs/Devices list](#)

Alert Type ▲	Last 2 Hours	Last 24 Hours	Total
Configuration Mismatch All device types	0	0	13
Device Down All device types	5	58	182
2 Alert Types	5	58	195

1-20 ▼ of 195 Alerts Page 1 ▼ of 10 > > |

<input type="checkbox"/>	Trigger Type	Trigger Summary	Triggering Agent	Severity	Time ▼
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 9:14 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 9:11 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 9:06 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 8:59 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 8:20 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 7:50 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 7:25 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 7:14 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 7:00 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 5:54 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 5:38 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 5:20 AM
<input type="checkbox"/>	Device Down	Device uptime indicates that device has rebooted	Unnamed	Major	5/15/2009 5:12 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 4:42 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 4:35 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 4:27 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 4:11 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 3:46 AM
<input type="checkbox"/>	Device Down	All device types	MXR-2-314644	Major	5/15/2009 3:15 AM
<input type="checkbox"/>	Device Down	All device types	Unnamed	Major	5/15/2009 2:44 AM

Select All - Unselect All

- **IDS Events**—Clicking this link takes you to the **IDS Events Summary** page, which cites detailed information according to folder.

Figure 92 APs/Devices > List, Alert Summary, IDS Events Summary Page Illustration

Summary

IDS Events for devices in folder [Top > HQ](#) | [Return to APs/Devices list](#)

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Death-Broadcast	0	29	29
Netstumbler Generic	0	280	530
Null-Probe-Response	7	80	147
3 Attack Types	7	389	706

1-20 ▼ of 706 IDS Events Page 1 ▼ of 36 > > |

<input type="checkbox"/>	Attack	Attacker	AP	Radio	Device	Channel	SNR	Precedence	Time ▼
<input type="checkbox"/>	Death-Broadcast	00:0C:46:68:3A:2A	Facilities-AL37	802.11bgn	aerospace-1	-	12	-	3/4/2009 8:29 AM
<input type="checkbox"/>	Death-Broadcast	00:0C:46:68:3A:2A	AP 1	802.11bg	aerospace-1	-	37	-	3/4/2009 8:29 AM
<input type="checkbox"/>	Death-Broadcast	00:0C:46:68:3A:2A	AP 2	802.11bg	aerospace-1	-	37	-	3/4/2009 8:29 AM
<input type="checkbox"/>	Death-Broadcast	00:0C:46:68:3A:2A	AP 3	802.11bg	aerospace-1	-	47	-	3/4/2009 8:29 AM

Select All - Unselect All

- **Incidents**—Clicking this link takes you to the **Incidents Summary** page, which cites all Helpdesk incidents and provides detailed information. Helpdesk incidents are opened with the **Helpdesk** tab.

Note: The **Incidents** portion of this **Alert Summary** table only increments the counter for incidents that are open and associated to an AP. The incidents are based on the Top folder on the **Groups > Monitor** page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in this **Alert Summary**. To view all incidents, including those not associated to an AP, navigate to the **Helpdesk > Incidents** page.



Figure 93 APs/Devices > List, Alert Summary, Incidents Summary

State	Last 2 Hours	Last Day	Total
Open	0	0	2
Closed	0	0	0
Total	0	0	2

New Incident

1-2 ▼ of 2 Incidents Page 1 ▼ of 1

	ID	Summary	State	Opened By	Related	Created	Updated
<input type="checkbox"/>	156	Bryan's connection problems	Open	mbruno	2	2/27/2009 12:18 PM	2/27/2009 12:19 PM
<input type="checkbox"/>	146	Katie's connectivity problem	Open	mbruno	3	2/12/2009 11:48 AM	2/12/2009 11:49 AM

Select All - Unselect All

- **RADIUS Authentication Issues**—Click this link to go to the related Summary page, to include groupings of RADIUS Authentication issues by type, and all such issues listed in chronological sequence and by folder. [Figure 94](#) illustrates this page.

Figure 94 RADIUS Authentication Issues Summary

Summary

RADIUS Authentication Issues for devices in folder [Top > HQ](#) | [Return to APs/Devices list](#)

Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Authentication server request timed out for aruba-supersvr	1	3	9
Authentication server request timed out for vortex	2	8	23
Client authentication failed	11	64	249
3 RADIUS Authentication Issue Event Types	14	75	281

1-20 ▼ of 281 RADIUS Authentication Issues Page 1 ▼ of 14 > > |

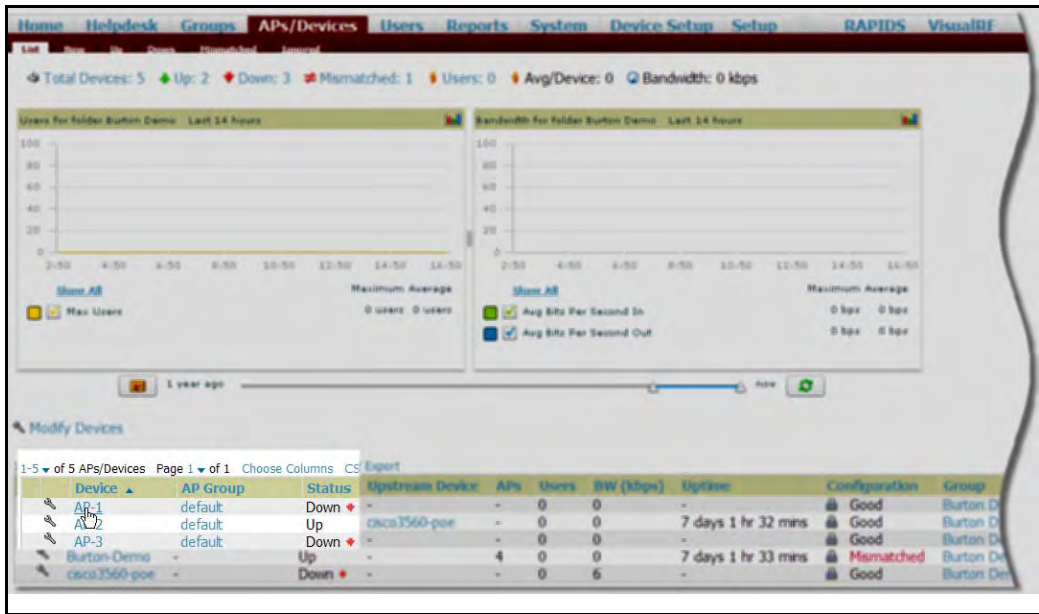
	Event	Username	User MAC Address	AP	Radio	Device	RADIUS Server	Time ▼
<input type="checkbox"/>	Client authentication failed for 00:1F:3B:00:1F:3B	-	00:1F:3B:00:1F:3B	-	-	aerospace-1	-	3/4/2009 12:19 PM
<input type="checkbox"/>	Client authentication failed for 00:1F:3B:00:1F:3B	-	00:1F:3B:00:1F:3B	-	-	aerospace-1	-	3/4/2009 12:19 PM
<input type="checkbox"/>	Client authentication failed for 00:1F:3B:00:1F:3B	-	00:1F:3B:00:1F:3B	-	-	aerospace-1	-	3/4/2009 12:17 PM
<input type="checkbox"/>	Client authentication failed for 00:21:5C:00:21:5C	-	00:21:5C:00:21:5C	-	-	aerospace-1	-	3/4/2009 7:26 AM

Select All - Unselect All

Understanding the APs/Devices > Monitor Pages for All Device Types

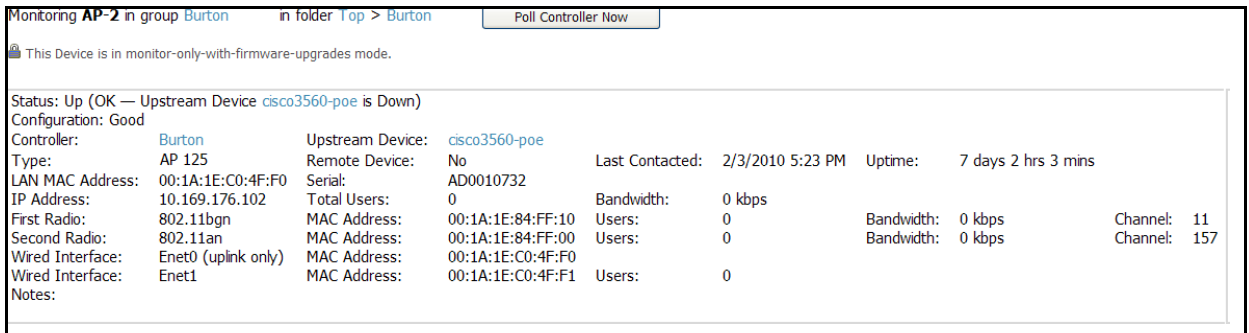
You can quickly go to any device's monitoring page once you navigate to its specific folder or group on the APs/Devices > List page, by clicking its hyperlinked name in the Device column of the table in which it is listed as shown in [Figure 98](#).

Figure 95 APs/Devices > List Page Showing Path to Monitor Page



All Monitor pages include a section at the top displaying information such as monitoring/configuration status, serial number, firmware version and so on, as shown in [Figure 96](#).

Figure 96 Monitoring Page Top Level Data Common to All Device Types



The alert summary, 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 97](#).

Figure 97 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'
Sat Jan 23 18:57:11 2010	admin	ap_group (id 2361): dot3_counters_enabled: '0' => '1', oldcisco_
Fri Jan 22 16:32:37 2010	admin	ap (id 15365): monitor_only: '0' => '1'

Monitoring pages vary slightly according to whether they are wired routers/switches or controllers/WLAN switches, or thin or fat APs. These differences are discussed in the sections that follow.

Monitoring Data Specific to Wireless Devices

APs/Devices > Monitor 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, a list of CDP and RF neighbors are also listed. A sample monitoring page for wireless devices is shown in [Figure 98](#).

Figure 98 APs/Devices > Monitor Page for Wireless Devices (partial view)

Monitoring AL7 in group Vaporsphere-wms3 in folder Top > HQ Poll Controller Now

This Device is in monitor-only-with-firmware-upgrades mode.

Status: Up (OK)
 Configuration: Good

Controller: ethosphere-lms3 Aruba AP Group: corp1344-2ndfloor Upstream Device: - Upstream Port: -
 Type: Aruba AP 125 Remote Device: No Last Contacted: 8/5/2010 1:36 PM Uptime: 102 days 3 hrs 50 mins
 LAN MAC Address: 00:1A:1E:CD:51:22 Serial: A30108337
 IP Address: 10.6.1.199 Total Users: 8 Bandwidth: 280 kbps Users: 2 Bandwidth: 0 kbps Channel: 11
 First Radio: 802.11bgn MAC Address: 00:1A:1E:55:12:20 Bandwidth: 280 kbps Channel: 149
 Second Radio: 802.11an MAC Address: 00:1A:1E:55:12:30 Bandwidth: 280 kbps Channel: 149
 Transmit Power: 9 dBm Antenna Type: Internal
 Transmit Power: 15 dBm Antenna Type: Internal

Notes:

Users on AL7 Last 1 day

Maximum Average
 Max Users (Radio 1) 0 users 0 users
 Max Users (Radio 2) 13 users 4 users

Bandwidth on AL7 Last 1 day

Maximum Average
 Avg In (Radio 1) 0 bps 0 bps
 Avg In (Radio 2) 465.1 kbps 31.8 kbps
 Avg Out (Radio 1) 0 bps 0 bps
 Avg Out (Radio 2) 11.6 Mbps 126.8 kbps

Location: HQ (Floor 1)

1 year ago now

Connected Users

1-11 of 11 Connected Users Page 1 of 1 Choose Columns Choose Columns for Roles CSV Export

Username	Role	MAC Address	SSID	VLAN	AP Radio	Connection Mode	Ch	BW	Association Time	Duration	Auth. Type	Cipher	Auth. Time	Sig. Qual.	BW
kaveh	employee	00:21:5C:09:86:57	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 11:40 AM	34 mins	WPA2	AES	34 mins	24	3 kbps
quest	visitor	00:1F:3C:23:91:0E	wpa2	63	802.11an	802.11a	-	-	2/17/2010 10:59 AM	1 hr 15 mins	No Encryption (PAP)	-	1 hr 15 mins	42	2 kbps
marcus	employee	00:21:5D:98:A1:82	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 9:39 AM	2 hrs 35 mins	WPA2	AES	2 hrs 35 mins	42	24 kbps
anderson	employee	00:1C:26:C5:39:D3	wpa2	65	802.11an	802.11a	-	-	2/17/2010 9:18 AM	2 hrs 55 mins	WPA2	AES	2 hrs 55 mins	42	1 kbps
garcia	employee	00:1F:38:79:EC:73	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 9:03 AM	3 hrs 10 mins	WPA2	AES	3 hrs 10 mins	42	2 kbps
peter	employee	00:1F:38:79:EC:E3	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 8:58 AM	3 hrs 16 mins	WPA2	AES	3 hrs 16 mins	23	5 kbps
tmazurco	employee	00:21:5C:09:28:85	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 8:18 AM	3 hrs 56 mins	WPA2	AES	3 hrs 56 mins	39	88 kbps
tlichti	employee	00:21:6A:7F:53:80	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 7:23 AM	4 hrs 51 mins	WPA2	AES	4 hrs 51 mins	31	3 kbps
dsanchez	employee	00:21:6A:48:F9:26	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 7:13 AM	5 hrs 1 min	WPA2	AES	5 hrs 1 min	43	153 kbps
aaron	employee	00:23:12:53:A1:58	wpa2	65	802.11an	802.11n (5GHz)	HT40	-	2/17/2010 6:38 AM	5 hrs 36 mins	WPA2	AES	5 hrs 36 mins	29	0 kbps
alopez	employee	00:1F:38:91:67:03	wpa2	65	802.11an	802.11a	-	-	2/17/2010 6:33 AM	5 hrs 41 mins	WPA2	AES	5 hrs 41 mins	40	0 kbps

1-11 of 11 Connected Users Page 1 of 1

RF Neighbors

AP/Device	Channel	Signal
AP-3	11	67
AL5	48	38
AL40	5	33
AL1	153	32
AL10	11	28

Show all neighboring APs

Table 82 describes the fields and information displayed in the General field.

Table 82 APs/Devices > Monitor > General Fields and Default Values

Field	Description
Poll Controller Now	Button 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.
Status	Displays ability of AWMS to connect to the AP. Up (no issue) means everything is working as it should. Down (SNMP "get" failed) means AWMS can get to the device but not speak with it using SNMP. Check the SNMP credentials AWMS is using the view secrets link on the APs/Devices > Manage page and verify SNMP is enabled on the AP. Many APs ship with SNMP disabled. Down (ICMP ping failed after SNMP get failed) means AWMS is unable to connect to the AP using SNMP and is unable to ping the AP. This usually means AWMS is blocked from connecting to the AP or the AP needs to be rebooted or reset.

Table 82 APs/Devices > Monitor > General Fields and Default Values (Continued)

Field	Description
Configuration	Good means all the settings on the AP agree with the settings AWMS wants them to have. Mismatched means there is a configuration mismatch between what is on the AP and what AWMS wants to push to the AP. The Mismatched link directs you to this specific APs/Devices > Audit page where each mismatch is highlighted.
Firmware	Displays the firmware version running on the AP.
Controller	Displays the controller for the associated AP device. Click the controller name hyperlink to display the APs/Devices > Monitor page, which contains detailed controller information. Controller information includes Status , operational metrics, Controller Client Count by SSID , Controller Bandwidth by SSID , CPU Utilization , Memory Utilization , APs Managed by this Controller , Alerts , and Recent Events . Figure 98 illustrates the Controller page.
Portal ^a	Specifies the mesh AP acting as the wired connection to the network for this mesh AP.
Mesh Mode ^b	Specifies whether the AP is a portal device or a mesh AP. The portal device is connected to the network over a wired connection. A mesh AP is a device downstream of the portal that uses wireless connections to reach the portal device.
Hop Count ^c	Displays the number of mesh links between this AP and the portal.
Type	Displays the make and model of the access point.
Last Polled	Displays the most recent time AWMS has polled the AP for information. The polling interval can be set on the Groups > Basic page.
Uptime	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 AWMS.
LAN MAC Address	Displays the MAC address of the Ethernet interface on the device.
Serial	Displays the serial number of the device.
Radio Serial	Displays the serial number of the radios in the device. NOTE: This field is not available for all APs.
Antenna Type	Indicates internal or external radio. For devices where antenna type is defined per AP, including Aruba devices, the same antenna type will be listed for each radio.
Radio Transmit Power	Some devices report transmit power reduction rather than transmit power; no value is reported for those devices.
Location	Displays the SNMP location of the device.
Contact	Displays the SNMP contact of the device.
IP	Displays the IP address that AWMS 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.
SSID	Displays the SSID of the primary radio.
Total Users	Displays the total number of users associated to the AP regardless of which radio they are associated to, at the time of the last polling.
First Radio	Displays the Radio type of the first radio (802.11a, 802.11b or 802.11g).
Second Radio	Displays the Radio type of the second radio (802.11a, 802.11b or 802.11g).
Channel	Displays the channel of the corresponding radio.
Users	Displays the number of users associated to the corresponding radio at the time of the last polling.
Bridge Links	Displays the number of bridge links for devices that are point-to-multi-point (see the Groups > PTMP/WiMAX page for more details).
Mesh Links ^d	Displays the total number of mesh links to the device including uplinks and downlinks.

Table 82 APs/Devices > Monitor > General Fields and Default Values (Continued)

Field	Description
Bandwidth	Displays the amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.
MAC Address	Displays the MAC address of the corresponding radio in the AP.
Last RAD Scan	Displays the last time the device performed a wireless rogue scan and the number of devices discovered during the scan.
Notes	Provides a free-form text field for entering fixed asset numbers or other device information. This information is printed on the nightly inventory report. Notes can be entered on the APs/Devices > Manage page.

- a. Field is only visible for Mesh APs.
- b. Field is only visible for Mesh APs.
- c. Field is only visible for Mesh APs.
- d. Field is only visible for Mesh APs.

Table 83 describes graph information displayed in the Graphical Data pane.

Table 83 APs/Devices > Monitor > Graphical Data Fields and Default Values

Graph	Description
User	Shows the max and average user 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.
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.
CPU Utilization (controllers only)	Reports overall CPU utilization (not on a per-CPU basis) of the controller.
Memory Utilization (controllers only)	Reports average used and free memory and average max memory for the controller.
Channel Utilization (Aruba controllers on supported firmware versions only)	Displays max and average percentages per-radio for busy, interfering receiving and transmitting signals. Special configuration on the controller is required to enable this data; consult the Aruba Best Practices Guide for details.

Table 84 describes the fields and information displayed for the Connected Users display.

Table 84 APs/Devices > Monitor > Connected Users Fields and Default Values

Field	Description
User	Provides the name of the User associated to the AP. AWMS gathers this data in a variety of ways. It can be taken from RADIUS accounting data, traps from Cisco VxWorks APs and tables on Colubris APs.
MAC Address	Displays the Radio MAC address of the user associated to the AP. Also provides a link that redirects to the Users > Detail page.
Radio	Displays the radio to which the user is associated.
Association Time	Displays the first time AWMS recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.

Table 84 APs/Devices > Monitor > Connected Users Fields and Default Values (Continued)

Field	Description
Auth. Type	<p>Displays the type of authentication employed by the user. Supported auth types are as follows:</p> <ul style="list-style-type: none"> ● EAP—Extensible Authentication Protocol, only reported by Cisco VxWorks using SNMP traps. ● PPTP—Point-to-Point Protocol, supported by Colubris APs acting as VPNs. ● RADIUS accounting—RADIUS accounting servers integrated with AWMS provide the RADIUS Accounting Auth type. ● Authenticated—a general category supporting additional authentication types. AWMS considers all other types as not authenticated. <p>The information AWMS displays in Auth Type and Cipher columns depends on what information the server receives from the APs and/or controllers 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 Auth Type or Cipher values may be reported to the AWMS server.</p> <p>If all APs are the same model and all are set up the same way, then another reason for differing Auth Types might be the use of multiple VLANs or SSIDs. One client device might authenticate on one SSID using one Auth Type and another client device might authenticate on a second SSID using a different Auth Type.</p>
Cipher	<p>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 Auth Type or Cipher values may be reported to the AWMS server.</p>
Auth. Time	Shows when the user authenticated.
Signal Quality	Displays the average signal quality the user experienced.
BW	Displays the average bandwidth consumed by the MAC address.
Location	Displays the QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP	Displays the IP assigned to the user MAC. This information is not always available. AWMS can gather it from the association table of Colubris APs or from the ARP cache of switches discovered by AWMS.
VPN IP	Displays the VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to AWMS.

Table 85 describes the fields of this QuickView page.

Table 85 QuickView Fields

Field	Description
AP Name	Displays the name of the AP that is linked with the currently viewed AP.
MAC Address	Displays the radio MAC address of the AP that is linked with the currently viewed AP.
Link Time	Displays date and time the link was initiated.
Duration	Displays length of time the two APs have been linked.
Link Type	Specifies the type of link, either uplink or downlink, connecting the two APs. An uplink leads to the portal AP. A downlink connects serves the viewed APs connection to the portal AP to other APs.
RSSI	Displays the RSSI observed between the two linked devices.
Hop Count	Displays the number of hops between the device and its portal.

The Recent Events area lists the most recent events specific to the AP. This information also appears on the System > Events Log page. Table 86 describes the fields in this page display.

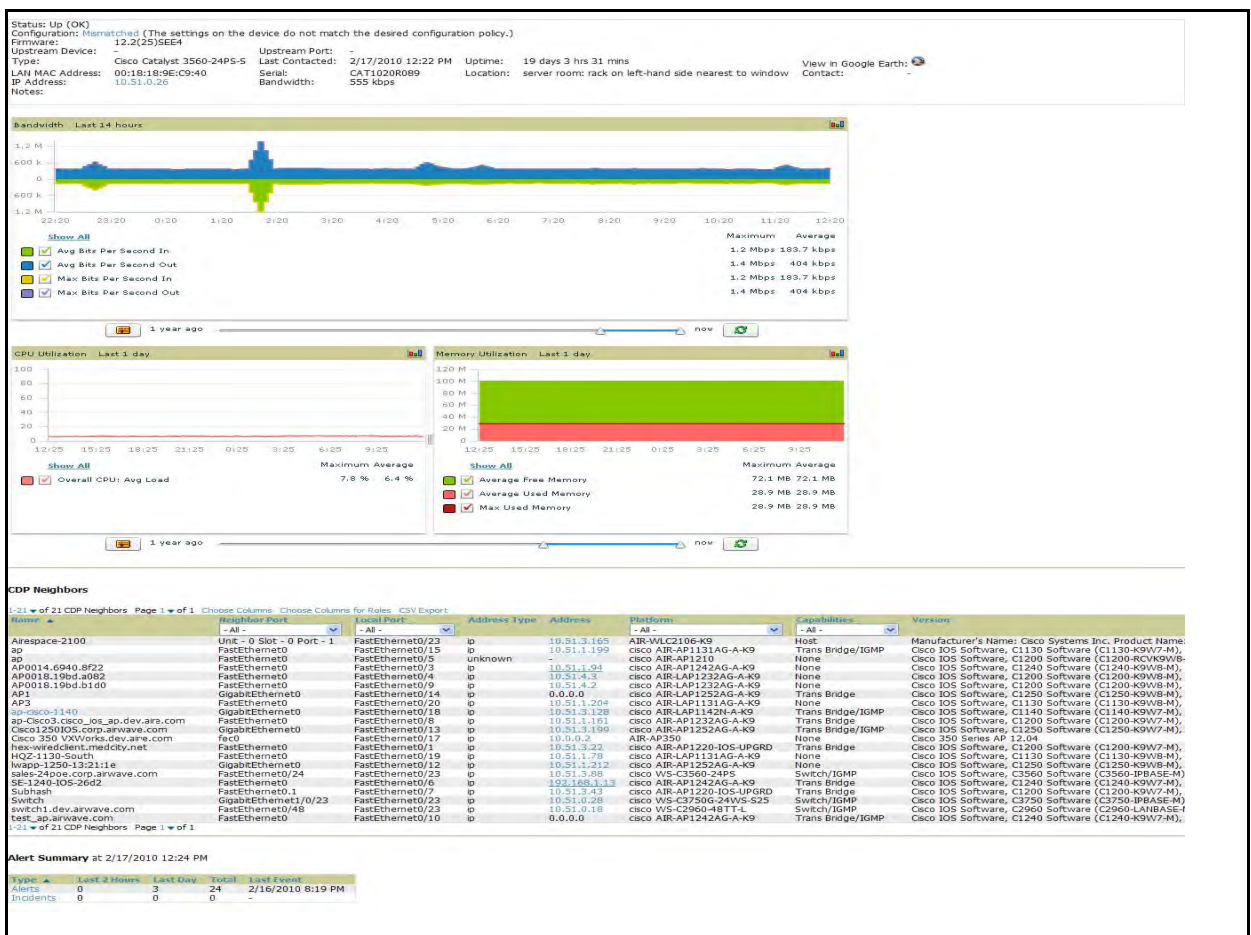
Table 86 APs/Devices > Monitor > Recent Events Fields and Default Values

Field	Description
Time	Displays the day and time the event was recorded.
User	Displays the user that triggered the event. Configuration changes are logged as the AWMS user that submitted them. Automated AWMS events are logged as the System user.
Event	Displays a short text description of the event.

Monitoring Data Specific to 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 99.

Figure 99 APs/Devices > Monitor Page for Wired Devices



All managed wired devices also include an Interfaces tab, as shown in Figure 100.

Figure 100 APs/Devices > Interfaces Page for Wired Devices (partial view)

The screenshot shows the 'Interfaces' page for a group of devices. At the top, there is a navigation bar with tabs for Home, Helpdesk, Groups, APs/Devices, Users, Reports, System, Device Setup, Setup, RAPIDS, and VisualRF. Below this is a sub-navigation bar with tabs for List, Monitor, Interfaces, Manage, Audit, Compliance, New, Up, Down, Mismatched, and Tempored.

The main content area is titled 'Interface Summary for C3750.corp.aire.com in group Cisco Gear in folder Top > HQ > Lab > RoutersSwitches'. It contains a small table with columns 'Switch', 'Total', 'Up', and 'Down'.

Below the summary is the 'Physical Interfaces' section. It has an 'Add' button and a 'New Interface' button. A red arrow points to the 'Edit Interfaces' link. Below this is a table with 78 interfaces. The table has columns: Name, Description, Alias, Interface Labels, Shutdown, MAC Address, Admin Status, and Switchport Trunk Allowed VLAN. A red arrow points to the 'Edit Interfaces' link below the table.

Below the physical interfaces is the 'Virtual Interfaces' section. It has an 'Add' button and a 'New Interface' button. A red arrow points to the 'Edit Interfaces' link. Below this is a table with 16 virtual interfaces. The table has columns: Device, Name, Description, Type, Interface Type, Alias, Interface Labels, Shutdown, and IP Address. Below the table are buttons for 'Delete' and 'Import Interfaces'.

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, labelled **Physical** and **Virtual**.

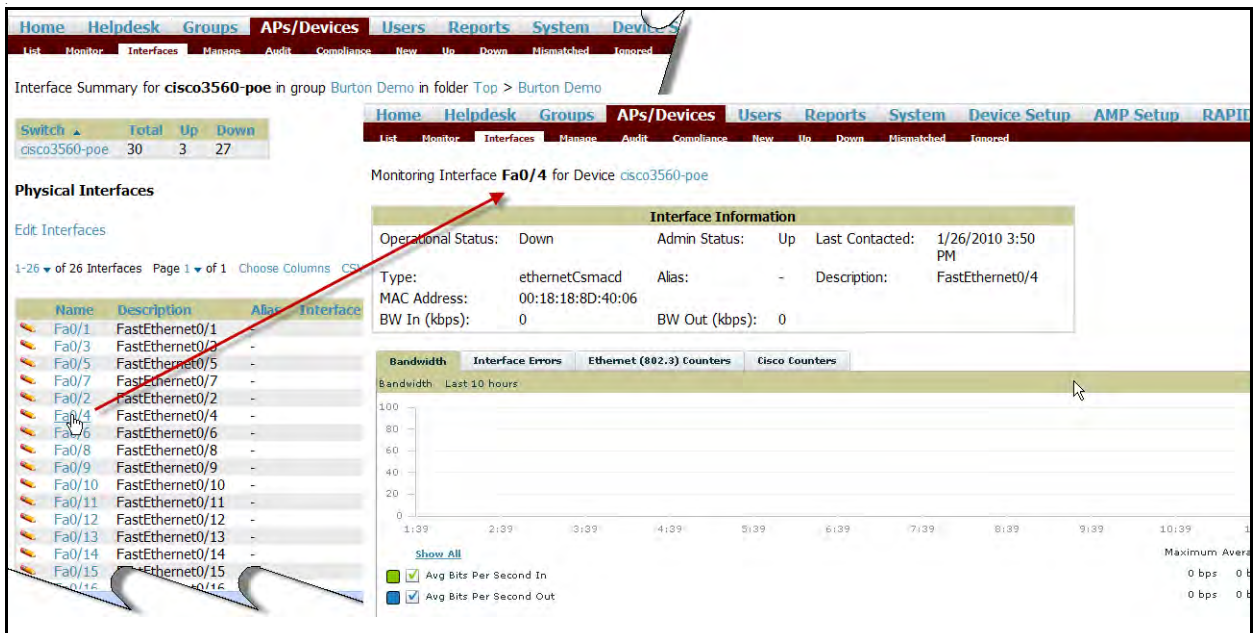
AWMS now monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by clicking one of the two **Edit Interfaces** hyperlinks as shown using red arrows in [Figure 100](#) above. You can edit both monitoring and configuration settings this way.

Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers. For more information on interface bandwidth triggers, see “[Monitoring and Supporting AWMS with the System Pages](#)” on page 249” on page 213.

Understanding the APs/Devices > Interfaces Page

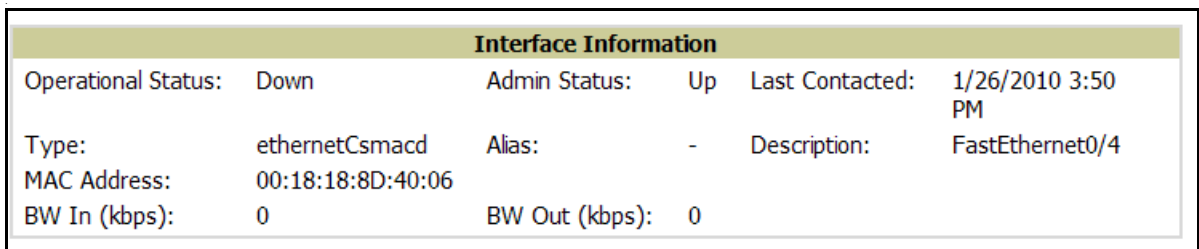
“[Monitoring Data Specific to Wired Devices \(Routers and Switches\)](#)” on page 153 shows you how to view high level interface information for all physical and virtual interfaces on an entire router or switch. Click any interface hotlink in the **Name** column of the Physical or Virtual Interfaces tables on the stacked switches **Interfaces** monitoring page to navigate to an **Interfaces** page displaying data relevant to that specific interface, as shown [Figure 101](#).

Figure 101 Individual Interface Monitoring Page



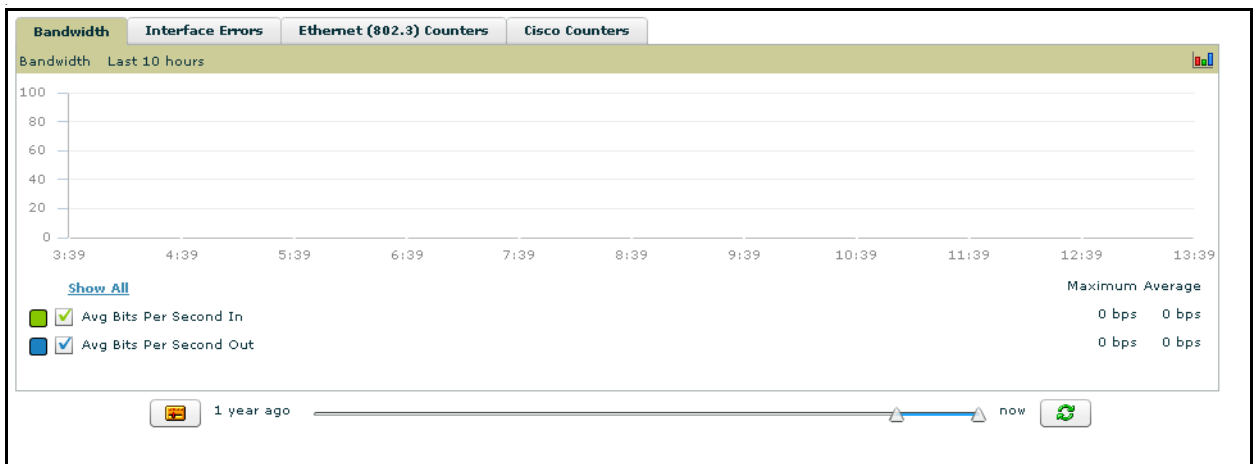
An individual **Interface** monitoring page includes is comprised of 2 panes. Specifics of the interface are in the upper pane, as depicted in [Figure 102](#).

Figure 102 Individual Interface Operational Status Information Pane



Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower pane in a tabbed graph as shown in [Figure 103](#).

Figure 103 Individual Interface Bandwidth and Error Counting Graph



What Next?

All device monitoring pages act as portals to management pages if you have the proper (read/write) privileges. Clicking the wrench or pencil icon next to a device table entry, or clicking **Modify Devices** where appropriate

above a device table, will take you to the appropriate Management page (APs/Devices > Manage). See “Configuring and Managing Devices” on page 158 for more information, and detailed procedures.

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.

AWMS 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 169 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 AWMS.
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**, click 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.



Note: After upgrade, the APs/Devices > Audit page, and certain additional pages, show only **Mismatched** status by default for non-template devices.

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 104 illustrates this page.

Figure 104 APs/Devices > Audit Page Illustration

Device Configuration of **ServerRoom-AL39** in group **Arba HQ** in folder **Top > HQ**
This Device is in monitor-only-with-firmware-upgrades mode.
Configuration read from device at 5/18/2009 2:26 PM

Configuration: Mismatched

Audit the device's current configuration.

[Show Archived Device Configuration](#)

Choose settings to ignore during configuration audits.

[Show entire config](#)

[Refresh this page](#)

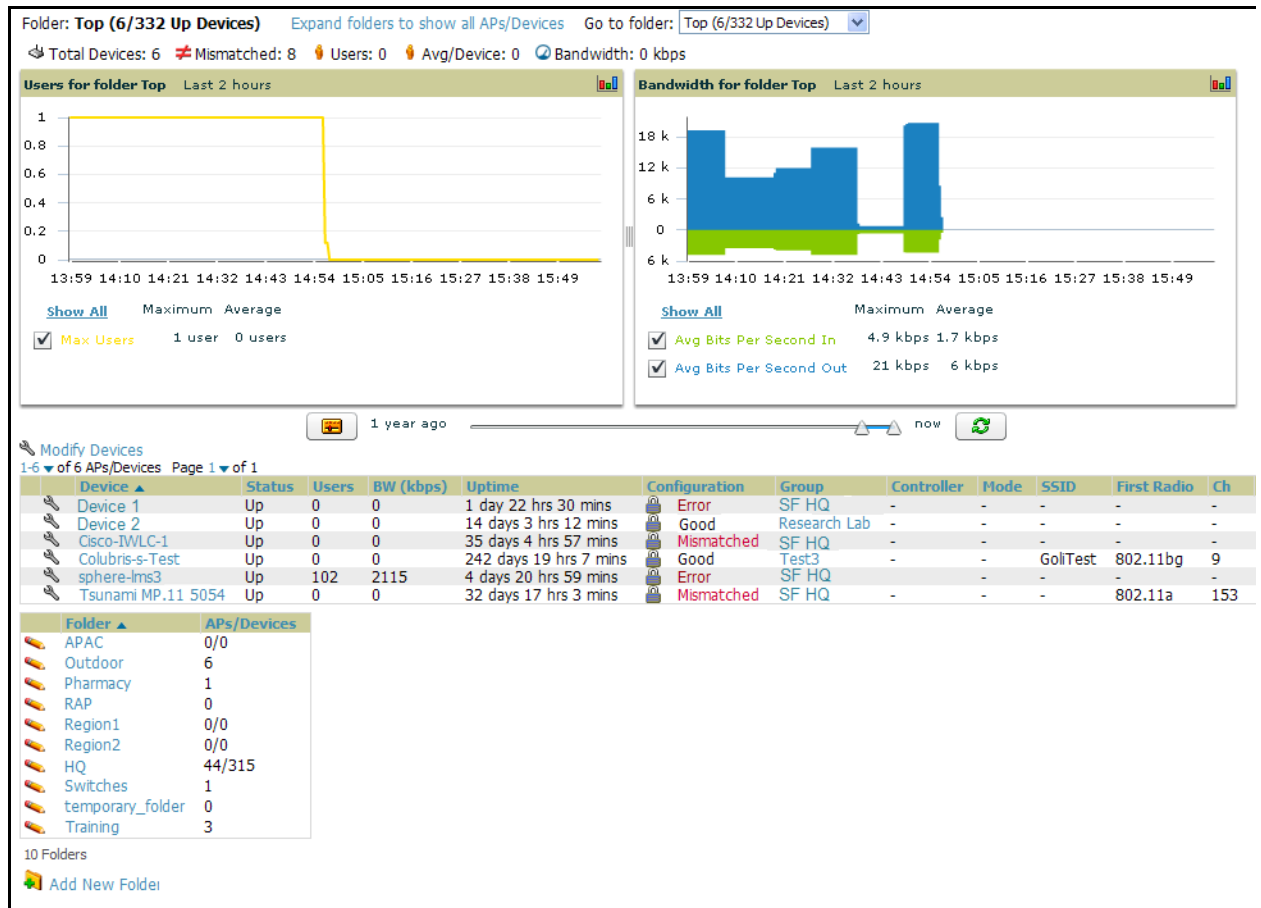
AP Settings		
	Current Device Configuration	Desired Configuration
Mesh Role	None	Mesh AP
Name	AL39	ServerRoom-AL39
System Properties		
	Current Device Configuration	Desired Configuration
Location	(not set)	Not Available

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 AWMS users can see. [Figure 105](#) and [Figure 106](#) illustrate this component.

Figure 105 APs/Devices > Up Page Example



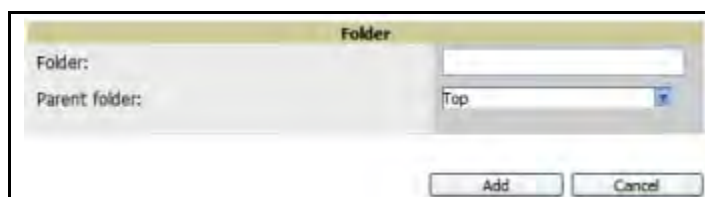
Folder views are persistent in AWMS. If you select the **Top** folder and then click the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

If you want to see every **down** device, click the **Expand Folders to show all devices** link. When the folders are expanded, you see all of the devices on AWMS 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 AWMS.

1. To add a folder, click the **Add New Folder** link. [Figure 106](#) illustrates the page that appears.

Figure 106 Folder Creation



2. Enter the name of the new folder.
3. Select the **Parent** folder.

4. Click 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 AWMS.

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” on page 158](#)
- [“Configuring AP Settings” on page 159](#)
- [“Configuring Device Interfaces for Cisco Catalyst Switches” on page 165](#)
- [“Individual Device Support and Firmware Upgrades” on page 169](#)

While most device configuration settings are managed by AWMS at a Group level to enable efficient change management, 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 would not make sense to configure RF channel settings at a Group level. Instead, channel settings are managed at an individual device level to avoid RF interference between two or more devices.



Note: Any changes made at an individual device level will automatically override Group level settings.

AWMS 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; devices 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 AWMS pages where any mismatched settings can be configured.



Note: 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 27](#).

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.



Note: Once a device is in Manage mode, AWMS 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** to **Manage Read/Write** mode, perform the following steps.

1. Navigate to the **APs/Devices > List** page and click 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 107](#).

Figure 107 APs/Devices > Manage > General Section Illustration

General	
Name:	symbol-3021-1
Status:	Up (OK)
Configuration:	Good (Ignoring mismatches)
Last Contacted:	5/19/2009 12:21 PM
Type:	Symbol 3021
Firmware:	04.02-19
Group:	HQ
Folder:	Top > HQ
Management Mode:	<input type="radio"/> Monitor Only + Firmware Upgrades <input checked="" type="radio"/> Manage Read/Write

3. Click **Manage Read/Write** on the **Management Mode** radio button to shift the device from **Monitor Only** to **Manage Read/Write** mode.
4. Click **Save and Apply** to retain these settings and to push configuration to the device.
5. AWMS presents a confirmation window reminding you of all configuration changes that will be applied to the device in **Manage** mode.
6. Click **Confirm Edit** to apply the changes to the device immediately, click **Schedule** to schedule the changes to occur during a specific maintenance window, or click **Cancel** to return to the **APs/Devices > Manage** page.
7. Some device configuration changes may require the device to reboot. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.
8. To move multiple devices into managed mode at once, use the **Modify these devices** link. Refer to “Modifying Multiple Devices” on page 122 for more information.

Configuring AP Settings

1. Browse to the **APs/Devices > List** page and click 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 108](#) illustrates this page.

Figure 108 APs/Devices > Manage Page Illustration

General		Settings	
Name:	ap125-meshportal-karen	Name:	ap125-meshportal-karen
Status:	Up (OK)	Domain Name:	
Configuration:	Good	Location:	
Last Contacted:	2/12/2010 10:29 AM	Contact:	
Type:	AP 125	Latitude:	10.02450899096407
Controller:	sphere-ims	Longitude:	0.7395866645358211
Group:	sphere-ims	Altitude (m):	0
Folder:	Top > HQ	Group:	sphere-ims3
Management Mode:	<input type="radio"/> Monitor Only + Firmware Upgrades <input checked="" type="radio"/> Manage Read/Write	Folder:	HQ
Notes		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:		<input type="text" value="16.2.250"/>	
Master Controller IP Address/DNS Name:		<input type="text" value="16.2.250"/>	
Link Priority Settings			
Link Priority Ethernet (0-255):		<input type="text"/>	
Link Priority Cellular (0-255):		<input type="text"/>	
USB Settings			
USB User Name:		<input type="text"/>	
USB Password:		<input type="text"/>	
Confirm USB Password:		<input type="text"/>	
USB Device Type:		any	
USB Device Identifier:		<input type="text"/>	
USB Dial String:		<input type="text"/>	
USB Initialization String:		<input type="text"/>	
USB TTY Device Path:		<input type="text"/>	
Network Settings			
Use DHCP:		<input type="radio"/> Yes <input checked="" type="radio"/> No	
LAN IP Address:		<input type="text"/>	
Subnet Mask:		<input type="text"/>	
Gateway:		<input type="text"/>	
DNS IP Address:		<input type="text"/>	
<input type="button" value="Save and Apply"/>		<input type="button" value="Revert"/>	
<input type="button" value="Ignore"/>		<input type="button" value="Delete"/>	
		<input type="button" value="Import Settings"/>	
		<input type="button" value="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 the **System > Configuration Change Job Detail** page for the job.

