AirWave 7.7

ARUBA networks

User Guide

Copyright

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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved.This product includes software developed by Lars Fenneberg et al. 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.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

Chapter 1
Introduction

Thank you for choosing AirWave 7.7. AirWave makes it easy and efficient to manage your wireless network by combining industry-leading functionality with an intuitive user interface, enabling network administrators and helpdesk staff to support and control even the largest wireless networks in the world.

The User Guide provides instructions for the configuration and operation of AirWave. This section includes the following topics:

- "A Unified Wireless Network Command Center" on page 13
- "Integrating AMP into the Network and Organizational Hierarchy " on page 15

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

NOTE

Refer to the *AirWave 7.7 Installation Guide* for information on installing and upgrading AirWave.

A Unified Wireless Network Command Center

AirWave 7.7 is the only network management software that offers you a single intelligent console from which to monitor, analyze, and configure wireless networks in automatic fashion. Whether your wireless network is simple or a large, complex, multi-vendor installation, AirWave manages it all.

AirWave supports hardware from leading wireless vendors including the following:

- Aruba Networks®
- Avaya™
- Cisco® (Aironet and WLC)
- Dell PowerConnect™ W-Series
- Enterasys®
- Juniper Networks®
- LANCOM Systems
- Meru Networks®
- Nortel Networks™
- ProCurve™ by HP®
- Proxim®
- Symbol™
- Trapeze™
- Tropos™

and many others.

The components of AirWave are described in the next section.

AirWave Management Platform

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

- Core network management functionality:
  - Network discovery
  - Configuration of APs & controllers

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

Controller Configuration

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

AirWave consolidates and pushes global controller configurations from within AMP.

Two pages in AirWave support controller configuration:

- **Device Setup > Aruba Configuration** for global Aruba Configuration. This page is available if Use Global Aruba Configuration is set to Yes in **AMP Setup > General**.
- **Groups > Controller Config** for group-level configuration.

For additional information that includes a comprehensive inventory of all pages and settings that support Aruba Configuration, refer to the *AirWave 7.7 Controller Configuration Guide*.

Switch Configuration

AirWave supports group-level configuration of an Aruba Mobility Access Switch (MAS), the operating system, software suite, and application engine that operates mobility and centralizes control over the entire network environment. For a complete description of ArubaOS, refer to the *ArubaOS User Guide* for your specific Aruba Mobility Access Switch version.

AirWave consolidates and pushes group switch configurations from within AirWave using the **Groups > Switch Config** page. This page is available if Use Global Aruba Configuration is set to No in **AMP Setup > General**.

For additional information that includes a comprehensive inventory of all pages and settings that support Switch Configuration, refer to the *AirWave 7.7Switch Configuration Guide* available at support.arubanetworks.com.

VisualRF

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

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

- Planning of new floor plans and AP placement recommendations

RAPIDS

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

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

Master Console and Failover

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

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

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

Integrating AMP into the Network and Organizational Hierarchy

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

The power, performance, and usability of AMP become more apparent when considering the diverse components within a WLAN. Table 1 itemizes some example network components.

Table 1: *Components of a WLAN*

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

Administrative Roles

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

- A Help Desk user can be given read-only access to monitoring data without being permitted to make configuration changes.
- A U.S.-based network engineer can 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 can be given read-write access to configure security policies across the entire WLAN.
- NOC personnel can be given read-only access to monitoring all devices from the Master Console.

Chapter 2
Configuring AMP

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

- "Formatting the Top Header" on page 17
- "Customizing Columns in Lists" on page 19
- "Resetting Pagination Records" on page 20
- "Using the Pagination Widget" on page 21
- "Using Export CSV for Lists and Reports" on page 21
- "Defining Graph Display Preferences" on page 21
- "Customizing the Dashboard" on page 22
- "Setting Severe Alert Warning Behavior" on page 27
- "Defining General AMP Server Settings" on page 28
- "Defining AMP Network Settings" on page 39
- "Creating AMP User Roles" on page 43
- "Creating AMP Users" on page 41
- "Configuring Login Message, TACACS+, RADIUS, and LDAP Authentication" on page 48
- "Enabling AMP to Manage Your Devices" on page 56
- "Setting Up Device Types" on page 63
- "Configuring Cisco WLSE and WLSE Rogue Scanning" on page 64
- "Configuring ACS Servers" on page 68
- "Integrating AMP with an Existing Network Management Solution (NMS) " on page 70
- "Auditing PCI Compliance on the Network" on page 71
- "Deploying WMS Offload" on page 75

NOTE

Additional configurations are available after basic configuration is complete.

Before You Begin

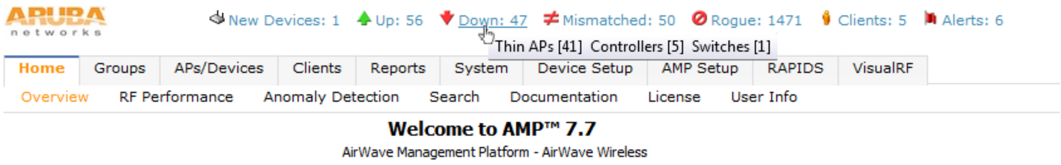
Remember to complete the required configurations in this chapter before proceeding. Aruba support remains available to you for any phase of AirWave installation.

Formatting the Top Header

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

A row of statistics hyperlinks called Top Header Stats above the tabs represents commonly used subtabs. These hyperlinks provide the ability to view certain key statistics by mousing over, such as number and type of **Down** devices, and serve as shortcuts to frequently viewed subtabs. Figure 1 illustrates the navigation bar. More information on hyperlinks, tabs, and subtabs is a available in the *AirWave 7.7 Installation Guide*.

Figure 1 *Navigation Bar Displaying Down Device Statistics*



You can control the **Top Header Stats** links that appear from the **AMP Setup** > **General** page, as described in "Defining General AMP Server Settings" on page 28. Top Header Stats can also be customized for individual users on the **Home** > **User Info** page. There you can select the statistics to display for certain device types and override the AMP Setup page.

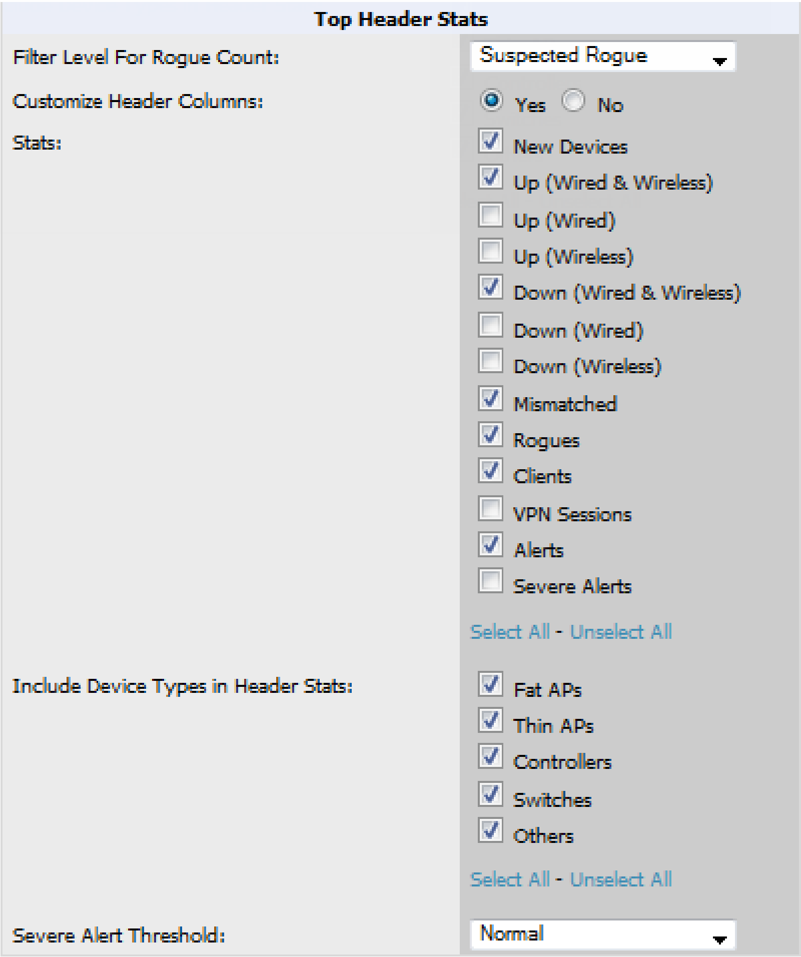
All possible display options for users are show in Figure 2.

NOTE

A confirmation message does not appear when you make modifications to the Top Header Stats.

Refer to "Configuring Your Own User Information with the Home > User Info Page" on page 263 for more information.

Figure 2 *Home > User Info Top Header Stats Display Options*



Top Header Stats

Filter Level For Rogue Count: Suspected Rogue

Customize Header Columns: ● Yes ○ No

Stats:
- ☑ New Devices
- ☑ Up (Wired & Wireless)
- □ Up (Wired)
- □ Up (Wireless)
- ☑ Down (Wired & Wireless)
- □ Down (Wired)
- □ Down (Wireless)
- ☑ Mismatched
- ☑ Rogues
- ☑ Clients
- □ VPN Sessions
- ☑ Alerts
- □ Severe Alerts

Select All - Unselect All

Include Device Types in Header Stats:
- ☑ Fat APs
- ☑ Thin APs
- ☑ Controllers
- ☑ Switches
- ☑ Others

Select All - Unselect All

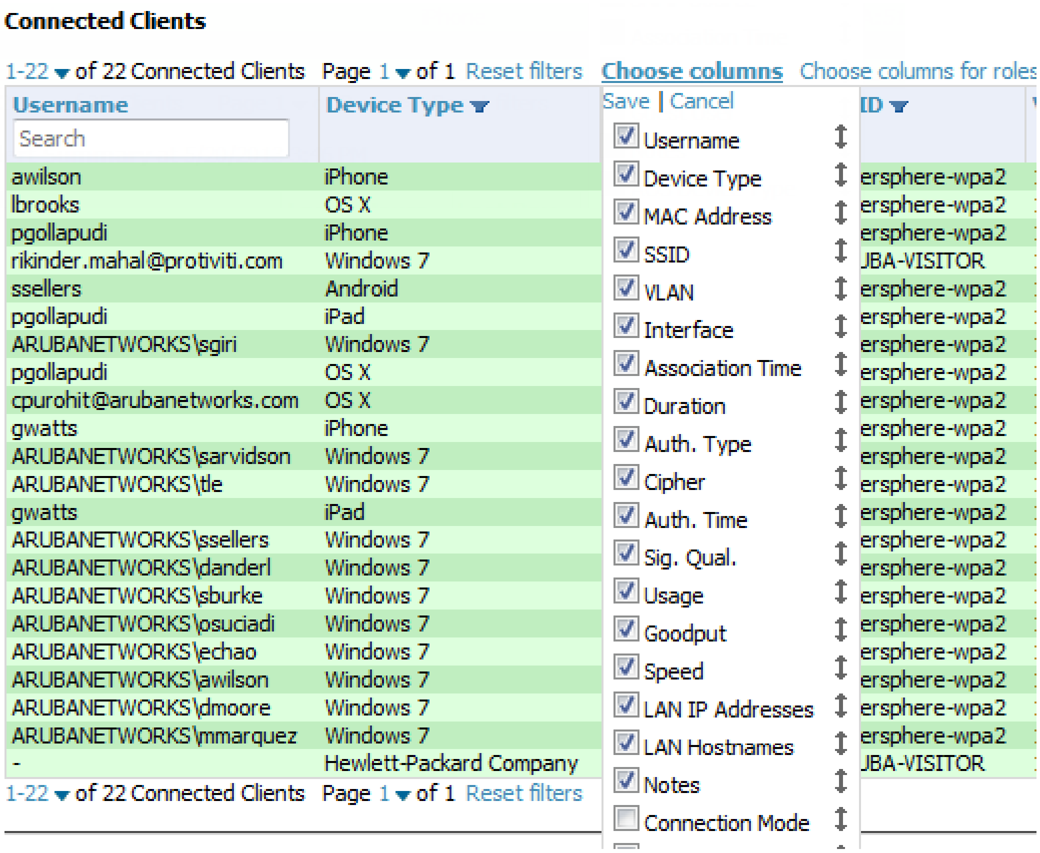
Severe Alert Threshold: Normal

You can also set the severity level of critical alerts displayed for a user role. For details including a description of what constitutes a severe alert, see "Setting Severe Alert Warning Behavior" on page 27.

Customizing Columns in Lists

Customize the columns for any list table selecting **Choose Columns**, as shown in the figure below. Use the up/down arrows to change the order in which the column heads appear.

Figure 3 ***Choose Columns*** *Drop down List*



Connected Clients

1-22 ▾ of 22 Connected Clients Page 1 ▾ of 1 Reset filters **Choose columns** Choose columns for roles

Username	Device Type ▾	ID ▾
Search		
awilson	iPhone	ersphere-wpa2
lbrooks	OS X	ersphere-wpa2
pgollapudi	iPhone	ersphere-wpa2
rikinder.mahal@protiviti.com	Windows 7	JBA-VISITOR
ssellers	Android	ersphere-wpa2
pgollapudi	iPad	ersphere-wpa2
ARUBANETWORKS\sgiri	Windows 7	ersphere-wpa2
pgollapudi	OS X	ersphere-wpa2
cpurohit@arubanetworks.com	OS X	ersphere-wpa2
gwatts	iPhone	ersphere-wpa2
ARUBANETWORKS\sarvidson	Windows 7	ersphere-wpa2
ARUBANETWORKS\tle	Windows 7	ersphere-wpa2
gwatts	iPad	ersphere-wpa2
ARUBANETWORKS\ssellers	Windows 7	ersphere-wpa2
ARUBANETWORKS\danderl	Windows 7	ersphere-wpa2
ARUBANETWORKS\sburke	Windows 7	ersphere-wpa2
ARUBANETWORKS\psuciadi	Windows 7	ersphere-wpa2
ARUBANETWORKS\echao	Windows 7	ersphere-wpa2
ARUBANETWORKS\awilson	Windows 7	ersphere-wpa2
ARUBANETWORKS\dmoore	Windows 7	ersphere-wpa2
ARUBANETWORKS\mmarquez	Windows 7	ersphere-wpa2
-	Hewlett-Packard Company	JBA-VISITOR

1-22 ▾ of 22 Connected Clients Page 1 ▾ of 1 Reset filters

Save | Cancel

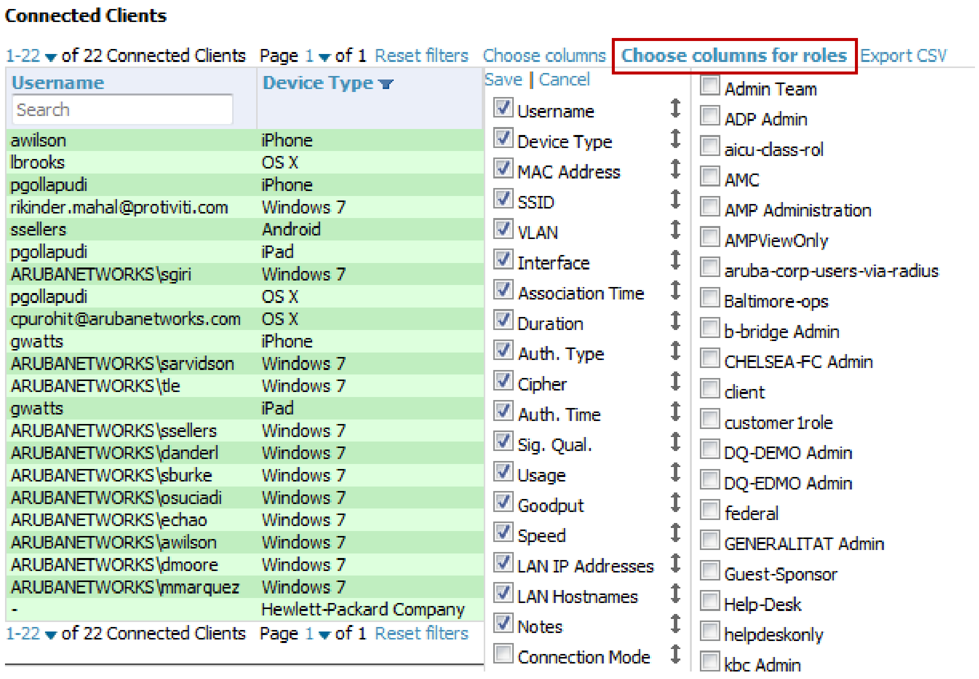
- ☑ Username ↕
- ☑ Device Type ↕
- ☑ MAC Address ↕
- ☑ SSID ↕
- ☑ VLAN ↕
- ☑ Interface ↕
- ☑ Association Time ↕
- ☑ Duration ↕
- ☑ Auth. Type ↕
- ☑ Cipher ↕
- ☑ Auth. Time ↕
- ☑ Sig. Qual. ↕
- ☑ Usage ↕
- ☑ Goodput ↕
- ☑ Speed ↕
- ☑ LAN IP Addresses ↕
- ☑ LAN Hostnames ↕
- ☑ Notes ↕
- □ Connection Mode ↕

More information about the universal list elements is available in "Common List Settings" in the *AirWave 7.7 Installation Guide.*

You can also control which column heads appear for each user role. Navigate to the **Home > User Info** page, and then select **Yes** in the **Customize Columns for Other Roles** field. This exposes the **Choose Columns for Roles** drop down menu in all tables shown in Figure 4.