2. Locate the **General** section—this section provides general information about the APs current status. [Table 87](#) describes the fields, information, and settings.

Table 87 APs/Devices > Manage > General Fields and Default Values

Message	Meaning
Name	Displays the name currently set on the device.
Status	Displays the current status of an AP. If an AP is Up , then AWMS is able to ping it and fetch SNMP information from the AP. If the AP is listed Down then AWMS is either unable to ping the AP or unable to read the necessary SNMP information from the device.
Configuration	Displays the current configuration status of the AP. To update the status, click Audit on the APs/Devices > Audit page.
Last Contacted	Displays the last time AWMS successfully contacted the AP.
Type	Displays the type of AP.
Firmware	Displays the version of firmware running on the AP.
Group	Links to the Group > Monitoring page for the AP.
Template	Displays the name of the group template currently configuring the AP. Also displays a link to the Groups > Template page. This is only visible for APs that are being managed using templates.
Folder	Displays the name of the folder containing the AP. Also displays a link to the APs/Devices > List page for the folder.
Management Mode	Displays the current management mode of the AP. No changes are made to the AP when it is in Monitor Only mode. AWMS pushes configurations and makes changes to an AP when it is in Manage Read/Write mode.
Notes	Provides a free-form text field to describe device information.

- 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, AWMS manages that device as if it were a single slot device.


 **Note:** 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 88 describes field settings, default values, and information for the **Sections** area of this page.

Table 88 APs/Devices > Manage > Settings Fields and Default Values

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain	None	IOS	Field populated upon initial device discovery or upon refreshing settings. Enable this option from AMP Setup > Network page to display this field on the APs/Devices > Manage page, with fully-qualified domain names for IOS APs. This field is used in conjunction with Domain variable in IOS templates.
Location	Read from the device	All	The SNMP location set on the device.
Latitude	None	All	Text field for entering the latitude of the device. The latitude is used with the Google earth integration.

Table 88 APs/Devices > Manage > Settings Fields and Default Values (Continued)

Setting	Default	Device Type	Description
Longitude	None	All	Text field for entering the longitude of the device. The longitude is used with the Google earth integration.
Altitude (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.
Group	Default Group	All	Drop-down menu that can be used to assign the device to another Group.
Folder	Top	All	Drop-down menu that can be used to assign the device to another Group.
Auto Detect Upstream Device	Yes	All	Selecting Yes enables automatic detection of upstream device, which is automatically updated when the device is polled. Selecting No displays a drop-down menu of upstream devices.
Down Status Message	None	All	Enter a text message that provides information to be conveyed if the device goes down.
Administrative Status	Enable	All	Enables or disables administrative mode for the device.
Mode	Local	All	Designates the mode in which the device should operate. Options include the following: <ul style="list-style-type: none"> Local H-REAP Monitor Rogue Detector Sniffer

- Complete additional settings on the APs/Devices > Manage page, to include H-REAP, certificates, radio settings, and network settings. [Table 89](#) describes many of the possible fields.



Note: For complete listing and discussion of settings applicable only to Aruba devices, see the *Aruba AirWave Wireless Management Suite Configuration Guide* for this release.

Table 89 APs/Devices > Manage Page Illustration, Additional Settings

Setting	Default	Device Type	Description
Mesh Role	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP as shown: <ul style="list-style-type: none"> Mesh AP —The AP will act like a mesh client. It will use other APs as its uplink to the network. Portal AP —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. None —The AP will act like a standard AP. It will not perform any meshing functions
Mesh Mobility	Static	Mesh Devices	Select Static if the AP is static, as in the case of a device mounted on a light pole or in the ceiling. Select Roaming if the AP is mobile. Two examples would be an AP mounted in a police car or utility truck.
Bridge Role	Base Station	PTMP/WiMAX	Base Station units provide backhaul connections for satellite units, to which wireless users connect.
Mode of Operation	Bridge	PTMP/WiMAX	Units that can operate in bridge or router mode.
Ethernet Interface Configuration	100 Mbps Full Duplex	PTMP/WiMAX	Bandwidth rates for uploading and downloading data.

Table 89 APs/Devices > Manage Page Illustration, Additional Settings

Setting	Default	Device Type	Description
Dynamic Data Rate Selection	Enabled	PTMP/WiMAX	Allows subscribers to receive the maximum data rate possible.
Subscriber Station Class	G711 VoIP UGS	WiMAX Subscriber Stations	Defines the subscriber station class for the AP. Subscriber station classes are defined on the Groups > WiMAX page.
Uplink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Drop-down menu that defines the uplink modulation type for the subscriber station.
Downlink Modulation	bpsk-1-2	WiMAX Subscriber Stations	Drop-down menu that defines the downlink modulation type for the subscriber station.
VLAN Mode	Inherit	WiMAX Subscriber Stations	Drop-down menu that defines the VLAN mode of the AP. Inherit - The AP will inherit the VLAN settings from the subscriber class. Transparent - Tagged and untagged traffic is passed along unless blocked by a PIR restriction.
Receive Antenna	Diversity	Cisco	Drop-down menu for the receive antenna provides three options: Diversity —Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the Diversity setting should be used for both receive and transmit antennas. Right —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 both receive and transmit. Left —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.
Transmit Antenna	Diversity	Cisco	See description in Receive Antenna above.
Antenna Diversity	Primary Only	Intel 2011, Symbol 4131	Drop-down menu provides the following options: Full Diversity —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. Primary Only —The AP transmits and receives on the primary antenna only. Secondary Only: The AP transmits and receives on the secondary antenna only. Rx Diversity —The AP receives information on the antenna with the best signal strength and quality. The AP transmits information on the primary antenna only.
Transmit Power Reduction	0	Proxim	Transmit Power Reduction determines the APs transmit power. The max transmit power is reduced by the number of decibels specified.
Channel	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.
Neighboring APs	Blank	All	Represents top five contiguous access points calculated by summing the number of rooms to and from the access point and the access point of focus. 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.

Table 89 APs/Devices > Manage Page Illustration, Additional Settings

Setting	Default	Device Type	Description
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Colubris, Intel, 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: Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Intel/Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW) Colubris (High or 23 dBm, Med. or 17 dBm, Low or 13 dBm)
Distance Between APs	Large	Colubris	Determines how far a user can roam before roaming to another AP.
Notes (Optional)	Blank	All	Free form text field for entering fixed asset numbers or other device information. This information is printed on the nightly inventory report.
Radio (Enable/Disable)	Enable	All	The Radio option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. AWMS 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.
DHCP	Yes	All (except Colubris)	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, Aruba recommends disabling DHCP and using static IP addresses.
LAN IP	None	All (except Colubris)	The IP Address of the AP Ethernet interface. If One-to-One NAT is enabled, AWMS will communicate with the AP on a different address (the IP Address defined in the "Device Communication" area). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
BSID	00:00:00:00:00	WiMAX Base Station	Defines the BSID for the base station. This BSID should match the BSID on the Groups > WiMAX page if you want subscriber stations to associate with the base station. Subscriber stations use the BSID defined on the Groups > WiMAX page to determine which base stations to associate with.
Subnet Mask	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.
Gateway	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 **IOS Template Options** area on the **APs/Devices > Manage** page.



Note: This field only appears for IOS APs in groups with Templates enabled.

Table 90 describes field settings, default values, and additional information for this page.

Table 90 APs/Devices > Manage > IOS Template Options Fields and Default Values

Setting	Default	Device Type	Description
WDS Role	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.
SSL Certificate	None	Cisco IOS	AWMS will read the SSL Certificate off of the AP when it comes UP in AWMS. The information in this field will defines what will be used in place of %certificate%.
Extra IOS Commands	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.
switch_command	None	Cisco IOS	Defines lines included for each of the members in the stack. This field appears only on the master's Manage page. The information in this field will determine what is used in place of the %switch_command% variable.

- For Cisco WLC devices, navigate to the interfaces section of the **AP > Manage** page. Click **Add new interface** to add another controller interface, or click the pencil icon to edit an existing controller interface. [Figure 109](#) describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by AWMS, refer to the Cisco WLC product documentation.

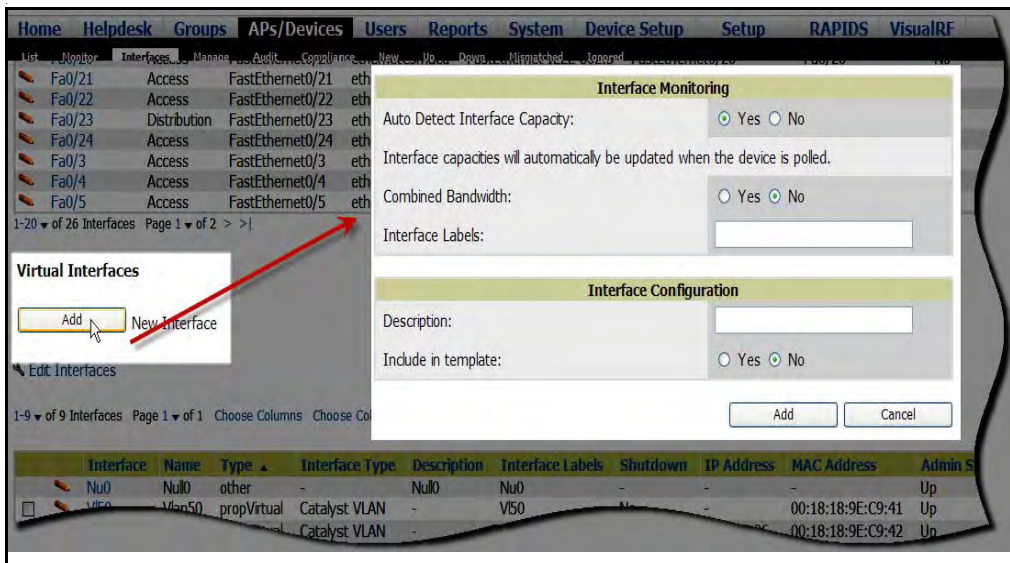
Figure 109 APs/Devices > Manage Fields and Default Values

Field	Default	Description
Name	None	The name of the interface on the controller.
VLAN ID	None	The VLAN ID for the interface on the controller.
Port	None	The port on the controller to access the interface.
IP Address	None	The IP address of the controller.
Subnet Mask	None	The subnet mask for the controller.
Gateway	None	The controller's gateway.
Primary and Secondary DHCP Servers	None	The DHCP servers for the controller.
Guest LAN	Disabled	Indicates a guest LAN.
Quarantine	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.

Configuring Device Interfaces for Cisco Catalyst Switches

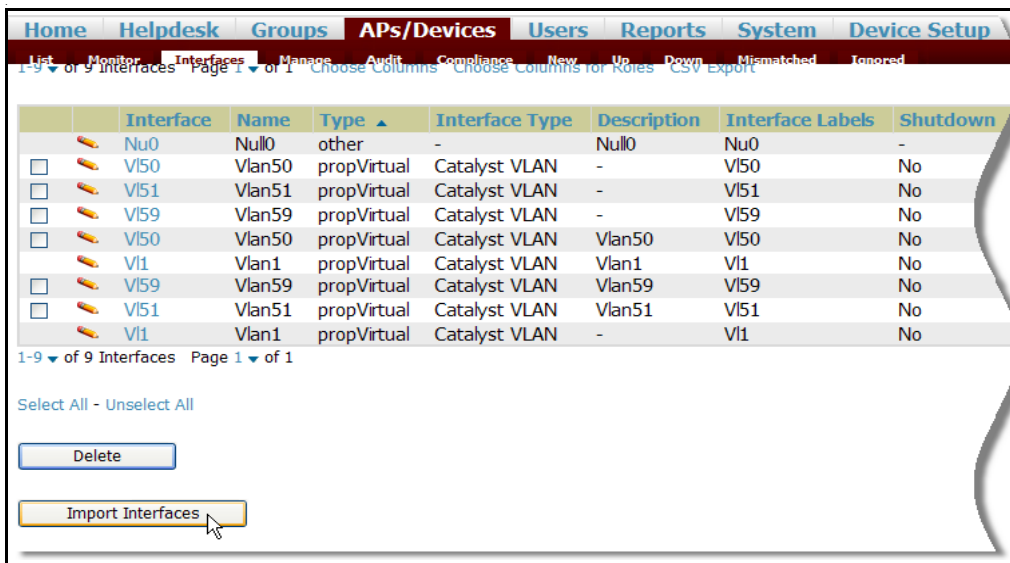
You can add a Virtual interface by clicking **Add** and entering the appropriate information in the Interface and Interface Capacity panes of the page that then appears as shown in [Figure 110](#).

Figure 110 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 128. To refresh and reload all current interface information from a device, click **Import Interfaces** on the bottom of the page as shown in Figure 111.

Figure 111 Import Interfaces for Refresh and Reload (lower portion of page)



You can view details for each interface on a wired device, from its individual interface page, as well. For a detailed explanation of the data available on each individual interface monitoring page, see “Understanding the APs/ Devices > Interfaces Page” on page 154.

You can configure interface settings individually or in groups. To configure individual interface settings, click the pencil icon to the left of the interface name appearing from the AP/Devices > Interfaces page, as shown in Figure 112.

Figure 112 *Editing Individual Interfaces Page*

	Interface	Name	Type	Interface Type	Description	Interface Labels	Shutdown	IP Ad
	Nu0	Null0	other	-	Null0	Nu0	-	-
<input type="checkbox"/>	V150	Vlan50	propVirtual	Catalyst VLAN	-	V150	No	-
<input type="checkbox"/>	V151	Vlan51	propVirtual	Catalyst VLAN	-	V151	No	10.51.
<input type="checkbox"/>	V159	Vlan59	propVirtual	Catalyst VLAN	-	V159	No	-
<input checked="" type="checkbox"/>	V150	Vlan50	propVirtual	Catalyst VLAN	Vlan50	V150	No	-
<input type="checkbox"/>	V1	Vlan1	propVirtual	Catalyst VLAN	Vlan1	V1	No	-
<input type="checkbox"/>	V159	Vlan59	propVirtual	Catalyst VLAN	Vlan59	V159	No	-
<input type="checkbox"/>	V151	Vlan51	propVirtual	Catalyst VLAN	Vlan51	V151	No	-
<input type="checkbox"/>	V1	Vlan1	propVirtual	Catalyst VLAN	-	V1	No	-

1-9 of 9 Interfaces Page 1 of 1

Select All - Unselect All

This takes you to the **Interfaces Monitoring and Configuration** window, that has a slightly different appearance depending on whether you are configuring a physical or virtual interface, as shown in [Figure 113](#) and [Figure 114](#).

Figure 113 *Physical Interfaces Monitoring and Configuration Window*

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:

Figure 114 *Virtual Individual Interfaces Configuration Pane*

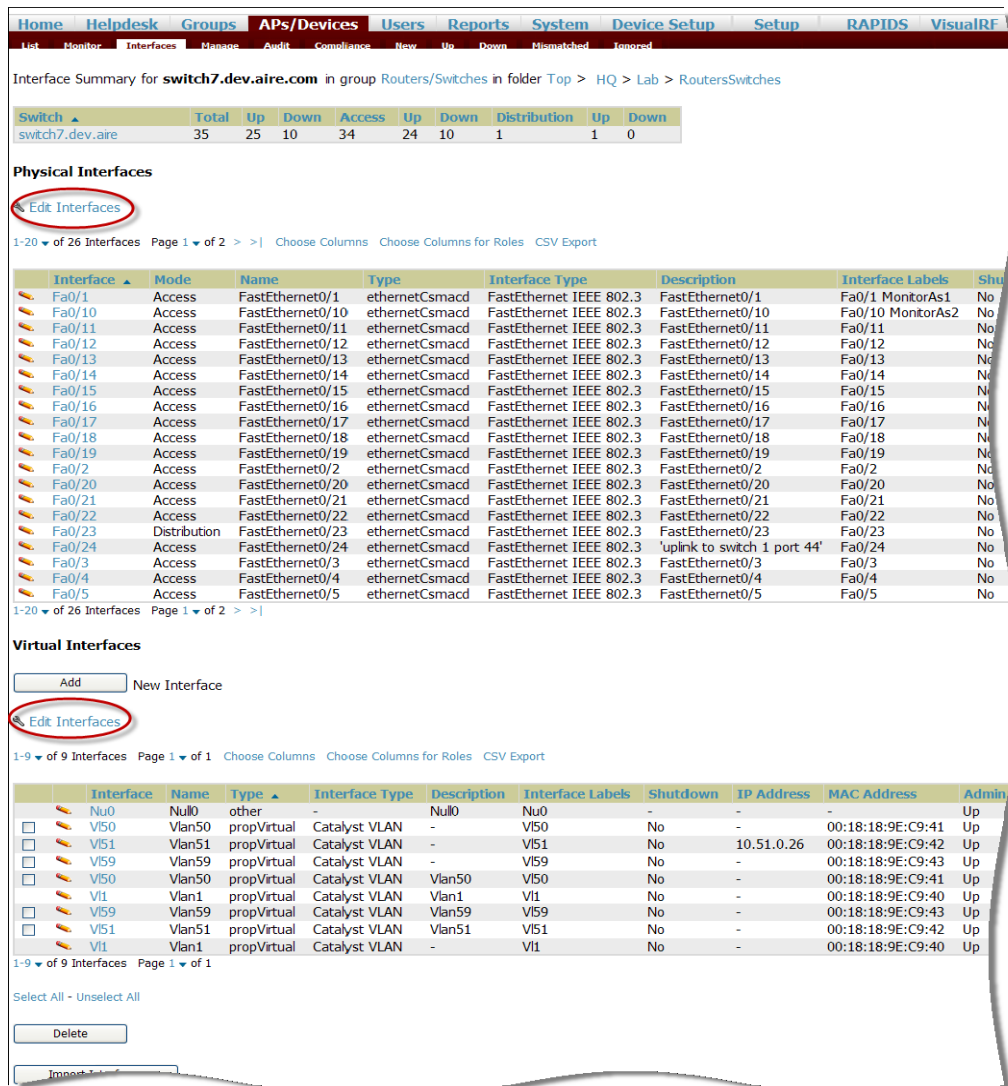
Interface Configuration

Description:

Interface Type: Catalyst VLAN

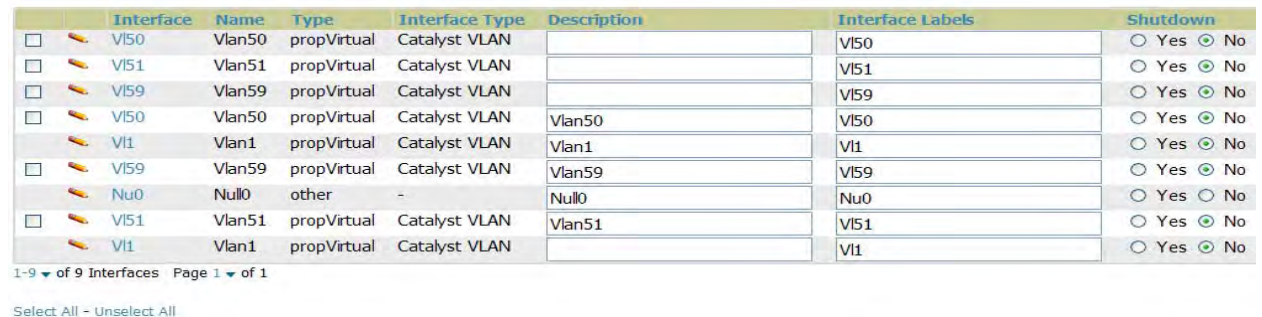
To configure interfaces as a group, click the **Edit Interfaces** button above the Physical or Virtual Interfaces table that includes the interfaces you want to edit collectively as shown in [Figure 115](#).

Figure 115 *Edit Multiple Interfaces*



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 116](#).

Figure 116 *Multiple Interface Edit UI*



AWMS assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on the use of templates, see [Chapter 6, "Creating and Using Templates" on page 175](#).

Configuring Cisco Router and Switch Interface Settings

When you select an interface on a Cisco wired device to edit in AWMS, the fields available in the virtual or physical **Interface Configuration** pane will auto-populate according to the existing interface device configuration as shown in [Figure 117](#).

Figure 117 *Physical Interfaces Configuration Pane (Interfaces Monitoring and Configuration Window)*

The screenshot shows the 'Physical Interfaces Configuration Pane' with two main sections: 'Interface Monitoring' and 'Interface Configuration'.
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: Fa0/11
- Mode: Auto
Interface Configuration:
- Description: FastEthernet0/11
- Shutdown: Yes No
- Interface Type: FastEthernet IEEE 802.3
- Switchport Access VLAN: 51
- Switchport Mode: Dynamic (Auto)
- Switchport Trunk Native VLAN:
- Switchport Trunk Allowed VLANs: all
- Switchport Trunk Pruning VLANs:
- Switchport Trunk Encapsulation: Negotiate
- Speed: Auto
- Additional Commands: ip dhcp snooping trust
Buttons: Save, Cancel

Not all interface settings are valid for all switches. You can change or overwrite any of the pre-populated settings as well as revise or add to the Additional Commands fields to tailor the template configuration to the needs of your production environment. For further details and assistance with settings configuration, refer to your Cisco product documentation.

AWMS assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on the use of templates, see [Chapter 6, “Creating and Using Templates”](#) on page 175.

Individual Device Support and Firmware Upgrades

Perform the following steps to configure AP communication settings for individual 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 118](#) illustrates this page.

Figure 118 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 the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View AP Credentials** link in AWMS by the root user. Contact Dell support for detailed instructions to disable the link.
5. (Optional-Not pictured.) Enter the appropriate SSH and Telnet credentials if you are configuring Dell, Aruba Networks, Alcatel-Lucent or any Cisco device except Cisco wireless LAN controllers.
6. Click **Apply**. AWMS presents a confirmation window reminding you of all configuration changes that will be applied to the AP. Click **Confirm Edit** to apply the changes to the AP immediately, **Schedule** to schedule the changes to occur during a specific maintenance window, or **Cancel** to return to the **APs/Devices > Manage** page.



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.

Click **Upgrade Firmware** to upgrade the device's firmware. [Figure 119](#) illustrates this page and [Table 91](#) describes the settings and default values.

Figure 119 APs/Devices > Manage Firmware Upgrades

Desired Version

Choose the desired firmware version to be applied to **Proxim-AP-4000-partner** (10.51.1.65). Upload firmware files on the Device Setup [Firmware Files](#) page.

Current Version:

Desired version:

Firmware Upgrade Job Options

Job name:

Serve firmware files from this interface:

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:

Sender Address:

Start or Schedule Firmware Upgrade Job:

Table 91 APs/Devices > Manage Firmware Upgrades Fields and Default Values

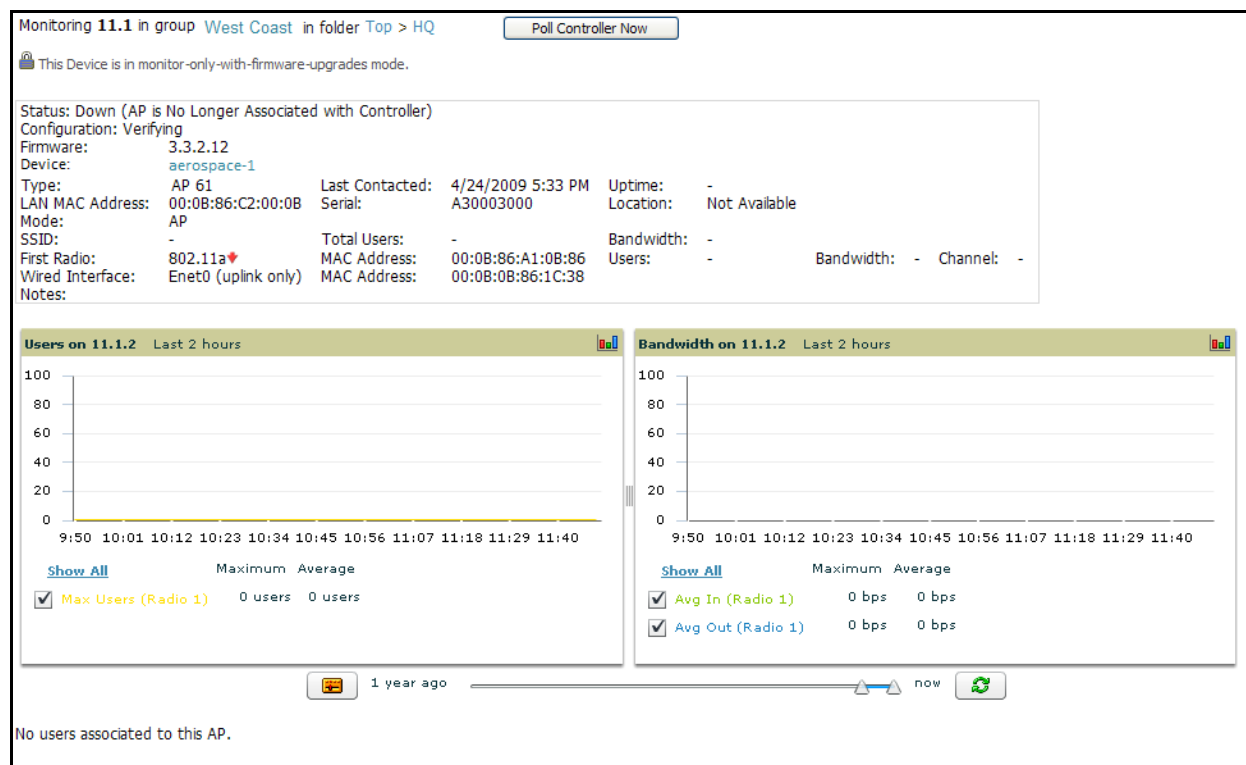
Setting	Default	Description
Desired Version	None	Drop-down menu that specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the Device Setup > Firmware Files page.
Job Name	None	Sets a user-defined name for the upgrade job. Aruba recommends using a meaningful and descriptive name.
Use "/safe" flag for Cisco IOS firmware upgrade command	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.
Email Recipients	None	Displays a list of email addresses that should receive alert emails if a firmware upgrade fails.
Sender Address	None	Displays the From address in the alert email.

Troubleshooting a Newly Discovered Device with Down Status

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. Click the Name of the down device in the list of devices on the APs/Devices > List page. This automatically directs you to the APs/Device > Monitor page for that device, shown in [Figure 120](#).

Figure 120 APs/Devices > Monitor Page Illustration for a Down Device



2. Locate the **Status** section. If the Status is **Down**, there is an onscreen error message indicating the cause of the problem. Some of the common system messages are as follows in [Table 92](#):

Table 92 Common System Messages for Down Status

Message	Meaning
SNMP Get Failed	SNMP community string specified for that device is incorrect or an incorrect SNMP port is specified. If SNMP is not enabled on the device you will also receive this message. Some factory default APs, including Cisco IOS devices, do not have SNMP enabled by default.
Telnet Error: command timed out	Telnet username and password specified for that device is incorrect or an incorrect telnet port is specified.
ICMP Ping Failed (after SNMP Get Failed)	The device is not responding on the network and is likely non-operational.

3. If the **SNMP Get Failed** message appears, click the APs/Devices > **Manage** tab to go to the management page for that device.
4. If visible, click the **View device credentials** link in the **Device Communications** area. This displays the credentials AWMS is using unsuccessfully to communicate with the device. This link can be removed from AWMS for security reasons by setting a flag in AWMS. Only users with root access to the AMP command line

can show or hide this link. If you are interested in disabling this feature, please contact Dell support. [Figure 121](#) illustrates this page.

Figure 121 View AP Credentials



Note: The **View AP 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. [Figure 122](#) illustrates this page.

Figure 122 APs/Devices > Manage > Device Communication Section Illustration

A screenshot of a web form titled 'Device Communication'. The form contains several sections of input fields. The first section is for IP and port information: 'IP Address: 10.5.5.5' and 'SNMP Port: 161'. The second section is for credentials: 'Community String: [redacted]', 'Confirm Community String: [redacted]', 'SNMPv3 Username: [redacted]', 'Auth Password: [redacted]', 'Confirm Auth Password: [redacted]', 'Privacy Password: [redacted]', 'Confirm Privacy Password: [redacted]'. The third section is for authentication protocol: 'SNMPv3 Auth Protocol: SHA-1'. The fourth section is for Telnet/SSH credentials: 'Telnet/SSH Username: admin', 'Telnet/SSH Password: [redacted]', 'Confirm Telnet/SSH Password: [redacted]'. The fifth section is for enable password: '"enable" Password: [redacted]', 'Confirm "enable" Password: [redacted]'. A note at the top states: 'If this device is down because its IP address or management ports have changed, update the fields below with the correct information.' Another note states: 'If this device is down because the credentials on the device have changed, update the fields below with the correct information.' A status message says: 'This device is currently using SNMP version 2c.'

Note: The **Device Communication** area may appear slightly different depending on the particular vendor and model.

6. Enter the appropriate credentials, and click **Apply**.
7. Return to the **APs/Devices\ List** page to see if the device appears with a Status of **Up**.

This chapter provides an overview and several tasks supporting the use of device configuration templates in AWMS, and contains the following topics:

- “Group Templates” on page 175
- “Viewing and Adding Templates” on page 177
- “Configuring General Template Files and Variables” on page 181
- “Configuring Cisco IOS Templates” on page 186
- “Configuring Cisco Catalyst Switch Templates” on page 188
- “Configuring Symbol Controller / HP WESM Templates” on page 188
- “Configuring a Global Template” on page 191

Group Templates

Supported Device Templates

Templates are helpful configuration tools that allow AWMS 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



Note: Dell recommends using the graphical AOS Config feature in support of Dell devices, particularly for AOS 3.3.2.x and later. Refer to the *Dell PowerConnect W AirWave Wireless Management Suite Configuration Guide* for additional information.

- Cisco Aironet IOS and 4800 autonomous APs
- Cisco Catalyst Switches
- HP ProCurve 530 and WeSM controllers
- Hirschmann
- LANCOM
- 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 AWMS template understands many variables including the following:

- %ap_include_1% through %ap_include_10%
- %channel%
- %hostname%
- %ip_address%
- %ofdm_power%

The variable settings correspond to device-specific values on the **APs/Devices > Manage** configuration page for the specific AP that is getting configured.



Note: 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. Navigate 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 clicking 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 AWMS” on page 79](#).

2. From the AWMS navigation pane, click **Templates**. The **Templates** page appears. [Figure 123](#) illustrates the **Groups > Templates** configuration page, and [Table 93](#) describes the information columns.

Figure 123 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-rn-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
<input type="checkbox"/>	Aruba 800 - 3.3.1.3	Aruba 800	Template saved	7/16/2008 2:55 PM	None
<input type="checkbox"/>	Cisco Aironet 1200 IOS - 12.3(7)JA2	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:52 PM	12.3(7)JA2
<input type="checkbox"/>	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	2/27/2008 9:49 PM	12.3(8)JA
<input type="checkbox"/>	Cisco Aironet 350 IOS - 12.3(4)JA	Cisco Aironet 350 IOS	Template saved	5/23/2007 1:54 AM	None
<input type="checkbox"/>	Hirschmann BAT-54 - 7.00.0070	Hirschmann BAT54-Rail	Template saved	8/10/2007 10:27 AM	7.00.0070
<input type="checkbox"/>	HP ProCurve ZLWeSM - WT.01.03	HP ProCurve ZLWeSM	Template saved	1/25/2008 1:51 PM	None
<input type="checkbox"/>	LANCOM 3550 - 7.10.0022	LANCOM 3550	Template saved	8/10/2007 10:27 AM	None
<input type="checkbox"/>	Office WPA/WPA2	Aruba 800	Template saved	2/27/2008 10:55 PM	3.3.1.3
<input type="checkbox"/>	Symbol WS2000 - 2.3.1.0-012R	Symbol WS2000	Template saved	1/9/2009 9:51 AM	None

14 Templates

Select All - Unselect All

Table 93 Groups > Templates Fields and Default Values

Setting	Description
Notes	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Click the link from such a note to launch the Add Template configuration page for that device.
Name	Displays the template name.
Device Type	Displays the template that applies to APs or devices of the specified type. If vendor (Any Model) 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.

Table 93 *Groups > Templates Fields and Default Values (Continued)*

Setting	Description
Status	Displays the status of the template.
Fetch Date	Sets the date that the template was originally fetched from a device.
Version Restriction	Designates that the template only applies to APs running the version of firmware specified. If the restriction is None , 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 AWMS template inventory, navigate to the **Groups > List** page, and select the group to which you will apply the template. Click the group name and the **Details** page appears. Click **Templates**, then click **Add**.
4. Complete the configurations illustrated in [Figure 124](#), and the settings described in [Table 94](#).

Figure 124 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 -- ▾

Template

The following variables may be used in the template value of each variable is configured on the APs/C Management page for each device in the group. Each must be surrounded by percent signs: `%hostname%`. % statements must be terminated by `%end` 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: MDS ▾

Privacy Password:

Confirm Privacy Password:

SNMPv3 Privacy Protocol: DES ▾

Table 94 *Groups > Templates > Add Template Fields and Default Values*

Setting	Default	Description
Use Global Template	No	Uses a global template that has been previously configured on the Groups > Templates configuration page. Available templates will appear in the drop-down menu. If Yes 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 Groups > Templates section of the <i>User Guide</i> .
Fetch	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 APs/Devices > Manage configuration page for each AP.
Name	None	Defines the template display name.
AP Type	Cisco IOS (Any Model)	Determines that the template applies to APs or devices of the specified type. If Cisco IOS (Any Model) is selected, the template applies to all IOS APs that do not have a version specific template specified.
Reboot APs After Configuration Changes	No	Determines reboot when AWMS applies the template, copied from the new configuration file to the startup configuration file on the AP. If No is selected, AWMS uses the AP to merge the startup and running configurations. If Yes is selected, the configuration is copied to the startup configuration file and the AP is rebooted. NOTE: This field is only visible for some devices.
Restrict to this version	No	Restricts the template to APs of the specified firmware version. If Yes is selected, the template only applies to APs on the version of firmware specified in the Template Firmware Version field.
Template firmware version	None	Designates that the template only applies to APs running the version of firmware specified.
Community String	None	If the template is updating the community strings on the AP, enter the new community string AWMS should use here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Username	None	If the template is updating the Telnet/SSH Username on the AP, enter the new username AWMS should use here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Password	None	If the template is updating the Telnet/SSH password on the AP, enter the new Telnet/SSH password AWMS should use here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
"enable" Password	None	If the template is updating the enable password on the AP, enter the new enable password AWMS should use here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Username	None	If the template is updating the SNMP v3 Username password on the AP, enter the new SNMP Username password here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
Auth Password	None	If the template is updating the SNMP v3 Auth password on the AP, enter the new SNMP Username password here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
Privacy Password	None	If the template is updating the SNMP v3 Privacy password on the AP, enter the new SNMP Username password here. AWMS updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Auth Protocol	MD5	Specifies the SNMPv3 Auth protocol, either MD5 or SHA-1 .
SNMPv3 Privacy Protocol	DES	Specifies the SNMPv3 Privacy protocol, either DES or AES .

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.



Note: Dell recommends starting with a small group of access points and placing these APs in Monitor Only mode, which is read-only. Do this via 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. Navigate to the **Groups > Templates** configuration page. Click **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 click **Fetch**.
6. AWMS 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 183. 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 Dell support before proceeding.

7. Specify the device types for the template. The templates only apply to devices of the specified type.
 - Specify whether AWMS should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then AWMS instructs the AP to copy the configuration from AWMS to the startup configuration file of the AP and reboot the AP.
 - If the **Reboot Devices after Configuration Changes** option is not selected, then AWMS 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.
 - Dell recommends using 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. Click the **Save and Apply** button 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 AWMS will audit the devices and compare their current configuration to the one defined in the template.



Note: 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 **AP 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 AWMS.



Note: 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

AWMS 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, AWMS 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 AWMS from reporting mismatches for this type of variance.

AWMS provides two types of directives that can be used within a template to control how AWMS 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 AWMS ignores them when verifying configurations. Lines enclosed in `<ignore_and_do_not_push>` cause AWMS 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 AWMS 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.



Note: 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 AWMS excludes them when calculating and reporting configuration mismatches.



Note: 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 95](#):

```
%if variable=value%
...
%endif%
```

Table 95 Conditional Variable Syntax Components

Variable	Values	Meaning
interface	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
radio_type	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
wds_role	backup	The wds role of the AP is the value selected in the drop down menu on the APs/Devices > Manage configuration page for the device.
	client	
	master	
IP	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 96](#) are substituted with values specified on each access point's **APs/Devices > Manage** configuration page within the AWMS 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. AWMS would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent AWMS from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, AWMS suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way AWMS 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 96](#).

Table 96 *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
hostname	Name	hostname %hostname%	-
channel	Channel	channel %channel%	-
ip_address netmask	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp ...	
gateway	Gateway	ip default-gateway %gateway%	-
antenna_receive	Receive antenna	antenna receive %antenna_receive%	diversity
antenna_transmit	Transmit antenna	antenna transmit %antenna_transmit%	diversity
cck_power	802.11g radio module CCK power level	power local cck %cck_power%	maximum
ofdm_power	802.11g radio module OFDM power level	power local ofdm %ofdm_power%	maximum
power	802.11a and 802.11b radio module power level	power local %power%	maximum
location	The location of the SNMP server.	snmp-server location %location%	-
contact	The SNMP server contact.	snmp-server contact %contact%	
certificate	The SSL Certificate used by the AP	%certificate%	-
ap include	The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the APs/Devices > Manage configuration page replace this variable.	%ap_include_1% through %ap_include_10%	-

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 AWMS.

The power lines set the power local cck and ofdm values to the numerical values that are stored in AWMS.

Configuring Cisco IOS Templates

Cisco IOS access points have literally hundreds of configurable settings. For simplicity and ease of use, AWMS enables you to control them via the **Groups > Templates** configuration page. This configuration page defines the startup-config file of the devices rather than utilizing the AWMS normal **Group** configuration pages. AWMS 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 AWMS **Group** configuration pages. Perform these steps to configure a Cisco IOS Template for use with one or more groups, and the associated devices within those groups.

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

AWMS instructs each of the APs in the Group to copy its unique startup-config file from AWMS via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then AWMS instructs the AP to copy the configuration from AWMS to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then AWMS 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. Dell recommends using 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.

For additional information, refer to [“Access Point Notes” on page 309](#) for a full Cisco IOS template.