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

Figure 4 *Table with Choose Columns for Roles Menu Selected*



Connected Clients

1-22 ▾ of 22 Connected Clients Page 1 ▾ of 1 Reset filters Choose columns **Choose columns for roles** Export CSV

Username	Device Type ▾
Search	
awilson	iPhone
lbrooks	OS X
pgollapudi	iPhone
rikinder.mahal@protiviti.com	Windows 7
ssellers	Android
pgollapudi	iPad
ARUBANETWORKS\sgiri	Windows 7
pgollapudi	OS X
cpurohit@arubanetworks.com	OS X
gwatts	iPhone
ARUBANETWORKS\sarvidson	Windows 7
ARUBANETWORKS\tle	Windows 7
gwatts	iPad
ARUBANETWORKS\ssellers	Windows 7
ARUBANETWORKS\danderl	Windows 7
ARUBANETWORKS\sburke	Windows 7
ARUBANETWORKS\osuciadi	Windows 7
ARUBANETWORKS\echao	Windows 7
ARUBANETWORKS\awilson	Windows 7
ARUBANETWORKS\dmoore	Windows 7
ARUBANETWORKS\mmarquez	Windows 7
-	Hewlett-Packard Company

1-22 ▾ of 22 Connected Clients Page 1 ▾ of 1 Reset filters

Save | Cancel

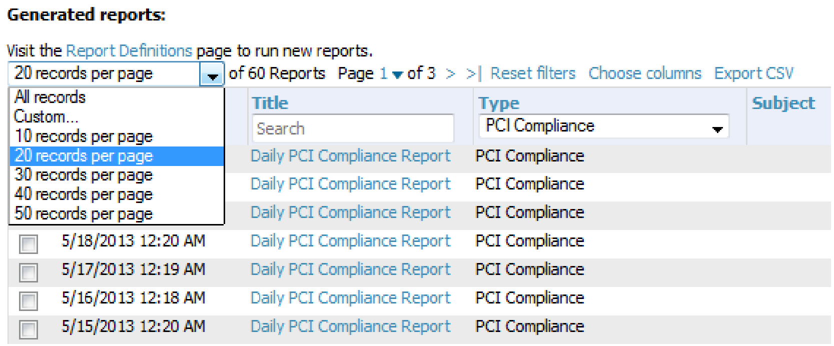
- ☑ Username
- ☑ Device Type
- ☑ MAC Address
- ☑ SSID
- ☑ VLAN
- ☑ Interface
- ☑ Association Time
- ☑ Duration
- ☑ Auth. Type
- ☑ Cipher
- ☑ Auth. Time
- ☑ Sig. Qual.
- ☑ Usage
- ☑ Goodput
- ☑ Speed
- ☑ LAN IP Addresses
- ☑ LAN Hostnames
- ☑ Notes
- ☐ Connection Mode

- ☐ Admin Team
- ☐ ADP Admin
- ☐ aicu-class-rol
- ☐ AMC
- ☐ AMP Administration
- ☐ AMPViewOnly
- ☐ aruba-corp-users-via-radius
- ☐ Baltimore-ops
- ☐ b-bridge Admin
- ☐ CHELSEA-FC Admin
- ☐ client
- ☐ customer1role
- ☐ DQ-DEMO Admin
- ☐ DQ-EDMO Admin
- ☐ federal
- ☐ GENERALITAT Admin
- ☐ Guest-Sponsor
- ☐ Help-Desk
- ☐ helpdeskonly
- ☐ kbc Admin

Resetting Pagination Records

To control the number of records in any individual list, select the link with **Records Per Page** mouseover text at the top left of the table, as shown in Figure 5. AMP remembers each list's pagination preferences.

Figure 5 *Records Per Page Drop Down Menu*



Generated reports:

Visit the Report Definitions page to run new reports.

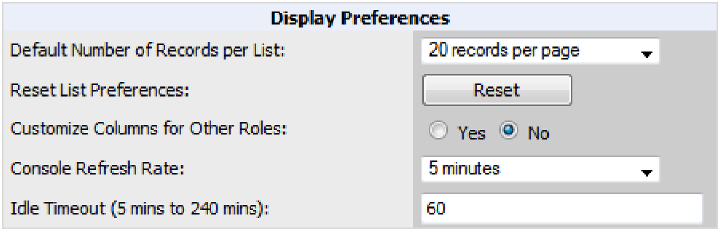
20 records per page ▾ of 60 Reports Page 1 ▾ of 3 > >| Reset filters Choose columns Export CSV

- All records
- Custom...
- 10 records per page
- 20 records per page
- 30 records per page
- 40 records per page
- 50 records per page

		Title	Type	Subject
		Search	PCI Compliance ▾	
		Daily PCI Compliance Report	PCI Compliance	
		Daily PCI Compliance Report	PCI Compliance	
		Daily PCI Compliance Report	PCI Compliance	
☐	5/18/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance	
☐	5/17/2013 12:19 AM	Daily PCI Compliance Report	PCI Compliance	
☐	5/16/2013 12:18 AM	Daily PCI Compliance Report	PCI Compliance	
☐	5/15/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance	

To reset all Records Per Page preferences, click the **Reset** reset button in the **Display Preferences** section of the **Home** > **User Info** page, as shown in Figure 6.

Figure 6 *Home > User Info > Display Preferences section*



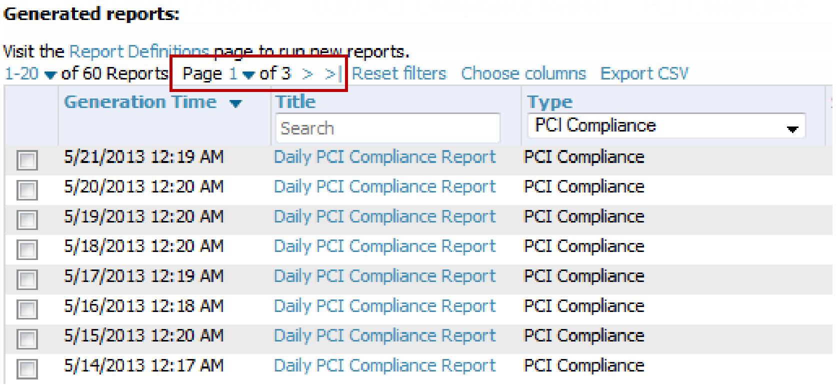
Display Preferences

Default Number of Records per List:	20 records per page ▾
Reset List Preferences:	Reset
Customize Columns for Other Roles:	○ Yes ● No
Console Refresh Rate:	5 minutes ▾
Idle Timeout (5 mins to 240 mins):	60

Using the Pagination Widget

The pagination widget is located at the top and bottom of every list table, as shown in Figure 7.

Figure 7 *Pagination Widget*



Generated reports:

Visit the Report Definitions page to run new reports.

1-20 ▾ of 60 Reports Page 1 ▾ of 3 > >| Reset filters Choose columns Export CSV

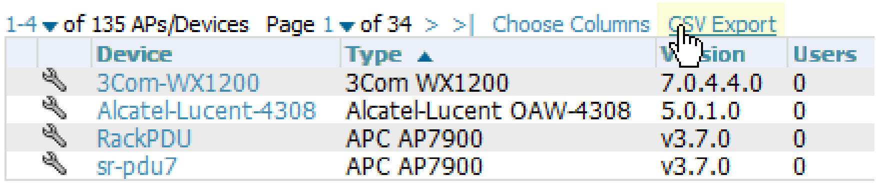
	Generation Time ▾	Title	Type
		Search	PCI Compliance ▾
□	5/21/2013 12:19 AM	Daily PCI Compliance Report	PCI Compliance
□	5/20/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance
□	5/19/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance
□	5/18/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance
□	5/17/2013 12:19 AM	Daily PCI Compliance Report	PCI Compliance
□	5/16/2013 12:18 AM	Daily PCI Compliance Report	PCI Compliance
□	5/15/2013 12:20 AM	Daily PCI Compliance Report	PCI Compliance
□	5/14/2013 12:17 AM	Daily PCI Compliance Report	PCI Compliance

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

Using Export CSV for Lists and Reports

Some tables have a **Export CSV** setting you can use export the data as a spreadsheet. See Figure 8 for an example of a list with the **Export CSV** option selected.

Figure 8 *List with CSV Export Selected*



1-4 ▾ of 135 APs/Devices Page 1 ▾ of 34 > >| Choose Columns CSV Export

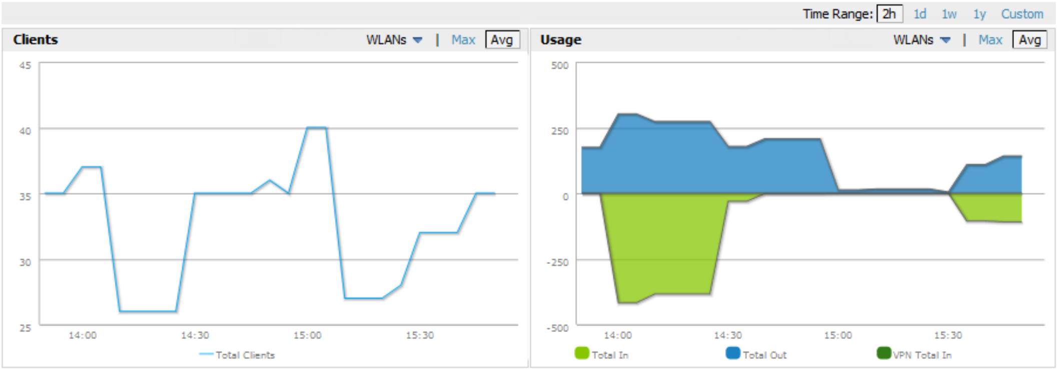
	Device	Type ▲	Version	Users
🔧	3Com-WX1200	3Com WX1200	7.0.4.4.0	0
🔧	Alcatel-Lucent-4308	Alcatel-Lucent OAW-4308	5.0.1.0	0
🔧	RackPDU	APC AP7900	v3.7.0	0
🔧	sr-pdu7	APC AP7900	v3.7.0	0

AMP also enables CSV exporting of all report types. For more information, see "Exporting Reports to XML, CSV, or PDF" on page 313.

Defining Graph Display Preferences

Many of the graphs in AMP are Highcharts, which allow you to adjust the graph settings attributes as shown in Figure 9.

Figure 9 *Interactive Graphs on the* ***Home > Overview*** *Page*



Highcharts are built with JavaScript, so the graphs can run directly through your browser without the need for additional client-side plugins. This makes it possible to view your AirWave charts on a mobile device.

These charts can be used and customized as follows.

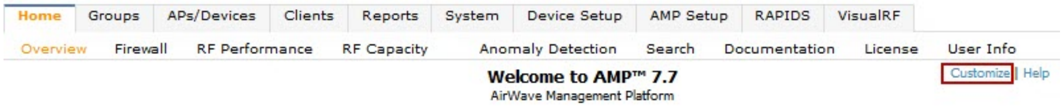
- A Time Range selector in the upper right portion of the charts (including pop-up charts) allows you to select a common or a custom date range for your data. The preconfigured ranges for AirWave charts are current 2 hours, 1 day, 1 week, and 1 year.
- Drop-down menus are available for viewing client and usage for specific SSIDs and/or all SSIDs. A search field is available to help you quickly find a specific WLAN.

  You can select up to six options from each drop-down menu. Once selected, each option will appear in the color-coded legend below the chart. Clicking on an option in this legend will disable or enable that information in the graph. Note that even if an option is disabled from viewing in the graph, that option will still remain in the legend until you deselect it from the drop-down menu.
- Max and Avg options allow you to change the chart view to show the maximum or average client and usage information.
- Plot points display within the chart at varying intervals, depending on the selected time range. Tooltips and a plot line appear as you hover over each plot point, showing you the detailed information for that specific time.
- Click on any chart to view a pop-up version. In this version, you can easily zoom in on a range of data by using your mouse to drag a rectangle in the chart. While you are zoomed in, a **Reset zoom** button appears, enabling you to return to the original view. The pop-up charts also include a legend that displays the Last, Min, Max, and Avg values for the selected graph.
- Some charts include a drop-down option next to the graph title. For example, on the **APs/Devices** > **Monitor** page for Radio Statistics, you can select the drop-down beside the graph title to view a graph for Client, Usage, Radio Channel, Radio Noise, Radio Power, Radio Errors, and 802.11 Counters information. In prior versions of AirWave, these graphs appeared as separate tabs.

Customizing the Dashboard

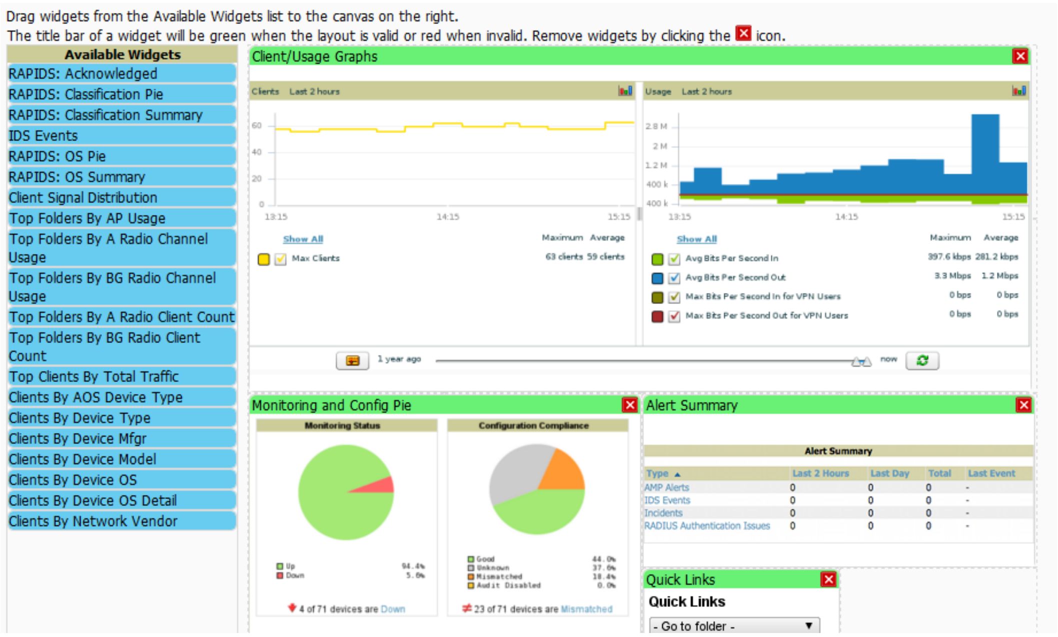
You can rearrange or remove widgets appearing on the **Home** > **Overview** dashboard by selecting the **Customize** link to the right of this window, as shown in Figure 10.

Figure 10 ***Customize*** *Button on the* ***Home > Overview*** *Page*



The **Customize** workspace that appears is shown in Figure 11.

Figure 11 ***Customize Overview*** *Page*



Drag widgets from the Available Widgets list to the canvas on the right.
The title bar of a widget will be green when the layout is valid or red when invalid. Remove widgets by clicking the ☒ icon.

Available Widgets
- RAPIDS: Acknowledged
- RAPIDS: Classification Pie
- RAPIDS: Classification Summary
- IDS Events
- RAPIDS: OS Pie
- RAPIDS: OS Summary
- Client Signal Distribution
- Top Folders By AP Usage
- Top Folders By A Radio Channel Usage
- Top Folders By BG Radio Channel Usage
- Top Folders By A Radio Client Count
- Top Folders By BG Radio Client Count
- Top Clients By Total Traffic
- Clients By AOS Device Type
- Clients By Device Type
- Clients By Device Mfgr
- Clients By Device Model
- Clients By Device OS
- Clients By Device OS Detail
- Clients By Network Vendor

Client/Usage Graphs

	Maximum	Average
🟨 ☑ Max Clients	63 clients	59 clients

	Maximum	Average
🟩 ☑ Avg Bits Per Second In	397.6 kbps	281.2 kbps
🟦 ☑ Avg Bits Per Second Out	3.3 Mbps	1.2 Mbps
■ ☑ Max Bits Per Second In for VPN Users	0 bps	0 bps
🟥 ☑ Max Bits Per Second Out for VPN Users	0 bps	0 bps

Monitoring and Config Pie

Monitoring Status

🟩 Up	94.4%
🟥 Down	5.6%

4 of 71 devices are Down

Configuration Compliance

🟩 Good	44.0%
□ Unknown	37.6%
🟧 Mismatched	18.4%
🟨 Audit Disabled	0.0%

23 of 71 devices are Mismatched

Alert Summary

Alert Summary

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
IDS Events	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Quick Links

Quick Links

- Go to folder - ▼

Adding Widgets

The **Home** > **Overview** page displays the currently selected widgets (charts/graphs). You can change the widgets on this page by selecting the **Customize** link in the upper-right corner.

The **Available Widgets** section on the left holds all available graphical elements (widgets). Select any blue widget tile with a verbal description enclosed, and it immediately turns into a graphical element with a description.

Drag the widgets you want to appear on the **Home** > **Overview** dashboard across to the gridlines and arrange them in the right section, within the gridlines. A widget snaps back to the nearest available gridline if you drop it across two or more lines and turns red if you attempt to place it over gridlines already occupied by widgets. Widgets with a green top banner are properly placed and set to appear when you select **Save**. Widgets that remain in the left section will not appear; although they can be reinstated by selecting **Restore Defaults**.

Available Widgets

Table 2 describes the list of available widgets along with a description for each. Note that when a widget is enabled, the information that displays can vary based on the user's permission level. Certain roles, for example, limit the top folder that a user can view.

Table 2: *Available Widgets*

Widget	Description
Client/Usage Graphs	The **Client** graph is enabled by default and, by default, shows the maximum number of attached clients over the last two hours. Select the **Show All** link to view more specific client information on the graph, such as the total and average clients for a specific SSID, the maximum VPN sessions, etc. The available check boxes within this graph are determined by the SSIDs that AMP is aware of from polling the device. The **Usage** graph is enabled by default and, by default, shows the average

Table 2: *Available Widgets (Continued)*

Widget	Description
	bits-per-second in/out information and average VPN in/out information. Select the **Show All** link to view usage information for specific SSIDs. The available checkboxes within this graph are determined by by the SSIDs that AMP is aware of from polling the device. The information in these graphs is color coded to match the selected check boxes.
Monitoring and Config Pie	The **Monitoring Status** pie shows the percentage of total devices that are up and the number and percentage of devices that are currently down. Clicking within this pie chart takes you to the **APs/Devices > Down** page. The **Configuration Compliance** pie shows the percentage of devices that are mismatched, good, unknown, and those with auditing disabled. It also provides a summary of the total number of devices that are mismatched. Clicking within this pie chart takes you to the **APs/Devices > Mismatch** page. These pie charts are enabled by default.
Alert Summary	The **Alert Summary** table is enabeld by default and provides the number of AMP alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last AMPreboot. ● Click on **AMP Alerts** to drill down to more detailed alert information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link. ● Click on **IDS Events** to drill to more detailed event information. This link takes you to the **RAPIDS > IDS Events** page. ● Click on **RADIUS Authentication Issues** to drill to more detailed RADIUS authentication information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link.
Quick Links	The **Quick Links** section is enabled by default. This section provides the user with easy navigation to a specific folder, group, report, or common task.
RAPIDS: Acknowledged	The **Acknowledged RAPIDS Devices** pie chart shows the percentage of acknowledged and unacknowledged RAPIDS that the user has visibility into. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This chart also displays on the **RAPIDS > Overview** page.
RAPIDS: Classification Pie	The **RAPIDS: Classification Pie** shows the percentage of devices classified as Valid, Suspected Neighbor, Suspected Valid, Suspected Rogue, Rogue, and Neighbor that are attached to AMP. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.
RAPIDS: Classification Summary	The **RAPIDS: Classification Summary** table shows the number of devices classified as Valid, Suspected Valid, Neighbor, Suspected Neighbor, Suspected Rogue, Rogue, and Unclassified that are attached to AMP. In addition, contained rogue information will appear if **Manage rogue AP containment** is set to **Yes** on the **RAPIDS > Setup** page.