Note: Changes made on the standard AWMS 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 BVI1
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 BVI1
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 AWMS to login to the AP must have level 15 privileges. Without them AWMS is not be 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 APs 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 certain radio types (that is, 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 data rates. You can 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. The below examples illustrate this usage:

```

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=Dot11Radiol%
interface Dot11Radiol
  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 Cisco Router and Switch Interface Settings](#)” on page 169. 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 181.



Note: 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 AWMS using templates. AWMS 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 186. 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. There is an option on the **Group > Templates** page to reboot 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-interoperability 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 AWMS users to define a single template in a global group that can be used to manage access points in subscriber groups. Such a template enables turning 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. Navigate to the **Group > Templates** configuration page for the global group that owns it.
2. Click the **Add** button to add a new template, or click the **pencil icon** next to an existing template to edit that template.
3. Examine the configurations illustrated in [Figure 125](#).

Figure 125 Group > Templates > Add Page Illustration



4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The drop-down 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 126](#).

Figure 126 Template Variables Illustration

Template Variables		
Variable Name	Variable Value	Delete
<input type="text"/>	<input type="text"/>	
<input type="button" value="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, click **Add** at the bottom of the configuration page. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, click the **Apply Changes Now** button. If you do not want to add the template, click the **Cancel and Discard Changes** button. 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. Navigate to the **Groups > Templates** configuration page and click 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. Navigate to the **Groups > Template** configuration page for the local group and click the pencil icon next to the name of the global template in the list. [Figure 127](#) illustrates this page.

Figure 127 Groups > Templates Edit, Topmost 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, navigate to the **Groups > Template** configuration page for the global group and click 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 AWMS, 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 detection using RAPIDS, and contains the following sections:

- “Overview Tab” on page 195
- “List” on page 197
- “RAPIDS Setup” on page 202
- “RAPIDS Rules” on page 204
- “Score Override” on page 210
- “Audit Log” on page 212
- “Additional Rogue Device Resources” on page 212

Overview Tab

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 to mitigate 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 eliminate the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- Over the Air
 - Using your existing enterprise APs (Aruba, Alcatel-Lucent, Cisco WLC, Symbol for example)
 - RF scanning using AirWave Management Client (AMC)—Optional
- On the Wire
 - Using HTTP and SNMP Scanning
 - Polling routers and switches to identify, classify, and locate unknown APs

Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Cisco WLSE** (1100 and 1200 IOS)—AWMS 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 AWMS.
- **AirDefense**—Uses the AWMS XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from AWMS.

The Overview tab displays a page of RAPIDS summary information (see [Figure 128](#)). This page also includes links to the AirWave Management Client, an optional utility that reports wireless discovery information to AWMS. [Table 97](#) defines the summary information that appears on the page.

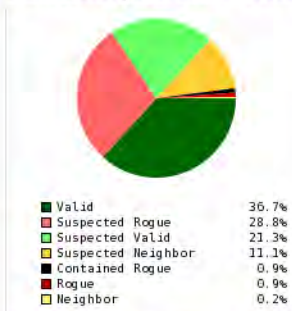
Figure 128 RAPIDS Overview tab

IDS Events

Attack	Last 2 Hours	Last 24 Hours	Total
IP Spoofing	559	3487	14329
Null-Probe-Response	0	12	14
Repeat WEP-IV Violation (AP)	1	5	5
Repeat WEP-IV Violation (Station)	2	21	73
4 Attack Types	562	3525	14421

Rogue Data

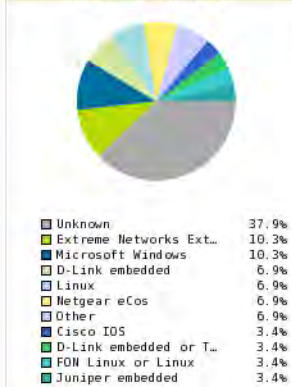
Device Count by RAPIDS Classification



RAPIDS Classification

RAPIDS Classification	Devices
Contained Rogue	4
Rogue	4
Suspected Rogue	127
Unclassified	0
Suspected Neighbor	49
Neighbor	1
Suspected Valid	94
Valid	162
Total	441

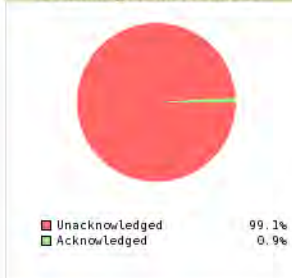
RAPIDS Devices by OS



Operating System

Operating System	Devices
Extreme Networks ExtremeXOS	3
Microsoft Windows	3
D-Link embedded	2
Linux	2
Netgear eCos	2
Cisco IOS	1
D-Link embedded or TRENDnet embedded	1
FON Linux or Linux	1
Juniper embedded	1
Unknown	11
Other	2
Not scanned	412

Acknowledged RAPIDS Devices



RAPIDS Changes (view RAPIDS audit log)

Time	User	Event
Feb 17 10:21:12 2010	admin	rapids_classification_rule (id 39): classification: '70' => '80'
Feb 17 10:20:20 2010	admin	seas_config (id 1): rapids_manage_containment: '0' => '1'
Feb 12 09:19:00 2010	jason	rapids_classification_rule (id 39): classification: '80' => '70'

Table 97 Overview Fields

Summary	Description
IDS Events	Displays a list of IDS events for the designated folder (Top is the default) 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.
Rogue Data	A summary of rogue device counts by RAPIDS classification in a color coded pie chart format and listed summary. View additional details for rogue devices via the RAPIDS > List page.
Operating System	Detected operating systems represented in both a color coded pie chart and a summary listing. OS scans can be run manually or enabled to run automatically on the RAPIDS > Setup page.
Acknowledge Devices	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
RAPIDS Changes	RAPIDS change log tracks every change made to the RAPIDS system including changes to rules, manual classification, and anything on the RAPIDS > Setup page.

List

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 129](#)). You can sort the table columns (up/down) by selecting the column head or filter data using the column head drop down menus.

Figure 129 Viewing a Rogue AP by Classification

Minimum Classification: Rogue

Modify Devices

1-9 of 9 Rogue APs Page 1 of 1 Choose Columns

Ack	RAPIDS Classification	Threat Level	Name	Classifying Rule	Wired	#APs Hearing	Location	SSID	Signal	RSSI	Network Type
No	Rogue	7	Linksys-4D:00:BF	Detected Wirelessly and on LAN	Yes	46	Sunnyvale > HQ	device-ssid	-20	30	AP
No	Rogue	7	Ambit Micr-5B:43:7A	Detected Wirelessly and on LAN	Yes	39	Sunnyvale > HQ	murtest1200	-20	37	AP
No	Rogue	7	PROXIM, IN-5A:A4:F0	Detected Wirelessly and on LAN	Yes	45	-	-	-20	8	AP
No	Rogue	7	PROXIM, DL-5A:64:27	Detected Wirelessly and on LAN	Yes	26	-	-	-20	32	AP
No	Rogue	7	Aironet Wi-45:0E:C5	Detected Wirelessly and on LAN	Yes	26	Sunnyvale > HQ	xxworks-350-00:40:96:41:89:FD	-20	9	AP
Yes	Rogue	7	Alpha Netw-17:55:DF	Detected Wirelessly and on LAN	Yes	32	Sunnyvale > HQ	default	-22	11	AP
No	Rogue	7	Juniper Ne-A7:C2:62	Detected Wirelessly and on LAN	Yes	50	Sunnyvale > HQ	dbishop-netscreen	-20	6	AP
Yes	Rogue	7	Allied Tel-68:3A:2B	Detected Wirelessly and on LAN	Yes	44	-	default	-20	11	AP
Yes	Rogue	7	3Com Access Point	Detected Wirelessly and on LAN	Yes	48	Sunnyvale > HQ	3com	-20	37	AP

1-9 of 9 Rogue APs Page 1 of 1

View Ignored Rogues



Note: The page displayed in [Figure 129](#) may require a moment to load; no rogues displayed for a given classification means that no such rogue device was discovered on your network.

[Table 98](#) details the column information displayed in [Figure 129](#). For additional information about RAPIDS rules, refer to “[RAPIDS Rules](#)” on page 204.

The active links on this page launch additional pages for RAPIDS configuration or device processing.

Table 98 RAPIDS > List Column Definitions

Column	Description
Ack	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 Modify Devices of the List page. Rogues should be acknowledged when the AWMS user has investigated them and determined that they are not a threat (see “Basic Configuration” on page 202).
RAPIDS Classification	Displays the current RAPIDS classification. This classification is determined by the rules defined on the RAPIDS > Rules page.
Threat Level	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 206 . The threat level is also supported with Triggers (see “Monitoring and Supporting AWMS with the System Pages” on page 249).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, AWMS assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see “Viewing and Configuring RAPIDS Rules” on page 206).
Controller Classification	Displays the classification of the device based on the controller’s hard-coded rules. NOTE: This column is hidden unless <i>Offload Dell PowerConnect W WMS Database</i> is enabled by at least one group on the Groups > Basic page.
Wired	Displays whether the rogue device has been discovered on the wire. This column displays Yes or is blank if wired information was not detected.
#APs Hearing	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.
Location	As with all List pages in AWMS, the RAPIDS > List page includes the Location column. Click the location associated to the rogue device to view the VisualRF floor plan that includes the specified device. RAPIDS and VisualRF must be licensed on the AWMS for this functionality to be supported.
SSID	Displays the most recent SSID that was heard from the rogue device.
Signal	Displays the strongest signal strength detected for the rogue device.
RSSI	Displays Received Signal Strength Indication (RSSI) designation, a measure of the power present in a received radio signal.
Network Type	Displays the type of network in which the rogue is present, for example: <ul style="list-style-type: none"> ● Ad-hoc—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. ● AP—This type of network usually indicates an infrastructure network comprised of ceiling-mounted APs, for example. This may be more of a threat. ● Unknown—The network type is not known.
Encryption Type	Displays the encryption that is used by the device as known. Possible contents of this field include the following encryption types: <ul style="list-style-type: none"> ● Open—Definition pending ● WEP—Wired Equivalent Privacy ● WPA—Wi-Fi Protected Access <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>
Ch	Indicates the RF channel on which the rogue device was detected.
LAN Vendor	Indicates the LAN vendor of the rogue device, when known.
Radio Vendor	Indicates the radio vendor of the rogue device, when known.

Table 98 *RAPIDS > List Column Definitions*

Column	Description
OS	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 based on the results of the scan.
Model	Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available.
IP Address	Displays the IP address of the rogue device. The IP address data comes from fingerprint scans or ARP polling of routers and switches.
Last Discovering AP	Displays the most recent AP to discover the rogue device. The device name in this column is taken from the device name in the group.
Switch/Router	Displays the switch or router where the device's LAN MAC address was last seen.
Port	Indicates the physical port of the switch or router where the rogue was last seen.
Last Seen	Indicates the date and time the rogue device was last seen.

To view the details for any rogue device, select the device name to launch the device's detail page ([Figure 130](#)).

Figure 130 Rogue APs Device Detail Page

Name:	<input type="text"/>	Model:	-	First Discovered:	2/9/2010 11:58 AM
Acknowledge:	<input type="radio"/> Yes <input checked="" type="radio"/> No	IP Address:	-	First Discovery Method:	Wireless AP scan
Controller Classification:	Unclassified	SSID:	3Com	First Discovery Agent:	AP125-A
RAPIDS Classification:	Contained Rogue	Channel:	6	Last Discovered:	3/11/2010 11:05 AM
Classification Rule:	Contain 3Com	WEP:	-	Last Discovery Method:	Wireless AP scan
RAPIDS Classification Override:	- No Override -	WPA:	-	Last Discovery Agent:	00:0b:86:c1:a0:88
Threat Level:	5	Network Type:	AP		
Threat Level Override:	<input type="text"/>				
Radio MAC Address:	00:0A:5E:08:A5:7B				
Radio Vendor:	3COM				
LAN MAC Address:	-				
LAN Vendor:	-				
OUI Score:	-				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				
Notes:	<input type="text"/>				

Location: Sunnyvale > 1344 Crossman > HQ (Floor 1)



Controller Containment Status

1-1 of 1 Rogue BSSIDs Page 1 of 1 Choose Columns Choose Columns for Roles CSV Export

Controller	BSSID	Containment State	Desired Containment State
A800	00:0A:5E:08:A5:7B	Not Contained	Contained

1-1 of 1 Rogue BSSIDs Page 1 of 1

Discovery Events

1-9 of 9 Discovery Events Page 1 of 1 Choose Columns Choose Columns for Roles CSV Export

RSST	Signal	Channel	SSID	WEP	WPA	BSSID	Network Type	IP Address	Time	Discovery Method	Discovery Agent	Role
43	-36	6	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:1a:1e:c0:1a:64 - AP	-
30	-72	36	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:0b:86:c0:b0:8a - AM	-
38	-65	36	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:1a:1e:c0:1a:64 - AP	-
37	-67	36	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	AP125-A	-
38	-58	6	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:0b:86:c0:b0:8a - AM	-
34	-67	36	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:0b:86:c1:a0:88	-
40	-42	6	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	AP125-A	-
38	-57	6	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/11/2010 11:05 AM	Wireless AP scan	00:0b:86:c1:a0:88	-
15	-97	6	3Com	-	-	00:0A:5E:08:A5:7B	AP	-	3/9/2010 4:50 PM	Wireless AP scan	AL32	-

1-9 of 9 Discovery Events Page 1 of 1



Note: The historical information displayed on the device detail page indicates the most recent discovery event per discovering device.

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.
- 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.
- Each rogue device typically 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 from this page. Otherwise, best practices strongly recommends that you extract the device from your building and delete the rogue device from the system.

To update a rogue device:

1. Select the device name from the list on the **RAPIDS > List** page to launch the device detail page (see [Figure 130](#)).
2. If an IP address is available for a given device, click the **Identify OS for Suspected Rogues** option to obtain operating system information.
3. Select the **Ignore** button if the rogue device is to be ignored.
4. Select the **Delete** button if the rogue device is to be removed from AWMS 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 AWMS. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, perform the following steps.

1. From the **RAPIDS > List** page, click **View Ignored Rogues** (at the bottom left of the page) to launch the **Ignored Rogues** page.
2. From the **Minimum Classification** drop-down menu, select the type of ignored rogue devices to display. [Table 98](#) explains the fields on this page.

Figure 131 Ignored Rogue Devices Page

OS	Vendor	IP Address	Last Discovered IP	Switch/Router	Port	Last Seen
WW PCBA Test				swr0210.dell.com	F30/2	4/9/2009 9:18 PM
Alcatel-Lucent				swr0210.dell.com	F30/18	4/14/2009 9:18 AM
Heureka-Packard				swr0210.dell.com	F30/9	4/14/2009 9:18 AM
Cisco Systems				swr0210.dell.com	S60/2	4/14/2009 9:18 AM

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.
- Click **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. AWMS performs a port scan on the device and attempts to determine the operating system (see [“RAPIDS Setup” on page 202](#))

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 mitigate the rogue remove it from the network and delete the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.



Note: Be aware that 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.

RAPIDS Setup

The RAPIDS > Setup page allows you to configure your AMP server for RAPIDS. Complete the settings on this page as desired, and click Save. Note that 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. Table 99 illustrates this page.

Table 99 RAPIDS > Setup Page Illustration

Basic Configuration		Containment Options	
ARP IP Match Timeout (1-168 hours):	<input type="text" value="24"/>	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
RAPIDS Export Threshold:	<input type="text" value="Rogue"/>	Manage rogue AP containment in monitor-only mode: Containment updates will always be pushed to devices running WMS offload, regardless of this setting.	<input type="radio"/> Yes <input checked="" type="radio"/> No
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="8"/>	Filtering Options	
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. Note: 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"/>	Filter Ad-hoc Rogues:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Delete Rogues not detected for (0-30 days, zero disables): Cannot be larger than the rogue discovery event expiration (30) configured on the AMP Setup page, unless that value is set to 0.	<input type="text" value="14"/>	Filter Rogues by Signal Strength:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Automatically OS scan rogue devices:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Filter Rogues Discovered by Remote APs:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Classification Options		<input type="button" value="Save"/> <input type="button" value="Save and Apply"/> <input type="button" value="Revert"/>	
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		

Table 100 RAPIDS > Setup > Classification Options

Field	Default	Description
Acknowledge Rogues by Default	No	Sets RAPIDS to acknowledge rogue devices upon initial detection, prior to their classification.
Manually Classifying Rogues Automatically Acknowledges them	Yes	Defines whether acknowledgement happens automatically whenever a rogue device receives a manual classification.

Table 101 RAPIDS > Setup > Filtering Options

Field	Default	Description
Filter ad-hoc rogues	No	Filters rogues according to ad-hoc status.

Table 101 *RAPIDS > Setup > Filtering Options*

Field	Default	Description
Filter rogues by signal strength	No	Filters rogues according to signal strength. Since anything below the established threshold will be ignored and possibly dangerous, we do not recommend enabling this setting. Instead, we recommend you incorporate signal strength into the classification rules on the RAPIDS > Rules page.
Filter rogues discovered by remote APs	No	Filters rogues according to the remote AP that discovers them. Enabling this option causes AWMS to drop all rogue discovery information coming from Remote APs.

Containment Options

Using RAPIDS, AMP can shield rogue devices from associating to Cisco WLC (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.



Note: WMS Offload is not required to manage containment in AMP.

Table 102 shows Containment Options.

Table 102 *RAPIDS > Setup > Containment Options*

Field	Default	Description
Manage Rogue AP Containment	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.
Manage Rogue AP Containment in Monitor-Only Mode	No	If No is selected, AMP will display the desired containment settings but not push them to the 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 Yes is selected, AMP will push the desired containment settings to the controllers in Monitor-Only mode, as well as the devices in managed mode.

1. Navigate to the **RAPIDS > SETUP** page to see Containment Options, as shown in [Figure 132](#).

Figure 132 *RAPIDS > Setup Containment Options Pane*

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.

Yes No

Manage Rogue AP Containment in Monitor-Only Mode:

Yes No

- From the **Containment Options** pane, click the Yes radio button to manage rogue AP containment. Once this is done, the Contained Rogue classification will appear as an option in the classification drop down menu as shown in [Figure 133](#).

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 133 *RAPIDS > Classification Rule Menu with Containment*

From the APs/Devices > **Rogues Contained** page, you can see the containment status information, as shown in [Figure 134](#).



Note: The Rogue Containment device tab is only present for devices that support containment.

Figure 134 *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 AWMS User Roles” on page 50](#).
- Use the **AMP Setup > General > Performance Tuning** page to define the processing priority of RAPIDS in relation to AWMS as a whole (see [Table 15 on page 45](#)).

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 205
- “Device OUI Score” on page 205
- “Rogue Device Threat Level” on page 206
- “Viewing and Configuring RAPIDS Rules” on page 206
- “Recommended RAPIDS Rules” on page 210
- “Using RAPIDS Rules with Additional AWMS Functions” on page 210

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 AWMS, which AWMS then processes. AWMS 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.



Note: RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between AWMS and ArubaOS, for scenarios involving WMS Offload.

Table 103 *Rogue Device Classification Matrix*

AWMS	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 Practices Guide*.

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 104](#) provides list the OUI scores definitions.

Table 104 *Device OUI Scores*

Score	Description
Score of 1	Indicates any device on the network; this is the lowest threat level on the network.

Table 104 Device OUI Scores

Score	Description
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 SOHO market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces SOHO 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, which is based on the classifying rule, ranging from 1 to 10, with a default value of 5. This classification process can help identify which of two rogues is likely to be a greater threat. Alerts can be defined and based on threat level; this is helpful for sorting rogue devices.

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 a device 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 AWMS, navigate to the **RAPIDS > Rules** page (Figure 135). Table 105 defines the content of the **RAPIDS > Rules** page.

Figure 135 RAPIDS > Rules Page Illustration

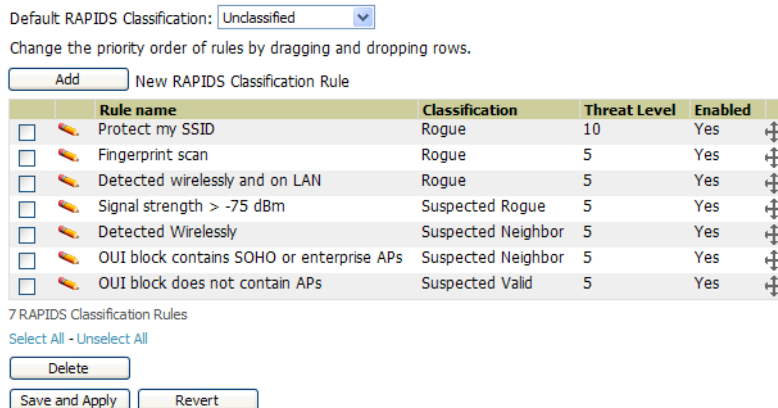



Table 105 RAPIDS > Rules Page

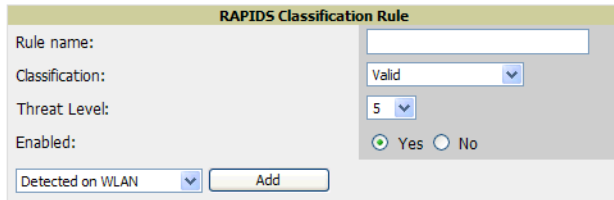
Field	Description
Default Classification	Sets the classification that a rogue device receives when it does not match any rules.
Add New RAPIDS Classification Rule	Click this button to create a RAPIDS classification rule.
Rule Name	Displays the name of any rule that has been configured. Rule names should be descriptive and should convey the core purpose for which it was created.
Classification	Displays the classification that devices receive if they meeting the rule criteria.
Threat Level	Displays the numeric threat level for the rogue device that pertains to the rule. Refer to “Rogue Device Threat Level” on page 206 for additional information.
Enabled	Displays the status of the rule, whether enabled or disabled.

Table 105 RAPIDS > Rules Page

Field	Description
Reorder Drag and Drop Icon 	Changes the sequence of rules in relation to each other. Click, 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. NOTE: The sequence of rules is very important to 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 136).

Figure 136 Classification Rule Page



Fill in the settings described in Table 105 then select an option from the drop down menu.

Table 106, Table 107, and Table 108 define the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 136). Once all rule settings are defined, click the Add button. The new rule automatically appears in the RAPIDS > Rules page.

Table 106 Wireless Properties Drop Down Menu

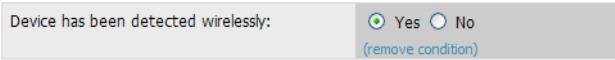
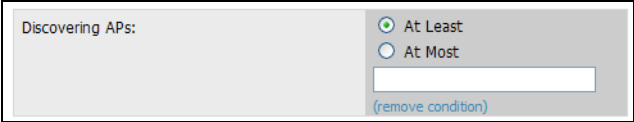
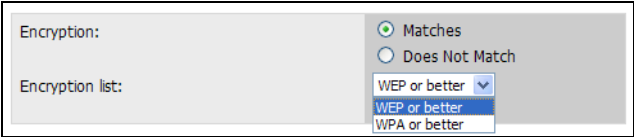
Option	Description
Detected on WLAN	Classifies based on how the rogue is detected on the wireless LAN. 
Discovering AP Count	Classifies based on the number of managed devices that can hear the rogue. Enter a numeric value and select At Least or At Most . 
Encryption	Classifies based on the rogue matching a specified encryption method. 

Table 106 Wireless Properties Drop Down Menu

Option	Description
Network type	<p>Rogue is running on the selected network type, either Ad-hoc or Infrastructure.</p> <div data-bbox="734 306 1362 527" style="border: 1px solid black; padding: 5px;"> <p>Network type: <input checked="" type="radio"/> Matches <input type="radio"/> Does Not Match</p> <p>Network type list: <input type="checkbox"/> Unknown <input type="checkbox"/> Infrastructure <input type="checkbox"/> Ad Hoc</p> <p>Select All - Unselect All (remove condition)</p> </div>
Signal Strength	<p>Rogue matches signal strength parameters. Specify a minimum and maximum value in DBm.</p> <div data-bbox="734 611 1362 726" style="border: 1px solid black; padding: 5px;"> <p>Signal maximum (-120-0): <input type="text" value="0"/></p> <p>Signal minimum (-120-0): <input type="text" value="-120"/></p> <p>(remove condition)</p> </div>
SSID	<p>Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression.</p> <div data-bbox="748 837 1347 1094" style="border: 1px solid black; padding: 5px;"> <p>SSID: <input checked="" type="radio"/> Matches <input type="radio"/> Does Not Match <input type="radio"/> Matches Regular Expression</p> <p>Enter a list of SSIDs, one per line. An asterisk (*) is a wildcard. Matching is case-insensitive, and ignores whitespace and non-alphanumeric characters.</p> <div style="border: 1px solid gray; height: 40px; width: 100%;"></div> <p>(remove condition)</p> </div> <p>NOTE: For SSID matching functions, AWMS processes only alpha-numeric characters and the asterisk wildcard character (*). AWMS ignores all other non-alpha-numeric characters. For example, the string of ethersphere-* matches the SSID of ethersphere-wpa2 but also the SSID of ethersphere_this_is_an_example (without any dashes).</p>

Table 107 Wireline Properties Drop Down Menu

Option	Description
Detected on LAN	<p>Rogue is detected on the wired network. Select Yes or No.</p> <div data-bbox="734 1472 1362 1545" style="border: 1px solid black; padding: 5px;"> <p>Device has been detected on LAN: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>(remove condition)</p> </div>
Fingerprint Scan	<p>Rogue matches fingerprint parameters.</p> <div data-bbox="734 1629 1362 1703" style="border: 1px solid black; padding: 5px;"> <p>Device discovered via wireline fingerprint scan: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>(remove condition)</p> </div>

Table 107 Wireline Properties Drop Down Menu

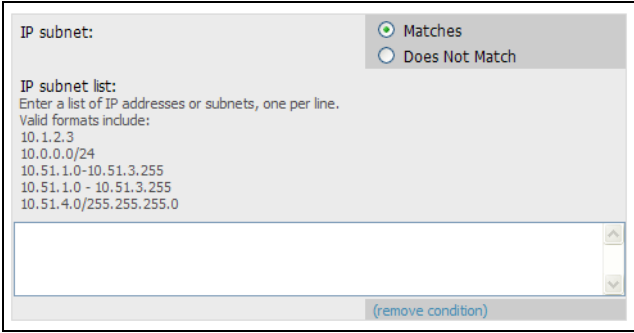
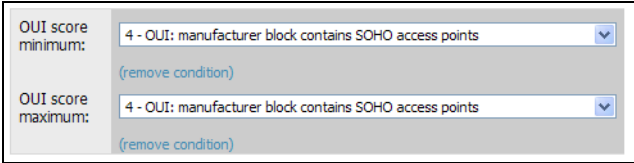
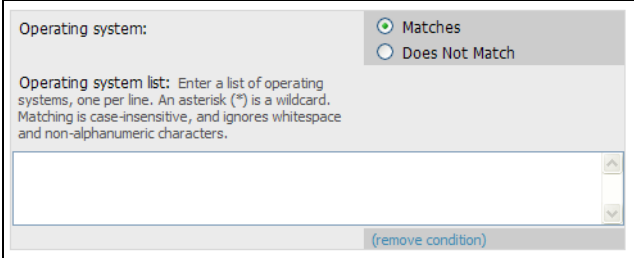
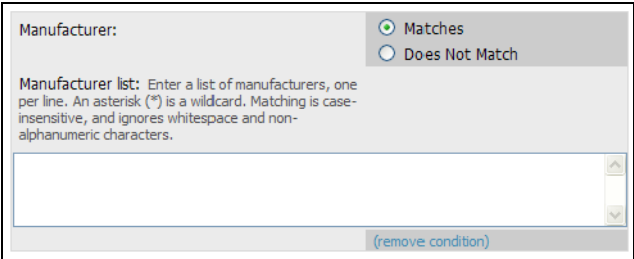
Option	Description
IP Address	<p>Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.</p>  <p>The screenshot shows a configuration form for IP Address. It includes a radio button group for 'Matches' (selected) and 'Does Not Match'. Below is a text area for 'IP subnet list' with instructions: 'Enter a list of IP addresses or subnets, one per line. Valid formats include: 10.1.2.3, 10.0.0.0/24, 10.51.1.0-10.51.3.255, 10.51.1.0 - 10.51.3.255, 10.51.4.0/255.255.255.0'. A 'remove condition' button is at the bottom right.</p>
OUI Score	<p>Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Click remove to remove one or both criteria, as desired.</p>  <p>The screenshot shows a configuration form for OUI Score. It features two dropdown menus: 'OUI score minimum' and 'OUI score maximum', both set to '4 - OUI: manufacturer block contains SOHO access points'. Each dropdown has a 'remove condition' button below it. A radio button group for 'Matches' (selected) and 'Does Not Match' is at the top right.</p>
Operating System	<p>Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.</p>  <p>The screenshot shows a configuration form for Operating System. It includes a radio button group for 'Matches' (selected) and 'Does Not Match'. Below is a text area for 'Operating system list' with instructions: 'Enter a list of operating systems, one per line. An asterisk (*) is a wildcard. Matching is case-insensitive, and ignores whitespace and non-alphanumeric characters.' A 'remove condition' button is at the bottom right.</p>

Table 108 Wireless/Wireline Properties Drop Down Menu

Option	Description
Manufacturer	<p>Rogue matches the manufacturer information of the rogue device.</p>  <p>The screenshot shows a configuration form for Manufacturer. It includes a radio button group for 'Matches' (selected) and 'Does Not Match'. Below is a text area for 'Manufacturer list' with instructions: 'Enter a list of manufacturers, one per line. An asterisk (*) is a wildcard. Matching is case-insensitive, and ignores whitespace and non-alphanumeric characters.' A 'remove condition' button is at the bottom right.</p>

After creating a new rule, click Add. This will return you to the **RAPIDS > Rules** page. Click Save and Apply to have the new rule take effect.

Deleting or Editing a Rules

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 click the **Delete** button. The rule is automatically deleted from the **RAPIDS > Rules** page.

To edit any existing rule, click the pencil icon next to that rule to launch the **RAPIDS Classification Rule** page (see [Figure 136](#)). Edit or revise the fields (see [Table 107](#)) as necessary then select the Save button.

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 AWMS. 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, AWMS 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.

Using RAPIDS Rules with Additional AWMS 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 AWMS, 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.

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 137](#), [Figure 138](#), and [Table 109](#) 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: 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 137 RAPIDS > Score Override Page

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables.

MAC Address Prefix	Vendor	Score
00:02:2D	Agere Systems	2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
00:02:6F	Senao International Co., Ltd.	4 - OUI: manufacturer block contains SOHO access points
00:03:03	JAMA Electronics Co., Ltd.	3 - OUI: manufacturer block contains enterprise access points
00:0D:54	3COM	4 - OUI: manufacturer block contains SOHO access points
00:10:40	INTERMEC CORPORATION	1 - Any device on the network not categorized with a higher score
00:13:72	Dell	1 - Any device on the network not categorized with a higher score
00:14:69	Cisco	4 - OUI: manufacturer block contains SOHO access points
00:15:2B	Cisco Systems	4 - OUI: manufacturer block contains SOHO access points
00:30:65	Apple Computer	3 - OUI: manufacturer block contains enterprise access points
00:30:89	Spectrapoint Wireless, LLC	4 - OUI: manufacturer block contains SOHO access points
00:CO:49	U.S. ROBOTICS, INC.	4 - OUI: manufacturer block contains SOHO access points

2. Click **Add** to create a new override or click the pencil icon next to an existing override to edit that override. The Score Override add or edit page appears (Figure 138).

Figure 138 Add/Edit Score Override Page

Table 109 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. Click **Add** to create the new override, or click **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 click **Delete**.

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**. See [Figure 139](#) for more information.

Figure 139 *Audit Log*

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 Rogue Device Resources

The following AWMS 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 [“Monitoring and Supporting AWMS with the System Pages” on page 249](#).
- **Reports**—The **Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see [“Defining Reports” on page 289](#).

Additional Security-Related Topics

For additional security-related features and functions, see the following topics in this guide.

- [“Configuring Group Security Settings” on page 91](#)
- [“Configuring Group SSIDs and VLANs” on page 94](#)
- [“Monitoring and Supporting AWMS with the System Pages” on page 249](#)

Daily WLAN administration often entails network monitoring, supporting WLAN and AWMS users, and monitoring AWMS system operations.

This chapter contains the following administration procedures:

- “Monitoring and Supporting WLAN Users” on page 228
- “Evaluating and Diagnosing User Status and Issues” on page 234
- “Supporting AWMS Stations with the Master Console” on page 239
- “Monitoring and Supporting AWMS with the Home Pages” on page 241
- “Upgrading AWMS” on page 256
- “Backing Up AWMS” on page 256
- “Monitoring and Supporting AWMS with the System Pages” on page 249

Overview of Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

- [Overview of Triggers and Alerts](#)
- [Viewing Triggers](#)
- [Creating New Triggers](#)
- [Delivering Triggered Alerts](#)
- [Viewing Alerts](#)
- [Responding to Alerts](#)

AWMS monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, AWMS generates (or triggers) alerts that enable you to address problems, frequently before users have a chance to report them. AWMS deploys two types of alerts:

Viewing Triggers

To view defined system triggers, navigate to the System > Triggers page. [Figure 140](#) illustrates this page.

Figure 140 System > Triggers Page Illustration (Split View)

Triggers:

New Trigger

	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

12 Triggers

Select All - Unselect All

Severity	Folder	Group	Include Subfolders	Logged Alert Visibility	Suppress Until Acknowledged
Warning	Top	-	Yes	By Role	Yes
Warning	Top	-	Yes	By Role	Yes
Normal	Top	-	Yes	By Role	-
Normal	Top	Outdoor	Yes	By Role	-
Normal	Top	-	Yes	By Role	Yes
Normal	Top	-	Yes	By Role	Yes
Normal	Top	-	Yes	By Role	-
Minor	Top	-	Yes	By Role	-
Major	Top	-	Yes	By Role	Yes

No Triggers for other roles found.

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, click the Add New Trigger button from the System > Triggers page. AWMS launches the Trigger Detail page, illustrated in [Figure 141](#).

Figure 141 System > Trigger Detail Page Illustration

Trigger

Type:

Severity:

Conditions

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

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. Configure the Trigger Restrictions settings. This establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. [Table 110](#) describes the options for trigger restrictions.

Table 110 System > Trigger Details Fields and Default Values

Notification Option	Description
Folder	Sets the trigger to apply only to APs/Devices in the specified folder or subfolders depending on the Include Subfolders option. NOTE: 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.
Include Subfolders	Sets the trigger to apply to all devices in the specified folder and all of the devices in folders under the specified folder.
Group	Sets the trigger to apply only to APs/Devices in the specified group. NOTE: 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.

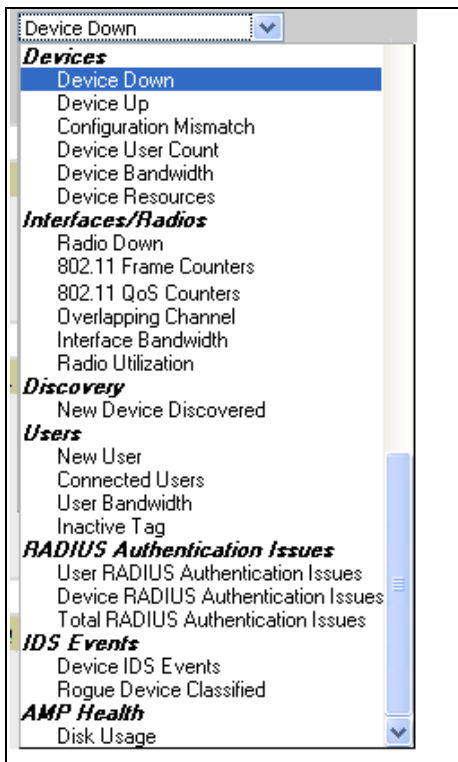
- b. Configure the Alert Notifications settings. In addition to appearing on the System > Triggers page, triggers can be configured to distribute to email or to a network management system (NMS), or to both.
 - If you select email, you are prompted to set the sender's email address and recipient email addresses.
 - If you select NMS, you are prompted to provide the IP address of the NMS Trap Destinations.
 - Define the Logged Alert Visibility, in which you can choose how this trigger is distributed. The trigger can distribute according to how is it 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.

Table 111 System > Trigger Condition Detail Alert Notifications for Defined Alerts

Notification Option	Description
Notification Type	Selects the action AWMS should take when an alert is triggered. When the NMS checkbox is checked AWMS sends an SNMP trap to the NMS servers defined for the role. When the Email checkbox is selected, AWMS sends an email to the specified address.
Sender Address	Displays the originator's email address in the From field of alert emails. NOTE: This field is only visible if the Email checkbox is selected.
Recipient Email Addresses	Displays the user, users or distribution lists that receive any email alerts. NOTE: This field is only visible if the Email checkbox is selected.
Logged Alert Visibility	Defines which users are able to view the alerts. When limited by role only users with the same role as the creator of the alert will be able to view it. When limited by triggering agent, any user who can view the device can view the alert.
Suppress new alerts until current alerts are acknowledged/deleted	Determines how often a trigger will fire. When No is selected a new alert will be created every time the trigger criteria are met. When Yes is selected an alert will only be received the first time the criteria is met. A new alert for the AP/device is not created until the initial one is acknowledged.

3. In the Trigger field, choose the desired trigger Type and the desired Severity, according to your needs. [Figure 142](#) illustrates the trigger types supported in AWMS. Severity levels are included in the email alerts. The alert summary information at the top of the AWMS screen can be configured to separately display severe alerts. Please see the Home > User Info section for more details.

Figure 142 *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.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- [“Setting Triggers for Devices” on page 216](#)
- [“Setting Triggers for Radios” on page 218](#)
- [“Setting Triggers for Discovery” on page 220](#)
- [“Setting Triggers for Users” on page 221](#)
- [“Setting Triggers for RADIUS Authentication Issues” on page 222](#)
- [“Setting Triggers for IDS Events” on page 223](#)
- [“Setting Triggers for AWMS Health” on page 225](#)

Setting Triggers for Devices

After completing steps 1-3 in [“Creating New Triggers” on page 214](#), perform the following steps to complete the configuration of device-related triggers.

- a. If you have not already done so, choose a device type from the Devices listed in the Type drop-down menu. See [Figure 142](#). [Table 112](#) itemizes and describes device trigger options and condition settings.

Table 112 *Device Trigger Types*

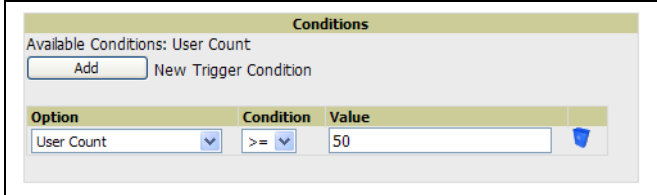
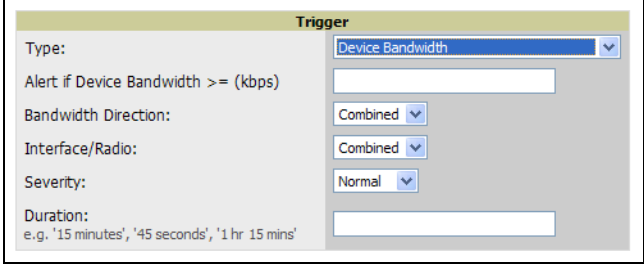
Device Trigger Options	Description
Device Down	<p>This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, managed AP has failed to respond to SNMP queries from AWMS.</p> <p>To set the conditions for this trigger type, click Add in the Conditions section. Complete the conditions with the Option, Condition, and Value 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>
Device Up	<p>This trigger type activates when an authorized, previously down AP is now responding to SNMP queries.</p> <p>To set the conditions for this trigger type, click Add in the Conditions section. Complete the conditions with the Option, Condition, and Value drop-down menus. The conditions establish the type that a device is or is not. Multiple conditions can apply to this type of trigger.</p>
Configuration Mismatch	<p>This trigger type activates when the actual configuration on the AP does not match the defined Group configuration policy.</p> <p>To set the conditions for this trigger type, click Add in the Conditions section. Complete the conditions with the Option, Condition, and Value drop-down menus. The conditions establish the type that a device is or is not. Multiple conditions can apply to this type of trigger.</p>
AP User Count	<p>This trigger type activates when the user count on a given AP device reaches a specific threshold. The number of user devices associated to an AP has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 10 users associated for more than 60 seconds). Selecting AP User Count displays an additional Duration setting. Define the Duration, which can be expressed as hours, minutes, seconds, or a combination of these. Click the Add New Trigger Condition button to create one or more conditions for the User Count trigger.</p> <p>Figure 143 <i>Sample of Trigger Condition for AP Device User Count</i></p>  <p>The screenshot shows a window titled "Conditions". At the top, it says "Available Conditions: User Count" and has an "Add" button followed by "New Trigger Condition". Below this is a table with three columns: "Option", "Condition", and "Value". The "Option" column has a dropdown menu with "User Count" selected. The "Condition" column has a dropdown menu with ">=" selected. The "Value" column has a text input field containing "50". There is a trash icon to the right of the value field.</p>

Table 112 *Device Trigger Types*

Device Trigger Options	Description
Device Bandwidth	<p>This trigger type indicates that the total bandwidth through the AP has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting Device Bandwidth as the trigger type displays the following new fields in the Type section. Define these settings.</p> <p>Figure 144 <i>Trigger Type Section for Device Bandwidth Type</i></p>  <ul style="list-style-type: none"> ● Alert if Device Bandwidth >= (kbps)—This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole. ● Bandwidth Direction—Choose In, Out, or Combined. This bandwidth is monitored on the device itself, not on the network as a whole. ● Interface/Radio—Choose either First or Second. ● Severity—The Severity level is likely defined already from an earlier step in this procedure. See “Creating New Triggers” on page 214. ● Duration—The Duration level is likely defined already from an earlier step in this procedure. See “Creating New Triggers” on page 214.
Device Resources	<p>This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined a defined percentage for a specified period of time. Selecting the Device Resources trigger type displays a new Duration setting. Define the Duration, which can be expressed as hours, minutes, seconds, or a combination of these.</p>

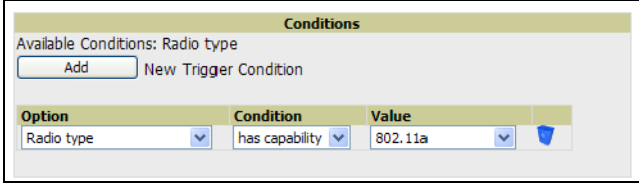
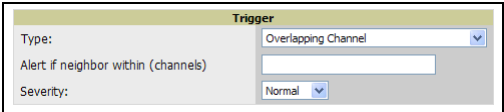
- b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in [Table 112](#).
 - To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 214](#) to create a new trigger.



Setting Triggers for Radios

After completing steps 1-3 in [“Creating New Triggers” on page 214](#), perform the following steps to complete the configuration of radio-related triggers.

- a. If you have not already done so, choose a trigger type from the Radios category, listed in the Type dropdown menu. [Table 113](#) itemizes and describes the Radios-related trigger types, and condition settings for each.

Table 113 Radio-Related Trigger Types

Radio Trigger Options	Description
Radio Down	<p>This trigger indicates when a device's radio is down on the network. Once you choose this trigger type, click Add New Trigger Condition to create at least one condition. The Radio Down trigger requires that a radio capability be set as a condition. The Value drop-down menu supports several condition options. The following example illustrates a Radio trigger that has 802.11a capability:</p> <p>Figure 145 Sample of Trigger Condition for Radio Type</p> 
802.11 Frame Counters	<p>This trigger type enables monitoring of traffic levels. When 802.11 Frame Counters is the trigger type, there are multiple rate-related parameters for which you define conditions. The rate of different parameters includes ACK Failures, Retry Rate and Rx Fragment Rate. See the drop-down Field menu in the Conditions section of the trigger page for a complete list of parameters. Click Add New Trigger Condition to access these settings. Define at least one condition for this trigger type.</p> <p>Selecting this trigger type displays a new Duration setting. Define the Duration, which can be expressed as hours, minutes, seconds, or a combination of these.</p>
802.11 QoS Counters	<p>This trigger type 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. Click Add New Trigger Condition to access these settings. Define at least one condition for this trigger type.</p> <p>Selecting this trigger type displays a new Duration setting. Define the Duration, which can be expressed as hours, minutes, seconds, or a combination of these.</p>
Overlapping Channel	<p>This type of trigger indicates that the neighboring AP is within a specified number of channels. This is calculated based on the AP with the most roams as reflected on the APs/Devices > Manage page, the Neighbors section.</p> <p>Selecting this trigger type displays a new option which you can enable as desired: Alert if neighbor within channels.</p> <p>Figure 146 Trigger Type Section for Overlapping Channel Type</p>  <p>NOTE: There is no Conditions configuration for Radios: Overlapping Channel triggers.</p>
Interface Bandwidth	<p>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 Device Type, Interface Description, Interface Label, Interface Mode, Interface Speed In (Mbps), Interface Speed Out (Mbps), Interface Type, and Radio Type.</p>

- b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 -  To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in [Table 112](#).
 -  To delete a trigger, check the box next to the trigger to remove, and click Delete.

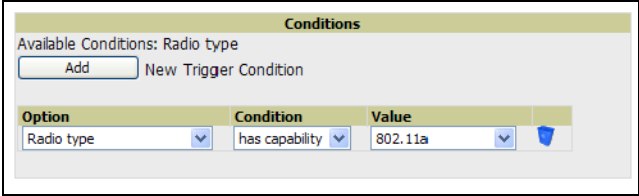
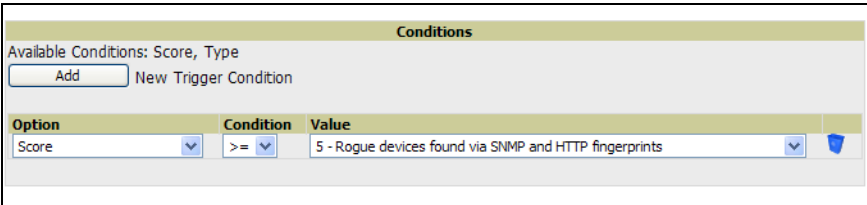
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 214](#) to create a new trigger.

Setting Triggers for Discovery

After completing steps 1-3 in [“Creating New Triggers” on page 214](#), perform the following steps to complete the configuration of triggers related to device discovery.

- a. If you have not already done so, choose a trigger type from the Discovery category, listed in the Type drop-down menu. See [Figure 142](#). [Table 114](#) itemizes and describes the Discovery-related trigger types, and condition settings for each discovery trigger type.

Table 114 *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	Description
New Devices Discovered	<p>This trigger type flags the discovery of a new and manageable AP, router or switch connected to the network (an AP that AWMS can monitor and configure). Once you choose this trigger type, click Add New Trigger Condition to specify a device type.</p> <p>The following example illustrates the Add Condition section for a New Devices Discovered trigger.</p> <p>Figure 147 <i>Sample of Condition for New Device Discovered Trigger Type</i></p> 
New Rogue Device Detected	<p>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 the Yes button. See “Using RAPIDS and Rogue Classification” on page 195 for more information on score definitions and discovery methods.</p> <p>Once you choose this trigger type, click Add New Trigger Condition to create one or more conditions. A condition for the Rogue Detected trigger enables you to specify the nature of the rogue device in multiple ways.</p> <ul style="list-style-type: none"> • All menus change according to the setting you define in the Options drop-down menu. You can define the rogue trigger according to the device type or according to the rogue score, or both if you set two or more conditions. See the Options drop-down menu for these choices. • You can define the discovery of a rogue device according to whether it meets certain mathematical parameters, or whether it is or is not a specific device type. See the Condition drop-down menu for these options, and note that they change according to your choice in the Options drop-down menu. • You can define either the rogue score or the rogue device type in the Value drop-down menu, according to what you chose in the Options drop-down menu. <p>Figure 148 <i>Sample of Trigger Condition for A Rogue Detected Trigger</i></p> 

- b. Delete conditions as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.

- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - ☞ To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in [Table 112](#).
 - ☞ To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “[Creating New Triggers](#)” on page 214 to create a new trigger.

Setting Triggers for Users

After completing steps 1-3 in “[Creating New Triggers](#)” on page 214, perform the following steps to complete the configuration of user-related triggers.

- a. If you have not already done so, choose a trigger type from the Users category, listed in the Type drop-down menu. See [Figure 142](#). [Table 115](#) itemizes and describes the User-related trigger types, and condition settings for each discovery trigger type.

Table 115 *User Trigger Types and Condition Settings*

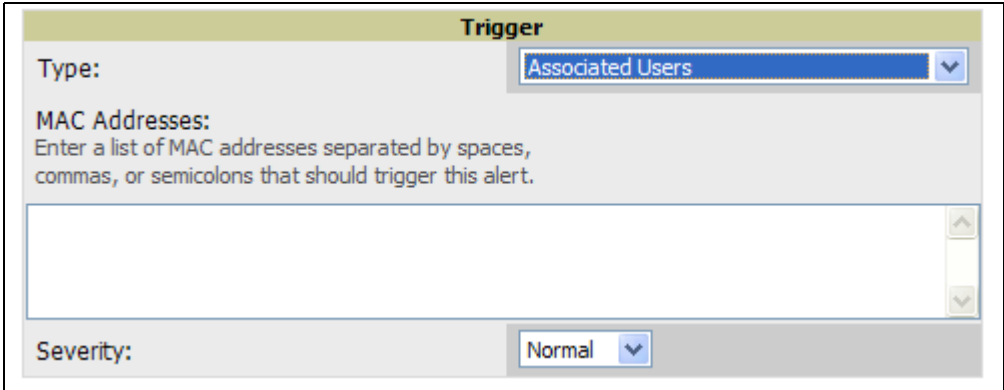
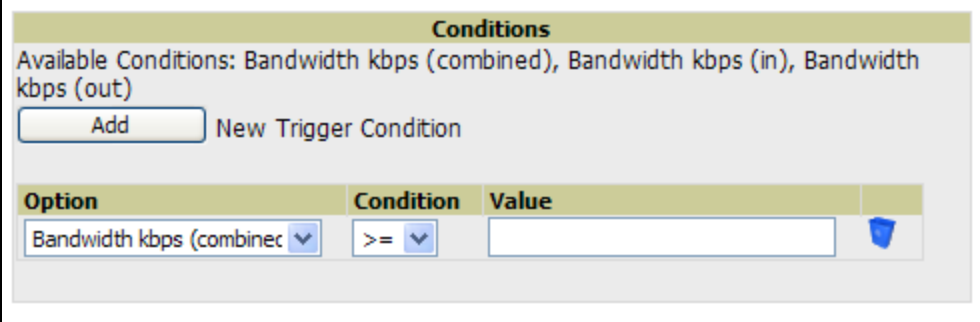
User Trigger Option	Description
New User	This trigger type indicates when a new user has associated to a device within a defined set of groups or folders. Note that the New User trigger type does not require the configuration of any condition settings, so the Condition section disappears.
Associated Users	<p>This trigger type indicates when 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.</p> <p>Figure 149 <i>Example of Associated User Configuration Section</i></p> 

Table 115 *User Trigger Types and Condition Settings (Continued)*

User Trigger Option	Description
User Bandwidth	<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 1500 kbps for more than 120 seconds).</p> <p>Once you choose this trigger type, click Add New Trigger Condition to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger.</p> <p>The Option drop-down menu provides these options:</p> <ul style="list-style-type: none"> ● Bandwidth kbps (Combined) ● Bandwidth kbps (in) ● Bandwidth kbps (out) <p>The Condition drop-down menu provides these options:</p> <ul style="list-style-type: none"> ● = — Bandwidth count equals... ● > — Bandwidth count is greater than... ● < — Bandwidth count is less than... ● >= — Bandwidth count is greater than or equal to... ● <= — Bandwidth count is less than or equal to... <p>The Value field requires that you input a numerical figure for kilobits per second (kbps).</p> <p>Figure 150 <i>Sample of User Bandwidth Trigger Condition</i></p> 
Inactive Tag	<p>This tags flags events in which an RFID tag has not been reported back to AWMS 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.</p>

- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - ✎ To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in [Table 112](#).
 - ✎ To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers”](#) on page 214 to create a new trigger.

Setting Triggers for RADIUS Authentication Issues



Note: AWMS first checks its own database prior to checking the RADIUS server database.

After completing steps 1-3 in “Creating New Triggers” on page 214, perform the following steps to complete the configuration of RADIUS-related triggers.

- a. If you have not already done so, choose a trigger type from the RADIUS... list in the drop-down Type menu. See Figure 142. Table 116 itemizes and describes the condition settings for each RADIUS Authentication trigger type.

Figure 151 RADIUS Authentication Trigger Condition Settings

Table 116 RADIUS Authentication Trigger Types and Condition Settings

RADIUS Trigger Options	Description
User RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Click Add New Trigger Condition to specify the count characteristics that trigger an alert. The Option, Condition, and Value fields allow you to define the numeric value of user issues.
Device RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a device. The Option, Condition, and Value fields allow you to define the numeric value of device issues.
Total RADIUS Authentication Issues	This trigger sets the threshold for the maximum number of failures before an alert is issued for both users and devices. The Option, Condition, and Value fields allow you to define the numeric value of device and user issues combined.

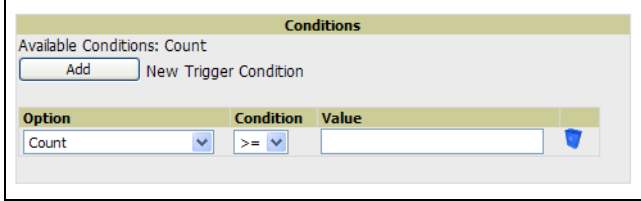
- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in Table 112.
 - To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “Creating New Triggers” on page 214 to create a new trigger.

Setting Triggers for IDS Events

After completing steps 1-3 in “Creating New Triggers” on page 214, perform the following steps to complete the configuration of Intrusion Detection System (IDS)-related triggers.

- a. If you have not already done so, choose the Device IDS Events trigger type from the drop-down Type menu. See Figure 142. Table 117 describes condition settings for this trigger type.

Table 117 Device IDS Events Authentication Trigger Types and Condition Settings

IDS Trigger Options	Description
Device IDS Events	<p>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. Click Add New Trigger Condition to specify the count characteristics that trigger an IDS alert. The Option, Condition, and Value fields allow you to define the numeric count of device IDS thresholds.</p> <p>Figure 152 <i>IDS Events Trigger Condition Settings</i></p> 

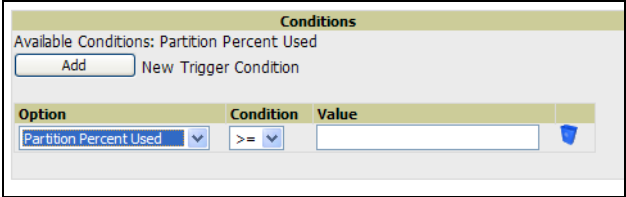
- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - To edit an existing trigger, click the pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in [Table 112](#).
 - To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of [“Creating New Triggers” on page 214](#) to create a new trigger.

Setting Triggers for AWMS Health

After completing steps 1-3 in “Creating New Triggers” on page 214, perform the following steps to complete the configuration of IDS-related triggers.

- a. If you have not already done so, choose the Disk Usage trigger type from the drop-down Type menu. See Figure 142 for trigger types. Table 118 describes the condition settings for this trigger type.

Table 118 Disk Usage Trigger and Condition Settings

AWMS Health Trigger	Description
Disk Usage	<p>This trigger type is based on the disk usage of the AMP (AWMS) system. This type of trigger indicates that disk usage for the AWMS server has met or surpassed a defined threshold. Click Add New Trigger Condition to specify the disk usage characteristics that trigger an alert. The Option, Condition, and Value fields allow you to define the numeric count of partition percent used.</p> <p>Figure 153 Condition Settings for Disk Usage Trigger</p> 

- b. Delete conditions for any trigger as desired by clicking the trash can icon to the right of the condition to be removed.
- c. Click Save. The trigger appears on your next viewing of the System > Triggers page with all other active triggers.
- d. You can edit or delete any trigger as desired from the System > Triggers page.
 - To edit an existing trigger, click the Pencil icon next to the respective trigger and edit settings in the Trigger Detail page described in Table 112.
 - To delete a trigger, check the box next to the trigger to remove, and click Delete.
- e. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of “Creating New Triggers” on page 214 to create a new trigger.

Delivering Triggered Alerts

AWMS uses Postfix to deliver alerts and reports via email, because it provides a high level of security and queues email locally until delivery. If AWMS 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.Aruba.com]
where mail.Aruba.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