Table 2: *Available Widgets (Continued)*

Widget	Description
	The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
IDS Events	The **IDS Events** table shows the number and type of attacks logged by the intrusion detection system over the last 2 hours, the last 24 hours, and the total since the last AMP reboot. This is the same table that displays on the **RAPIDS > Overview** page.
RAPIDS: OS Pie	The **RAPIDS: OS Pie** chart shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This pie chart can also be viewed on the **RAPIDS > Overview** page.
RAPIDS: OS Summary	The **RAPIDS: OS Summary** table shows the top 9 rogue devices by OS, Others, Unknown, and Not Scanned. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Note that ignored rogues are not included in this chart. This table can also be viewed on the **RAPIDS > Overview** page.
Top Folders By AP Usage	This chart lists the folders and the number of APs in each folder whose usage is greater than the cutoff (or usage threshold). The cutoff represents 75% of the maximum usage, where the maximum usage is the AP with the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. The chart takes into account approved APs with radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By A Radio Channel Usage	This chart shows the folders and the number of A radios (5GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **AMP Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'A' radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By BG Radio Channel Usage	This chart shows the folders and the number of BG radios (2.4GHz) in each folder whose channel usage is greater than the cutoff (or usage threshold) as measured by Mbps. This cutoff is on the on the **AMP Setup > General** page using the **Configure Channel Busy Threshold** option. If this option is not configured, then the cutoff is 75% of the 'maximum,' where the 'maximum' refers to the AP that has the highest usage regardless of the folder in which it resides. The cutoff value is displayed within the title, and this value can vary. This chart takes into account approved APs with 'BG' radios based on the last 24 hours. In addition, this chart is updated every hour.

Table 2: *Available Widgets (Continued)*

Widget	Description
Top Folders By A Radio Client Count	This chart shows the folders and the number of A radios (5GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with A radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Folders By BG Radio Client Count	This chart shows the folders and the number of BG radios (2.4GHz) in each folder whose client count is greater than the cutoff. The cutoff represents 75% of the 'maximum,' where the 'maximum' is the radio that has the highest client count regardless of the folder. The cutoff value is displayed within the title and can vary. This chart takes into account approved APs with BG radios based on the last 24 hours. In addition, this chart is updated every hour.
Top Clients By Total Traffic	The widget looks at currently connected clients as well has client historical information over the past 24 hours and then displays the top 10 clients with the must usage. You can click on a MAC address to view more information about any of the clients that display on this table. This table is updated every hour.
Clients By AOS Device Type	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the AOS device type.
Clients By Device Type	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the device type (such as a specific operating system or smart phone type).
Clients By Device Mfgr	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the client manufacturer.
Clients By Device Model	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the device model (such as the smart phone type).
Clients By Mfgr & Model	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the client manufacturer and model.
Clients By Device OS	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the device operating system (such as Windows or Android).
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on the device operating system version (such as Windows NT 6.1).
Clients By Network Vendor	This pie chart shows the percentage of clients that have attached to AMP over the last 24 hours based on each device's network interface vendor.
Client Signal Distribution	The **Client Signal Distribution** chart shows the number of attached devices that have a signal quality within a set of ranges.

Search Preferences

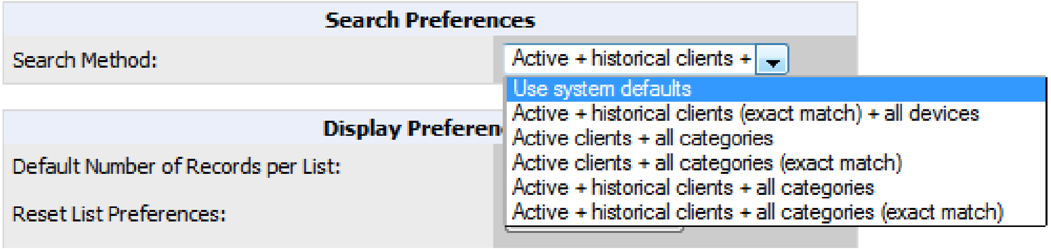
For each user, you can customize the search results to display only desired categories of matches on the **Home > User Info** page. Go to the **Search Preferences** section and select the desired search type from the **Search Method** drop down. This search type will be used when a user types an entry in the Search field and then clicks Enter without selecting a specific search type.

- Use System Defaults: The Search Method will be based on the system-wide configuration setting. This method is configured on the **AMP Setup > General** page.
- Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a popup window rather than on the **Home > Search** page. This popup window includes top-level navigation that allows you to filter the results based on Clients, APs, Controllers, and Switches.
- Active clients + all categories: This looks at all active clients (not historical) and all categories. This search is not case-sensitive. This search returns results on partial matches for usernames if that username is included in either the beginning or the end of a user name string
- Active clients + all categories (exact match): This looks at all active clients (not historical) and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields.
- Active + historical clients + all categories: This looks at all active and historical clients and all categories. This search is not case-sensitive.
- Active + historical clients + all categories (exact match): This looks at all active and historical clients and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields.

NOTE

A confirmation message does not appear after you make modifications to Search Preferences.

Figure 12 *Home > User Info Search Preferences*



Search Preferences

Search Method: Active + historical clients +

Display Preferen

Default Number of Records per List:

Reset List Preferences:

Use system defaults
Active + historical clients (exact match) + all devices
Active clients + all categories
Active clients + all categories (exact match)
Active + historical clients + all categories
Active + historical clients + all categories (exact match)

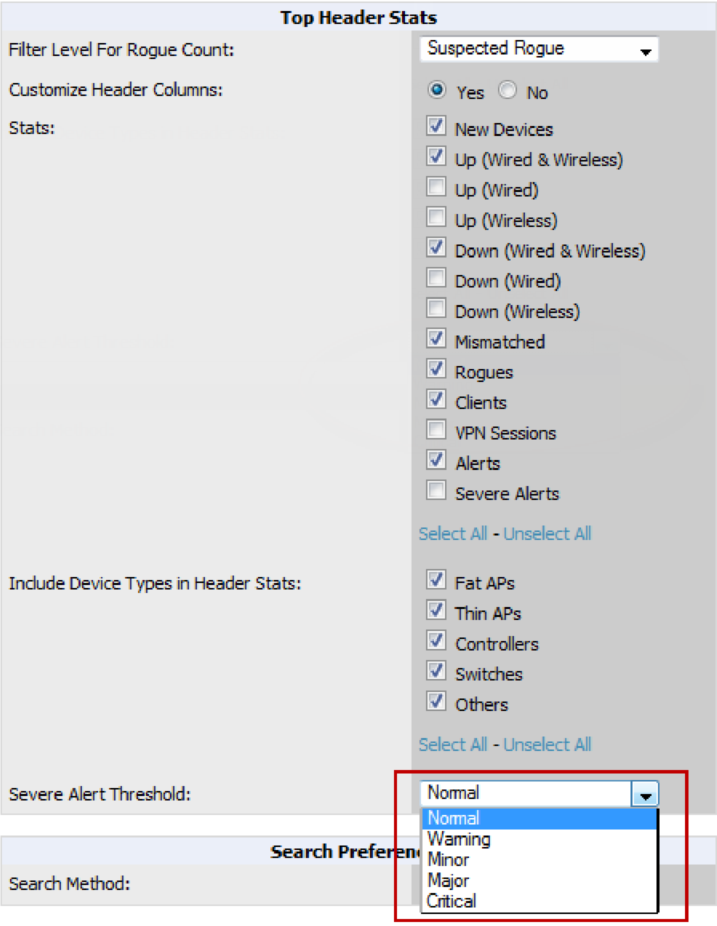
Setting Severe Alert Warning Behavior

You can control the alert levels you can see on the **Alerts** top header stats link from the **Home > User Info** page. The **Severe Alert Threshold** determines the severity level that results in a Severe Alert. Specify either Normal, Warning, Minor, Major, or Critical as the severity alert threshold value. These threshold values are tied to triggers that are created on the **System > Triggers** page. For example, if a trigger is defined to result in a Critical alert, and if the Severe Alert Threshold here is defined as Major, then the list of Severe Alerts will include all Major and Critical alerts. Similarly, if this value is set to Normal, which is the lowest threshold, then the list of Severe Alerts will include all alerts.

When a Severe Alert exists, a new component named **Severe Alerts** will appear at the right of the **Status** field in bold red font. This field is hidden if there are no Severe Alerts. In addition, only users who are enabled for viewing Severe Alerts on the **Home > User Info** page can see severe alerts.

The **Severe Alert Threshold** drop down menu, located in the **Top Header Stats** section of the **Home > User Info** page is shown in Figure 13.

Figure 13 *Home > User Info > Severe Alert Threshold Drop Down Menu*



Top Header Stats

Filter Level For Rogue Count: Suspected Rogue

Customize Header Columns: ● Yes ○ No

Stats:
☑ New Devices
☑ Up (Wired & Wireless)
□ Up (Wired)
□ Up (Wireless)
☑ Down (Wired & Wireless)
□ Down (Wired)
□ Down (Wireless)
☑ Mismatched
☑ Rogues
☑ Clients
□ VPN Sessions
☑ Alerts
□ Severe Alerts
Select All - Unselect All

Include Device Types in Header Stats:
☑ Fat APs
☑ Thin APs
☑ Controllers
☑ Switches
☑ Others
Select All - Unselect All

Severe Alert Threshold: Normal

Defining General AMP Server Settings

This section describes all pages accessed from the **AMP Setup** tab. It also describes two pages in the **Device Setup** tab: the **Communication** and **Upload Files** pages. After required and optional configuration tasks 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.

Refer to the following topics for configuration information:

- "AMP Setup > General" on page 29
- "Defining AMP Network Settings" on page 39
- "AMP User Roles" on page 43
- "Creating AMP Users" on page 41
- "Configuring Login Message, TACACS+, RADIUS, and LDAP Authentication" on page 48
- "Enabling AMP to Manage Your Devices" on page 56
- "Setting Up Device Types" on page 63

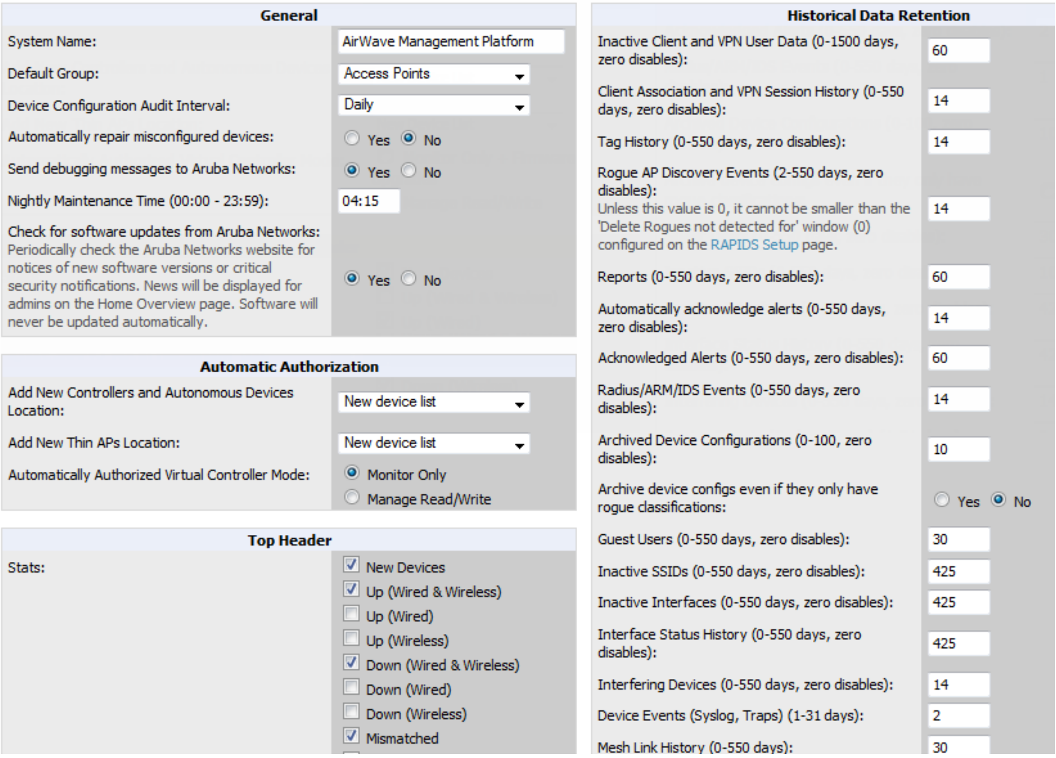
AMP Setup > General

The first step in configuring AMP is to specify the general settings for the AMP server. Figure 14 illustrates the **AMP Setup > General** page. Select **Save** when the **General Server** settings are complete and whenever making subsequent changes. These settings are applied globally across the product (for all users).

Refer to the following sections for information about the available settings:

- "General Settings" on page 29
- "Automatic Authorization Settings" on page 30
- "Top Header Settings" on page 31
- "Search Method" on page 31
- "Home Overview Preferences" on page 31
- "Display Settings" on page 32
- "Device Configuration Settings" on page 33
- "AMP Features" on page 33
- "External Logging Settings" on page 34
- "Historical Data Retention Settings" on page 35
- "Firmware Upgrade Defaults" on page 36
- "Additional AMP Services" on page 37
- "Performance Settings" on page 38

Figure 14 *AMP Setup > General Page Illustration (Partial View)*



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

Automatic Authorization	
Add New Controllers and Autonomous Devices Location:	New device list
Add New Thin APs Location:	New device list
Automatically Authorized Virtual Controller Mode:	● Monitor Only ○ Manage Read/Write

Top Header	
Stats:	☑ New Devices ☑ Up (Wired & Wireless) □ Up (Wired) □ Up (Wireless) ☑ Down (Wired & Wireless) □ Down (Wired) □ Down (Wireless) ☑ Mismatched

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

General Settings

Browse to the **AMP Setup > General** page, locate the **General** section, and enter the information described in Table 3:

Table 3: *AMP Setup > General > General Section Fields and Default Values*

Setting	Default	Description
System Name		Defines your name for your AMP server, with a maximum limit of 20 alphanumeric characters.
Default Group	Access Points	Sets the device group that this AMP 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 "Configuring and Using Device Groups" on page 77.
Device Configuration Audit Interval	Daily	This setting defines the interval of queries which compares actual device settings to the Group configuration policies stored in the AMP database. If the settings do not match, the AP is flagged as mismatched and AMP sends an alert via email, log, or SNMP. **NOTE:** Enabling this feature with a frequency of Daily or more frequently is recommended to ensure that your AP configurations comply with your established policies. Specifying **Never** is not recommended.
Automatically repair misconfigured devices	Disabled	If enabled, this setting automatically reconfigures the settings on the device when the device is in **Manage** mode and AMP detects a variance between actual device settings and the Group configuration policy in the AMP database.
Send debugging messages	Enabled	If enabled, AMP automatically emails any system errors to Aruba support to assist in debugging.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the local time of day AMP should perform daily maintenance. During maintenance, AMP cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
Check for software updates	Yes	Enables AMP to check automatically for multiple update types. Check daily for AMP updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct Internet connection via AMP.

Automatic Authorization Settings

On the **AMP Setup** > **General** page, locate the **Automatic Authorization** section. These settings allow you to control the conditions by which devices are automatically authorized into AP groups and folders. AMP validates the Folder and Group to ensure that both settings have been set to valid drop down options. Table 4 describes the settings and default values in this section.

Table 4: *AMP Setup > General > Automatic Authorization Fields and Default Values*

Setting	Default	Description
Add New Controllers and Autonomous Devices Location	New Device List	Globally add new controllers and autonomous devices to: ● The New Device List (located in **APs/Devices > New**). ● The same folder and group as the discovering device. ● The same group and folder of their closest IP neighbor on the same subnet. ● Choose a group and folder. If you select this option, enter the folder/group

Table 4: *AMP Setup > General > Automatic Authorization Fields and Default Values (Continued)*

Setting	Default	Description
		in the **Auto Authorization Group** and **Auto Authorization Folder** fields that display. **NOTE:** This setting can be overridden in **Groups > Basic**.
Add New Thin APs Location	New Device List	Globally add new thin APs to: ● The **New Devices** list. ● The same folder and group as the discovering device. ● The same group and folder of their closest IP neighbor on the same subnet. ● Choose a group and folder. If you select this option, enter the folder/group in the **Auto Authorization Group** and **Auto Authorization Folder** fields that display. **NOTE:** This setting can be overridden in **Groups > Basic**.
Automatically Authorized Virtual Controller Mode	Manage Read/Write	Specify whether Virtual Controller mode for Instant APs will be in Manage Read/Write mode or Monitor Only mode.

Top Header Settings

On the **AMP Setup** > **General** page, locate the **Top Header** section to select the Top Header Stats to be displayed at the top of the interface.

Search Method

On the **AMP Setup** > **General** page, locate the **Search Method** section. Select one of the following drop down options as the system-wide default search method. This default search type will be used when a user types an entry in the Search field and then clicks Enter without selecting a specific search type.

- Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a popup window rather than on the **Home** > **Search** page. This popup window includes top-level navigation that allows you to filter the results based on Clients, APs, Controllers, and Switches.
- Active clients + all categories: This looks at all active clients (not historical) and all categories. This search is not case-sensitive.
- Active clients + all categories (exact match): This looks at all active clients (not historical) and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields.
- Active + historical clients + all categories: This looks at all active and historical clients and all categories. This search is not case-sensitive.
- Active + historical clients + all categories (exact match): This looks at all active and historical clients and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields.

Per-user search preferences can be set in the **Home** > **User Info** page; refer to "Search Preferences" on page 27.

Home Overview Preferences

On the **AMP Setup** > **General** page, locate the **Home Overview Preferences** section. Table 5 describes the settings and default values in this section.