```
tail -f /var/log/maillog
```

Viewing Alerts

AWMS displays alerts and provides additional alert details in two ways, as follows:

1. The Alerts Summary table is one way to monitor and process AWMS alerts. The Alert Summary table is available on the following AWMS pages, and is illustrated in [Figure 154](#):
 - APs/Devices > List
 - Groups > Monitor
 - Home > Overview
 - Users > Connected
 - Users > User Detail

Figure 154 *Alert Summary Table Illustration*

Alert Summary at 8/13/2009 10:16 AM				
Type ▲	Last 2 Hours	Last Day	Total	Last Event
System Alerts	6	100	216	8/13/2009 9:23 AM
IDS Events	0	14	40	8/13/2009 4:24 AM
Incidents	0	0	7	7/15/2009 12:32 PM
RADIUS Authentication Issues	45	358	760	8/13/2009 10:08 AM

This table displays alerts as follows; click 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.
- Incidents—Displays recent helpdesk incidents in which the incidents are open and associated to an AP. For a complete listing of incidents, navigate to the Helpdesk > Incidents page.

Note: The Incidents portion of this Alert Summary table only increments the counter for incidents that are open and associated to an AP. The incidents are based on the Top folder on the Groups > Monitor page and on the Home > Overview page. Incidents that are not related to devices in that folder are not counted in this Alert Summary.

To view all incidents, including those not associated to an AP, navigate to the Helpdesk > Incidents page.

- RADIUS Authentication Issues—Displays RADIUS-related alerts for devices in the top viewable folder available to the AWMS 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.
2. The second way to display and process alerts is to use the Alerts and Severe Alerts counters in the Status bar at the top of all AWMS pages, illustrated in [Figure 155](#).

Figure 155 *Alerts in the AWMS Status Bar*

New Devices: 29	Up: 349	Down: 176	Mismatched: 132	Rogue: 484	Users: 213	Alerts: 217	Severe Alerts: 217
-----------------	---------	-----------	-----------------	------------	------------	-------------	--------------------

Click the Alerts or the Severe Alerts counter or navigate to the System > Alerts page. [Figure 156](#) illustrates this page.

Figure 156 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:09:89:09	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
<input type="checkbox"/>	User Bandwidth	>= 100 kbps for 30 seconds	00:90:4B:F1:F0:D9	2/12/2007 9:09 AM	Warning
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Locally Ad-03:00:43	2/12/2007 3:00 AM	Minor
<input type="checkbox"/>	New Rogue AP Detected	>= 5 for rogue score	Unknown Gr-02:02:01	2/11/2007 12:58 PM	Minor
<input type="checkbox"/>	Configuration Mismatch		Tsunami_MP11	2/10/2007 8:16 PM	Major

For each new alert, the System > Alerts page displays the items listed in [Table 119](#).

Table 119 System > Alerts Fields and Default Settings

Field	Description
Trigger Type	Displays and sorts triggers by the type of trigger.
Trigger Summary	Provides an additional summary information related to the trigger.
Triggering Agent	Lists the name of the AP that generated the trigger. Clicking the AP name to display the APs/ Devices > Manage page for that AP.
Time	Displays the date and time the trigger was generated.
Severity	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. For example, if device AP 7 exceeds a maximum bandwidth trigger, that trigger does not create another alert for AP 7 until the first alert is recognized.
- Move the alert to the Alert Log by selecting the alert and clicking the Acknowledge button at the bottom of the page.
- You may see all logged alerts by clicking the View logged alerts link at the top of the System > Alerts page. Click the New Alerts link to return to the list of new alerts.
- Delete the alert by selecting the alert from the list and clicking the Delete button at the bottom of the System > Alerts page.

Monitoring and Supporting WLAN Users

The AWMS Users pages support WLAN users in AWMS. This section describes the Users pages as follows:

- [Overview of the Users Pages](#)
- [Monitoring WLAN Users With the Users > Connected and Users > All Pages](#)
- [Supporting Guest WLAN Users With the Users > Guest Users Page](#)
- [Supporting Users on Thin AP Networks With the Users > Tags Page](#)
- See also [Evaluating and Diagnosing User Status and Issues](#).

For information about creating AWMS users and AWMS user roles, refer to the following sections in this guide:

- [Creating AWMS Users](#)
- [Creating AWMS User Roles](#)

If you need to create an AWMS user account for frontline personnel who are to support Guest WLAN users, refer to “[Supporting Guest WLAN Users With the Users > Guest Users Page](#)” on page 231.

Overview of the Users Pages

The Users pages display multiple types of user data for existing WLAN users. The data comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and AWMS-generated data. AWMS supports the following Users pages:

- **Users > Connected**—Displays active users that are currently connected to the WLAN. For additional information, refer to “[Monitoring WLAN Users With the Users > Connected and Users > All Pages](#)” on page 229.
- **Users > All**—Displays all users of which AWMS 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 With the Users > Connected and Users > All Pages](#)” on page 229.
- **Users > Guest Users**—Displays all guest users in AWMS and allows you to create, edit, or delete guest users. See “[Supporting Guest WLAN Users With the Users > Guest Users Page](#)” on page 231.
- **Users > User Detail**—Displays client device information, alerts, signal quality, bandwidth, and association history. This page appears when you select a user’s MAC address from one of the following pages:
 - **Users > Connected**
 - **Users > All**
 - **Home > Search page results or Search field results that display the user MAC address**See “[Evaluating and Diagnosing User Status and Issues](#)” on page 234.
- **Users > 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:
 - **Users > Connected**
 - **Users > All**
 - **Home > Search page results or Search field results that display the user MAC address**See “[Evaluating and Diagnosing User Status and Issues](#)” on page 234.
- **Users > 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 AWMS. AWMS displays the information it receives from the controller in a table on this page. “[Supporting Users on Thin AP Networks With the Users > Tags Page](#)” on page 233.

Monitoring WLAN Users With the Users > Connected and Users > All Pages

The Users > Connected page displays all users currently connected in AWMS, and is illustrated in [Figure 157](#) and described in [Table 120](#). The information displayed on this page can be adjusted in the following ways:

- You can expand or customize the graphics to show maximum users, maximum average users, and additional custom view options.
- You can expand bandwidth to include custom view options.
- You can display all users, a specific number of users per page, or another custom setting.
- The Alerts section displays custom configured alerts that were defined in the System > Alerts page.

AWMS enhances the Users > Connection page to include SSID information for users. This enhancement applies to additional graph-based pages in AWMS. Furthermore, the Users > Connected page can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.



Note: Data that was gathered prior to an upgrade may be reported under an unknown SSID.

Figure 157 Users > Connected Page Illustration

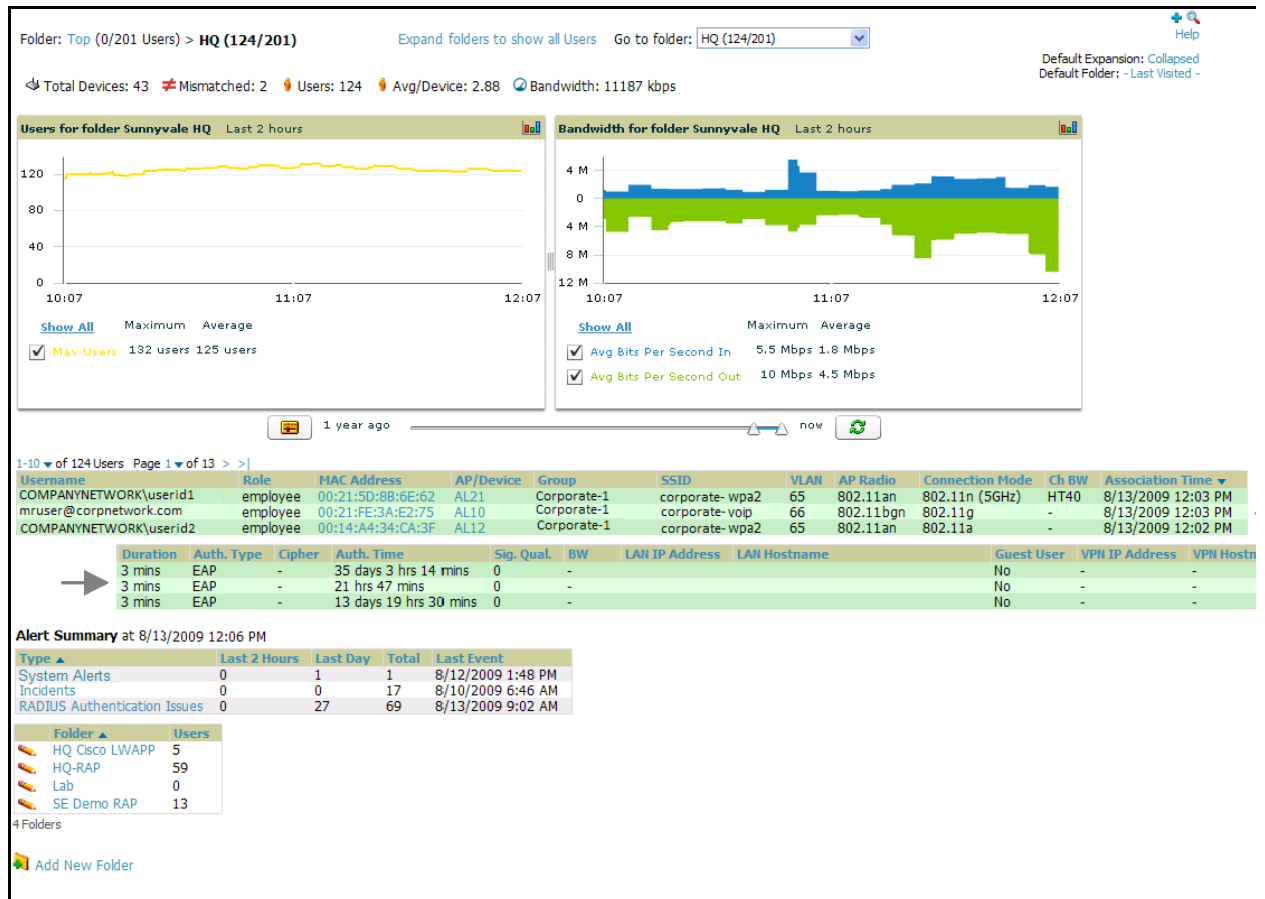


Table 120 Users > Connected Fields and Default Values

Field	Description
Username	Displays the name of the User associated to the AP. AWMS gathers this data in a variety of ways. It can be taken from RADIUS accounting data, traps from Cisco VxWorks APs and tables on Colubris APs. Usernames appear in italics when a username for that MAC address has been stored in the database from a previous association, but AWMS is not getting a username for the current association. This may indicate that the user has not yet been authenticated for this session (as indicated if you mouse over the username) or AWMS may not be getting a username from an external source like a RADIUS server for this association.
Role	Specifies the role by which the user is connected.
MAC Address	Displays the radio MAC address of the user associated to the AP. Also displays a link that redirects to the Users > Detail page.
AP/Device	Displays the name of the AP to which the MAC address is associated Also displays a link that takes you to this AP's Monitoring page.
Group	Displays the group containing the AP that the user is associated with.
SSID	Displays the SSID with which the user is associated.
VLAN	Displays the VLAN assigned to the user.
AP Radio	Displays the radio type of the radio that the user is associated with.
Connection Mode	Displays the 802.11 mode by which the user is connected.
Ch BW	Displays the channel bandwidth that currently supports the user.
User Radio Mode	Displays the Radio mode used by the user to associate to the AP. It will display 802.11a/b/g/bg. 802.11bg is reported when the AP does not provide AWMS with enough information to determine the exact radio type.
Association Time	Displays the first time AWMS recorded the MAC address as being associated.
Duration	Displays the length of time the MAC address has been associated.
Auth. Type	Displays the type of authentication employed by the user: EAP, PPTP, RADIUS accounting, or not authenticated. <ul style="list-style-type: none"> ● EAP is only reported by Cisco VxWorks via SNMP traps. ● PPTP is supported by Colubris APs acting as VPNs. ● RADIUS accounting servers integrated with AWMS will provide the RADIUS Accounting Auth type. ● All others are considered to be not authenticated.
Cipher	Displays WEP with keys. Cipher options are as follows: <ul style="list-style-type: none"> ● WEP with 802.11x ● WPA PSK (TKIP) ● WPA with 802.11x ● WPA2 PSK (AES) ● WPA2 with 802.11x (AES) This data is also displayed in the User Session report.
Auth. Time	Displays the how long ago the user authenticated.
Signal Quality	Displays the average signal quality the user enjoyed.
BW	Displays the average bandwidth consumed by the MAC address.
Location	Displays the QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP	Displays the IP assigned to the user MAC. This information is not always available. AWMS can gather it from the association table of Colubris APs or from the ARP cache of switches set up in AWMS.
LAN Hostname	Displays the LAN hostname of the user MAC.

Table 120 Users > Connected Fields and Default Values (Continued)

Field	Description
Guest User	Specifies whether the user is a guest or not.
VPN IP	Displays the VPN IP of the user MAC. This information can be obtained from VPN servers that send RADIUS accounting packets to AWMS.
VPN Hostname	Displays the VPN hostname of the user MAC.

Supporting Guest WLAN Users With the Users > Guest Users Page

AWMS supports guest user provisioning for Dell PowerConnect W, Aruba Networks 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 first step in creating a guest access user on the WLAN is to define a role for the AWMS users who will be responsible for associated tasks, if those users are to have a role other than Admin. Perform the following steps in the pages described to configure these settings.

1. Navigate to the AMP Setup > Roles page and create a new role of the type Guest Access Sponsor. Click Add New Role, select this role type, and enter a role name. Also, select the top folder for which this role should have access. [Figure 158](#) illustrates this page.

Figure 158 AMP Setup > Roles Page Illustration

The screenshot shows a 'Role' configuration form. The 'Name' field contains 'Front Desk Receptionist'. The 'Enabled' section has 'Yes' selected with a radio button. The 'Type' dropdown menu is set to 'Guest Access Sponsor'. The 'Top Folder' dropdown menu is set to 'Top'. At the bottom of the form are 'Add' and 'Cancel' buttons.

2. Next, navigate to the AMP Setup > Users page and create a new user with the role that was just created for Guest Access Sponsors. [Figure 159](#) illustrates this page.

Figure 159 AMP Setup > Users Page Illustration

The screenshot shows a 'User' configuration form. The 'Username' field contains 'Muir'. The 'Role' dropdown menu is set to 'Front Desk Receptionist'. The 'Password' and 'Confirm Password' fields both contain '****'. The 'Name' field contains 'Muir M.'. There are empty fields for 'Email Address' and 'Phone'. The 'Notes' field contains the text 'Will create guest access users for visitors at front desk.'. At the bottom of the form are 'Add' and 'Cancel' buttons.

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users. Anyone with an Admin role can also create guest access users.
4. The next step in creating a guest access user is to navigate to the Users > Guest Users 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 160](#) illustrates this page and [Table 121](#) describes the fields and information displayed.

Figure 160 Users > Guest Users Page Illustration

Guest Users:

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"/>	bobo	No	bobo@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

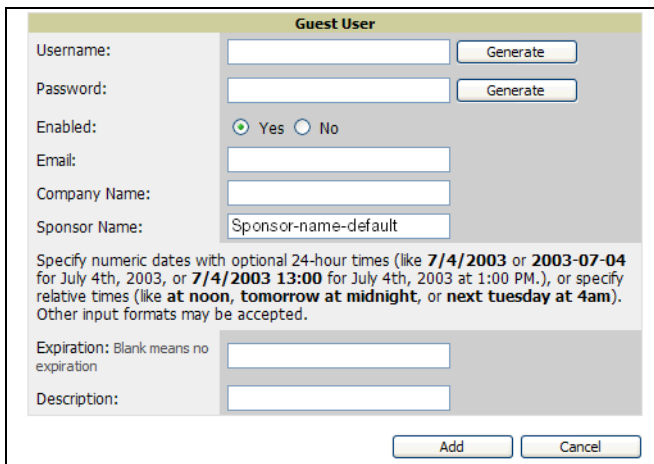
Table 121 Users > Guest Users Fields

Field	Description
Repair Guest User Errors button	Sets AWMS to attempt to push the guest user again in an attempt to repair any errors in the Status column.
Add New Guest Users button	Adds a new guest user to a controller via AWMS.
Username	Randomly generates a user name for privacy protection. This name appears on the Guest User detail page.
Enabled	Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled). Configure the user on the Guest User edit page by clicking the pencil icon.
Email	Displays the optional email address of the user. Set the email address with the Guest User edit page by clicking the pencil icon.
Company Name	Displays the optional company name for the user. Set the company name with the Guest User edit page by clicking the pencil icon.
Sponsor Name	Displays the name of the sponsor for the guest user. This setting is optional. Set the sponsor with the Guest User edit page by clicking the pencil icon.
Expiration	Displays the date the guest user's access is to expire. Set the expiration with the Guest User edit page by clicking the pencil icon.
Profile/SSID	Sets the SSID that the guest user can access. This setting applies to Cisco WLC only. Set the SSID with the Guest User edit page by clicking the pencil icon.
Status	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and click the Repair guest user errors button.
Print button (for checked users)	Sends the selected guest user's information to an external printer.
Delete button (for checked users)	Removes the selected guest user from AWMS and from the controller.

Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the SSID column, when this column is present for Cisco WLC. The User Detail page for a guest user also contains a box with the same guest information that appears for each user on the Users > Guest Users list.

- To add a new guest user, click Add, and complete the required and optional fields in the User Detail page, illustrated in [Figure 161](#). [Table 121](#) describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 161 Users > Guest Users > Add New Guest User Page Illustration



To make the Username or Password anonymous and to increase security, complete these fields then click Generate. The anonymous and secure Username and Password appear in the respective fields.

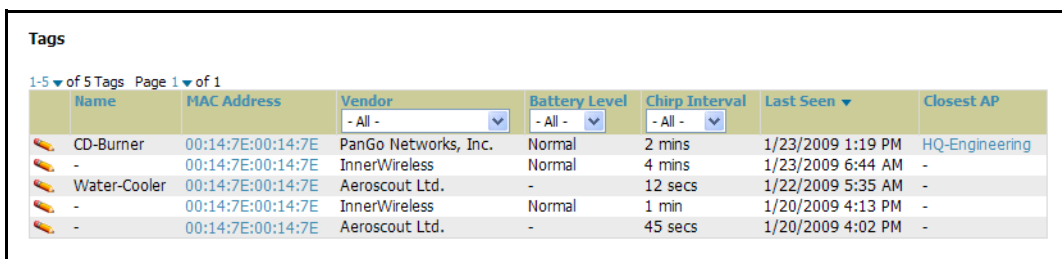
6. Click Add to complete the new guest user, or click Cancel to back out of new user creation. The Users > Guest Users page appears and displays results, as applicable.

Supporting Users on Thin AP Networks With the Users > Tags Page

Radio Frequency Identification (RFID) is an industry-standard method that 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 innovations that improve network integration, battery life, and other functions.

The Users > 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 AWMS monitors. AWMS displays the information it receives from the controller in a table on this page. [Figure 162](#) illustrates this page, and [Table 122](#) describes fields and information displayed.

Figure 162 Users > Tags Page Illustration



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	-
-	00:14:7E:00:14:7E	Aeroscout Ltd.	-	45 secs	1/20/2009 4:02 PM	-

Table 122 Users > Tags Fields

Field	Description
Name	Displays the user-editable name associated with the tag.
MAC Address	Displays the MAC address of the AP that reported the tag.
Vendor	Displays the vendor of the tag (Aeroscout, PanGo and Newbury)—display all or filter by type.
Battery Level	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.

Table 122 *Users > Tags Fields*

Field	Description
Chirp Interval	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.
Last Seen	Date and time the tag was last reported to AWMS.
Closest AP	The AP that last reported the tag to the controller (linked to the AP monitoring page in AWMS).

- To edit the name of the tag, or to add notes to the tag's record, click 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.
- There is also a Tag Not Heard trigger, which can be used to generate an alert if a tag is not reported to AWMS 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 AWMS with the System Pages” on page 249](#).

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 User Detail and Diagnostic pages. This section describes these two pages as follows:

- [Evaluating User Status with the Users > User Detail Page](#)
- [Evaluating User Status with the Users > Diagnostics Page](#)

Evaluating User Status with the Users > User Detail Page

The Users > User Detail page is a focused sub-menu that becomes visible when you select a specific user. Access the Users > User Detail page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
 - Users > Connected
 - Users > All
- Search for a user and click the associated MAC address in the search results, then select the User Detail page from the navigation pane.

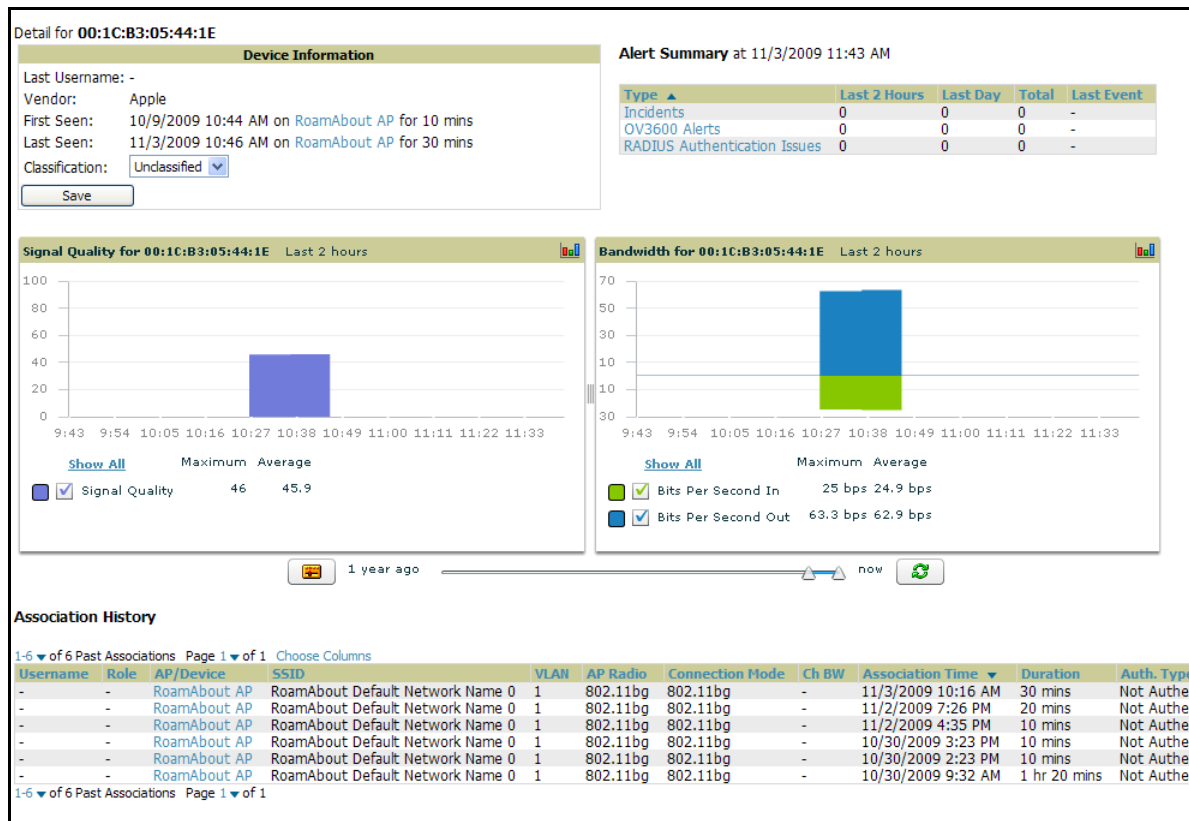
[Figure 163](#) illustrates the contents of Users > User Details page.

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, when VisualRF is licensed and enabled, this page provides a graphical map of the user location and facility information.

If you have deployed WLAN switches and have WMS offload enabled on the network, the Users > User Detail page allows you to classify the device in the Device Information section, and to push this configuration to the WLAN switches that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—Designates the device as a legitimate network device. Once this Valid setting is pushed to the WLAN switch, and if the Protect Valid Stations option is also enabled on the switch, then this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—Controls the user on the device, as defined with containment configurations set with WMS Offload in AOS.

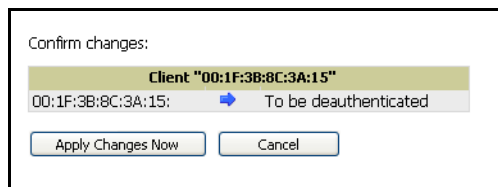
Figure 163 Users > User Detail Page Illustration



Using the Deauthenticate User Feature

Some displays of the User > User Detail page includes the Deauthenticate User feature in the Current Association field. Click the Deauthenticate User button to use this feature. Refer to [Figure 164](#) as an illustration:

Figure 164 Users > User Detail > Deauthenticate User Page



Evaluating User Status with the Users > Diagnostics Page

Introduction and Overview of the Diagnostics Page

The Users > Diagnostics page is a focused sub-menu that becomes visible when you select user-specific information. Access the Users > Diagnostics page in one of the following ways:

- Click the MAC Address for a specific user from one of the following pages:
 - Users > Connected
 - Users > All
- You can search for a user and click the associated MAC address from the search results.

This page provides an overview of a user's general status and connectivity on the network.

Each section of the Users > Diagnostics page displays information by which to evaluate possible user issues. Refer to [Table 123](#) for explanation and illustration of page components.

Table 123 Users > Diagnostics Page Sections

Section	Description																																	
Possible Issues	<p>This section summarizes the most likely items to create issues for a user on the network. Figure 165 illustrates this section.</p> <p>Figure 165 Groups > Diagnostics > Possible Issues Illustration</p> <table border="1"> <thead> <tr> <th colspan="3">Possible Issues</th> </tr> <tr> <th>Issue</th> <th>Ideal</th> <th>Actual</th> </tr> </thead> <tbody> <tr> <td>Low signal quality:</td> <td>>= 20</td> <td>0</td> </tr> <tr> <td>Excessive roaming in last two hours:</td> <td><= 10 roams</td> <td>0</td> </tr> <tr> <td>High user bandwidth:</td> <td><= 50% of radio capacity</td> <td>0 kbps (0.00%)</td> </tr> <tr> <td>Unauthenticated user:</td> <td>Authenticated</td> <td>EAP</td> </tr> <tr> <td>High user load on AP/radio:</td> <td><= 15</td> <td>26</td> </tr> <tr> <td>High AP/radio bandwidth:</td> <td><= 75% of radio capacity</td> <td>1910 kbps (0.77%)</td> </tr> <tr> <td>802.11b users associated to 802.11bg radio:</td> <td>None</td> <td>0</td> </tr> <tr> <td>802.11bg or 802.11a users associated to 802.11n radio:</td> <td>None</td> <td>5</td> </tr> <tr> <td>High FCS error rate:</td> <td><= 100</td> <td>0</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • Low signal quality—If signal quality falls outside of ideal range, then possible resolution might be installation of more or better antennas on the APs, adding APs, increasing the transmit power of the APs, investigating intermittent RF interference, such as the startup schedule of a nearby air conditioning unit, or evaluating the client settings. • Excessive roaming in last 2 hours—Roaming means that a user’s connection moves from one AP to another. Excessive roaming is generally classified as 10 or more roaming instances in the past two hours. If there is excessive roaming, but the user has been stationary, then the user might be located where there is weak coverage from two overlapping APs. In this case, adjusting the signal strength for one of those APs may resolve the issue. • High User Bandwidth—If a user reports issues with network performance, the issue could derive from excessive bandwidth consumption. Additionally, another user on the same AP might be consuming excessive bandwidth. In that latter case, investigate user bandwidth consumption for all users on a given AP, not strictly the user who reports an issue. • Unauthenticated User—This section conveys the user’s current authentication status and the actual authentication type. If a network deploys RADIUS authentication, then the RADIUS server could be experiencing issues even if a user attempts to log in with valid authentication credentials but shows as Unauthenticated on this page. • High user load on AP/radio—This field indicates if the number of users on a given AP has exceeded that AP’s functional capacity. Excessive users on an AP could degrade performance for all users on that AP. Some users will start to experience performance issues, may start to drop off, You may need to add an additional AP in that area, or take other steps to distribute the user load more evenly across multiple APs. Refer to the Current User Counts section on this page for additional details. • High AP radio bandwidth—This figure derives from how groups of users share radio bandwidth on a shared AP. You may get a high figure in this category if nearby APs have gone down. You may not need to add an additional AP to resolve this issue, but you would need to determine why neighboring APs are not functioning properly. • 802.11 radio parameters—These two sections indicate the likelihood that a user’s issues are derived from mismatched 802.11 deployment. That is, an 802.11ab or g user who is connected through an 802.11n radio might not benefit from full 802.11n functionality. These two fields indicate the likelihood of such an issue impacting a user’s experience on the network. 	Possible Issues			Issue	Ideal	Actual	Low signal quality:	>= 20	0	Excessive roaming in last two hours:	<= 10 roams	0	High user bandwidth:	<= 50% of radio capacity	0 kbps (0.00%)	Unauthenticated user:	Authenticated	EAP	High user load on AP/radio:	<= 15	26	High AP/radio bandwidth:	<= 75% of radio capacity	1910 kbps (0.77%)	802.11b users associated to 802.11bg radio:	None	0	802.11bg or 802.11a users associated to 802.11n radio:	None	5	High FCS error rate:	<= 100	0
Possible Issues																																		
Issue	Ideal	Actual																																
Low signal quality:	>= 20	0																																
Excessive roaming in last two hours:	<= 10 roams	0																																
High user bandwidth:	<= 50% of radio capacity	0 kbps (0.00%)																																
Unauthenticated user:	Authenticated	EAP																																
High user load on AP/radio:	<= 15	26																																
High AP/radio bandwidth:	<= 75% of radio capacity	1910 kbps (0.77%)																																
802.11b users associated to 802.11bg radio:	None	0																																
802.11bg or 802.11a users associated to 802.11n radio:	None	5																																
High FCS error rate:	<= 100	0																																

Table 123 Users > Diagnostics Page Sections

Section	Description																																																
Possible Issues (Cont'd)	<ul style="list-style-type: none"> High FCS error rates—Frame Check Sequence (FCS) errors indicate that frames of data that transmit across the network are experiencing corruption. A high FCS error rate indicates wireless link interference in the area. <p>Frames that are transmitted by APs managed in AWMS are susceptible to interference from other devices with radios operating in the same frequencies range (same channel), or electromagnetic interference from electronic devices such as power cables in the office.</p> <p>The 802.11 MAC layer uses the Frame Check Sequence (FCS) field to determine if errors have occurred during the transmission. Each MAC layer frame has a FCS field that is used to store a checksum. The checksum is added at the source AP, and verified at the destination.</p> <p>If the FCS checksum included in the frame does not match the recalculated number, then an error has occurred during the transmission, the frame is discarded, and the destination host requests it to be resent. This can effectively reduce the bandwidth and throughput in the network.</p> <p>A high FCS error rate in this field could indicate that the APs are experiencing a high level of link interference and the clients are getting less bandwidth and throughput due to MAC layer frame retransmissions.</p> <p>One response is to assign a different channel to the AP to improve the performance from your AWMS server. Use the Optimize feature to assign the best available channel to the AP.</p> <ol style="list-style-type: none"> Log in to your AWMS. From the AP/Devices > List page, click the Modify Devices link. Select the APs that are running into channel interference problems by checking the corresponding box for each. Several new settings appear below the device list by which to configure these devices. <p>NOTE: Toward the bottom of this section, click Optimize for the Optimize channel assignment to reduce overlap setting. A confirm changes page appears by which to apply and schedule this change, or to cancel out of this setting. This explanation derived from the following location:</p> <ul style="list-style-type: none"> <i>Airheads Online Forum</i>, explanation by bjacobs: <ol style="list-style-type: none"> http://airheads.arubanetworks.com/vBulletin/showthread.php?p=1266#post1266 																																																
Diagnostics Summary	<p>This section summarizes bandwidth, user count, and signal quality parameters for specific windows of time. This section is useful when diagnosis or troubleshooting follows issues that had been observed a few or several hours prior. Figure 166 illustrates this section.</p> <p>Figure 166 Diagnostics Summary Illustration (Partial Display)</p> <table border="1" data-bbox="500 1136 1455 1352"> <thead> <tr> <th colspan="6">Diagnostic Summary</th> </tr> <tr> <th></th> <th>Current</th> <th>Last Hour</th> <th>Last 2 Hours</th> <th>Last 4 Hours</th> <th>Last 8 Hours</th> </tr> </thead> <tbody> <tr> <td>User Bandwidth</td> <td>0 kbps (0.00%)</td> <td>69 kbps (0.03%)</td> <td>121 kbps (0.05%)</td> <td>198 kbps (0.08%)</td> <td>198 kbps (0.08%)</td> </tr> <tr> <td>Radio Bandwidth</td> <td>1910 kbps (0.77%)</td> <td>4377 kbps (1.76%)</td> <td>4377 kbps (1.76%)</td> <td>33963 kbps (13.69%)</td> <td>33963 kbps (13.69%)</td> </tr> <tr> <td>AP Bandwidth</td> <td>1911 kbps (0.39%)</td> <td>4377 kbps (0.88%)</td> <td>4377 kbps (0.88%)</td> <td>33963 kbps (6.85%)</td> <td>33963 kbps (6.85%)</td> </tr> <tr> <td>Radio User Count</td> <td>19</td> <td>20</td> <td>20</td> <td>20</td> <td>20</td> </tr> <tr> <td>AP User Count</td> <td>26</td> <td>27</td> <td>27</td> <td>27</td> <td>27</td> </tr> <tr> <td>Signal Quality</td> <td>0</td> <td>50</td> <td>50</td> <td>49</td> <td>49</td> </tr> </tbody> </table> <p>The following categories link to additional details pages:</p> <ul style="list-style-type: none"> User Bandwidth—click this link to display flash graphs for user bandwidth metrics. Radio Bandwidth—click this link to display flash graphs for radio bandwidth consumption. AP Bandwidth—click this link to display flash graphs for AP bandwidth consumption. Radio User Count—click this link to display flash graphs for user count metrics. AP User Count—click this link to display flash graphs for user count metrics. Signal Quality—click this link to display flash graphs for signal quality. 	Diagnostic Summary							Current	Last Hour	Last 2 Hours	Last 4 Hours	Last 8 Hours	User Bandwidth	0 kbps (0.00%)	69 kbps (0.03%)	121 kbps (0.05%)	198 kbps (0.08%)	198 kbps (0.08%)	Radio Bandwidth	1910 kbps (0.77%)	4377 kbps (1.76%)	4377 kbps (1.76%)	33963 kbps (13.69%)	33963 kbps (13.69%)	AP Bandwidth	1911 kbps (0.39%)	4377 kbps (0.88%)	4377 kbps (0.88%)	33963 kbps (6.85%)	33963 kbps (6.85%)	Radio User Count	19	20	20	20	20	AP User Count	26	27	27	27	27	Signal Quality	0	50	50	49	49
Diagnostic Summary																																																	
	Current	Last Hour	Last 2 Hours	Last 4 Hours	Last 8 Hours																																												
User Bandwidth	0 kbps (0.00%)	69 kbps (0.03%)	121 kbps (0.05%)	198 kbps (0.08%)	198 kbps (0.08%)																																												
Radio Bandwidth	1910 kbps (0.77%)	4377 kbps (1.76%)	4377 kbps (1.76%)	33963 kbps (13.69%)	33963 kbps (13.69%)																																												
AP Bandwidth	1911 kbps (0.39%)	4377 kbps (0.88%)	4377 kbps (0.88%)	33963 kbps (6.85%)	33963 kbps (6.85%)																																												
Radio User Count	19	20	20	20	20																																												
AP User Count	26	27	27	27	27																																												
Signal Quality	0	50	50	49	49																																												

Table 123 Users > Diagnostics Page Sections

Section	Description																																			
Current User Counts	<p>The Current User Counts section displays user counts for APs and radios, and includes additional summary information for APs. Figure 167 illustrates this section:</p> <p>Figure 167 Users > Diagnostics > Current User Counts Illustration</p> <table border="1"> <thead> <tr> <th colspan="3">Current User Counts</th> </tr> <tr> <th></th> <th>User Count on AP</th> <th>User Count on Radio</th> </tr> </thead> <tbody> <tr> <td>802.11a</td> <td>4</td> <td>0</td> </tr> <tr> <td>802.11n (5GHz)</td> <td>6</td> <td>0</td> </tr> <tr> <td>802.11g</td> <td>10</td> <td>10</td> </tr> <tr> <td>Total</td> <td>20</td> <td>10</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">AP Information</th> </tr> </thead> <tbody> <tr> <td>Name:</td> <td>AL1</td> </tr> <tr> <td>Uptime:</td> <td>1 day 15 hrs 44 mins</td> </tr> <tr> <td>Location:</td> <td>-</td> </tr> <tr> <td>Type:</td> <td>Aruba AP 125</td> </tr> <tr> <td>Controller IP Address:</td> <td>10.252.252.252</td> </tr> </tbody> </table>	Current User Counts				User Count on AP	User Count on Radio	802.11a	4	0	802.11n (5GHz)	6	0	802.11g	10	10	Total	20	10	AP Information		Name:	AL1	Uptime:	1 day 15 hrs 44 mins	Location:	-	Type:	Aruba AP 125	Controller IP Address:	10.252.252.252					
Current User Counts																																				
	User Count on AP	User Count on Radio																																		
802.11a	4	0																																		
802.11n (5GHz)	6	0																																		
802.11g	10	10																																		
Total	20	10																																		
AP Information																																				
Name:	AL1																																			
Uptime:	1 day 15 hrs 44 mins																																			
Location:	-																																			
Type:	Aruba AP 125																																			
Controller IP Address:	10.252.252.252																																			
	<p>Use this section in combination with the Possible Issues section.</p>																																			
802.11 Counters Summary	<p>The 802.11 Counters Summary section conveys the same information that is available from the Radio Statistics link from the APs/Devices > Monitor page. Figure 168 illustrates this section.</p> <p>Figure 168 Users > Diagnostics > 802.1 Counters Summary Illustration</p> <table border="1"> <thead> <tr> <th colspan="5">802.11 Counters Summary</th> </tr> <tr> <th></th> <th>Current</th> <th>Last Hour</th> <th>Last Day</th> <th>Last Week</th> </tr> </thead> <tbody> <tr> <td>Unacked</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Retries</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Failures</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Dup Frames</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>FCS Errors</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table> <p>NOTE: This section is supported for Cisco devices. AWMS does not gather device counter information from certain other device vendors.</p> <p>For additional information, click a Cisco device from the APs/Devices > List page, and on the Monitor page for that device, click Statistics. The ensuing page displays the 802.11 Counters Summary table, which summarizes counters on the AP level. Scroll down on this page to convey additional information from which the counters summary on the Diagnostics page is derived. Some of the sections on the Statistics page only populate when there is a user when an associated user is generating traffic on the network. Other sections convey information if there is no user associated and the device is strictly listening for traffic.</p>	802.11 Counters Summary						Current	Last Hour	Last Day	Last Week	Unacked	0	0	0	0	Retries	0	0	0	0	Failures	0	0	0	0	Dup Frames	0	0	0	0	FCS Errors	0	0	0	0
802.11 Counters Summary																																				
	Current	Last Hour	Last Day	Last Week																																
Unacked	0	0	0	0																																
Retries	0	0	0	0																																
Failures	0	0	0	0																																
Dup Frames	0	0	0	0																																
FCS Errors	0	0	0	0																																
Radios That Can Hear This User	<p>The Radios That Can Hear This User section summarizes the AP correspondence to Radios, with SNR values, user count metrics, bandwidth consumption and additional information that collectively describe the user's device-level activity on the network. Figure 169 illustrates this section.</p> <p>Figure 169 Users > Diagnostics > Radios That Can Hear This User Illustration</p> <table border="1"> <thead> <tr> <th colspan="7">Radios That Can Hear This User</th> </tr> <tr> <th>AP</th> <th>Radio</th> <th>SNR</th> <th>User Count</th> <th>Bandwidth (kbps)</th> <th>Uptime</th> <th>Recently Associated</th> </tr> </thead> <tbody> <tr> <td>AL39</td> <td>802.11an</td> <td>25</td> <td>2</td> <td>0.93712090369561</td> <td>8 days 16 hrs 12 mins</td> <td>No</td> </tr> <tr> <td>00:1a:1e:c0:55:46</td> <td>802.11an</td> <td>26</td> <td>0</td> <td>0</td> <td>32 days 12 hrs 5 mins</td> <td>No</td> </tr> <tr> <td>AL30</td> <td>802.11an</td> <td>24</td> <td>0</td> <td>0</td> <td>8 days 14 hrs 56 mins</td> <td>No</td> </tr> </tbody> </table>	Radios That Can Hear This User							AP	Radio	SNR	User Count	Bandwidth (kbps)	Uptime	Recently Associated	AL39	802.11an	25	2	0.93712090369561	8 days 16 hrs 12 mins	No	00:1a:1e:c0:55:46	802.11an	26	0	0	32 days 12 hrs 5 mins	No	AL30	802.11an	24	0	0	8 days 14 hrs 56 mins	No
Radios That Can Hear This User																																				
AP	Radio	SNR	User Count	Bandwidth (kbps)	Uptime	Recently Associated																														
AL39	802.11an	25	2	0.93712090369561	8 days 16 hrs 12 mins	No																														
00:1a:1e:c0:55:46	802.11an	26	0	0	32 days 12 hrs 5 mins	No																														
AL30	802.11an	24	0	0	8 days 14 hrs 56 mins	No																														

Supporting AWMS Stations with the Master Console

The Master Console (MC) is used to monitor multiple AWMS stations from one central location. The Master Console is designed for customers running multiple AWMS servers. Once an AWMS station has been added to the MC, it will be polled for basic AWMS information.

- Reports can be run from the Master Console to display information from multiple AWMS 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 AWMS installations using the Global Groups feature.
- The Master Console supports:
 - 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, to include Home > Overview, APs Devices > List, RAPIDS > Rogue APs, and additional such pages.
 - The Public Portal of the Master Console supports configuration of the iPhone interface. This can be configured using the Master Console AWMS page. See “[Defining General AWMS Server Settings](#)” on page 39.
 - The Master Console and Failover servers can be configured with a Device Down trigger that generates an alert if communication is lost to a managed or watched AWMS station. In addition to generating an alert, the Master Console or Failover server can also send email or NMS notifications about the event. See “[Monitoring and Supporting AWMS with the System Pages](#)” on page 249.



Note: The license key determines if the server will behave as a Master Console or as a standard AWMS server.

The Master Console also contains an optional Public Portal, which allows any user to view basic group-level data for each managed AWMS. This feature is disabled by default for security reasons, no AWMS or Master Console login is required to view the public portal. It can be enabled by navigating to the AMP Setup > General and then to the Master Console section. Once enabled, a new Portal tab will appear to the right of the Groups tab. The URL of the public portal will be <https://your.AMP.name/public>. When you upgrade to the latest version of AWMS, the public portal is disabled by default, regardless of the type of license.

Much like the normal Home > Overview page, the Master Console Home > Overview page provides summary statistics for the entire network at a glance.

Adding a Managed AMP with the Master Console

Perform the following steps to add a managed AWMS console.

1. Navigate to the Home > Managed AMP page.
2. Click the pencil Icon to edit or reconfigure an existing AWMS console.
3. Click the Add New Managed AMP button to create a new AWMS console. The Managed AWMS page appears. Complete the settings on this page as described in [Table 124](#).

Table 124 *IP/Hostname Fields and Default Values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the AWMS server that will be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed AWMS server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed AWMS server.

Table 124 IP/Hostname Fields and Default Values (Continued)

Field	Default	Description
Username	N/A	The username used by the Master Console to login to the managed AWMS server. The user needs to be an AP/Device Manager or AWMS Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console AWMS to login to the managed AWMS.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed AWMS server.
Manage Group Configuration	No	Defines whether the Master Console can manage device groups on the managed AWMS server.

- To push configurations to managed groups using AWMS' global groups feature, first navigate to the Master Console's Groups > List page.
- Click the Add button to add a new group, or click the name of the group to edit settings for an existing group.
- Click 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).
- Clicking the name of an existing group on the Master Console loads the subtabs for Basic, Security, SSIDs, AAA Servers, Radio, WLC Radio, LWAPP APs, PTMP/WiMAX, 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 AWMS, 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. In the case of the Groups > SSIDs page, override options are available only on the Add page (navigate to the Groups > SSIDs page and click the Add button).

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. 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 AWMS.

To configure subscriber groups, navigate to the Group > Basic page of a group on a managed AWMS 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 click Save and Apply for the configuration from the global group to be pushed to the subscriber group on the managed AWMS.

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.

In the example below, the field Name was overridden with the checkbox in the global group on the Master Console, so it can be configured for each subscriber group on the managed AWMS. The other four fields in the

Basic section were not overridden, so they are static fields that will be the same for each subscriber group. These fields can only be altered on the global group on the Master Console.

The global groups feature can also be used without the Master Console. For more information about how this feature works, refer to the chapter [“Configuring and Using Device Groups in AWMS” on page 79](#).

Monitoring and Supporting AWMS with the Home Pages

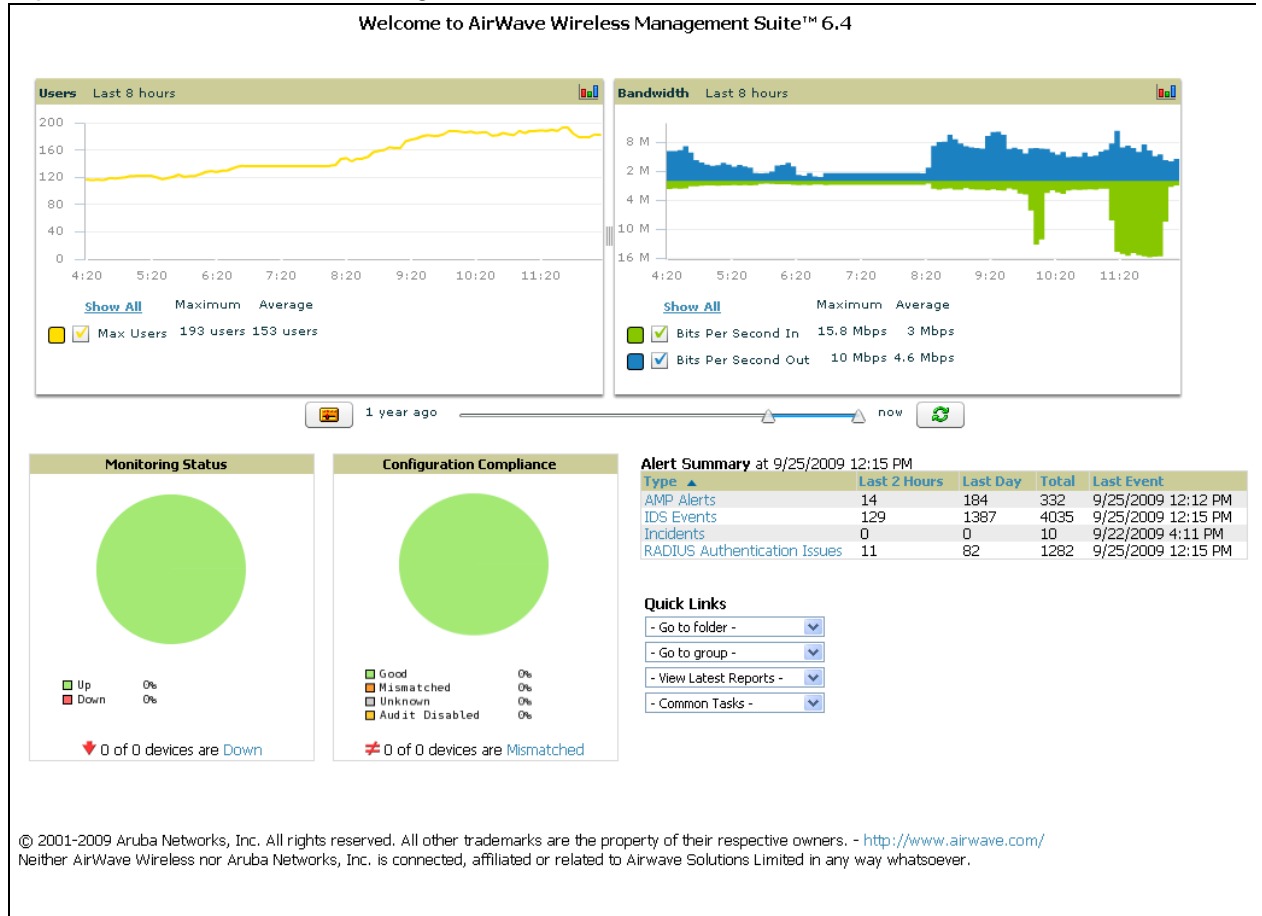
The Home section of AWMS provides the most frequent starting point for monitoring network status and establishing primary AWMS functions, once AWMS configuration is complete. Access the following pages in the Home section of the AWMS graphical user interface (GUI):








- The Home > Overview and the Home > License pages condense a large amount of information about your AWMS. From these two pages you can view the health and usage of your network as well as click common links and shortcuts to view system information. Refer to [“Monitoring AWMS with the Home > Overview Page” on page 241](#).
- The Home > Search page provides a simple way to find users and managed devices. AWMS enhances searching by adding an ability to search for rogue devices by multiple criteria. Refer to [“Searching AWMS with the Home > Search Page” on page 246](#).
- The Home > Documentation page provides easy access to all relevant AWMS documentation. See [“Accessing AWMS Documentation with the Home > Documentation Page” on page 247](#).
- The Home > License page provides product licensing information. See [“Viewing and Updating License Information with the Home > License Page” on page 245](#).
- The Home > User Info page displays information about the users logged in to AWMS, including the role, authentication type (local user or TACACS+) and access level. See [“Configuring Your Own User Information with the Home > User Info Page” on page 248](#).
- The Home > Customize Dashboard allows you to customize the Home > Overview page. See [“Customizing the Overview Subtab Display” on page 36](#).

Monitoring AWMS with the Home > Overview Page

Navigate to Home > Overview page with the standard AWMS menus. [Figure 170](#) illustrates this page, and [Table 125](#) describes the contents. For information on customizing the dashboard display on the Home > Overview tab, see [“Customizing the Overview Subtab Display” on page 36](#).

Figure 170 Home > Overview Page Illustration




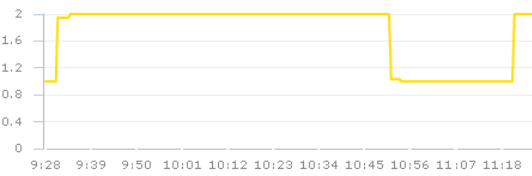
Alcatel-Lucent  New Devices: 32  Up: 32  Down: 6  Mismatched: 31  Rogue: 127  Users: 2  Alerts: 0

Home | [Helpdesk](#) | [Groups](#) | [APs/Devices](#) | [Users](#) | [Reports](#) | [System](#) | [Device Setup](#) | [OV3600 Setup](#) | [RAPIDS](#) | [VisualRF](#)

Overview | [Search](#) | [Documentation](#) | [License](#) | [User Info](#)


Welcome to OmniVista 3600 Air Manager™ 6.4.0
AirWave Management Platform - AirWave - k o k u - INTERNAL USE ONLY Days Rema

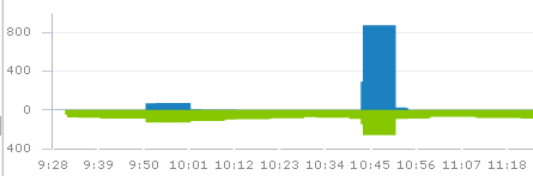
Users Last 2 hours 



[Show All](#) Maximum Average

Max Users 2 users 1.7 users




Bandwidth Last 2 hours 




[Show All](#) Maximum Average

Bits Per Second In 261.6 bps 102 bps

Bits Per Second Out 873.9 bps 67.7 bps


 1 year ago  now 

Monitoring Status




Up 84.2%

Down 15.8%

 6 of 38 devices are Down

Configuration Compliance




Good 48.6%

Mismatched 44.3%

Unknown 7.1%

Audit Disabled 0.0%

 31 of 38 devices are Mismatched

Alert Summary at 10/30/2009 11:28 AM

Type	Last 2 Hours	Last Day	Total	Last Event
IDS Events	0	0	0	-
Incidents	0	0	0	-
OV3600 Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Quick Links

- Go to folder -

- Go to group -

- View Latest Reports -

- Common Tasks -

© 2009 Alcatel-Lucent. All rights reserved. - <http://www.alcatel-lucent.com/enterprise>

Table 125 *Home > Overview Sections and Descriptions*

Section	Description
Users	The Users section displays a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Click Show All to display a complete list of users. Remove the check in the Max Users option to change the display of the graph. The graph displays the maximum number of users by default.
Bandwidth	The Bandwidth section displays bandwidth data, and this display can be adjusted. To remove bandwidth in or out from the graphical display, clear the check box for In or Out. To display details for specific devices, click Show All and select the devices to be included in the graphical bandwidth summary chart.
Monitoring Status	This Monitoring Status chart displays the percentage of devices that are up and down on the network. This chart covers 100% of the known devices on the network. To review devices that are down, click Down, and the APs/Devices > Down page displays.
Configuration Compliance	The Configuration Compliance chart displays all known device configuration status on the network. Devices are classified as Good, Unknown, or Mismatched. Click the Mismatched link to obtain additional information, and the APs/Devices > Mismatched page displays.

Table 125 Home > Overview Sections and Descriptions

Section	Description
Alert Summary	<p>The Alert Summary section displays all known and current alerts, as previously configured and enabled in the System > Alerts page. Alerts can be sorted using the column headers (Type, Last 2 Hours, Last Day, Total, or Last Event). The Alert Summary field displays four types of alerts, as follows:</p> <ul style="list-style-type: none"> ● AWMS Alerts ● IDS Events ● Incidents ● RADIUS Authentication Issues <p>Click any alert type, and the Alert Summary page appears for that alert type, enabling further analysis and investigation.</p> <p>NOTE: The Incidents portion of this summary table only increments the counter for incidents that are open and associated to an AP. This is also the case if you click Incidents and view incident details. To view all incidents, including those not associated to an AP, navigate to the Helpdesk > Incidents page.</p>
Quick Links	<p>The Quick Links section of the Home > Overview page provides drop-down menus that enable you to move to the most common and frequently used pages in AWMS, as follows:</p> <ul style="list-style-type: none"> ● Go to folder—This menu lists all folders defined in AWMS from the APs/Devices List page, and enables you to display information for any or all of them. See “Using Device Folders (Optional)” on page 157. ● Go to group—This menu lists all groups defined in AWMS, and enables you to display information for any or all of them. Use the Groups pages to edit, add, or delete groups that appear in this section. See “Configuring and Using Device Groups in AWMS” on page 79. ● View latest reports—AWMS supports 13 reports, enabling you to generate custom reports, or to display the latest daily version of any report. Click any report type to display the daily version. See “Creating, Running, and Emailing Reports” on page 261. ● Common tasks—This menu provides an inventory of and quick links to the most heavily used task-oriented pages in AWMS, to include the following: <ul style="list-style-type: none"> ■ Configure Alert Thresholds—This link takes you to the System > Triggers page. See “Monitoring and Supporting AWMS with the System Pages” on page 249 on page 213. ■ Configure Default Credentials—This link takes you to the Device Setup > Communication page. See “Configuring Communication Settings for Discovered Devices” on page 53. ■ Discover New Devices on Your Network—This link takes you to the Device Setup > Discover page. See “Discovering, Adding, and Managing Devices” on page 127. ■ Supported Devices and Features—This link launches and displays a PDF file that summarizes all supported devices and features in chart format for AWMS. Adobe Reader is required. ■ Upload Device Firmware—This link launches and displays the Device Setup > Upload Files page. See “Overview of the Device Setup > Upload Files Page” on page 58. ■ View Event Log—This link launches and displays the System > Event Log page. See “Using the System > Event Logs Page” on page 252.

Viewing and Updating License Information with the Home > License Page

Navigate to the Home > License page using the standard AWMS menu. [Figure 171](#) illustrates this page, and [Table 126](#) describes the contents.

Please be aware that you cannot enter multiple licenses. To combine multiple license entitlements into one new license, contact Dell support.

Figure 171 Home > License Page Illustration

System Overview			
System Name:	aire.com	Time:	9/23/2009 7:25 PM
Organization:	Aire Networks	Uptime:	1 day 12 hrs 50 mins
Hostname:	aire.com	Version:	6.4
IP Address:	10.19.19.19	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 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+lw
--- Signature ---
iD8DBQFJrwUzvN8PdJTKS2ERAUzmAJ9EwAYfhciAI7C3oPCOYjoAipUZxgCfaw9q
UmDiGqRmGOH7s3S2F37H2d0=
=6V+1
--- End AMP License Key ---

```

Table 126 Home > License Fields

Field	Description
System Name	Displays a user-definable name for AWMS (maximum 20 characters). The System Name can be configured from the AMP Setup > General page.
Organization	Displays the organization listed on your license key.
Hostname	Displays the DNS name assigned to AWMS.
IP Address	Displays the static IP address assigned to AWMS. The IP Address can be configured from the AMP Setup > Networking page.
Current Time	Displays the current date and time set on AWMS.
Uptime	Displays the amount of time since the operating system was last booted. AWMS processes get restarted daily as part of the nightly maintenance.
Software Version	Displays the version number of AWMS code currently running.
Operating system	Displays the version of Linux installed on the server.

Searching AWMS with the Home > Search Page

The Home > Search page provides a simple way to find users, managed devices, rogue devices, groups, folders, and more. 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, User, LAN IP and VPN IP fields.

Figure 172 illustrates this page.

Figure 172 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. 00:42:96).

00:

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
00:0b:86:66:03:4e	Down	0	0	-	Unknown	Access Points	.airespace	-	-
00:0b:86:c1:a0:52	Up	0	0	16 hrs 59 mins	Mismatched	Access Points	.airespace	-	-
1250-91:14:42	Up	0	0	8 days 19 hrs 3 mins	Mismatched	iwlc thin aps	.airespace	airespace-4400-1	-
1250-91:14:42	Up	0	0	12 days 20 hrs 18 mins	Mismatched	iwlc thin aps	.airespace	airespace-4400-1	-
Airespace-4012-2	Up	0	0	54 days 22 hrs 46 mins	Mismatched	Access Points	.airespace	-	-
airespace-4400-1	Up	0	0	12 days 21 hrs 28 mins	Mismatched	4400	.airespace	-	-

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
logon	-	00:00:48:39:96:08	00:0b:86:c1:a0:52	alpaca-alpaca	51	802.11bg	802.11g	0	2/13/2009 12:50 PM	-
-	-	00:04:23:4C:C1:33	AP2	ws5100_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:B1	-	-	-	-	-	-	-	-
GuestLogon	-	00:06:25:2C:A5:AD	00:0b:86:c1:a0:52	guest	51	802.11bg	802.11b	0	1/23/2009 9:07 AM	-
-	-	00:09:EF:05:1E:B2	-	-	-	-	-	-	-	-
-	-	00:09:EF:05:20:CF	-	-	-	-	-	-	-	-
logon	-	00:0A:88:7F:0B:01	00:0b:86:c1:a0:52	-	51	802.11bg	802.11b	0	1/29/2009 2:25 PM	-
GuestLogon	-	00:0A:88:7F:0B:11	ap-Not set	dpb_test_guest	51	802.11bg	802.11b	0	1/29/2009 2:19 PM	-
-	-	00:0A:88:7F:0B:1E	-	-	-	-	-	-	-	-
-	-	00:0C:F1:3B: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:CC:CE:F3	-	-	-	-	-	-	-	-
-	-	00:0E:98:D7:35:8A	ap	open-ops	0	802.11a	802.11a	-	1/29/2009 8:59 AM	-
-	-	00:0F:86:B1:D5:3F	-	-	-	-	-	-	-	-
-	-	00:0F:CB:82:33:A4	-	-	-	-	-	-	-	-
-	-	00:11:24:C6:2B:52	-	-	-	-	-	-	-	-
-	-	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:7C:3E	-	-	-	-	-	-	-	-
-	-	00:13:02:C2:39:28	-	-	-	-	-	-	-	-
-	-	00:13:02:CD:F3:D5	00:0b: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	-	Enterasys-68:FA:C3	<user set>	Unclassified	-	6	test012
No	Suspected Neighbor	5	Tropos Net-04:0F:8B	Suspected Neighbor - detected wirelessly	Unclassified	-	5	TroposNetworks
No	Suspected Neighbor	5	Cisco Syst-A7:89:ED	Suspected Neighbor - detected wirelessly	Valid	-	3	dbshop-airespace-open
No	Valid	-	Aruba Netw-88:98:32	<user set>	Unclassified	-	5	ethersphere-voip
No	Valid	-	Enterasys-27:F6:48	<user set>	Unclassified	-	6	RoamAbout Default Network Name
No	Suspected Neighbor	5	SYMBOL TEC-D7:64:A6	Suspected Neighbor - detected wirelessly	Valid	-	6	ws5100_102
No	Valid	-	NOMADIX IN-05:02:D0	<user set>	Unclassified	-	6	Nomadix
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	Chirp Interval	Last Seen	Closest AP
-	00:0C:CC:5E:7F:9E	Aeroscout Ltd.	-	45 secs	3/12/2009 10:25 AM	1250-91:14:42
-	00:14:7E:00:4C:DC	InnerWireless	Normal	1 min	3/12/2009 10:24 AM	1250-91:14:42
-	00:0C:CC:7A:3B:8A	Aeroscout 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.

Note: The AWMS Search utility is case-insensitive.

2. Click Search, and the results display after a short moment. Results support several hypertext links to additional pages, and drop-down menus 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:

- APs/Devices
- Users
- Rogues
- Tags
- Folder
- Group

Accessing AWMS Documentation with the Home > Documentation Page

The Home > Documentation page provides easy access to all relevant AWMS documentation. All of the documents on the Home > Documentation page are hosted locally by AWMS and can be viewed by any PDF viewer. [Figure 173](#) illustrates this page.

Figure 173 *Home > Documentation Page Illustration*



If you have any questions that are not answered by the documentation please contact Dell 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 AWMS. This page includes the authentication type (local user or TACACS+) and access level. This page also provides the user with the ability to customize some of the information displayed in AWMS and change their password.

To create new users, navigate to the AMP Setup > Users page, and refer to “Creating AWMS Users” on page 48. Users can customize the information displayed in the AWMS header.

Figure 174 Home > User Info Page Illustration

admin is logged in as a local user with role AMP Administration and Read/Write access to RAPIDS.

User Information

Name:

New Password:

Confirm New Password:

Email Address:

Phone:

Notes:

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:

- Fat APs
- Thin APs
- Controllers
- Switches
- Others

Select All - Unselect All

Search Preferences

Customize Search: Yes No

Search Preferences:

- APs/Devices
- Users (Connected)
- Users (Historical)
- Folders
- Groups
- Tags
- Rogues

Select All - Unselect All

Display Preferences

Default Number of Records per List:

Reset List Preferences:

Customize Columns for Other Roles: Yes No

Console Refresh Rate:

Table 127 Home > User Info Fields

Field	Description
Customize Header columns	Enables/disables the ability to control which statistics hyperlinks are displayed at the top of every AWMS screen.
Stats	Select the specific data you would like to see in the header.
Severe Alert Threshold	Configures the minimum severity of an alert to be included in the Severe Alerts count. Note: The severe alerts count header info will only be displayed if 'Severe Alerts' is selected in the Stats section above.
Include Device Types	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.
Customize Search/Search Preferences	Set to no by default; when set to yes, user can select which search categories to display when search results are returned.
Default Number of Records per list	Defines the number of rows to appear in any list that has not had a row count manually set. If a row count is manually set it will override the default setting.
Reset List PReferences	Reset all list preferences including number of records per list, column order and hidden column information.
Customize Columns for Other Roles	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 click the Choose Columns for roles link above the list. Make the desired column changes; select the roles to update and click save.
Filter Level For Rouge Count	Specifies the minimum classification that will cause a device to be included in the Rogue count header information.

Perform the following steps to configure your own user account with the Home > User Info page:

1. In the User Information section, enter the following information:

- Name—Enter the ID by which a you logs into and operate in AWMS.
- Email Address—Enter the email address to be used for alerts, triggers, and additional AWMS 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 AWMS users or administrators to understand the functions, roles, or other rights of the user being created.

Monitoring and Supporting AWMS with the System Pages

The System pages provide a centralized location for system-wide AWMS 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 AWMS services. Refer to [“Using the System > Status Page” on page 251](#).
- System > Event Log—This useful debugging tool keeps a list of recent AWMS events, including APs coming up and down, services restarting, and most AWMS-related errors as well as the user that initiated the action. Refer to [“Using the System > Event Logs Page” on page 252](#).
- System > Configuration Change Jobs—Manages configuration changes in AWMS. Refer to [“Using the System > Configuration Change Jobs Page” on page 253](#).

- System > Performance—Displays basic AWMS hardware information as well as resource usage over time. Refer to [“Using the System > Performance Page”](#) on page 254.
- System > Firmware Upgrade Jobs—Displays information about current and scheduled firmware upgrades.

Using the System > Status Page

The System > Status page displays the status of all of AWMS services. Services will either be OK, Disabled, or Down. OK and Disabled, displayed in green, are the expected states of the services. If any service is Down, displayed in red, please contact Dell support. The Reboot button provides a graceful way to power cycle your AWMS remotely when it is needed. The Restart AWMS button will restart the AWMS services without power cycling the server or reloading the OS. Figure 175 illustrates this page.

Figure 175 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](#) downloads a tar file that contains reports and logs that are helpful to AirWave support in troubleshooting and solving problems. AirWave support may request that you submit this file along with other logs that are linked on this page. Logs that are contained in [diagnostics.tar.gz](#) include `cron_stopped_maintenance`, `AWMS_events`, `AWMS_watcher`, `async_logger`, `ssl_error` and `pgsql`.
- Similarly, the [VisualRFdiag.tar.gz](#) link downloads a diagnostic file containing VisualRF information that might be requested by AirWave support.

- A summary table lists logs that appear on the System > Status page. These are used to diagnose AWMS problems. Additional logs are available via SSH access in the /var/log and /tmp directories; AirWave support engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. [Table 128](#) describes the log information.

Table 128 Status Log

Log	Description
pgsql	Logs database activity.
ssl_error_log	Reports problems with the web server. This report is also linked from the internal server error page that displays on the web page; please send this log to AirWave support whenever reporting an internal server error.
maillog	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
radius	Displays error messages associated with RADIUS accounting.
async_logger	Tracks many device processes, including user-AP association.
config_verifier	Logs device configuration checks.
config_pusher	Logs errors in pushing configuration to devices.
visualrf.log	Details errors and messages associated with the VisualRF application.

Using the System > Event Logs Page

The System > Event Logs page is a very useful debugging tool. The event log keeps a list of recent AWMS events, including APs coming up and down, services restarting, and most AWMS related errors as well as the user that initiated the action. [Figure 176](#) illustrates this page, and [Table 129](#) describes the page components.

Figure 176 System > Event Logs Page Illustration

Time	User	Type	Event
Mon Feb 12 15:31:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:31:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:29:38 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:29:38 2007	System	System	Wireless station 00:13:CE:14:5E:9B deauthenticated via EAP
Mon Feb 12 15:21:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:21:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:19:38 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:19:37 2007	System	System	Wireless station 00:90:96:F0:A9:EC deauthenticated via EAP
Mon Feb 12 15:09:37 2007	System	System	Wireless station 00:11:24:2D:78:12 deauthenticated via EAP
Mon Feb 12 15:09:01 2007	System	Router/Switch	corp1 (switch1.corp.airwave.com): can't reach device for CDP data collection
Mon Feb 12 15:08:32 2007	System	Router/Switch	corp2 (switch2.corp.airwave.com): can't reach device for CDP data collection
Mon Feb 12 15:08:03 2007	System	Router/Switch	Corporate Gateway (10.200.0.1): can't reach device for CDP data collection
Mon Feb 12 15:06:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down
Mon Feb 12 15:06:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Device uptime indicates that device has rebooted
Mon Feb 12 15:04:37 2007	System	System	Wireless station 00:13:02:9D:04:C2 deauthenticated via EAP
Mon Feb 12 15:01:33 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Configuration verification succeeded; configuration is good
Mon Feb 12 15:01:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Up
Mon Feb 12 15:01:32 2007	System	Device	Aruba AP 65 Aruba-AP65-ap.2.2.3 Down

Table 129 Event Logs Fields

Field	Description
Time	Date and time of the event.
User	The AWMS user that triggered the event. When AWMS itself is responsible for the event, System is displayed as the user.

Table 129 Event Logs Fields

Field	Description
Type	Displays the Type of event recorded, which is one of four types, as follows: <ul style="list-style-type: none"> AP—An event localized to one specific AP. Group—A group wide event. System—A system wide event. Alert—If a trigger is configured to report to the log an alert type event will be logged here.
Event	The event AWMS observed useful for debugging, user tracking, and change tracking.

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 177](#).

Figure 177 System > Configuration Change Jobs Page Illustration



1. To edit an existing configuration change job click on the linked description name. On the subsequent edit page you can choose to run the job immediately by clicking the Apply Changes Now button, reschedule the job using the Schedule box, delete the job using the Delete button, or cancel the job edit by clicking the Cancel button.
2. Click the linked AP or group name under the Subject column to go to the monitoring page of the AP or group.
3. Click 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 > Performance Page

The System > Performance page displays basic AWMS hardware information as well as resource usage over time. AWMS logs performance statistics such as load average, memory and swap data every minute. The historical logging can be used to help determine the best usable polling period and track the health of AWMS over time. [Figure 178](#) illustrates this page and [Table 130](#) describes fields and information displayed.

Figure 178 System > Performance Page Illustration (Partial Screen Shown)

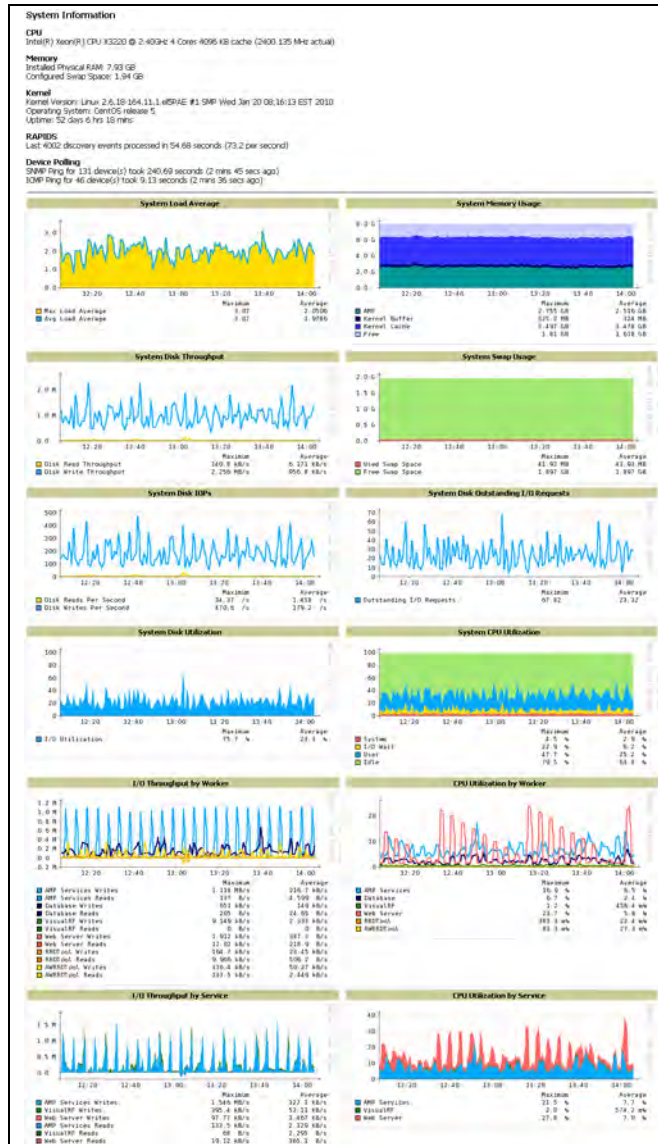


Table 130 System > Performance Page Fields

Field	Description
CPU(s)	Basic CPU information as reported by Linux.
Memory	The amount of physical RAM and Swap space seen by the operating system. AWMS requires a minimum of 1 gigabyte of physical RAM
Kernel	The version of Linux kernel running on the box.
RAPIDS	Displays how long it took to process the last payload of MAC address.
Device Polling	Displays some AP/Device polling statistics.

Table 130 System > Performance Page Fields (Continued)

Field	Description
System Load Average	The System Load average is 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 AWMS load is around 3. A constant load of 5 to 7 is cause for concern. A load above 10 is a serious issue and will probably result in AWMS becoming unusable. To lower the load average try increasing a few polling periods. Increasing the polling period for APs, routers/switches, WLSE, ACS, and so on, will decrease the amount of work AWMS needs to perform and lower the load average. If you have a load that is consistently below 3 you might consider shortening your polling period and observing. NOTE: If the load is less than one the y scale will be 1 to 1000 m standing for milliseconds or 1/1000ths of 1.
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for AWMS 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.
System Disk Utilization	The amount of data read from the disk and written to the disk.
Swap Usage	The amount of Swap memory used by AWMS. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If an AWMS consistently uses swap you should consider installing additional RAM for the box.
System CPU Usage	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
Application CPU Usage	CPU usage broken down by application. AWMS services includes all AWMS processes except the database and the webserver.
I/O Throughput	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).
CPU Utilization	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).
System Network Bandwidth (Eth0)	All traffic in and out of Eth0 measured in bits per second.
Bandwidth by Protocol (Eth0)	Displays the amount of traffic used by Telnet, HTTPS and SNMP on Eth0.
Legacy SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher (SNMP Get/walk Requests)	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher (SNMP OIDs Received)	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.
Top 5 Tables (by row count)	The five largest tables in AWMS. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Aruba recommends decreasing the length of time client data is stored on the AWMS page if a user/client table exceeds 250,000 rows.
Database Table Scans	The number of Database table scans performed by the database.
Database Row Activity	The number of insertions, deletions and updates performed to the database.

Table 130 System > Performance Page Fields (Continued)

Field	Description
Database Transaction Activity	The number of commits and rollbacks performed by the database.
Disk Usage	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 Historical Data Retention settings on the AWMS page or consider installing additional hard drive space.