Table 5: *AMP Setup > General > Home Overview Preferences Fields and Default Values*

Setting	Default	Description
Configure Channel Busy Threshold	Yes	Whether you want to configure the threshold at which a channel is considered to be busy at the **Top Folders By Radio Channel Usage** Overview widget.
Channel Busy Threshold (%)	n/a	The threshold percent at which the radio channel is considered busier than normal. This field is only available if the Configure Channel Busy Threshold setting is **Yes**.

Display Settings

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

NOTE

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

Table 6 describes the settings and default values in this section.

Table 6: *AMP Setup > General > Display Fields and Default Values*

Setting	Default	Description
APFully Qualified Domain Name Options	No	Sets AMP to use fully qualified domain names for APs instead of the AP name. For example, 'testap.yourdomain.com; would be used instead of 'testap.' Select one of the following options: - **Don't use FQDN** - This default value specifies that the fully qualified domain name will not be used. - **Use AP Name with FQDN** - The AP name will prepend the FQDN, for example "somehostname (my.hostname.com)." Note that if the AP name is not present, then the FQDN will still appear in parenthesis. - **Use only FQDN** - Only the fully qualified domain name will be used. **NOTE:** This option is supported only for Cisco IOS, Dell Networking W-Series, 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: - **All devices**–When selected, AMP displays all Group tabs and setting options. - **Only devices on this** AMP–When selected, AMP hides all options and tabs that do not apply to the APs and devices currently on AMP. - **Selected device type**–When selected, a new field appears listing many device types. This option allows you to specify the device types for which AMP displays group settings. You can override this setting.
Look up device and wireless user hostnames	Yes	Enables AMP to look up 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 AMP, after which AMP refreshes DNS lookup: - 1 hour - 2 hours

Table 6: *AMP Setup > General > Display Fields and Default Values (Continued)*

Setting	Default	Description
		● 4 hours ● 12 hours ● 24 hours
Device 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.

Device Configuration Settings

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

Table 7: *AMP Setup > General > Device Configuration 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**.
Allow WMS Offload configuration in monitor-only mode	No	When **Yes** is selected, you can enable the ArubaOS 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 and Dell Networking W-Series devices.
Allow disconnecting users while in monitor-only mode	No	Sets whether you can deauthenticate a user for a device in monitor-only mode. If set to **No**, the **Deauthenticate Client** button for in a **Clients > Client Detail** page is enabled only for Managed devices.
Use Global Aruba Configuration	No	Enables Aruba configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within **Groups > Controller Config**and **Groups > Switch Config** instead of globally. **NOTE:** Changing this setting may require importing configuration on your devices. When an existing Aruba configuration setup is to be converted from global to group, follow these steps: 1. Set all the devices to Monitor Only mode before setting the flag. 2. Each device Group will need to have an import performed from the **Audit** page of a controller in the AMP group. 3. All of the thin APs need to have their settings imported after the device group settings have finished importing. 4. If the devices were set to Monitor Only mode, set them back to Managed mode.

AMP Features

Locate the **AMPFeatures** section and adjust settings to enable or disable VisualRF and RAPIDS. Table 8 describes these settings and default values.

Table 8: *AMP Setup Setup > General > AMP Features Fields and Default Values*

Setting	Default	Description
Display VisualRF	No	Enable or disable the **VisualRF** navigation tab.
Display RAPIDS	No	Enable or disable the **RAPIDS** navigation tab.
Hide setup pages from non-admin users	Yes	Restrict access to following pages to users with the AMP Administration role only: ● VisualRF > Setup ● AMP Setup > NMS ● RAPIDS > Score Override ● RAPIDS > Rules ● RAPIDS > Setup ● System > Triggers
Allow role based report visibility	Yes	Enable or disable role-based reporting in AMP. When disabled, reports can only be generated with by-subject visibility.

External Logging Settings

Locate the **External Logging** section and adjust settings to send audit and system events to an external syslog server. Table 9 describes these settings and default values. You can also send a test message using the **Send Test Message** button after enabling any of the logging options.

Table 9: *AMP Setup > General > External Logging Section Fields and Default Values*

Setting	Default	Description
Syslog Server	N/A	Enter the IP address of the syslog server. Note that this field is hidden if both "Include event log messages" and "Include audit log messages" are set to **No**.
Syslog Port	514	Enter the port of the syslog server. Note that this field is hidden if both "Include event log messages" and "Include audit log messages" are set to **No**.
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. This field is only available if the "Include event log messages" setting is **Yes**.
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. This field is only available if the "Include audit log messages" setting is **Yes**
Send Test Message	N/A	If messaging is enabled and a server and port are configured, click this button to send a test message. Upon completion, a message will appear at the top of this page indicating that the message was sent successfully.

Historical Data Retention Settings

Locate the **Historical Data Retention** section and specify the number of days you want to keep client session records and rogue discovery events. Table 10 describes the settings and default values of this section. Many settings can be set to have no expiration date.

Table 10: *AMP Setup > General > Historical Data Retention Fields and Default Values*

Setting	Default	Description
Inactive Client and VPN User Data (0-1500 days, zero disables)	60	Defines the number of days AMP stores basic information about inactive clients and VPN users. A shorter setting of 60 days is recommended for customers with high user turnover such as hotels. The longer you store inactive user data, the more hard disk space you require.
Client Association and VPN Session History (0-550 days, zero disables)	14	Defines the number of days AMP stores client and VPN session records. The longer you store client session records, the more hard disk space you require.
Tag History (0-550 days, zero disables)	14	Sets the number of days AMP retains location history for Wi-Fi tags.
Rogue AP Discovery Events (14-550 days, zero disables)	14	Defines the number of days AMP stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.
Reports (0-550 days, zero disables)	60	Defines the number of days AMP stores Reports. Large numbers of reports, over 1000, can cause the **Reports > Generated** page to be slow to respond.
Automatically Acknowledge Alerts (0-550 days, zero disables)	14	Defines automatically acknowledged alerts as the number of days AMP retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function, and alerts will never expire or be deleted from the database.
Acknowledged Alerts(0-550 days, zero disables)	60	Defines the number of days AMP retains information about acknowledged alerts. Large numbers of Alerts, over 2000, can cause the **System > Alerts** page to be slow to respond.
Radius/ARM/IDS Events(0-550 days, zero disables)	14	Defines the number of days AMP retains information about RADIUS, ARM, and IDS events. Setting this value to **0** disables this function, and the information will never expire or be deleted from the database.
Archived Device Configurations (0-100, zero disables)	10	Defines the number of configurations that will be retained for archived devices.. Whether rogue information is included depends on the setting of the **Archive device configs even if they only have rogue classifications** setting.
Archive device configs even if they only have rogue classifications	No	Sets whether to archive device configurations even if the device only has rogue classifications.
Guest Users (0-550 days, zero disables)	30	Sets the number of days that AMP is to support any guest user. A value of **0** disables this function, and guest users will never expire or be deleted from the AMP database.

Table 10: *AMP Setup > General > Historical Data Retention Fields and Default Values (Continued)*

Setting	Default	Description
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days AMP retains historical information after AMP 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 database.
Inactive Interfaces (0-550 days, zero disables)	425	Sets the number of days AMP 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 database.
Interface Status History (0-550 days, zero disables)	425	Sets the number of days AMP retains historical information on interface status. Setting this value to **0** disables this function.
Interfering Devices (0-550 days, zero disables)	14	Sets the number of days AMP retains historical information on interfering devices. Setting this value to **0** disables this function.
Device Events (Syslog, Traps)(1-31 days)	2	Sets the number of days AMP retains historical information on device events such as syslog entries and SNMP traps. Setting this value to **0** disables this function. Refer to "Viewing Device Events in System > Syslog & Traps" on page 216. **NOTE:** If your data table has more than 5 million rows, AMPwill truncate the device event retention data. In this case, the "number of days" setting becomes "number of hours."
Mesh Link History (0-550 days)	30	Sets the number of days AMP retains historical information for mesh links.
Device Uptime (0-120 months, zero disables)	60	Sets the number of months AMP retains historical information on device uptime. Setting this value to **0** disables this function.
Client Data Retention Interval (1-425 days)	425	Sets the number of days AMP retains historical information for clients.

Firmware Upgrade Defaults

Locate the **Firmware Upgrade Defaults** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for AMPTable 11 describes the settings and default values of this section.

Table 11: *AMP Setup > General > Firmware Upgrade Defaults Fields and Default Values*

Setting	Default	Description
Allow firmware upgrades in monitor-only mode	No	If **Yes** is selected, AMP upgrades the firmware for APs in **Monitor Only** mode. When AMP upgrades the firmware in this mode, the desired configuration are not be pushed to AMP. Only the firmware is applied. The firmware upgrade may result in configuration changes AMP does not correct those changes when the AP is in **Monitor Only** mode.
Maximum Interleaved Jobs (1-	20	Defines the number of jobs AMP runs at the same time. A job can include multiple APs. When jobs are started by multiple users, AMP will interleave

Table 11: *AMP Setup > General > Firmware Upgrade Defaults Fields and Default Values (Continued)*

Setting	Default	Description
20)		upgrades so that one user's job does not completely block another's.
Maximum Interleaved Devices Per Job (1-1000)	20	Defines the number of devices that can be in the process of upgrading at the same time. Within a single job, AMP may start the upgrade process for up to this number of devices at the same time. However, only one device will be actively downloading a firmware file at any given time.
Failures before stopping (0-20, zero disables)	1	Sets the default number of upgrade failures before AMP pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to **0** disables this function.