There are several initial steps that you can take to troubleshoot AWMS 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 *AWMS Sizing Guide* or contact Dell support for the latest recommendations

Upgrading AWMS

The AWMS upgrade process may change. Please consult support of the latest AWMS release announcement for detailed instructions. The following is sample instructions from the 6.4 announcement email:

Upgrade Instructions

To upgrade your AWMS:

1. Login to the AWMS server as the root user.
2. Run the following command (where x.x.x is equal to the latest AWMS version)

```
# start_amp_upgrade -v x.x.x
```

Upgrading Without Internet Access

If your AWMS cannot get to the Internet:

1. Download the latest AWMS version from our download page: www.airwave.com/support/download
2. Copy the file to AWMS /root directory using WinSCP.
3. On the AWMS, 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 AWMS services.

Backing Up AWMS

Overview of Backups

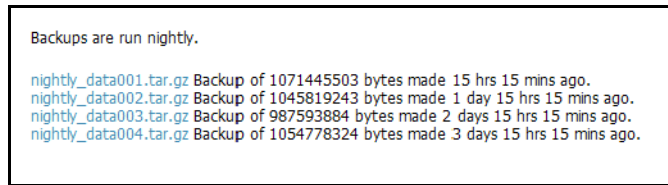
AWMS creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the AMP Setup > General page under the Nightly Maintenance Time setting.

Although AWMS only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. AWMS 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 AWMS settings.

Viewing and Downloading Backups

To view current AWMS backup files, go to the System > Backups page. [Figure 179](#) illustrates this page.

Figure 179 System > Backups Page Illustration



To download a backup file, click the filename URL and the File Download popup page appears. Proceed as prompted.

AirWave recommends regularly saving the data backup file to another machine or media. This process can be automated easily with a nightly script.



Note: Nightly maintenance and amp_backup scripts back up the full AMPdata and save the file as nightly_data001.tar.gz. In previous AWMS versions, the scripts created both config backup and data backup files. In order to restore the AMPdata, it is only necessary to have most recent data backup file, and AWMS no longer uses or supports the config backup file, effective with AWMS 6.3.2 and later AWMS versions.

Running Backup on Demand

To create an immediate backup, use the following procedure:

1. Log into the AWMS system as root.
2. Change to the scripts directory by typing 'scripts'.
3. Run the backup script by typing /bin/sh 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 use the following procedure:

1. Use your AWMS Installation CD to build a new machine. The new machine must be running the same version as the AWMS that created the backup file.
2. Copy the nightly_data00[1-4].tar.gz file to the new AWMS. The /tmp directory is an appropriate destination.

A good open source Windows file transfer client that supports SFTP and SCP for is WinSCP which is available from <http://winscp.sourceforge.net/eng/>.

WINSCP allows you to transfer the nightly00[1-4].tar.gz file from your local PC to the new AWMS 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.
- 6.

AWMS Failover

The failover version of AWMS provides a “many to one” hot backup server. The Failover AWMS polls the watched AMPs to verify that each is up and running. If the watched AWMS is unreachable for the specified number of polls, the Failover AWMS will enter failover mode. When AWMS enters failover mode it automatically restores the most recent saved backup from the watched AWMS and begins polling its APs.

Navigation Section of AWMS Failover

The Navigation section displays tabs to all main GUI pages within AWMS Failover. The top bar is a static navigation bar containing tabs for the main components of AWMS, while the lower bar is context-sensitive and displays the sub-menus for the highlighted tab. [Table 131](#) describes the contents of this page.

Table 131 Contents of the Navigation Section of Failover

Main Tab	Description	Sub-Menus
Home	The Home page provides basic AWMS Failover information, including system name, hostname, IP address, current time, running time, software version, and watched AWMS information.	<ul style="list-style-type: none">● Overview● Watched● AWMS● License (viewable only by demo versions)
System	The System page provides information related to AWMS operation and administration (including overall system status, performance monitoring and backups).	<ul style="list-style-type: none">● Status● Event● Log● Backups● Performance
AMP Setup	The Setup page provides all information relating to the configuration of AWMS itself and its connection to your network.	<ul style="list-style-type: none">● General● Network● Users● TACACS+

Adding Watched AWMS Stations

Navigate to the Home > Watched AWMS page to begin backing up and monitoring AWMS stations. Once an AWMS installation has been added to the Watched AWMS list, the Failover AWMS will download the most recent backup and begin polling. The Failover AWMS and the Watched AWMS must be on the same version or else the watched AWMS will be unable to restore properly. If any of the watched AWMS are not on the same version of AWMS you will need to upgrade. The Failover AWMS will need HTTPS access (port 443) to the watched AWMS to verify that the web page is active and to fetch downloads.

Once the Failover AWMS determines that the Watched AWMS is not up (based on the user-defined missed poll threshold) it will restore the data backup of the Watched AWMS and begin monitoring the watched AMP APs/Devices. There are many variables that affect how long this will take, including how long client historical data is being retained, but for an AWMS with 1000 APs it might take up to 10 minutes. For an AMP with 2500 APs it might take as long as 20 minutes. The Failover AWMS will retain its original IP address.

In summary, the Failover AWMS could take over for the Watched AWMS in as little as five minutes; it might take up to an additional 10-20 minutes to unpack the watched AWMS' 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 AWMS run the backup script from the command line and copy the current data file and the old Watched AWMS configuration file to the Watched AWMS. Then run the restore script. More information about backups and restores can be found in [“Backing Up AWMS” on page 256](#).

Table 132 *Home > Watched Page Fields and Default Values*

Setting	Default	Description
IP/Hostname	None	The IP address or Hostname of the watched AWMS. The Failover AWMS needs HTTPS access to the watched AMPs.
Username	None	A username with management rights on the watched AWMS.
Password	None	The password for the username with management rights specified above.
HTTP Timeout (5-1000 Sec)	60	The amount of time before AWMS considers a polling attempt failed.
Polling Enabled	Yes	Enables or disables polling of the Watched AWMS. NOTE: You do not need to disable polling of the watched AWMS system if it is set to be down during nightly maintenance or is being upgraded.
Polling Period	5 minutes	The amount of time between polls of the Watched AWMS.
Missed Poll Threshold	None	The number of polls that can be missed before the failover AWMS will begin actively monitoring the Watched AWMS APs.

This chapter describes AWMS reports, including report access, creation, scheduling, and distribution via email and XML processing.

This chapter includes the following sections:

- “Overview of AWMS Reports” on page 261
- “Using Daily Reports” on page 264
- “Defining Reports” on page 289
- “Emailing and Exporting Reports” on page 292

AWMS ships with several reports as enabled by default. Default reports may run each night or weekly, depending on the AWMS release. Aruba recommends that you 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 report.

AWMS supports additional and more 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 the *VisualRF User Guide*.

Overview of AWMS 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, allowing you to act upon information in the reports. You can generate an export a wide variety of reports in AMP.

AWMS reports have the following general parameters:

- AWMS runs daily versions of all reports during predefined windows of time. All reports can be scheduled so that they run in the background.
- The daily version of any report is available instantly using the **Reports > Generated** page and scrolling to the report links at the bottom of the page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that do not span a period of time. Instead, these two reports provide a detailed 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 to take inventory of reports already defined.

The **Definitions** page includes these sections:

- **Report definitions pane**—The **Add** button allows you to define a custom report using the **Custom Options** drag and drop UI or any of the report types from a 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 right then.
- **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** pane—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 Reports** table 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 custom report from the **Definition** page, it appears on the **Generated** page. The **Report > Definition** page is shown in [Figure 180](#), and [Table 133](#) describes the fields available when you select a specific report definition.

Figure 180 Report > 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 > >|

<input type="checkbox"/>		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-upptime	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-upptime	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

<input type="checkbox"/>	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 Research Lab and Folder Top > Sunnyvale HQ > HQ Cisco LWAPP and SSID wpa2
<input type="checkbox"/>	Partner	PCICompliance-Detailed-3wks-Acme	PCI Compliance	Group HQ

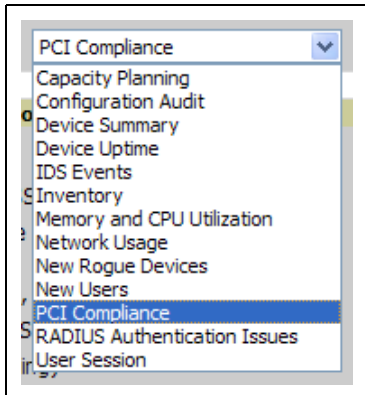
Latest Report	Report Start	Report End	Last Run Time	Scheduled
-	yesterday	now	4/27/2009 2:21 PM	-
Device Summary Report	5/5/2009	5/8/2009	5/8/2009 10:58 AM	-
-	1/1/2009	3/31/2009	3/31/2009 6:08 AM	-
PCICompliance-Detailed-3wks-Acme	3 weeks ago	now	4/28/2009 7:12 AM	-

Select All - Unselect All

Table 133 Report > Definition Page Fields and Descriptions

Field	Description
Report Definition	Displays a field for entering report title and dropdown menu, shown in Figure 181 , displaying all possible report types.
Report Restrictions	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.
Scheduling Options	Reveals options for one time or regularly scheduled reporting by selecting the Yes radio button. Options include report frequency, start time, and current system time.
Report Visibility	Allows you to determine a report's visibility according to user role.
Email Options	Reveals email address preferences for sending reports by selecting the Yes radio button.
Add and Run	Allows you to create a report definition and run that report right then.
Run Now	Allows you to run any report that has been defined on the spot without saving settings or creating a new report definition.
Add	Saves report definition you just created.
Cancel	Returns you to Reports > Definitions page.

Figure 181 Report Type Drop-down Menu in Reports > Definitions > Add Illustration



Note: Only **admin** users have complete access to complete report information. The AWMS 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 defined in the Reports > Definitions page. This page also enables you to display the most recent daily version of any report. Reports comply with the access permissions defined for AWMS users. An **Admin** user can see and edit all report definitions in AWMS. 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 four primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The option to view the latest daily reports with a single click for immediate online viewing

Figure 182 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

Latest Capacity Planning Report
 Latest Configuration Audit 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 RADIUS Authentication Issues Report
 Latest User Session Report

Figure 183 Reports > Generated Page with Single-click Report Viewing Options

Latest Capacity Planning Report
 Latest Configuration Audit 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 RADIUS Authentication Issues Report
 Latest User Session Report



Note: Clicking any report from the list shown in [Figure 183](#) displays the **Detail** page for the most recent version of that report.

Using Daily Reports

This section describes the reports supported in AWMS. These reports can be accessed from the bottom of the **Reports > Generated** page, and are presented in alphabetical order as follows in [Table 134](#):

Viewing Generated Reports

To display all generated reports that are currently scheduled on AWMS, navigate to the **Reports > Generated** page. [Figure 182](#) and [Figure 183](#) illustrate this page. This 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 category (column header) in sequential or reverse sequential order.
- Click a report title to view details for each scheduled report. Click **Add** to create new generated reports. Generated reports are scheduled and custom configurable.
- Scroll to the bottom of the **Reports > Generated** page, and click any of the 13 report types to view the most recent version of any report. This function is independent of scheduled reports.
- The **Reports > Detail** page launches when you click any report title from this page. The content of the **Reports > Detail** page varies significantly according to the report type.

The **Generated Reports** page contains less columns and information than the **Definitions** page. [Table 134](#) describes each column for the **Reports > Generated** page.

Table 134 Report > Definition Page Fields and Descriptions

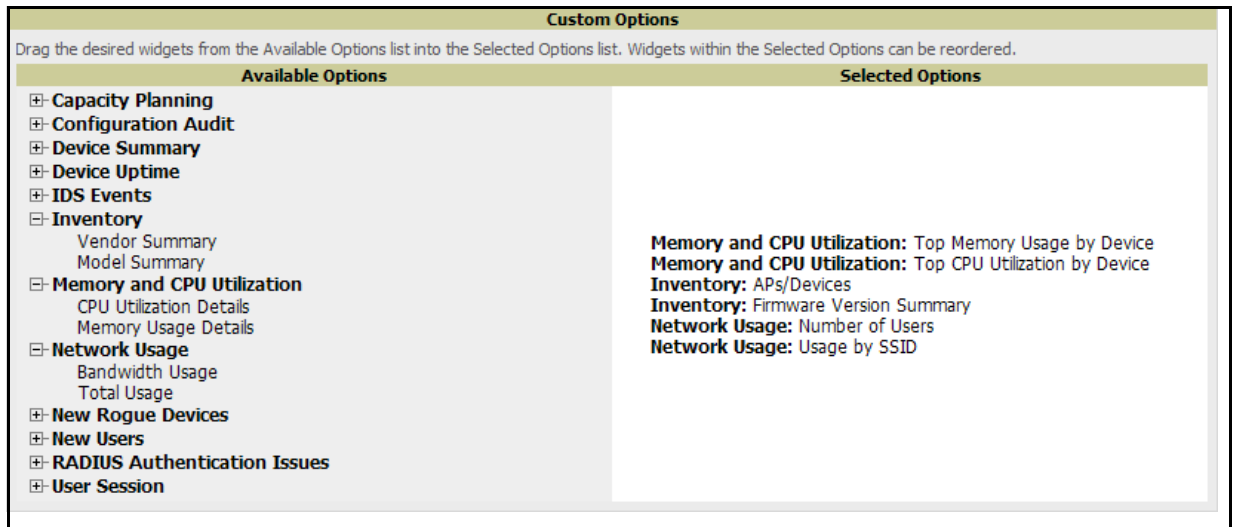
Field	Description
Generated Time	Displays the date and time of the last time the report was run, or when the latest report is available. Clicking the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and clicking Run .
Title	Displays title of the report. This is a user-configured field when creating the report.
Type	Displays the type of the report. This can be one of 13 report types in AWMS.
Subject	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
Report Start	Displays the beginning of the time period covered in the report.
Report End	Displays the end of the time period covered in the report.
Role	Added to the Reports definitions for other roles section, this column cites 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 and how it should be displayed. Perform these steps to create a **Custom Report**.

1. Navigate to the **Reports > Definitions** page.
2. Click the **Add** button.
3. Select **Custom** in the type dropdown. The **Custom Options** section will open up as shown in [Figure 184](#).

Figure 184 AWMS Custom Options Page



The left pane of the **Custom Options** window lists all available data that can be included in the report. The data is broken down by report. If for example, the data you want to include is in the **Inventory** report, click **Inventory** to view a list of all available inventory 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.

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 clicking the column heading.

Refer also to the “Using the Network Usage Report” on page 276 for additional bandwidth information.

Perform these steps to view the most recent Capacity Planning Report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Latest Capacity Planning Report** to display **Detail** device capacity information for all devices. The report provides multiple links to additional device configuration, folders, and additional AWMS pages.

The following figures and Table 135 illustrate and describe the contents of the Capacity Planning Report.

Figure 185 AWMS Capacity Planning Report Page (split view)

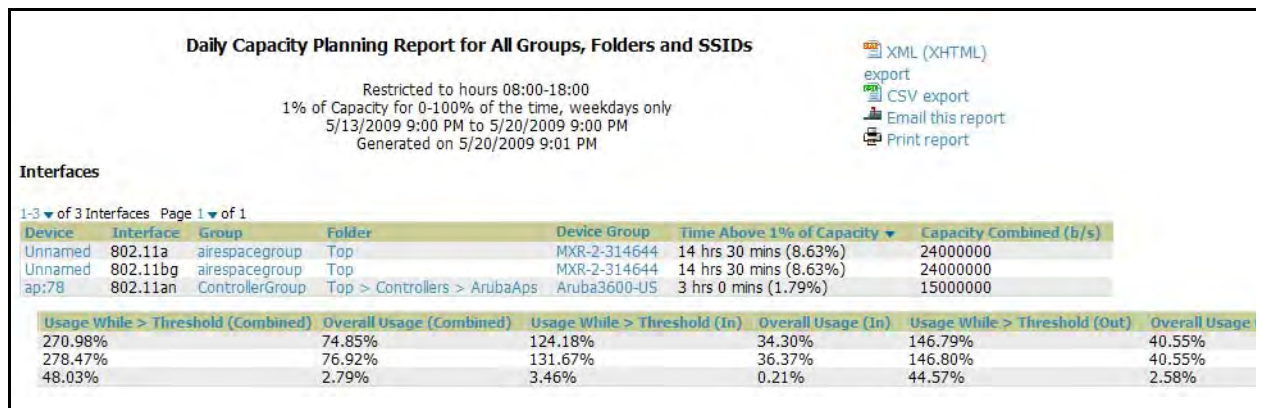


Table 135 Capacity Planning Report Fields and Contents, Top Portion

Field	Description
Device	Displays the device type or name.
Interface	Displays the type of 802.11 wireless service supported by the device.
Group	Displays the device group with which the device is associated.
Folder	Displays the folder with which the device is associated.
Controller	Displays the controller with which a device operates.
Time Above 1% of Capacity	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.
Capacity Combined (b/s)	Displays the combined capacity in and out of the device, in bits-per-second.
Usage While > Threshold (Combined)	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
Overall Usage (Combined)	Displays the overall usage of the device, both combined in and out traffic.
Usage While > Threshold (in)	Displays device usage that exceeds the defined and incoming threshold capacity.
Overall Usage (In)	Displays overall device usage for incoming data.

Table 135 Capacity Planning Report Fields and Contents, Top Portion (Continued)

Field	Description
Usage While > Threshold (Out)	Displays device usage for outgoing data that exceeds defined thresholds.
Overall Usage (Out)	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 click **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, click 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. Click **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Click **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Click **Show Archived Device Configuration**.

[Figure 186](#) and [Table 136](#) illustrate and describe the general **Configuration Audit** report and related contents.

Figure 186 Reports > Generated > Daily Configuration Audit Report Page, abbreviated example

Daily Configuration Audit Report for All Groups, Folders and SSIDs												
Generated on 5/21/2009 2:21 AM												
XML (XHTML) export CSV export Email this report Print report												
Name	Folder	Group	Mismatches									
11.1.3	Top > Sunnyvale HQ	Corp HQ	<table border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <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> </tbody> </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 border="1"> <thead> <tr> <th></th> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <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> </tbody> </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										
<pre> Template: 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 </pre>												
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 136 | Daily Configuration Audit Report

Field	Description
Name	Displays the device name for every device on the network. Clicking a given device name in this column allows you to display device-specific configuration.
Folder	Displays the folder in which the device is configured in AWMS. Clicking the folder name in this report displays the APs/Devices > List page for additional device, folder and configuration options.
Group	Displays the group with which any given device associates. Clicking the group for a given device takes you to the Groups > Monitor page for that specific group, to display graphical group information, modification options, alerts, and an audit log for the related group.
Mismatches	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 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 AWMS. By default is sorted alphabetically by device name.



Note: 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:

- Rank
- AP/Device
- Number of Users
- Max Simultaneous Users
- Total Bandwidth (MB)
- Average Bandwidth (kbps)
- Location
- Controller
- Folder
- Group

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.

Perform these steps to view the most recent version of this report, and to adjust configurations for over-used or under-used devices.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Summary Report** to display **Detail** device information. You can use this report as the central starting point to reconfigure over-used or under-used devices.
3. To generate more reports that cover a greater span of time, refer to “[Viewing Generated Reports](#)” on page 264.

Figure 187 and **Table 137** illustrate and describe the **Reports > Generated > Device Summary Detail** page.

Figure 187 Reports > Generated > Daily Device Summary Report Illustration

Daily Device Summary Report for All Groups, Folders and SSIDs									
5/20/2009 2:00 AM to 5/21/2009 2:00 AM Generated on 5/21/2009 2:22 AM									
XML (XHTML) export CSV export Email this report Print report									
Most Utilized by Maximum Number of Simultaneous Users									
Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	AL16	210	165	34028.71	3150.81	Corp Headquarters	-	Top	HQ
2	RAP-Local	210	94	24047.37	2226.61	1344 Server Room	-	Top > HQ > HQ-RAP	HQ-RemoteAP
3	Finance-AL27	42	27	3132.23	290.02	Not Available	sphere-ims3	Top > HQ	HQ
4	AL12	32	20	1262.57	116.90	Not Available	sphere-ims3	Top > HQ	HQ
5	Operations-AL25	38	19	3705.61	343.11	Not Available	sphere-ims3	Top > HQ	HQ
6	Sales-AL7	33	19	2011.28	186.23	Not Available	sphere-ims3	Top > HQ	HQ
7	AL16	25	18	1133.07	104.91	Not Available	sphere-ims3	Top > HQ	HQ
8	TrainingCenter-AL31	26	17	1946.03	180.19	Not Available	sphere-ims3	Top > HQ	HQ
9	DevPit-AL1	31	17	9556.34	884.85	Not Available	sphere-ims3	Top > HQ	HQ
10	Legal-AL21	36	15	2851.14	263.99	Not Available	sphere-ims3	Top > HQ	HQ
Most Utilized by Bandwidth									
Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	jluther-ap7	210	94	34028.71	3150.81	Aruba Networks	-	Top	HQ
2	RAP-Local	210	94	24047.37	2226.61	1344 Server Room	-	Top > HQ > HQ-RAP & HQ-RAP	HQ-RemoteAP
3	DevPit-AL1	31	17	9556.34	884.85	Not Available	sphere-ims3	Top > HQ	HQ
4	Operations-AL25	38	19	3705.61	343.11	Not Available	sphere-ims3	Top > HQ	HQ
5	Finance-AL27	42	27	3132.23	290.02	Not Available	sphere-ims3	Top > HQ	HQ
6	Legal-AL21	36	15	2851.14	263.99	Not Available	sphere-ims3	Top > HQ	HQ
7	MainLobby-AL15	13	6	2582.02	239.08	Not Available	sphere-ims3	Top > HQ	HQ
8	mnaadella-ap65	1	2	2524.86	233.78	Not Available	sphere-ims3	Top > HQ	HQ
9	jluther-ap70	1	1	2393.47	221.62	Not Available	sphere-ims3	Top > HQ	HQ-RAP
10	Sales-AL7	33	19	2011.28	186.23	Not Available	sphere-ims3	Top > HQ	HQ
Least Utilized by Maximum Number of Simultaneous Users									
Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ-Re
2	LWAPP_A082	0	0	0.00	0.00	default location	Airwave_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	HQ-R
3	mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	HQ-R
4	1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	-
5	jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
6	wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
7	jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
8	AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	-
9	hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
10	SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	-
Least Utilized by Bandwidth									
Rank	AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group
1	dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
2	LWAPP_A082	0	0	0.00	0.00	default location	Air_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	HQ-R
3	mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
4	1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	-
5	jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
6	wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
7	jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
8	AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	-
9	hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-
10	SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	-
Devices									
1-20 of 487 Devices Page 1 of 25 >> >									
AP/Device	Number of Users	Max Simultaneous Users	Total Bandwidth (MB)	Average Bandwidth (kbps)	Location	Device Group	Folder	Group	
brmoyle-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
Test Devices	0	0	0.00	0.00	-	-	Top	HQ-Re	
psanford-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
(id: 13653)	0	0	0.00	0.00	-	-	Top	-	
SV-1252-SHIP-22:60	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	-	
dmontgomery-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
jhoward-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
mkirby-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
lwapp-1250-13:21:1e	0	0	0.00	0.00	somewhere	CiscoController	Top > Sunnyvale HQ > Lab	-	
Cisco-IWL-C-1	0	0	0.00	0.00	Indoor Laborador	-	Top	-	
jtse-ap65	0	0	0.00	0.00	-	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
LWAPP_A082	0	0	0.00	0.00	default location	Airwave_Cisco_LWAPP	Top > Sunnyvale HQ > HQ Cisco LWAPP	-	
1210-5	0	0	0.00	0.00	-	-	Top > Sunnyvale HQ > Lab	-	
wding-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
dfisken-ap70	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
SW-3	0	0	0.00	0.00	Not Available	alpha-master-1	Top > Outdoor	-	
AP4	0	0	0.00	0.00	-	WS2000	Top > Pharmacy	-	
Aruba800	0	0	0.00	0.00	-	-	Top	-	
hkurmala-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	
svtamanti-ap65	0	0	0.00	0.00	Not Available	RAP-Local	Top > Sunnyvale HQ > HQ-RAP	-	

Table 137 Reports > Generated > Daily Device Summary Report Fields and Descriptions

Field	Description
Rank	The rank column for any section of this report establishes the top 10 devices for any category, and these are listed in sequential or reverse-sequential order.
AP/Device	Displays the name of the device, which can be a MAC address or other identifier.
Number of Users	Displays the number of users associated with each device.
Max Simultaneous Users	Displays the maximum number of users that were active on the associated device during the period of time that the report covers.
Total Bandwidth (MB)	Displays the bandwidth in megabytes that the device supported during the period of time covered by the report.

Table 137 *Reports > Generated > Daily Device Summary Report Fields and Descriptions*

Field	Description
Average Bandwidth (kbps)	Displays the average bandwidth throughput for the device during the period of time covered by the report.
Location	Displays the location of the device that is included in any category of the report.
Controller	Displays the controller to which any included device is associated.
Folder	Displays the folder with which a device is associated.
Group	Displays the device group with which a device is associated.

Using the Device Uptime Report

The **Device Uptime Report** monitors device performance and availability on the network, tracking uptime by multiple criteria to include the following:

- Total average uptime by SNMP and ICMP
- Average uptime by device group
- Average uptime by device folder

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. This report 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.

Perform these steps to view the most recent version of the **Device Uptime** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Device Uptime Report** to display report **Detail** information.
3. To generate more reports of this type that cover a greater span of time, refer to “[Reports > Definitions Page Overview](#)” on page 261.

[Figure 188](#) and [Table 137](#) illustrate and describe the **Reports > Generated > Device Uptime Detail** report.

Figure 188 Reports > Generated > Device Uptime Report Illustration

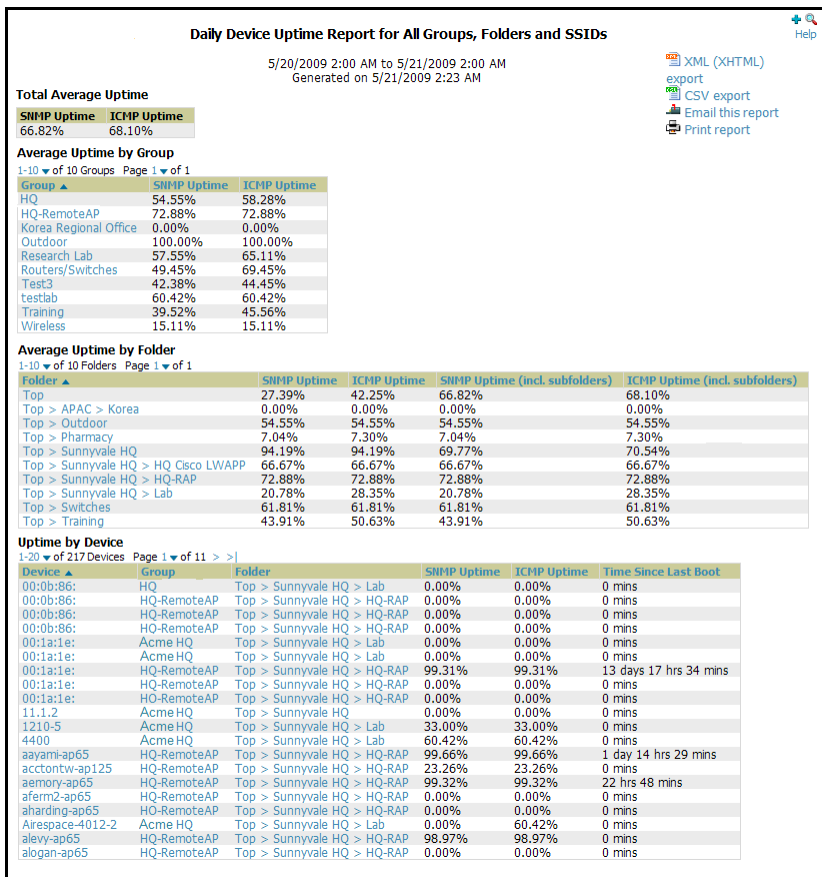


Table 138 Reports > Generated > Device Uptime Report Fields and Descriptions

Field	Description
Device	Displays the name of the device.
Group	Displays the name of the device's group.
Folder	Displays the folder to which the device belongs.
SSID	Displays the Service Set Identifier (SSID) set on the device.
SNMP Uptime	Displays the percentage of time the device was reachable via ICMP. AWMS polls the device via SNMP at the rate specified on the Groups > Basic page.
ICMP Uptime	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. AWMS only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
Time Since Last Boot	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 Access Points (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.

The **Home > License** page also cites IDS events, and triggers can be configured for IDS events. Refer to [“Setting Triggers for IDS Events” on page 223](#) for additional information.

Perform these steps to view the most recent version of the **IDS Events** report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **IDS Events Report** to display report **Detail** information.
3. Clicking the AP device or controller name takes you to the **APs/Devices > List** page.

Figure 189 and **Table 139** illustrate and describe the **Reports > Generated > IDS Events Detail** page.

Figure 189 *Reports > Generated > IDS Events Report Illustration*

The screenshot shows the 'IDS event yesterday for All Groups and Folders' report. It includes a date range of 5/20/2009 2:00 AM to 5/21/2009 2:00 AM, generated on 5/21/2009 2:23 AM. There are utility links for XML (XHTML) export, CSV export, Email this report, and Print report. The report is divided into sections for 'Top IDS Events by AP' and 'Top IDS Events by Controller', each with a summary table. At the bottom, there is a detailed table of events with columns for Attack, Attacker, AP, Controller, Radio, Channel, SNR, Precedence, and Time.

AP	Total Events ▲	First Event	Most Recent Event
idhasoft-ap70-2	2	5/20/2009 11:06 PM	5/20/2009 11:06 PM

Controller	Total Events ▲	First Event	Most Recent Event
RAP-Local	2	5/20/2009 11:06 PM	5/20/2009 11:06 PM

Attack	Attacker	AP	Controller	Radio	Channel	SNR	Precedence	Time ▼
Null-Probe-Response	00:1A:70:77:9C:CF	idhasoft-ap70-2	RAP-Local	802.11bg	-	4	-	5/20/2009 11:06 PM
Null-Probe-Response	00:1A:70:77:9C:CF	idhasoft-ap70-2	RAP-Local	802.11bg	-	4	-	5/20/2009 11:06 PM

Table 139 *Reports > Generated > IDS Events Detail Fields*

Field	Description
AP	This column lists the AP devices for which IDS events have occurred in the prior 24 hours, and provides a link to the APs/Devices > Monitor page for each.
Total Events	This column cites the total number of IDS events for each device that has experienced them during the prior 24-hour period.
First Event	This column cites the first IDS event in the prior 24-hour period.
Most Recent Event	This column cites the most recent or latest IDS event in the prior 24-hour period.
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 APs/Devices > Monitor 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:

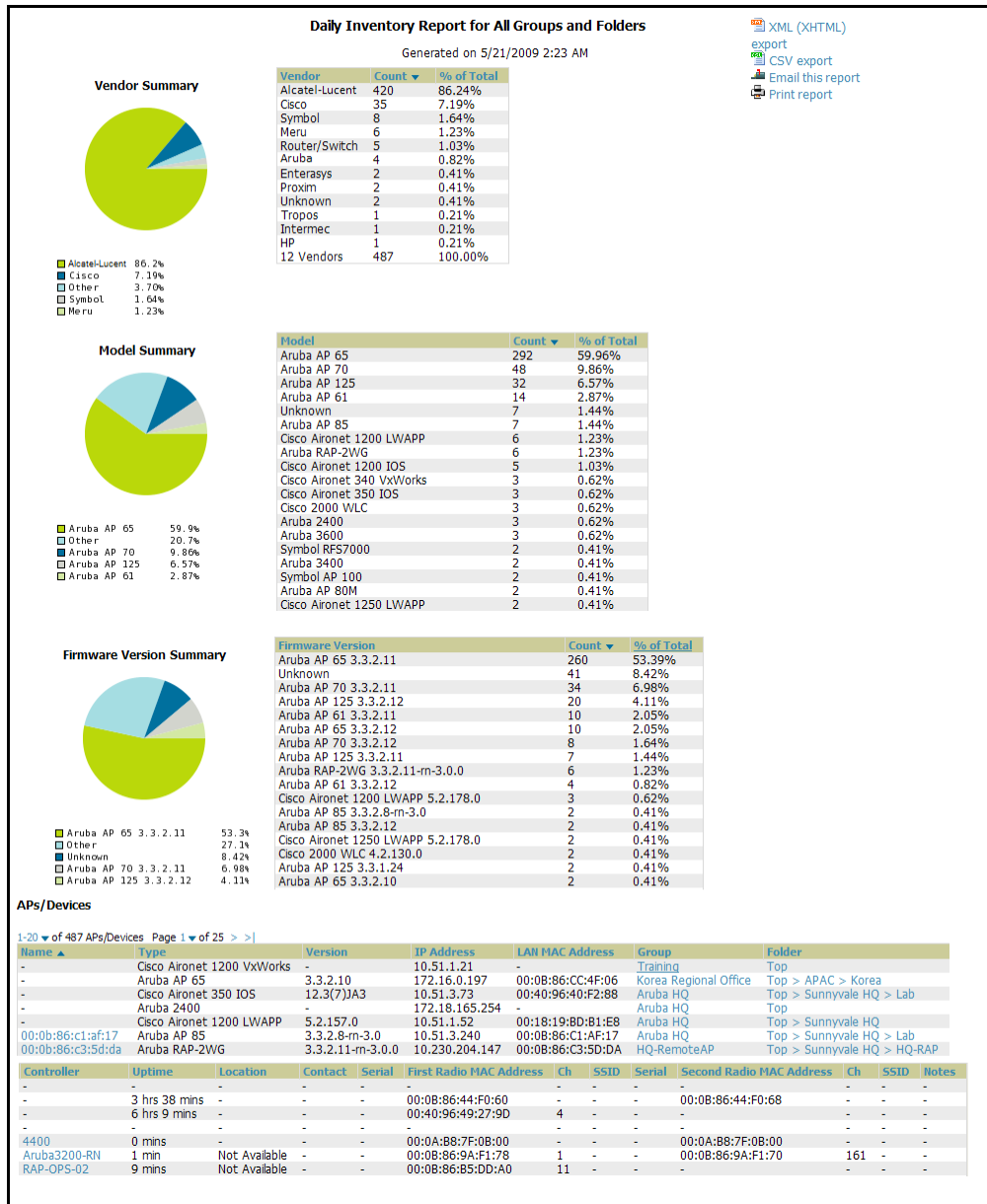
- **Vendor Summary**—Lists the vendors for all devices or firmware on the network.
- **Model Summary**—Lists the model numbers for all devices or firmware on the network.
- **Firmware Version Summary**—Lists the firmware version for all firmware used on the network.

- APs/Devices—Lists all devices on the network.

Perform these steps to view the most recent version of the **Inventory** report, illustrated in [Figure 190](#)

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Daily Inventory Report** to display report **Detail** information.
3. The **Detail** page allows you to view device or other information by clicking the device name, IP address, MAC Address, Group, Folder, or associated controller links.

Figure 190 Reports > Generated > Inventory Report Illustration (Split View)



Using the Memory and CPU Usage Report

The **Memory and CPU Usage Report** displays the top memory usage by device, and CPU usage on the network by device. The usage for any given resource, whether CPU or RAM usage, is listed as a percentage.

To create a scheduled and generated report of this type, refer to [“Using Daily Reports” on page 264](#).

Perform these steps to view the most recent version of the **Memory and CPU Usage Report**.

1. Navigate to the **Reports > Generated** page.

2. Scroll to the bottom, and click **Daily Memory and CPU Usage** to display report **Detail** information.
3. The **Detail** page allows you to view device or other information by clicking the device name, IP address, MAC Address, Group, Folder, or associated controller links.

Figure 191 illustrates the Reports > Generated > Daily Memory and CPU Usage Detail page.

Figure 191 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 three categories:

- Bandwidth usage by device—maximum and average bandwidth in kbps
- Number of users by device—maximum and average by connection instances
- Number of users by time period—average bandwidth in and out

Perform these steps to view the most recent version of the **Network Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Network Usage** to display report **Detail** information.
3. The **Detail** page allows you to view bandwidth and device usage in three sections, illustrated below.

Figure 192 illustrates the **Reports > Generated > Daily Memory and CPU Usage Detail** page.

Figure 192 *Reports > Generated > Network Usage Report Illustration (Partial Example)*



Using the New Rogue Devices Report

The **New Rogue Devices Report** summarizes rogue device information in a number of ways, to include the following categories of information:

- Rogue devices by RAPIDS classification—described in “[Using RAPIDS and Rogue Classification](#)” on page 195
- 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 AWMS pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional AWMS pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional AWMS pages

Perform these steps to view the most recent version of the **New Rogue Devices Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Rogue Devices** to display report **Detail** information.
3. The **Detail** page allows you to view bandwidth and device usage in multiple sections, illustrated below. Several figures below illustrate the multiple fields and information in the **New Rogue Devices Report**.

Figure 193 Reports > Generated > New Rogue Devices Report Illustration, Top Half of Report

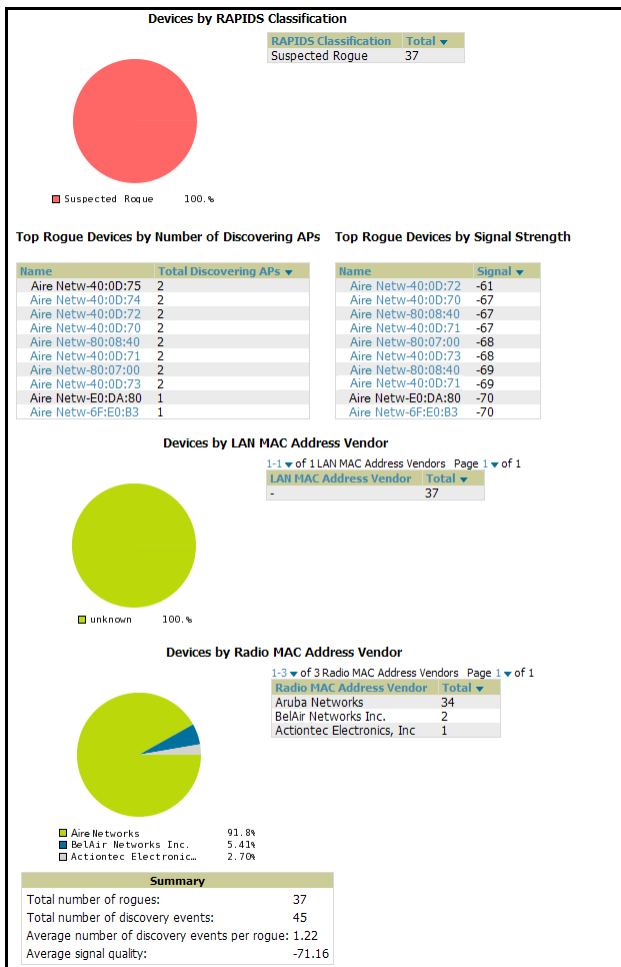


Figure 194 Reports > Generated > New Rogue Devices Report Illustration, Bottom Half of Report (Partial View)

Devices Discovered Only Wirelessly									
1-20 of 37 Rogue Devices Page 1 of 2 > > >									
Name	RAPIDS Classification	Threat Level	Ack	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP	Type	
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:38 PM	Wireless AP scan	SW-2	SW-2	-	
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire tac-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 8:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-3	SW-3	-	
Aire Netw-E1:15:C2	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-A2:71:30	Suspected Rogue	5	No	5/20/2009 4:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-A0:A5:23	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-8B:74:43	Suspected Rogue	5	No	5/20/2009 5:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-E1:16:E3	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-40:0D:72	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Netw-C8:3D:60	Suspected Rogue	5	No	5/20/2009 6:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/20/2009 5:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 7:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/21/2009 1:52 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 8:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 8:40 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	

Rogue Devices									
1-20 of 37 Rogue Devices Page 1 of 2 > > >									
Name	RAPIDS Classification	Threat Level	Ack	First Discovered	First Discovery Method	First Discovery Agent	Last Discovering AP	Type	
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 9:22 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire tac-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 9:10 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire Netw-E1:15:C2	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-2	SW-2	-	
Aire Netw-A2:71:30	Suspected Rogue	5	No	5/20/2009 7:07 AM	Wireless AP scan	SW-3	SW-3	-	
Aire Netw-A0:A5:23	Suspected Rogue	5	No	5/20/2009 7:12 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-6F:E0:B3	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire Netw-A0:A5:20	Suspected Rogue	5	No	5/20/2009 4:35 AM	Wireless Management Client scan	-	-	-	
Aire tac-F1:CD:02	Suspected Rogue	5	No	5/20/2009 4:38 PM	Wireless AP scan	SW-2	SW-2	-	
Aire Netw-80:0B:80	Suspected Rogue	5	No	5/20/2009 8:40 AM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-E0:DA:80	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-8B:74:43	Suspected Rogue	5	No	5/20/2009 12:10 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-E1:16:E3	Suspected Rogue	5	No	5/20/2009 4:11 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Netw-40:0D:72	Suspected Rogue	5	No	5/20/2009 8:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Netw-C8:3D:60	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Netw-40:0D:71	Suspected Rogue	5	No	5/20/2009 12:41 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	
Aire Net-0F:C8:05	Suspected Rogue	5	No	5/20/2009 7:42 PM	Wireless AP scan	Corp1344-SW-AP85	Facilities-AL37	-	
Aire Net-0F:C8:04	Suspected Rogue	5	No	5/20/2009 10:52 PM	Wireless AP scan	Corp1344-SW-AP85	Corp1344-SW-AP85	-	

Discovery Events										
1-20 of 45 Discovery Events Page 1 of 3 > > >										
Rogue	RSSI	Channel	SSID	WEP	Network Type	Switch/Router	Port	IP Address	Time	Discovery Method
Aire Netw-E4:50:21	21	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	12	11	sus_4	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	12	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	23	11	sus_4	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	20	11	gre2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	18	11	sus_3	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	13	11	gre2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	25	52	ethersphere-wpa2	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	24	52	guest	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	14	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	17	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	10	11	aruba-ap	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	19	11	qa-hk-soak-chuck-bridge	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	13	11	qa-hk-soak-chuck-bridge-persist	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	10	11	qa-hk-soak-chuck-bridge-always	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	qa-hk-soak-chuck-bridge-always	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E4:50:21	13	11	qa-hk-soak-chuck-bridge	-	AP	-	-	-	5/21/2009 2:22 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	sus_3	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan
Aire Netw-E4:50:21	22	11	gre2	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan
Aire Netw-E1:B3:C3	22	11	gre2	-	AP	-	-	-	5/21/2009 1:52 AM	Wireless AP scan

The rogue device inventories that comprise this report contain many fields, described in [Table 140](#).

Table 140 New Rogue Devices Report Fields

Field	Description
Name	Displays the device name, as able to be determined.
RAPIDS Classification	Displays the RAPIDS classification for the rogue device, as classified by rules defined on the RAPIDS > Rules page. Refer to “Using RAPIDS and Rogue Classification” on page 195 for additional information.
Threat Level	Displays the numeric threat level by which the device has been classified, according to rules defined on the RAPIDS > Rules page. Refer to “Using RAPIDS and Rogue Classification” on page 195 for additional information.
Ack	Displays whether the device has been acknowledged with the network.
First Discovered	Displays the date and time that the rogue device was first discovered on the network.
First Discovery Method	Displays the method by which the rogue device was discovered.
First Discovery Agent	Displays the network device that first discovered the rogue device.
Last Discovering AP	Displays the network device that most recently discovered the rogue device.

Table 140 New Rogue Devices Report Fields (Continued)

Field	Description
Type	Displays the rogue device type when known.
Operating System	Displays the operating system for the device type, when known.
IP Address	Displays the IP address of the rogue device when known.
SSID	Displays the SSID for the rogue device when known.
Network Type	Displays the network type on which the rogue was detected, when known.
Channel	Displays the wireless RF channel on which the rogue device was detected.
WEP	Displays Wired Equivalent Privacy (WEP) encryption usage when known.
RSSI	Displays Received Signal Strength (RSSI) information for radio signal strength when known.
Signal	Displays signal strength when known.
LAN MAC Address	Displays the MAC address for the associated LAN when known.
LAN Vendor	Displays LAN vendor information associated with the rogue device, when known.
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Displays the vendor information for the radio device when known.
Port	Displays the router or switch port associated with the rogue device when known.
Last Seen	Displays the last time in which the rogue device was seen on the network.
Total Discovering APs	Displays the total number of APs that detected the rogue device.
Total Discovery Events	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).

Perform these steps to view the most recent version of the **New Users Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **New Users** to display report **Detail** information.
3. The **Detail** page allows you to view information for new users that have appeared on the network during the time period defined for the report.

Figure 195 illustrates the fields and information in the **New Users Report**.

Figure 195 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 r
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
-	pod-visitor-logon	00:03:2A:00:03:2A	Cisco-Linksys, LLC	Facilities-AL37	1/20/2009 11:05 AM	2 hrs 38 m
NETWORKS\xyz	employee	00:16:CF:00:16:CF	Intel Corporate	ExecutiveSuite-AL16	1/20/2009 9:06 AM	1 hr 13 mir
71150	pod-visitor-logon	00:03:2A:00:03:2A	Intel Corporate	StorageRooms-AL5	1/20/2009 8:28 AM	9 hrs 56 m






-  XML (XHTML)
-  export
-  CSV export
-  Email this report
-  Print report

Table 141 Reports > Generated > New Users Report Fields

Field	Description
Username	Displays the username when known.
Role	Displays the role with which the user is associated.
MAC Address	Displays the MAC address of the AP device by which the user connected.
Vendor	Displays vendor information for the AP device by which the user connected.
AP/Device	Displays the device type by which the user connected.
Association Time	Displays the time in which the AP device associated with the controller.
Duration	Displays the duration of the user’s connection.

Using the PCI Compliance Report

AWMS 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.

In addition to citing simple pass or fail status with regard to each PCI requirement, AWMS 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 74](#) 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.

Perform these steps to view the most recent version of the **PCI Compliance Report**.

1. Verify that AWMS is enabled to monitor compliance with PCI requirements, as described in the [“Enabling or Disabling PCI Auditing” on page 76](#).
2. Navigate to the **Reports > Generated** page.
3. Scroll to the bottom, and click **PCI Compliance** to display **Detail** information.

Figure 196 illustrates the fields and information in the most recent **PCI Compliance Report**.

Figure 196 Reports > Generated > PCI Compliance Report Illustration, Pass or Fail 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 <https://www.pcisecuritystandards.org>.

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.

XML (XHTML) export
CSV export
Email this report
Print report

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
11.1	Identify unauthorized wireless devices. A report will indicate a failure if there are unacknowledged rogue APs present in RAPIDS or there are no wireless rogues discovered in the last three months.	Pass
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 AWMS is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Pass

Figure 197 Reports > Generated > PCI Compliance Report Illustration Example

Issues for requirement 1.1: Configuration standards for routers. (Fail)

1-20 of 466 PCI Compliance Issues Page 1 of 24 > >|

AP/Device	Status	Detail						
00:0b:86:c1:af:17	Unable to Determine	Device is currently down or was never contacted.						
00:0b:86:c3:5d:da	Unable to Determine	Device is currently down or was never contacted.						
00:0b:86:c7:71:bc	Unable to Determine	Device is currently down or was never contacted.						
00:0b:86:cd:d9:42	Fail	<table border="1"> <thead> <tr> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location (failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Name ahouk-ap65</td> <td>00:0b:86:cd:d9:42</td> </tr> </tbody> </table>	Current Device Configuration	Desired Device Configuration	Location (failed to fetch)	Not Available	Name ahouk-ap65	00:0b:86:cd:d9:42
Current Device Configuration	Desired Device Configuration							
Location (failed to fetch)	Not Available							
Name ahouk-ap65	00:0b:86:cd:d9:42							
00:1a:1e:c0:1a:dc	Unable to Determine	Device is currently down or was never contacted.						
00:1a:1e:c0:2b:32	Fail	<table border="1"> <thead> <tr> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Name aruba-124-c0:2b:32</td> <td>00:1a:1e:c0:2b:32</td> </tr> </tbody> </table>	Current Device Configuration	Desired Device Configuration	Name aruba-124-c0:2b:32	00:1a:1e:c0:2b:32		
Current Device Configuration	Desired Device Configuration							
Name aruba-124-c0:2b:32	00:1a:1e:c0:2b:32							
00:1a:1e:c5:a9:30	Fail	<table border="1"> <thead> <tr> <th>Current Device Configuration</th> <th>Desired Device Configuration</th> </tr> </thead> <tbody> <tr> <td>Location (failed to fetch)</td> <td>Not Available</td> </tr> <tr> <td>Name marcus-ap65</td> <td>00:1a:1e:c5:a9:30</td> </tr> </tbody> </table>	Current Device Configuration	Desired Device Configuration	Location (failed to fetch)	Not Available	Name marcus-ap65	00:1a:1e:c5:a9:30
Current Device Configuration	Desired Device Configuration							
Location (failed to fetch)	Not Available							
Name marcus-ap65	00:1a:1e:c5:a9:30							

Using the Port Usage Report

You can generate a wide array of port usage statistics from the **Port Usage Report** feature, including each of the following:

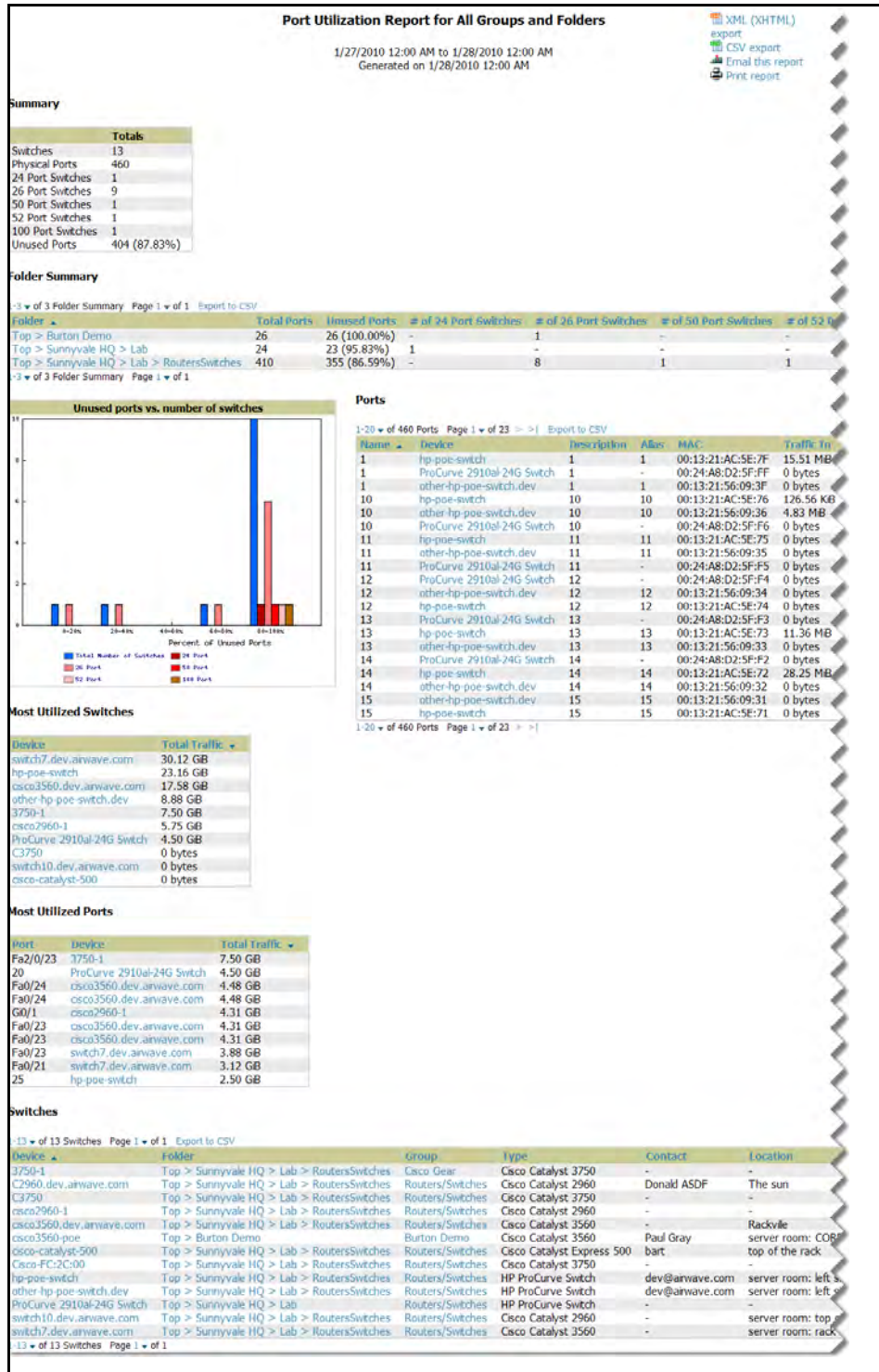
- List of all the switches and ports in your network by folder
- List of unused ports
- List of access and distribution ports
- Histogram displaying unused ports vs. unused switches by type (access or distribution)
- List of most used switches
- List of most used ports

Perform these steps to view the most recent version of the **Port Usage Report**.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **Port Usage Report** to display report **Detail** information.
3. The **Detail** page allows you to view all the information you selected from the **Port Usage** area of the **Reports > Definitions** page.

A sample of the types of information you might choose to generate in a **Port Usage Report** appears in [Figure 198](#).

Figure 198 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 AP controllers, RADIUS Servers, and users.

Perform these steps to view the most recent version of the RADIUS Authentication Issues Report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **RADIUS Authentication Issues Report** to display report **Detail** information.
3. The **Detail** page allows you to view information for RADIUS issues that have appeared on the network during the time period defined for the report.

Figure 199 illustrates the fields and information in the RADIUS Authentication Issues Report.

Figure 199 Reports > Generated > RADIUS Authentication Issues Detail Page Illustration

Daily RADIUS Authentication Issues Report for All Groups, Folders and SSIDs

1/20/2009 12:00 AM to 1/21/2009 12:00 AM
Generated on 1/21/2009 12:21 AM

[XML \(XHTML\)](#)
[export](#)
[CSV export](#)
[Email this report](#)
[Print report](#)

Top 10 RADIUS Authentication Issues by Controller

Device	Total Failures	First Event	Most Recent Event
airespace-1	1776	1/20/2009 12:00 AM	1/20/2009 11:59 PM

Top 10 RADIUS Authentication Issues by RADIUS Server

RADIUS Server	Total Failures	First Event	Most Recent Event
vortex	2	1/20/2009 10:41 AM	1/20/2009 10:41 AM

Top 10 RADIUS Authentication Issues by User

User	Total Failures	First Event	Most Recent Event
00:21:5C:00:21:5C	1732	1/20/2009 12:00 AM	1/20/2009 11:59 PM
00:1D:D9:00:1D:D9	15	1/20/2009 1:51 PM	1/20/2009 2:08 PM
00:16:CF:00:16:CF	6	1/20/2009 3:05 PM	1/20/2009 3:13 PM
00:21:5C:00:21:5C	5	1/20/2009 7:05 AM	1/20/2009 5:33 PM
00:1C:BF:00:1C:BF	3	1/20/2009 4:12 PM	1/20/2009 4:13 PM
00:16:CF:00:16:CF	2	1/20/2009 8:33 AM	1/20/2009 5:42 PM
00:14:A4:00:14:A4	2	1/20/2009 5:27 PM	1/20/2009 5:28 PM
00:1F:38:00:16:CF	1	1/20/2009 8:52 AM	1/20/2009 8:52 AM
00:19:7D:00:14:A4	1	1/20/2009 3:04 PM	1/20/2009 3:04 PM
00:21:FE:00:16:CF	1	1/20/2009 11:23 AM	1/20/2009 11:23 AM

1-20 of 1776 RADIUS Authentication Issues Page 1 of 89 > >|

Event	User MAC Address	Username	RADIUS Server	Event Time	Device	AP	Radio
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:59 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:59 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:58 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:58 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:57 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:57 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:56 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:56 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:55 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:55 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:54 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:54 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:53 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:53 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:52 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:52 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:51 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:51 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:50 PM	airespace-1	-	-
Client authentication failed for 00:21:5C:85:BD:0B	00:21:5C:00:21:5C	-	-	1/20/2009 11:50 PM	airespace-1	-	-

Using the Rogue Containment Audit Report

The rogue containment audit report that lets you know if any containment is failing. Figure 200 illustrates the fields and information in this report type.

Figure 200 Reports > Generated > Rogue Containment Audit Detail Page Illustration

Days Remaining: 89
[Help](#)

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 -
Airespace-5500	Apple-ED:3B:17	00:03:93:ED:3B:17	Contained	Not Contained	Signal strength > -75 dBm	-
Airespace-5500	Senao Inte-43:7B:81	00:02:6F:43:7B:81	Contained	Not Contained	Signal strength > -75 dBm	-
Airespace-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 User Session Report

The User Session Report itemizes user-level activity by session. A session is any instance in which a user connects to the network. You can track and display in list and chart form session information that includes all of the following:

- Connection Mode (wired, wireless or both depending on how report definition is created)
- SSID
- Role
- VLAN
- Cipher (\Summary)
- Summary
- Sessions
- User

Perform these steps to view the most recent version of the User Session Report.

1. Navigate to the **Reports > Generated** page.
2. Scroll to the bottom, and click **User Session Report** to display report **Detail** information.
3. The **Detail** page allows you to view multifaceted information for user sessions during the time period defined for the report.

The figures that follow illustrate the fields and information in the User Session Report.

Figure 201 User Session Detail, Connection Mode Information

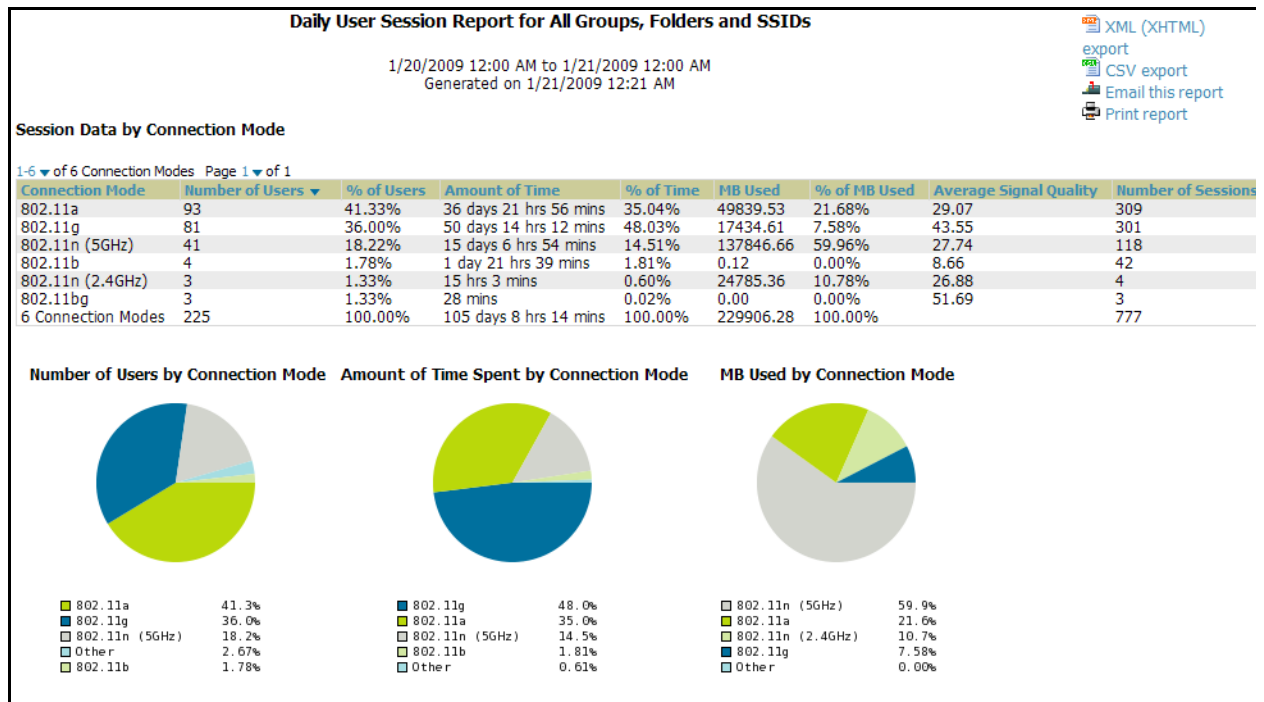


Figure 202 User Session Detail > SSID Information

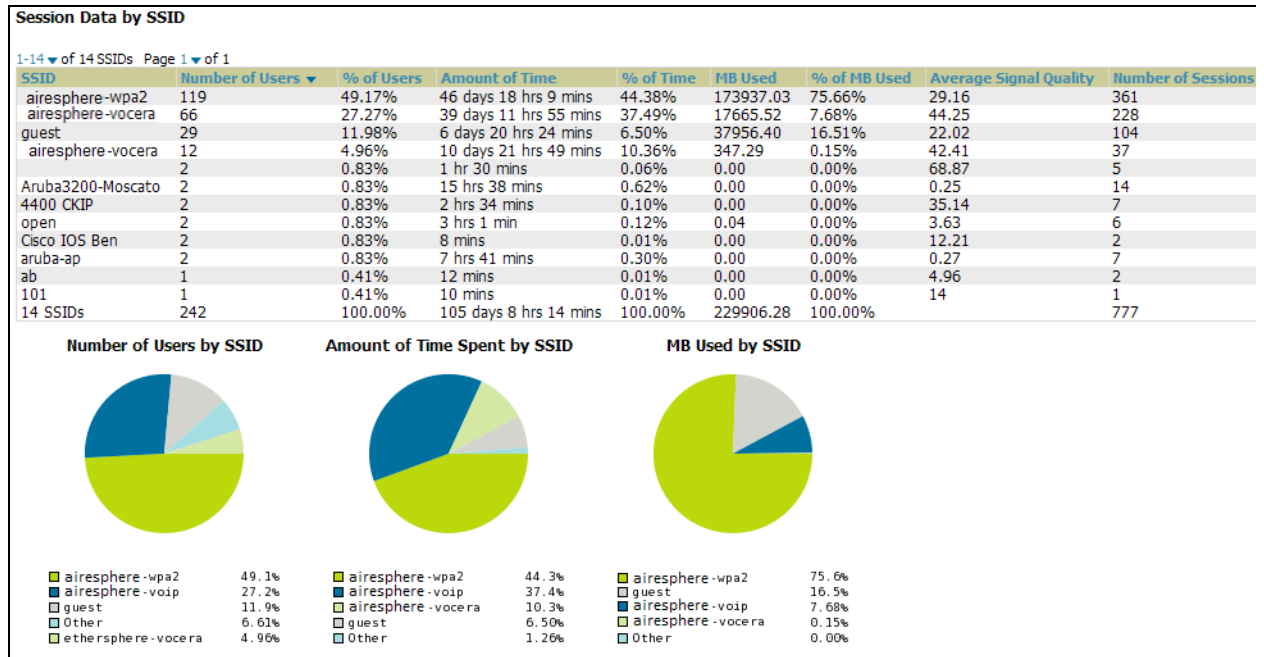


Figure 203 User Session Detail > Role Information

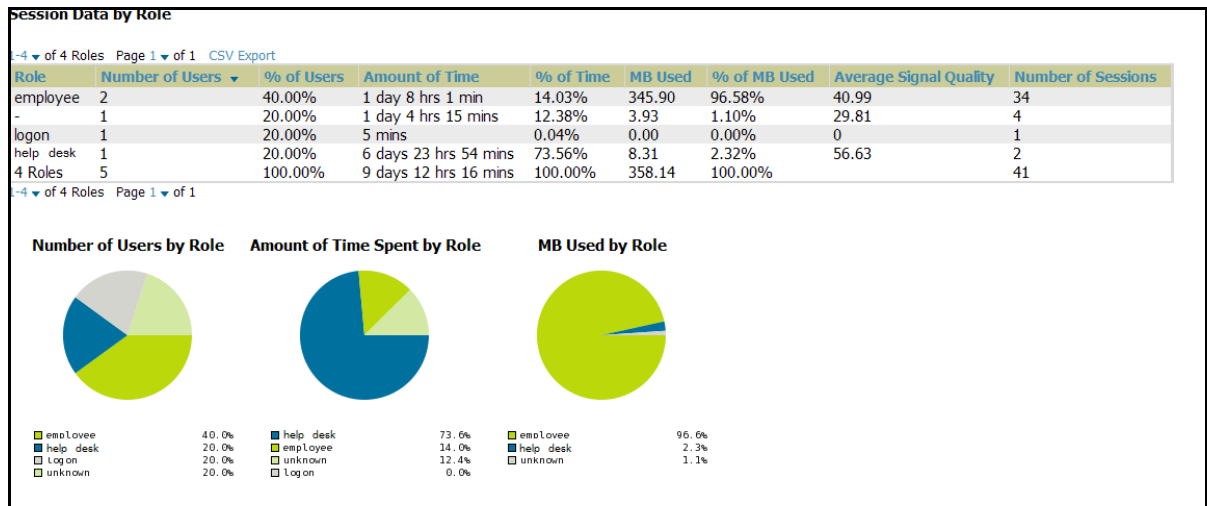


Figure 204 User Session Detail > VLAN Information

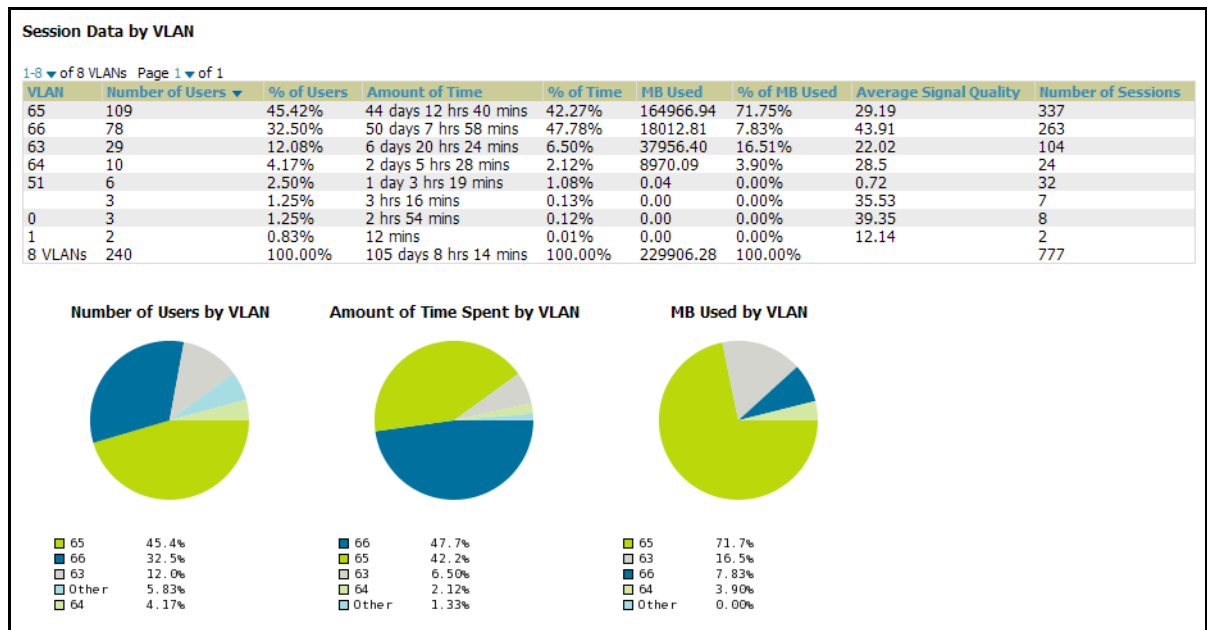


Figure 205 User Session Detail > Cipher Information

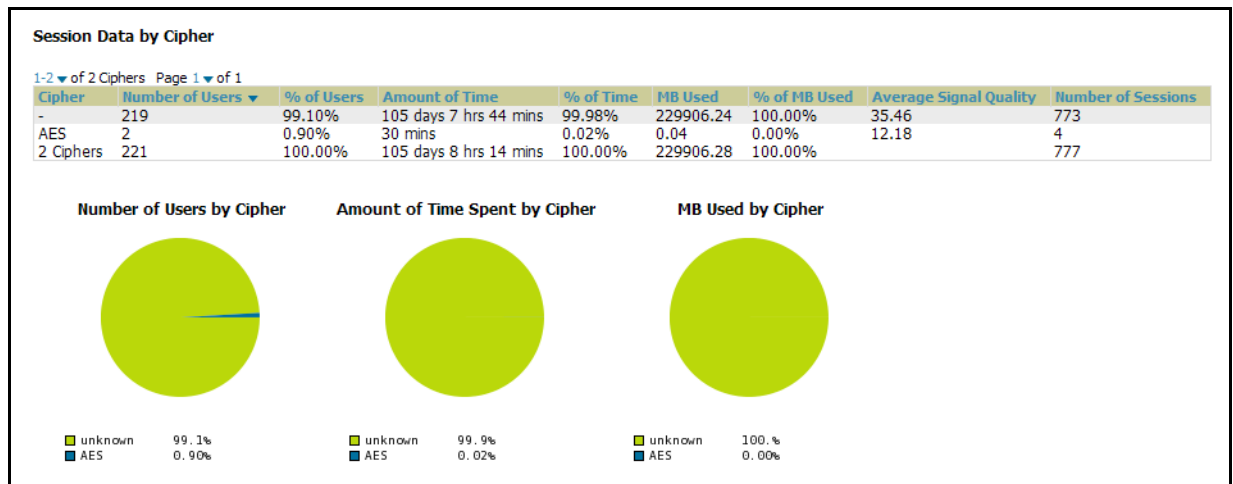


Figure 206 Summary and User Information (partial view)

Summary									
Number of sessions	777								
Number of unique users	220								
Number of guest users	0								
Number of unique APs	36								
Average session duration	3 hrs 15 mins								
Total traffic (MB)	229906.28								
Average traffic per session (MB)	295.89								
Average traffic per user (MB)	1045.03								
Average bandwidth per user (kbps)	289.39								
Average signal quality	35.45								

Sessions									
MAC Address	Username	Role	Device Name	Controller	Group	Folder	AP Location	Connect Time	
00:21:5C:6B:54:15	CORPNETWORK\lauserid	employee	aankumah-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:56 AM
00:1F:3B:3F:43:3F	CORPNETWORK\lauserid	employee	osucadi-RAP2WG	RAP-OPS-02	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:51 AM
00:19:7D:78:DE:CB	CORPNETWORK\lauserid	employee	khamilton-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:50 AM
00:24:36:54:02:18	khamilton	employee	khamilton-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:36 AM
00:21:5C:6B:54:15	CORPNETWORK\lauserid	employee	aankumah-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:36 AM
00:1D:09:05:05:BF	CORPNETWORK\lauserid	employee	mdvne-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:34 AM
00:03:2A:02:6B:34	wifphone	CORPNETWORK	AL19	ethersphere-ims3	Aruba HQ	Top	HQ	Not Available	5/21/2009 1:23 AM
00:19:79:0F:6E:72	dharkns	employee	perforce	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:21 AM
00:1F:3B:7D:A6:21	CORPNETWORK\lauserid	employee	phauff-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:11 AM
00:0E:9B:CA:64:FF	CORPNETWORK\lauserid	employee	kstan-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 1:01 AM
00:16:FC:BC:0F:C2	CORPNETWORK\lauserid	employee	thoida-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:53 AM
00:03:2A:02:6B:52	wifphone	employee	Finance-AL27	ethersphere-ims3	Aruba HQ	Top	HQ	Not Available	5/21/2009 12:48 AM
00:19:7E:76:90:AD	CORPNETWORK\lauserid	employee	jburg-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:47 AM
00:1E:4C:68:C3:C5	CORPNETWORK\lauserid	employee	thargln1-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:38 AM
00:1C:26:C5:39:D8	CORPNETWORK\lauserid	employee	ggopalan-ap	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:36 AM
00:05:4E:4E:85:25	CORPNETWORK\lauserid	employee	vravula-ap65-2	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:34 AM
00:16:CF:23:7B:7A	CORPNETWORK\lauserid	employee	fweisel-ap65	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:30 AM
00:05:4E:4E:85:25	CORPNETWORK\lauserid	employee	vravula-ap65-2	RAP-Local	HQ-RemoteAP	Top > HQ-RAP	HQ	Not Available	5/21/2009 12:30 AM
00:03:2A:02:6B:49	wifphone	employee	AL12	ethersphere-ims3	HQ	Top	HQ	Not Available	5/21/2009 12:27 AM
00:03:2A:02:6B:36	wifphone	employee	Haystack-AL29	ethersphere-ims3	HQ	Top	HQ	Not Available	5/21/2009 12:27 AM

Session Data by User									
MAC Address	Username	Roles	Amount of Time	MB Used	Avg Bandwidth (kbps)	Average Signal Quality	Vendor	Connection Modes	
00:03:2A:02:4F:95	wifphone	employee	23 hrs 59 mins	0.43	0.04	49.24	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:50:E3	wifphone	employee	1 day 0 hrs 0 mins	8.12	0.77	52.91	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:52:8C	wifphone	employee	23 hrs 59 mins	7.35	0.7	50.65	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:5F:84	wifphone	VoFi	5 hrs 34 mins	0.12	0.05	44.74	UniData Communication Systems, Inc.	802.11b	
00:03:2A:02:67:FD	wifphone	employee	14 hrs 58 mins	0.15	0.02	46.99	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:69:7A	azindel	employee	23 hrs 59 mins	5.65	0.54	40.53	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:69:88	wifphone	employee	23 hrs 59 mins	8382.05	794.75	44.87	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:69:CB	wifphone	employee	23 hrs 59 mins	16.70	1.58	41.3	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:69:D4	wifphone	employee	1 day 0 hrs 0 mins	12.53	1.19	55.55	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:69:F4	wifphone	employee	1 day 0 hrs 0 mins	16.04	1.52	53.05	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:05	wifphone	employee	23 hrs 59 mins	0.45	0.04	47.31	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:0B	wifphone	employee	23 hrs 59 mins	3.68	0.35	50.34	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:0C	wifphone	employee	23 hrs 59 mins	0.46	0.04	42.12	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:13	wifphone	employee	1 day 0 hrs 0 mins	0.37	0.04	47.81	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:61	wifphone	employee	23 hrs 59 mins	0.39	0.04	46.13	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:62	wifphone	employee	23 hrs 59 mins	0.43	0.04	42.36	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:63	wifphone	employee	23 hrs 59 mins	1.17	0.11	46.36	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:65	wifphone	employee	23 hrs 59 mins	0.39	0.04	51.69	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:03	wifphone	employee	1 day 0 hrs 0 mins	0.66	0.06	43.29	UniData Communication Systems, Inc.	802.11g	
00:03:2A:02:6A:D3	wifphone	employee	23 hrs 59 mins	0.37	0.04	42.15	UniData Communication Systems, Inc.	802.11g	

Defining Reports

You can create reports in AWMS 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 click the **Add** button, or click the pencil icon to edit an existing report definition. [Figure 207](#) illustrates one view of the **Reports > Definitions** page.

Figure 207 Defining a Report with **Reports > Definitions > Add Button**

The screenshot shows a web form titled "Report Restrictions". It contains the following fields and sections:

- Report Restrictions** (Section Header):
 - Group: -- All Groups -- (dropdown)
 - Folder: -- All Folders -- (dropdown)
 - Device Search Filter: This report will be run against Devices that match this search. (text input)
- Report Restrictions** section varies according to report type. (Text note)
- Report Start: (date input)
- Report End: (date input)
- Scheduling Options** (Section Header):
 - Schedule: Yes No
- Report Visibility** (Section Header):
 - Generated Report Visibility: By Role (dropdown)
- Email Options** (Section Header):
 - Email Report: Yes No
- Buttons: Add and Run, Run Now, Add, Cancel

2. Complete the fields described in [Table 142](#) 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 264.

Table 142 **Report > Definitions > Add Page Fields**

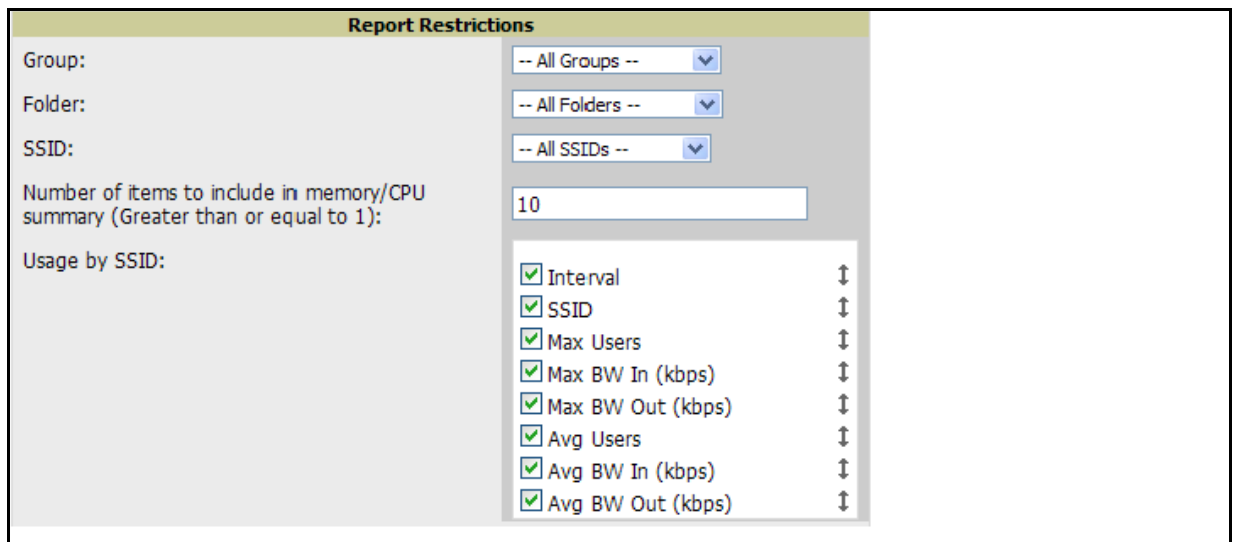
Field	Default	Description
Title	Empty	Enter a Report Title . Aruba recommends using a title that is a meaningful and descriptive, so it may be found easily on the lists of reports that appear on either Generated or Definitions pages.
Type	Capacity	Choose the type of report you wish to create in the Report Type drop-down menu.
Group	All Groups	Specify the groups and folders to be covered in the report by choosing All Groups (or All Folders) or specifying Use selected groups (or Use selected folders) in the drop-down menu. If Use selected groups is chosen, a menu with checkboxes appears, allowing you to choose the groups to include in the report.
Folder	All Folders	
Device Search Filter	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 New User and User Session , will allow you to search devices associated with a specific user or device.

Table 142 Report > Definitions > Add Page Fields (Continued)

Field	Default	Description
SSID	All SSIDs	This field displays for most report types. When this field appears, and when you select Use Selected IDs , a new list of SSIDs displays. Check (select) the specific SSIDs to be included in the report.
Report Start Report End	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 AWMS at the present time.
Schedule	No	When you select Yes , new fields display that allow you to define a specific time for report creation. The report schedule setting is distinct from the Report Start and Report End fields, as these define the period of time to be covered by the report. These Schedule fields establish the time that a report runs, independent of report scope: <ul style="list-style-type: none"> • Current Local Time—Displays for reference the time of the AWMS system. • Desired Start Date/Time—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. • Occurs—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.
Generated Report Visibility	By Role	This field allows you to display the report either by user role, with the report appearing in User Role lists on the Reports > Generated page. Alternatively, this field allows you to display reports by Subject on the Reports > Generated page.
Email Report	No	Select Yes to display sender and recipient fields. Enter the Sender Address where marked to indicate the address that appears in the From field of the emailed report. Enter recipient email addresses separated by commas when using multiple email addresses. NOTE: AWMS 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 208](#) shows a sample Report Restrictions page.

Figure 208 Report Restrictions Illustration



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:

- Click **Add and Run** to generate the report immediately, in addition to saving report settings.
- Click **Run Now** to generate the report immediately without creating a new report definition or saving the report settings.
- Click **Add** (only) to complete the report creation, to be run at the time scheduled.
- Click **Cancel** to exit from the **Add** page.

[Table 143](#) describes the configurable settings for the custom report to be created. Click any of the report names to view additional information on that report type.

Table 143 *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 AWMS, at report run time.
Using the Device Summary Report	Yes	Yes	Summarizes user and bandwidth statistics and lists devices in AWMS.
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 AWMS.
Using the Memory and CPU Usage 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 AWMS using the AWMS Setup > PCI Compliance page.

Table 143 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
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 Rogue Containment Audit Report	No	Yes	Identifies discrepancies between access point containment status specified in AMP compared to containment status identified by the controller at report run time.
Using the User Session Report	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 AWMS:

- [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 AWMS:

- 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.
- Click **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 289](#), and in [“Emailing Reports to Smarthost” on page 292](#).

Emailing Reports to Smarthost

AWMS uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If AWMS 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.Aruba.com]
```

Where: `mail.Aruba.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


```
tail -f /var/log/maillog
```

Exporting Reports to XML or CSV

AWMS 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 such as MS Notepad or Word.

Perform the following steps to export reports to XML, MS Excel, and CSV:

1. Navigate to the **Reports > Generated** page and click the name of the report you wish to export. You can also click on the link at the bottom of the page for the latest version of a report. The corresponding **Detail** page displays.
2. On the top right of the page, click **XML (XHTML) export** or **CSV export**. After a moment the XML page appears in your browser or, if you chose **CSV export**, a File Download window appears prompting you for a location on which it can save the .zip CSV files.
3. In your browser, click **File > Save As**. Define the filename and location, select **Web Page Complete** as the file type, then click **Save**. A brief **Save Webpage** status box appears to display the saving process. Allow the process sufficient time, particularly for reports that contain many links or large graphics. If you are downloading a .zip file, you only need to navigate to the desired location, and click **Save**.
4. Open the resulting file in MS Excel. You may need to display files of all type to access the file.
5. From Excel you can save the report as a single file using the **Save As > Excel Workbook** option (Excel 2007). You can also save it as an .xls file for compatibility with older versions of Excel though some formatting in the report might not be supported.



Note: 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. Contact Dell support for more information.

This chapter presents the functions, configuration, and use of the AWMS Helpdesk, and includes the following sections:

- [“AWMS Helpdesk Overview” on page 295](#)
- [“Monitoring Incidents with Helpdesk” on page 296](#)
- [“Creating a New Incident with Helpdesk” on page 297](#)
- [“Creating New Snapshots or Incident Relationships” on page 298](#)
- [“Using the Helpdesk Tab with an Existing Remedy Server” on page 299](#)

AWMS Helpdesk Overview

The Helpdesk module of the AirWave Wireless Management Suite allows front-line technical support staff to take full advantage of the data available in the AirWave Wireless Management Suite. The AWMS Helpdesk includes the following features and functions, with additional features described in this chapter:

- The **Helpdesk** tab appears to the right of the **Home** tab.
- Users with an **Admin** role have the **Helpdesk** option enabled by default.
- **Admin** users can make the Helpdesk available to users of any role by selecting the **enabled** radio button on the **role detail** page. To edit existing roles, click the **pencil icon** next to a role on the **AWMS Setup > Roles** page.
- The AWMS Helpdesk allows you to document incidents associated with users on the network.
- Installing Remedy allows you to disable Helpdesk, and use AWMS as an interface for creating, viewing, and editing incidents on the existing Remedy server. You can also associate snapshots with Remedy incidents and store them on your AWMS.

The option to use an external Remedy server is disabled by default. Navigate to the **Helpdesk > Setup** page to enable Remedy. See [“Using the Helpdesk Tab with an Existing Remedy Server” on page 299](#) for more information on how to configure AWMS to integrate with a Remedy server.

Monitoring Incidents with Helpdesk

For a complete list of incidents, or to open a new incident, navigate to the **Helpdesk > Incidents** page. [Figure 209](#) illustrates the components of the AWMS Helpdesk Incidents page.

Figure 209 *Helpdesk > Incidents Page Illustration*

State	Last 2 Hours	Last Day	Total
Open	0	0	126
Closed	0	0	0
Total	0	0	126

Add New Incident

1-20 of 126 Incidents Page 1 of 7 > > |

	ID	Summary	State	Opened By	Related	Created	Updated
<input type="checkbox"/>	202	Paul's connection issue	Open	mbruno	0	5/19/2009 9:37 AM	5/19/2009 9:37 AM
<input type="checkbox"/>	201	lotte's wlan issue	Open	aruba-se	0	5/13/2009 9:31 PM	5/13/2009 9:31 PM
<input type="checkbox"/>	199	testing - ps	Open	patrick	0	5/13/2009 7:42 PM	5/13/2009 7:42 PM
<input type="checkbox"/>	198	Damien - more typing issues	Open	patrick	0	5/13/2009 7:34 PM	5/13/2009 7:34 PM
<input type="checkbox"/>	197	thomas' wireless issue	Open	patrick	0	5/11/2009 11:01 PM	5/11/2009 11:01 PM
<input type="checkbox"/>	196	Martin Has a Problem	Open	ARUBATM	0	5/5/2009 6:25 AM	5/5/2009 6:25 AM
<input type="checkbox"/>	195	Katie's Problem	Open	aruba-se	0	4/27/2009 2:24 PM	4/27/2009 2:24 PM
<input type="checkbox"/>	194	test	Open	aruba-se	0	4/27/2009 2:00 PM	4/27/2009 2:00 PM
<input type="checkbox"/>	193	demo for X	Open	aruba-se	0	4/27/2009 8:33 AM	4/27/2009 8:33 AM
<input type="checkbox"/>	192	ym's wlan issue	Open	aruba-se	0	4/26/2009 9:49 PM	4/26/2009 9:49 PM
<input type="checkbox"/>	191	Nishith can't connect	Open	danccomfort	0	4/23/2009 2:12 PM	4/23/2009 2:23 PM
<input type="checkbox"/>	190	AHK	Open	aruba-se	0	4/21/2009 2:39 AM	4/21/2009 2:39 AM
<input type="checkbox"/>	189	Bryan's network problem	Open	mbruno	1	4/20/2009 11:25 AM	4/20/2009 11:26 AM
<input type="checkbox"/>	185	Peter's connection problems	Open	mbruno	1	4/9/2009 7:44 AM	4/9/2009 7:45 AM
<input type="checkbox"/>	184	dcomfort's wlan issue	Open	aruba-se	0	4/7/2009 1:02 AM	4/7/2009 1:02 AM
<input type="checkbox"/>	183	Joe's Incident	Open	aruba-se	0	4/6/2009 4:51 PM	4/6/2009 4:51 PM
<input type="checkbox"/>	182	Test	Open	ARUBATM	0	4/6/2009 7:58 AM	4/6/2009 7:58 AM
<input type="checkbox"/>	181	euf's wlan issue	Open	aruba-se	0	4/5/2009 10:19 PM	4/5/2009 10:19 PM
<input type="checkbox"/>	177	Axians connectie probleem	Open	aruba-se	0	3/31/2009 6:49 AM	3/31/2009 6:49 AM
<input type="checkbox"/>	175	gary-test	Open	aruba-se	0	3/25/2009 3:36 PM	3/25/2009 3:36 PM

Select All - Unselect All

Delete

The table in **Helpdesk > Incidents** displays the count of incidents by state and by time. You can sort incidents from within any category of information, whether in sequential or reverse-sequential order. You can display all incidents, or strictly open or closed incidents, and you can display incidents according to the person who created them. Finally, the **Helpdesk > Incidents** page allows you to add or delete incidents.

Table 144 *Helpdesk > Incidents Top Table*

Column	Description
State	Displays three states as they apply, as follows: <ul style="list-style-type: none"> Open (currently under investigation) Closed (resolved) The total incident count
Period of time and Total	Shows the count of incidents in the last two hours, the last day, and the total count.

The table at the bottom of the page, as described in [Table 145](#) below, summarizes the incidents that have been reported thus far, and which AWMS has not yet purged.

Use the **AWMS Setup > General** page and the **Historical Data Retention** page. Using the **Closed Helpdesk Incidents** field, set the number of days that AWMS is to retain records of closed Helpdesk incidents. Settings this value to 0 disables this function.

Clicking the pencil icon next to any incident opens an edit page where you can modify and update the incident. An incident can be deleted by selecting the checkbox next to it and clicking the **Delete** button at the bottom of the table.

Table 145 AWMS Helpdesk > Incidents Bottom Table

Column	Description
ID	Displays the ID number of the incident, which is assigned automatically when the incident is logged.
Summary	Presents a summary statement of the issue or problem—entered by the AWMS user when the incident is created.
State	The current state of the incident - this can be either open or closed. The drop-down menu at the top of the column can be used to show only open or closed incidents. The default is to show incidents of both states.
Opened By	Displays the username of the AWMS user who opened the incident. Helpdesk can be made available to users of any role by selecting the enabled radio button on the Role Detail page. Click the pencil icon next to a role on the AWMS Setup > Roles page.
Related	Displays the number of items that have been associated to the incident. These link different groups, APs or clients to the incident report.
Created	Displays the time and date the incident was created.
Updated	Displays the time and date the incident was last modified by an AWMS user.

Creating a New Incident with Helpdesk

To create a new Helpdesk incident, click the **Add New Incident** button underneath the top table. This launches and displays an incident edit page, as illustrated in [Figure 210](#). The contents of this page are described in [Table 146](#).

Figure 210 Add Incident Page Illustration

Table 146 Helpdesk Incident Edit Page Fields

Field	Description
Summary	Displays user-entered text that describes a short summary of the incident
State	Provides a drop-down menu with the options "Open" or "Closed"
Description	Provides a longer user-entered text area for a thorough description of the incident.



Note: The **Incidents** portion of the **Alert Summary** table on other AWMS pages only increments the counter for incidents that are open and associated to an AP. This field displays incidents based on folder, which is the Top folder on this page and on the **Home > Overview** page. Incidents that are not related to devices in that folder are not counted in the **Alert Summary** table on other pages.

To view all incidents, including those not associated to an AP, use the **Helpdesk > Incidents** page.

Helpdesk icons appear at the top of other AWMS pages, allowing graphical snapshots and other records to be associated to existing incidents. These appear in the upper right-hand corner next to the **Help** link. Refer to [Figure 211](#).

Figure 211 *Helpdesk Icons on Additional Pages*



[Table 147](#) describes the Helpdesk icon components.

Table 147 *Helpdesk Icon Components*

Icon	Description
	(ID number and description) Identifies the current incident of focus in the Helpdesk header. Clicking the link brings up the Incident Edit page (see above). Mousing over the incident brings up a summary popup of the incident.
	Relates the device, group or client to the incident (see below for more details).
	Attaches a snapshot of the page to the incident. This feature can be used to record a screenshot of information and preserve it for future troubleshooting purposes.
	Creates a new incident report.
	Choose a new incident from the list of created incidents to be the Current Incident (see description of icon above).

Creating New Snapshots or Incident Relationships

Snapshots or relationships can be created by clicking the Helpdesk header icon (see [Table 147](#)) on the screen that needs to be documented. Snapshots or relationships can then be related to the current incident in the ensuing popup window. In order to attach snapshots or relationships to another incident, click the **Choose a New Incident** icon to select a new current incident.

Relationships and snapshots appear on the **Incident Edit** page after they have been created. When a relationship is created the user can enter a brief note, and in the **Relationships** table the name of the relationship links to the appropriate page in AWMS. Clicking the snapshot description opens a popup window to display the screenshot. [Figure 212](#) illustrates these GUI tools.

Figure 212 Relationships and Snapshots on the Incident Edit Page

The screenshot shows the 'Incident' edit page. At the top, there's a 'Summary' field with the text 'Matt is seeing Mismatches.' and a 'State' dropdown menu set to 'Open'. Below that is a 'Description' field containing the text 'On an Access 247 controller.' There are 'Save' and 'Cancel' buttons. The 'Relationships' section contains a table with columns 'Name' and 'Notes'. It lists three items: 'Controller "Access247"', 'Folder "Top"', and 'Group "Access Points"'. The 'Notes' for 'Folder "Top"' is 'This is the Top folder.' and for 'Group "Access Points"' is 'The controller belongs here.' There are checkboxes next to each item and a 'Delete' button. The 'Snapshots' section shows a table with columns 'Description' and 'Created'. It lists one snapshot: 'Snapshot 11' created on '3/3/2010 3:32 PM'. There are checkboxes and a 'Delete' button.

Using the Helpdesk Tab with an Existing Remedy Server

If an external Remedy server exists, you can use the AWMS Helpdesk tab to create, view and edit incidents on the Remedy server. AWMS can only support integration with a Remedy server if it is a default installation of Remedy 7.0 with no changes to the web service definitions.

To use the Helpdesk tab with a Remedy server, first navigate to the **Helpdesk > Setup** page. In the **BMC Remedy Setup** area, click the **Yes** button to enable Remedy. This launches a set of fields for information about the Remedy server. Once enabled to use Remedy, the Helpdesk header icons work in the same way for a Remedy-configured Helpdesk as they do for the default AWMS Helpdesk. [Figure 213](#) illustrates this appearance, and [Table 148](#) describes the components. For more details, see [“Creating New Snapshots or Incident Relationships” on page 298](#).

Figure 213 Helpdesk > Setup with Remedy Enabled

The screenshot shows the 'BMC Remedy Setup' page. It has a title bar 'BMC Remedy Setup'. Below that, there are several fields: 'Remedy Enabled:' with radio buttons for 'Yes' (selected) and 'No'; 'Middle Tier Host:' with a text input field; 'Port:' with a text input field; 'SOAP URL:' with a text input field; 'Server:' with a text input field; 'Timeout:' with a text input field containing '60'; 'Username:' with a text input field; 'Password:' with a text input field; and 'Confirm Password:' with a text input field. At the bottom, there are 'Save' and 'Revert' buttons.

Table 148 *Components of Helpdesk > Setup with Remedy Enabled*

Field	Description
Remedy Enabled	If no (default) is selected, the existing AWMS Helpdesk functionality is available. If yes is selected, the Helpdesk functionality is disabled and the Helpdesk tab can be configured for use with an existing Remedy server. Fields for server data appear only when Remedy is enabled.
Middle Tier Host	The location of the Remedy installation's web server.
Port	The port for the HTTP interface with the web server (this is likely 8080, but there is no default value in AWMS).
SOAP URL	Gateway for web services on Remedy's middle tier host. This is usually arsys/services/ARService, but there is no default value in AWMS.
Server	The location of the backend server where Remedy data is stored.
Timeout	The timeout for HTTP requests (60 seconds by default).
Username	Username for an existing Remedy account; the role of this user defines the visibility AWMS will have into the Remedy server.
Password and Confirm Password	The password for the Remedy user account.

Once the server settings have been saved and applied, **Helpdesk** features become disabled. AWMS then displays incident data pulled from the **Remedy** server and push changes back. With the exception of snapshots, AWMS does not store any Remedy data locally.

To view **Remedy** incidents in AWMS, navigate to the **Helpdesk > Incidents** tab. [Figure 214](#) illustrates the appearance and [Table 149](#) describes the components of this page.

Figure 214 *Helpdesk > Incidents with Remedy Enabled*

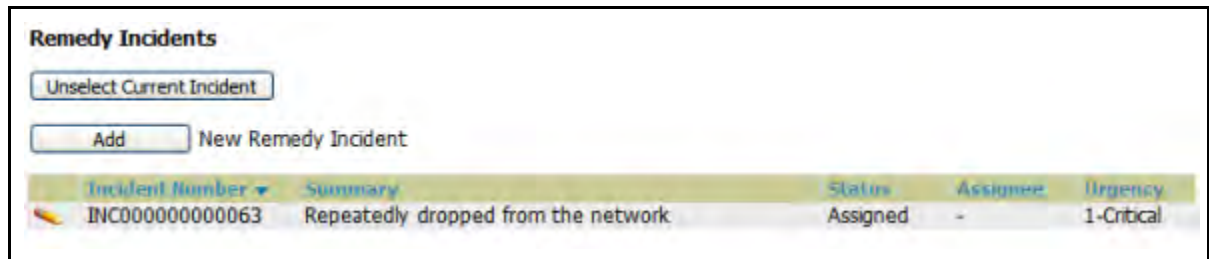


Table 149 *Helpdesk > Incidents Components with Remedy Enabled*

Field	Description
Incident Number	Displays a unique identifier for each incident; assigned by the Remedy installation.
Summary	Contains a brief incident summary as entered by AWMS or Remedy user.
Status	Displays the status as chosen by AWMS or the Remedy user: <ul style="list-style-type: none"> ● New ● Assigned ● In Progress ● Pending ● Resolved ● Closed ● Cancelled

Table 149 Helpdesk > Incidents Components with Remedy Enabled

Field	Description
Assignee	Assigned by Remedy installation; cannot be changed in AWMS.
Urgency	Displays the urgency level, as chosen by the AWMS or Remedy User: <ul style="list-style-type: none"> ● 1 - Critical ● 2 - High ● 3 - Medium ● 4 - Low

To change the current incident in the Helpdesk header, click the **Unselect Current Incident** button. To add a new Remedy incident, click the **Add** button. To edit an existing Remedy incident, click the pencil icon next to the incident you wish to edit. Refer to [Figure 215](#) and [Table 150](#) for additional illustration and explanation.

Figure 215 Helpdesk > Incidents > Add a New Remedy Incident Page Illustration

Table 150 Helpdesk > Incidents > Add a New Remedy Incident Fields

Field	Description
Customer First and Last Name	These must match exactly a customer that already exists on the Remedy server. There is no way to create a new customer from AWMS or to search Remedy customers remotely.
Impact	<ul style="list-style-type: none"> ● 1 - Extensive/Widespread (default) ● 2 - Significant/Large ● 3 - Moderate/Limited ● 4 - Minor/Localized
Urgency	<ul style="list-style-type: none"> ● 1 - Critical (default) ● 2 - High ● 3 - Medium ● 4 - Low
Summary	Free-form text field.



Note: A new incident is not created if the customer First and Last name do not exist on the Remedy server. However, in this scenario, there is no failure message or warning that the incident was not created.

Once an incident has been created, click the pencil icon in the incident list to edit the information. The status or urgency can be changed as the case progresses, and more detailed information about the incident can be added. Snapshots can also be related to Remedy incidents in the manner described in the Helpdesk section above. However, snapshots are only stored locally on the AWMS server—they are not pushed to the Remedy server.

Yum for AWMS

This appendix describes the Yum packaging management system. Dell recommends running Yum to ensure your packages are up to date, and so that your AWMS is as secure as possible if you are running RHEL 5 or CentOS 5.

Yum is an automated package management system that verifies AWMS is running the most recently released RPMs and upgrades any out-of-date packages. Yum accesses the Internet, and downloads and installs new versions of any installed RPMs. It is important to keep the AWMS RPMs as current as possible to close any known security holes in the OS as quickly as possible.

To run Yum on a CentOS 5 machine follow the instructions below:

1. Before running Yum for the first time, you need to install the GPG key. The GPG key is used to validate the authenticity of all packages downloaded by Yum.
2. To install the GPG key, type `rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5`. If the key was not manually installed before Yum is run for the first time the user will be prompted to install and accept a new key.
3. To run Yum manually, log in to the AWMS console and type `yum update` and press **Enter**. If the packages seem to be downloading slowly, press **Ctrl+C** to connect to a new mirror.
4. To configure Yum to run nightly, type `yum install yum-cron` and press **Enter**. Then type `service yum start` and press **Enter**. Note that `yum-cron` will default to off if the machine is restarted.
5. To configure `yum-cron` to start at system startup, type `chkconfig yum-cron on` and press **Enter**.
6. In some instances, running Yum may cause a problem with AWMS. If that happens, a good first step is to use SSH to go into the AWMS server as root, and issue the following command:

```
# root; make
```

If that does not resolve the issue, please contact Dell support for further assistance.

This appendix describes the optional integration of third party security products for AWMS, as follows:

- “Bluesocket Integration” on page 305
- “ReefEdge Integration” on page 305
- “HP ProCurve 700wl Series Secure Access Controllers Integration” on page 306

Bluesocket Integration

A Bluesocket security scheme for AWMS has the following prerequisites:

- Bluesocket version 2.1 or higher
- AWMS version 1.8 or higher
- Completion of AMP Setup > RADIUS Accounting page

Bluesocket Configuration

Perform these steps to configure a Bluesocket security scheme:

1. Log in into the Bluesocket Server via HTTP with proper user credentials.
2. Navigate to the **Users > External Accounting Servers** page.
3. Select **External RADIUS Accounting** from the **Create** drop-down list.
4. Click **Enable server** onscreen.
5. Enter the user-definable **Name** for the AWMS server.
6. Enter the **Server IP Address** or **DNS entry** for AWMS.
7. Accept the default Port setting of 1813.
8. Enter the **Shared Secret** (matching the AWMS shared secret).
9. Enter Notes (optional).
10. Click the **Save** button.
11. If you are you using an External LDAP Server, ensure that the accounting records are forwarding to AWMS upon authentication.
12. Navigate to **Users > External Authentication Servers**.
13. Modify the LDAP server.
14. Ensure under the Accounting server matches the server entered in step 5.
15. Click the **Save** button.
16. To verify and view the log files on the Bluesocket server, proceed to **Status > Log**.
17. To verify and view the log files on AWMS, proceed to **SYSTEM > Event Log**.

ReefEdge Integration

A ReefEdge security scheme for AWMS has the following prerequisites:

- ReefEdge version 3.0.3 or higher

- AWMS version 1.5 or higher
- Completion of the AMP Setup > Radius Accounting page configurations, as described in [“Integrating a RADIUS Accounting Server” on page 65](#).

ReefEdge Configuration

Perform these steps to configure a ReefEdge security scheme:

1. Login into the ReefEdge ConnectServer via HTTP with the proper user credentials.
2. Navigate to the **Connect System > Accounting** page.
3. Click **Enable RADIUS Accounting**.
4. Enter the Primary Server IP Address or DNS entry for AWMS server.
5. Enter Primary Server Port Number 1813.
6. Enter the Shared Secret (matching the AWMS shared secret).
7. To verify and view the log files on the **Connect Server** proceed to **Monitor > System Log**.
8. To verify and view the log files on AWMS, proceed to **System > Event Log**.

HP ProCurve 700wl Series Secure Access Controllers Integration

A ProCurve security scheme for AWMS has the following prerequisites:

- HP 700 version 4.1.1.33 or higher
- AWMS version 3.0.4 or higher
- Completion of the **AMP Setup > Radius Accounting** page configurations, as described in [“Integrating a RADIUS Accounting Server” on page 65](#).

Example Network Configuration

In this example, the APs are connected to the Access Controller. The Access Controller routes wireless user traffic to the Employee Network, while bridging AP management traffic. Each AP is presumed to have a static IP address.

Perform these steps for HP ProCurve 700wl Series Configuration, allowing AWMS to manage APs through **Control** pages.

1. Log in to the Access Control Server via HTTP with proper credentials.
2. Navigate to **Rights > Identity Profiles**.
3. Select **Network Equipment**.
4. Enter the **Name**, **LAN MAC** and ensure the device is identified as an **Access Points in the Identity Profile** section for all access points in the network.

The Access Points Identity Profile is the default profile for network equipment. Enabling this option instructs the Access Controller to pass management traffic between the Access Points and the Customer's wired network.

HP ProCurve 700wl Series Configuration

This procedure enables the sending of client authentication information to AWMS. Perform the following steps to enable this configuration.

1. Login to the Access Control Server via HTTP with proper credentials.
2. Navigate to the **Rights > Authentication Policies** configuration page.
3. Select **Authentication Services**.
4. Select **New Services**.

5. Select **RADIUS**.
6. Enter **Name - Logical Name**.
7. Enter **Server - AWMS IP Address**.
8. Enter **Shared Secret**.
9. Enter **Port - 1812**.
10. Enter the **Shared Secret and Confirm** (matching the AWMS shared secret).
11. Enter **Reauthentication Field - Session Timeout**.
12. Enter **Timeout - 5**.
13. Select the **Enable RADIUS Accounting RFC-2866** check box.
14. Enter **Port - 1813** for RFC-2866.
15. To verify and view the log files on AWMS, proceed to **System > Event Log** page.

This appendix contains a few additional notes relevant to Cisco devices monitored by AWMS, and includes the following sections:

- “Resetting Cisco (VxWorks) Access Points” on page 309
- “Cisco IOS Dual Radio Template” on page 311
- “Speed Issues Related to Cisco IOS Firmware Upgrades” on page 312

Resetting Cisco (VxWorks) Access Points

When using any WLAN equipment, it may sometimes be necessary to recover a password and/or to restore the default settings on the equipment. Unlike other access points, the Cisco Aironet hardware and software sometimes do not permit password recovery. In these instances, you may need to first return the equipment to its default state, from which it can then be reconfigured.

For any Cisco VxWorks AP, regardless of the software version being used, you must first connect to the AP via the serial console and then perform the required steps to reset the unit.

Note that Cisco changed the procedure for resetting the AP configuration beginning with software version 11.07. The procedure below helps you determine which software version your AP(s) is currently running and which procedure to use to reset the AP.

Connecting to the AP

Perform these steps to return VxWorks Access Points to their default state and to reset the unit.

1. Connect the COM 1 or COM 2 port on your computer to the RS-232 port on the AP, using a straight-through cable with 9-pin-male to 9-pin-female connectors.
2. Open a terminal-emulation program on your computer.



Note: The instructions below assume that you are using Microsoft HyperTerminal; other terminal emulation programs are similar but may vary in certain minor respects.

3. Go to the Connection Description window, enter a name and select an icon for the connection, and click OK.
4. Go to the Connect To window field, and use the pull-down menu to select the port to which the cable is connected, then click OK.
5. In the Port Settings window, make the following settings:
 - Bits per second (baud): 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow Control: Xon/Xoff
6. Click OK.
7. Press Enter.

Determining the Boot-Block Version

The subsequent steps that you must follow to reset the Cisco AP depend on the version of the AP's boot-block. Follow the steps below to determine which boot-block version is currently on your AP, then use the corresponding instructions detailed below.

When you connect to the AP, the Summary Status screen appears. Reboot the AP by pressing CTRL-X or by unplugging and then re-plugging the power connector. As the AP reboots, introductory system information will appear onscreen.

The boot-block version appears in the third line of this text and is labeled Bootstrap Ver.

```
System ID: 00409625854D
Motherboard: MPC860 50MHz, 2048KB FLASH, 16384KB DRAM, Revision 20
Bootstrap Ver. 1.01: FLASH, CRC 4143E410 (OK)
Initialization: OK
```

Resetting the AP (for Boot-Block Versions from 1.02 to 11.06)

Follow these steps to reset your AP if the boot-block version on your AP is greater than or equal to version 1.02 but less than 11.07:

1. If you have not done so already, connect to the AP (see above), click OK, and press Enter.
2. When the Summary Status screen appears, reboot the AP by pressing CTRL-X or by unplugging and then re-plugging the power connector.
3. When the memory files are listed under the heading Memory: File, press CTRL-W within five seconds to reach the boot-block menu.
4. Copy the AP's installation key to the AP's DRAM by performing the following steps:
 - Press C to select Copy File.
 - Press 1 to select DRAM.
 - Press the selection letter for AP Installation Key.
5. Perform the following steps to reformat the AP's configuration memory bank:
 - Press CTRL-Z to reach the Reformat menu.
 - Press ! (SHIFT-1) to select FORMAT Memory Bank.
 - Press 2 to select Config.
 - Press upper-case Y (SHIFT-Y) to confirm the FORMAT command.
 - Press CTRL-Z to reach the reformat menu and to reformat the AP's configuration memory bank.
6. Copy the installation key back to the configuration memory bank as follows:
 - Press C to select Copy file
 - Press 2 to select Config.
 - Press the selection letter for AP Installation Key.
7. Perform the following steps to run the AP firmware:
 - Press R to select Run
 - Select the letter for the firmware file that is displayed.

The following message appears while the AP starts the firmware: *Inflating <firmware file name>*.
8. When the Express Setup screen appears, begin reconfiguring the AP using the terminal emulator or an Internet browser.

Resetting the AP (for Boot-Block Versions 11.07 and Higher)

Follow these steps to reset your AP if the boot-block version on your AP is greater than 11.07:

1. If you have not done so already, connect to the AP (see above), click OK, and press Enter.
2. When the Summary Status screen appears after you have connected to the AP, reboot the AP by unplugging and then re-plugging the power connector.
3. When the AP reboots and the Summary Status screen reappears, type `:resetall` and press Enter.
4. Type yes, and press Enter to confirm the command.



Note: The `:resetall` command is valid for only two minutes after the AP reboots. If you do not enter and confirm the `:resetall` command during that two minutes, reboot the AP again.

5. After the AP reboots and the Express Setup screen appears, reconfigure the AP by using the terminal emulator or an Internet browser.

Cisco IOS Dual Radio Template

A dual-radio Cisco IOS AP template is included as reference.

```
! Template created from Cisco Aironet 1240 IOS 12.3(11)JA1 'newName'
! at 2/12/2007 10:14 AM by user 'admin'
<ignore_and_do_not_push>ntp clock-period</ignore_and_do_not_push>

version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname %hostname%
enable secret 5 $1$ceH2$/1BN2DQpOoBAz/KI2opH7/
ip subnet-zero
ip domain name Aruba.com
ip name-server 10.2.24.13
no aaa new-model
dot11 ssid OpenSSID
    authentication open
power inline negotiation prestandard source
username newpassword password 7 05050318314D5D1A0E0A0516
username Cisco password 7 01300F175804
bridge irb
interface Dot11Radio0
    %enabled%
    no ip address
    no ip route-cache
    ssid OpenSSID
    speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
    channel %channel%
    station-role root
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
    bridge-group 1 spanning-disabled
%if interface=Dot11Radio1%
interface Dot11Radio1
    no ip address
```

```

no ip route-cache
%enabled%
ssid OpenSSID
dfs band 3 block
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
channel %channel%
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
%endif%
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
interface BVI1
%if ip=dhcp%
ip address dhcp client-id FastEthernet0
%endif%
%if ip=static%
ip address %ip_address% %netmask%
%endif%
no ip route-cache
%if ip=static%
ip default-gateway %gateway%
%endif%
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
access-list 111 permit tcp any any neq telnet
snmp-server view iso iso included
snmp-server community public view iso RW
control-plane
bridge 1 route ip
line con 0
line vty 0 4
login local
end

```

Speed Issues Related to Cisco IOS Firmware Upgrades

AWMS provides a very robust method of upgrading firmware on access points. To ensure that firmware is upgraded correctly AWMS adds a few additional steps which are not included in vendor-supplied management software.

AWMS Firmware Upgrade Process

1. AWMS reads the firmware version on the AP to ensure the firmware to which the AP is upgrading is greater than the actual firmware version currently running on the AP.
2. AWMS configures the AP to initiate the firmware download from AWMS

3. AWMS monitors itself and the AP during the file transfer.
4. After a reboot is detected, AWMS verifies the firmware was applied correctly and all AP configuration settings match those in the AWMS database
5. AWMS pushes the configuration if necessary to restore the desired configuration. Some firmware upgrades reconfigure settings.

Cisco IOS access points take longer than most access points, because their firmware is larger.

The Support Connection Manager establishes a secure point-to-point connection between the customer AWMS and AirWave's support organization. Using this secure connection, AirWave support engineers can remotely diagnose problems or upgrade software without breaching security and exposing AWMS to the Internet.

This appendix includes the following sections:

- “Network Requirements” on page 315
- “Procedure” on page 315

Network Requirements

The AWMS Support Connection initiates a TCP connection on port 23 to AirWave's support server. Please ensure your firewall allows this. The connection can be configured to run on 22,80,443 and a few other ports if necessary. Please contact Dell support if you need to make any changes.



Caution: Initiating the support connection will create a point to point tunnel between AWMS and a support server at AirWave.

Procedure

Perform these steps to initiate a support connection for AWMS:

1. Sign into the serial or regular console with your root login.
2. Type `service support_connection start` at the command line interface.
3. Type `service support_connection status` to verify that the connection is running properly.
4. To end the connection to support, type `service support_connection stop` at the command line interface.

If you have any questions, please contact Dell support.

This appendix includes the following sections:

- “Prerequisites for Integrating AWMS with Cisco Clean Access” on page 317
- “Adding AWMS as RADIUS Accounting Server” on page 317
- “Configuring Data in Accounting Packets” on page 317

Prerequisites for Integrating AWMS with Cisco Clean Access

- Run Clean Access Software 3.5 or higher
- Run AWMS version 3.4.0 or higher
- Complete of the AMP SETUP > RADIUS Accounting section on AMP

Adding AWMS as RADIUS Accounting Server

Perform these steps to configure Cisco Clean Access integration:

1. Log in to the clean machine server and navigate to the **User Management > Accounting > Server Config** page.
 - Select **Enable RADIUS Accounting**.
 - Input the **AWMS Hostname or IP Address**.
 - For **Timeout (sec)** - leave default 30.
 - Ensure the **Server Port** is set for 1813.
 - Ensure that the input **Shared Secret** matches the AWMS shared secret.
2. Select **Update** button to save.

Configuring Data in Accounting Packets

1. Navigate to **User Management > Accounting > Shared Events**.
2. Map the following attributes to corresponding data elements as seen in the graphic:

```
Framed_IP_Address = "User IP"  
User_Name = "LocalUser"  
Calling_Station_ID = "User MAC"
```



Note: These attribute element pairs are mandatory for username display within AWMS.

To install HP/Compaq Insight Manager on the AWMS, perform the following steps:

1. Use SCP to move the two files over to the server:

```
hpasm-7.8.0-88.rhel4.i386.rpm <- This is the actual HP agents  
hpsmh-2.1.9-178.linux.i386.rpm <- This is the HP web portal to the agents
```
2. Type `rpm -i hpasm-7.8.0-88.rhel4.i386.rpm` at the command line interface.
3. Type `hpasm activate` at the command line interface.
Take the default values. You will need the SNMP RW and RO strings at this point.
4. Type `rpm -i --nopre hpsmh-2.1.9-178.linux.i386.rpm` at the command line interface. The `nopre` syntax component is required to keep the rpm from producing errors on CentOS, as opposed to Red Hat. This rpm *must* be run after the hpasm rpm, because the pre-install scripts in the hpsmh rpm are not being run.
5. Type `perl /usr/local/hp/hpSMHSetup.pl` at the command line interface.
This configures the web server.
Configure the **Add Group > Administrator** page with a name '0'.
Enable IP Binding—type `1` at the command line interface.
At the next interface enter the IP address and mask of the server.
6. Type `/etc/init.d/hpasm reconfigure` at the command line interface.
When going through this menu this time, select 'y' to use the existing snmpd.conf.
7. Type `vi /etc/snmp/snmpd.conf` at the command line interface.
Change the following two lines:

```
rwcommunity xxxstringxxx 127.0.0.1  
rocommunity xxxstringxxx 127.0.0.1
```


Change these lines to read as follows:

```
rwcommunity xxxstringxxx  
rocommunity xxxstringxxx
```
8. Type `service snmpd restart` at the command line interface.
9. Type `user add xxusernamexx` at the command line interface.
10. Type `passwd xxusernamexx` at the command line interface and enter a password for the user.
11. Type `vi /etc/passwd` at the command line interface.
Scroll to the bottom of the list and change the new users UID and GroupID to 0 (fourth and fifth column).
12. Connect to the server using `https://xxx.xxx.xxx.xxx:2381` and the username and password that you created in steps 9 and 10.

This appendix provides complete instructions for installing AWMS on VMware ESX (3i v. 3.5) and includes the following sections:

- “Creating a New Virtual Machine to Run AWMS” on page 321
- “Installing AWMS on the Virtual Machine” on page 321
- “AWMS Post-Installation Issues on VMware” on page 322

Creating a New Virtual Machine to Run AWMS

1. Click **Create a new virtual machine** from the VMware Infrastructure Client.
2. Click **Next** to select a **Typical > Virtual Machine Configuration**.
3. Name your virtual machine (AirWave Management Platform) and then click **Next**.
4. Select an available datastore with sufficient space for the number of APs your AWMS will manage, choosing the right server hardware to comply with the hardware requirements in this document. Click **Next**.
5. Click the **Linux** radio button and select **Red Hat Enterprise Linux 5 (32-bit)** from the drop-down menu, then click **Next**.
6. Select a minimum of two virtual processors, then click **Next**.
7. Enter **3072** as the minimum virtual RAM (more virtual RAM may be required; refer to the section “Choosing the Right Server Hardware” for a table listing RAM requirements for AWMS). Click **Next**.
8. Accept the VMware default virtual network adapter and click **Next**.
9. Allocate a virtual disk large enough to contain the AWMS operating system, application and data files (refer to the AWMS Best Practices Guide for suggested disk space allocations for typical wireless network deployments).
10. Click **Next**.
11. Review the virtual machine settings, then click **Finish** when done.

Installing AWMS on the Virtual Machine

Running AWMS installation on a VMware virtual machine is typically done in one of three ways:

1. By writing an AWMS ISO to CD, inserting the CD into a physical drive on a VMware server, then configure the AWMS virtual machine to boot from the CD.
2. By copying the AWMS ISO to the VMware server's datastore, or to a networked filesystem available to the VMware server, then configure the AWMS virtual machine to boot from the ISO file.
3. By using either a local physical CD or an AWMS ISO file from the VMware Infrastructure Client, then create a virtual CD on the virtual AWMS to point to and boot from that device.

Overall, the second option is likely the most efficient method to install AWMS. In addition, after booting the AWMS virtual machine with either a physical CD or a ISO image file, the installation process with this method is identical to the steps outlined in the *AirWave Wireless Management Suite Quick Start Guide*.

AWMS Post-Installation Issues on VMware

By default, AWMS runs the Linux 'smartd' service for detecting physical disk errors using the S.M.A.R.T. protocol. However, virtual disks do not support the S.M.A.R.T. protocol, so the AWMS smartd service will fail at startup.

The service can be prevented from starting at boot by running the following commands at the AWMS command line. Note that the first command prevents the service from starting, the last two commands remove the smartd service from the list of services to shutdown during a reboot or a complete system shutdown.

```
mv /etc/rc.d/rc3.d/S40smartd /etc/rc.d/rc3.d/Z40smartd
mv /etc/rc.d/rc0.d/K40smartd /etc/rc.d/rc3.d/Z40smartd
mv /etc/rc.d/rc6.d/K40smartd /etc/rc.d/rc3.d/Z40smartd
```

To install VMware Tools on AWMS, perform these steps:

1. From the VMware Infrastructure Client, select **Inventory > Virtual Machine > Install/Upgrade VMware Tools**.
2. At the AWMS console type `mkdir /media/cdrom`.
3. Then type `mount /dev/cdrom /media/cdrom`.
4. Next, type `cd /tmp/; tar -xvzf /media/cdrom/VMwareTools-3.5.0-67921.tar.gz\`.

The VMware Tools filename may be different, depending on the version of VMware installed.



Note: Desktop environments such as X Windows, GNOME, and KDE, that you will need to use for VMware tools installation will no longer work once you have AWMS installed.

5. Run the VMware Tools setup and install script by typing the following statement: `/tmp/vmware-toolsdistrib/vmware-install.pl`.
6. During the text-based VMware Tools install, select all default options.
7. Reboot the virtual machine once the VMware Tools install is complete.

contains some software provided by third parties (both commercial and open-source licenses).

Source code to third-party open-source packages are available on AirWave's website and by request:

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Google Earth and the Google Earth icon are the property of Google.

Packages

Net:IP:

Copyright (c) 1999 - 2002 RIPE NCC

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Net-SNMP:

---- Part 1: CMU/UCD copyright notice: (BSD like) ----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR

PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) ----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) ----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) ----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) ----

Copyright (c) 2003-2004, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) ----

Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Crypt::DES perl module (used by Net::SNMP):

Copyright (C) 1995, 1996 Systemics Ltd (<http://www.systemics.com/>)

All rights reserved.

This library and applications are FREE FOR COMMERCIAL AND NON-COMMERCIAL USE as long as the following conditions are adhered to.

Copyright remains with Systemics Ltd, and as such any Copyright notices in the code are not to be removed. If this code is used in a product, Systemics should be given attribution as the author of the parts used. This can be

in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Systemics Ltd

(<http://www.systemics.com/>)

THIS SOFTWARE IS PROVIDED BY SYSTEMICS LTD "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Perl-Net-IP:

Copyright (c) 1999 - 2002 RIPE NCC

All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS; IN NO EVENT SHALL AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Berkeley DB 1.85:

Copyright (c) 1987, 1988, 1990, 1991, 1992, 1993, 1994, 1996, 1997, 1998 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SWFObject v. 1.5:

Flash Player detection and embed - <http://blog.deconcept.com/swfobject/>

SWFObject is (c) 2007 Geoff Stearns and is released under the MIT License

mod_auth_tacacs - TACACS+ authentication module:

Copyright (c) 1998-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>)."
4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the Apache Group
for use in the Apache HTTP server project (<http://www.apache.org/>)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS" AND ANY EXPRESSED OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS
BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSS

A	
AAA servers	98
access control lists.....	118
access points	
adding with CSV file.....	139
ACLs.....	118
ACS	
integrating	71
servers	71
AirWave Management Platform.....	13
Alcatel.....	175
alerts	
viewing	226
warning behavior, setting.....	38
B	
backups.....	256
C	
CDP, enabling for device discovery	134
Cisco	
configuring IOS templates	182, 186
Cisco Catalyst Switches.....	175
Cisco Discovery Protocol	
see CDP	134
Cisco IOS	175
Cisco WLC	88
Cisco WLSE	
configuring	66
Colubris	56
CSV File.....	139
customer support, contacting	12
D	
dashboard	
customizing display	36
date and time	
configuring	18
devices	127
adding discovered devices to groups.....	134
adding manually	136
communication settings	53
discovering, managing, and troubleshooting ...	127
modifying	122
troubleshooting a newly discovered device	172
verifying	142, 156
F	
failover.....	15
firewall	
configuring.....	21
firmware	
loading device firmware	58
specifying minimum firmware.....	119
G	
global templates	191
groups	
assigning newly discovered devices to groups	134
changing multiple group configurations.....	121
configuring and using	79
configuring basic group settings	83
configuring group AAA servers.....	98
configuring group SSIDs and VLANs.....	94
configuring group templates	175
configuring PTMP/WiMAX settings	112
configuring radio settings.....	100
configuring security settings	91
deleting a group	121
global groups.....	125
MAC access control lists.....	118
overview	80
viewing.....	81
H	
Helpdesk	295
creating a new incident	297
creating snapshots and incident relationships.	298
monitoring incidents.....	296
using with remedy server	299
Hirschmann.....	175
host name	
assigning host name	20
HP ProCurve.....	88, 102, 175

I	
incidents	
creating	297
installation	
checking.....	19
IP address	
adding and assigning.....	19
iPhone	239
L	
Lancom.....	175
Linux CentOS 5	
installing.....	17
M	
MAC access control lists.....	118
Master Console	239
Master Console and Failover.....	15
N	
navigation	
understanding the UI	31
Network integration	15
network settings	
defining	47
NMS	73, 74
Nomdix	175
P	
pagination records	
setting, resetting	34
pagination widget, using	34
password	
changing default root.....	21
PCI Compliance	
Default Credential Compliance.....	77
PCI Requirements.....	75
product overview	
additional interfaces and tools.....	213
changing default root password	21
checking installation	19
configuring date and time	18
configuring mesh radio settings	116
defining a scan.....	130
executing a scan.....	131
getting started with	29
hardware requirements.....	17
initial login	29
installing.....	17, 21
naming the network administration system	20
Package Management.....	303
protocol and port diagram	21
Proxim 4900.....	104
Proxim/Avaya.....	88
PTMP	112
R	
radio settings	
configuring for groups	100
RADIUS	98
adding a server.....	98
authentication.....	62
configuring authentication and authorization	64
integrating.....	65
RAPIDS	25, 195
RAPIDs.....	14
reports.....	261
creating, running, and emailing	261
defining custom reports	289
rogue classification	195
rogue devices	
configuring WLSE scanning	66
WLSE rogue scanning	66
root password.....	21
routers and switches	
adding with a CSV file	139
S	
scanning	
defining credentials	129
security	
auditing PCI compliance	74
configuring ACS servers.....	71
configuring group security settings.....	91
configuring group SSIDs and VLANs	94
configuring RADIUS	62
configuring TACACS+	62
integrating NMS.....	73
RAPIDS and rogue classification.....	195
using triggers and alerts.....	213
servers	
specifying general settings.....	39
Smarthost	292
SNMP	
polling period.....	85
SSIDs	94
Symbol.....	105, 175

Symbol/Intel 89

T

TACACS+ 98
 adding a server 98
 configuring authentication 62
 integrating 62

templates 177
 adding 179, 191
 configuring a global template 191
 configuring Cisco IOS templates 186
 configuring for groups 175
 global template variables 192
 variables 192

Trapeze 175

U

UI
 understanding the navigation bar 31

user interface

AMP Setup 25
APs/Devices 24
 APs/Devices > Audit 156
 APs/Devices > Ignored 142
 APs/Devices > List 143
 APs/Devices > Manage 173
 APs/Devices > New 135
Authentication Dialog Box 29
Buttons and Icons 27
Configuration Change Confirmation 121
Device Setup > Add 140
Device Setup > Communication 54, 55, 56, 57
Device Setup > Discover 129, 132
Device Setup > Firmware Files 58
flash graphs 35, 36, 37, 38
Group SNMP Polling Period 85
Groups 24
 Groups > Basic 84, 85, 86, 87, 88, 89, 125
 Groups > Firmware 119
 Groups > List 81
 Groups > MAC ACL 118
 Groups > PTMP/WiMAX 112, 113, 114, 115
 Groups > Radio 100
 Groups > Templates 177, 179, 191, 192
Help 26
Helpdesk > Incident 299
Helpdesk > Incidents 296, 300
Helpdesk > Setup 299
Home 24, 241
 Home > Documentation 247
 Home > License 245
 Home > Overview 242
 Home > Search 246
 Home > User Info 248
Home Overview 35, 36, 37, 38

Master Console 239
Master Console > Groups > Basic 240, 241
Master Console > Groups > Basic, Managed .. 240
Master Console > Manage AMPs, IP/Hostname239
RAPIDS 25
RAPIDS > Rogue APs (Detail), Score Override 211
Reports 25
Reports > Definitions 264, 289
Reports > Generated > Port Utilization Report 283
sections
 Activity section 25
 Navigation section 23
 Status section 23
Setup > General 40
Setup > NMS 73, 74
Setup > Users 49
System 25, 249
System > Alerts 227
System > Backups 257
System > Configuration Change Jobs 253
System > Event Logs 252
System > Performance 254
System > Status 251
System > Status Log 252
System > Trigger Detail 214
System > Triggers 214
Triggers and Alerts 213
Users 24
Users > Connected 229
Users > Guest Users 232
Users > Tags 233
View AP Credentials 173
VisualRF 25

user roles

 creating 50

users

 creating 48

V

VisualRF 14, 25

VLANs 94

W

WiMAX 112

Wireless LAN

 components 15

WLSE

 configuring 66

WLSE rogue scanning 66