Additional AMP Services

Locate the **Additional**AMP **Services** section, and adjust settings as required. Table 12 describes the settings and default values of this section.

Table 12: *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 Aruba AirMesh and Cisco Aironet 4800 APs. Best practice is to disable the FTP server if you do not have any supported devices in the network.
Enable RTLS Collector	No	Enables or disables the RTLS Collector, which is used to allow ArubaOScontrollers to send signed and encrypted RTLS (real time locating system) packets to VisualRF-- in other words, AMP becomes the acting RTLS server. The RTLS server IP address must be configured on each controller. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Dell Networking W-Series, Alcatel-Lucent, and Aruba Networks devices. If **Yes** is specified, the following additional fields appear. These configuration settings should match the settings configured on the controller: ● **RTLS Port**–Specify the port for the AMP RTLS server. ● **RTLS Username**–Enter the user name used by the controller to decode RTLS messages. ● **RTLS Password**–Enter the RTLS server password that matches the controllers' value. ● **Confirm RTLS Password**–Re-enter the RTLS server password.
Use embedded Mail Server	Yes	Enables or disables the embedded mail server that is included with AMP. If **Yes** is specified, then enter information for an optional mail relay server. This field supports a **Send Test Email** button for testing server functionality. Clicking this button prompts you with **To** and **From** fields in which you must enter valid email addresses.
Process user roaming traps from Cisco WLC	Yes	Whether AMP should parse client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.

Table 12: *AMP Setup > General > Additional AMP Services Fields and Default Values (Continued)*

Setting	Default	Description
Enable AMON data collection	Yes	Allows AMP to collect enhanced data from Aruba devices on certain firmware versions. See the *Best Practices Guide* on the **Home > Documentation** page for more details.
Enable Firewall Data Collection	Yes	If AMON is enabled for a controller, you can enable this flag to instruct AMP to collect Policy Enforcement Firewall data from the controller. If this is enabled, then the Home > Firewall page will display.
Firewall Storage GibaBytes Allocated (Greater than or equal to 2 GiB)	50	If Firewall Data Collection is enabled, specify the amount of storage to allocate.
Prefer AMON vs SNMP Polling	No	If AMON is enabled for a controller, you can enable this flag so that AirWave monitoring relies solely on AMON and stops gathering data via SNMP polling.
Enable Syslog and SNMP Trap Collection	Yes	This option specifies whether traps used to detect roaming events, auth failures, AP up/down status, and IDS events will still be collected if they are sent by managed devices.

Performance Settings

Locate the **Performance** section. Performance tuning is unlikely to be necessary for many AMP implementations, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Aruba support if you think you might need to change any of these settings. Table 13 describes the settings and default values of this section.

Table 13: *AMP Setup> General > Performance 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 AMP to process more data per second, but it can take resources away from other AMP processes. Contact Aruba support if you think you might need to increase this setting for your network. Also note that the value range varies based on the number of available process cores.
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. Contact Aruba 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 Aruba support if you are considering increasing this setting for your network.
SNMP Fetcher Count (2-6)	2	Specify the number of SNMPv2 fetchers.

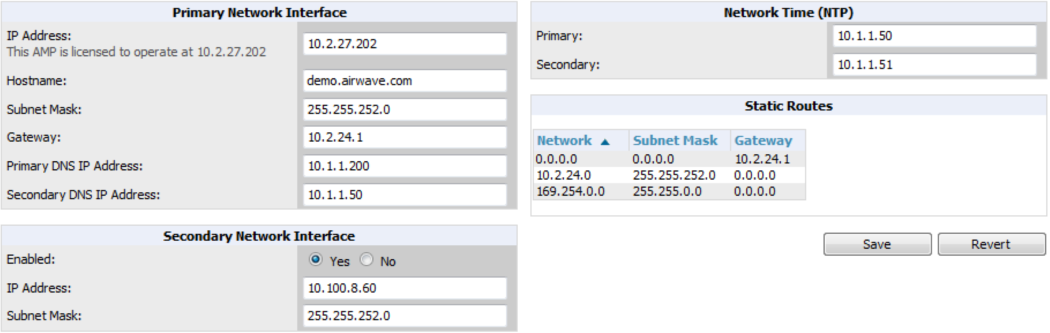
Table 13: *AMP Setup> General > Performance Fields and Default Values (Continued)*

Setting	Default	Description
Verbose Logging of SNMP Configuration	No	Enables or disables logging detailed records of SNMP configuration information.
SNMP Rate Limiting for Monitored Devices	No	When enabled, AMP fetches SNMP data more slowly, potentially reducing device CPU load. We recommend enabling this global setting if your network contains a majority of legacy controllers (800, 2400, 5000, or controllers that use Supervisor Module II). If your network mainly uses newer (30000 Series, 600 Series, or the M3 module in the 6000 series), we strongly recommend disabling this setting.
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to AMP as a whole. When AMP is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth usage) is not adversely impacted. The default priority is **Low**. You can also tune your system performance by changing group poll periods. If you select **Custom** for the priority, then also specify the RAPIDS custom process limit.
RAPIDS custom process limit (1-16)	1 when **Custom** is specified for the RAPIDS Processing Priority.	Sets the maximum number of monitoring process assigned to RAPIDS work. Note that this option is only available if **Custom** is specified for the RAPIDS Processing Priority.

Defining AMP Network Settings

The next step in configuring AMP is to confirm the AMP network settings. Define these settings by navigating to the **AMP Setup** > **Network** page. Figure 15 illustrates the contents of this page.

Figure 15 *AMP Setup > Network page illustration*



Primary Network Interface

IP Address: This AMP is licensed to operate at 10.2.27.202	10.2.27.202
Hostname:	demo.airwave.com
Subnet Mask:	255.255.252.0
Gateway:	10.2.24.1
Primary DNS IP Address:	10.1.1.200
Secondary DNS IP Address:	10.1.1.50

Secondary Network Interface

Enabled:	● Yes ○ No
IP Address:	10.100.8.60
Subnet Mask:	255.255.252.0

Network Time (NTP)

Primary:	10.1.1.50
Secondary:	10.1.1.51

Static Routes

Network ▲	Subnet Mask	Gateway
0.0.0.0	0.0.0.0	10.2.24.1
10.2.24.0	255.255.252.0	0.0.0.0
169.254.0.0	255.255.0.0	0.0.0.0

Specify the network configuration options described in the sections that follow to define the AMP network settings. Select **Save** when you have completed all changes on the **AMP Setup > Network** page, or select **Revert** to return to the last settings. **Save** restarts any affected services and may temporarily disrupt your network connection.

Primary Network Interface Settings

Locate the **Primary Network Interface** section. The information in this sections should match what you defined during initial network configuration and should not require changes. Table 14 describes the settings and default values.

Table 14: ***Primary Network Interface** Fields and Default Values*

Setting	Default	Description
IP Address	None	Sets the IP address of the AMP network interface. **NOTE:** This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the AMP server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.
Gateway	None	Sets the default gateway for the network interface.
Primary DNS IP	None	Sets the primary DNS IP address for the network interface.
Secondary DNS IP	None	Sets the secondary DNS IP address for the network interface.

Secondary Network Interface Settings

Locate the **Secondary Network Interface** section. The information in this section should match what you defined during initial network configuration and should not require changes. Table 15 describes the settings and default values.

Table 15: *Secondary Network Interface Fields and Default Values*

Setting	Default	Description
Enabled	No	Select **Yes** to enable a secondary network interface. You will be promted to define the IP address and subnet mask.
IP Address	None	Specify the IP address of the AMP secondary network. **NOTE:** This address must be a static IP address.
Subnet Mask	None	Specify the subnet mask for the secondary network interface.

Network Time Protocol (NTP) Settings

On the **AMP Setup > Network** page, locate the **Network Time Protocol (NTP)** section. The Network Time Protocol is used to synchronize the time between AMP and your network's 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 AMP server, not on individual access points.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between AMP and the NTP servers creates an entry in the event log. Table 16 describes the settings and default values in more detail. For more information on ensuring that AMP servers have the correct time, please see http://support.ntp.org/bin/view/Servers/NTPPoolServers.

Table 16: *AMP Setup > Network > Secondary Network Fields and Default Values*

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

Static Routes

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.

What Next?

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

Creating AMP Users

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

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

Each general user that you add must have a user name, a password, and a role. Use unique and meaningful user names as they are recorded in the log files when you or other users make changes in AMP.

NOTE

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

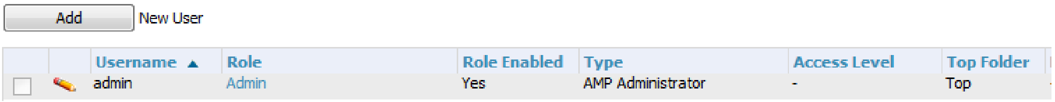
The user role defines the user type, access level, and the top folder for that user. User roles are defined on the **AMP Setup** > **Roles** page. Refer to the previous procedure in this chapter for additional information, "Creating AMP User Roles" on page 43.

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

1. Go to the **AMP Setup** > **Users** page. This page displays all users currently configured in AMP. Figure 16 illustrates the contents and layout of this page.

Figure 16 *AMP Setup > Users Page Illustration*



Add New User

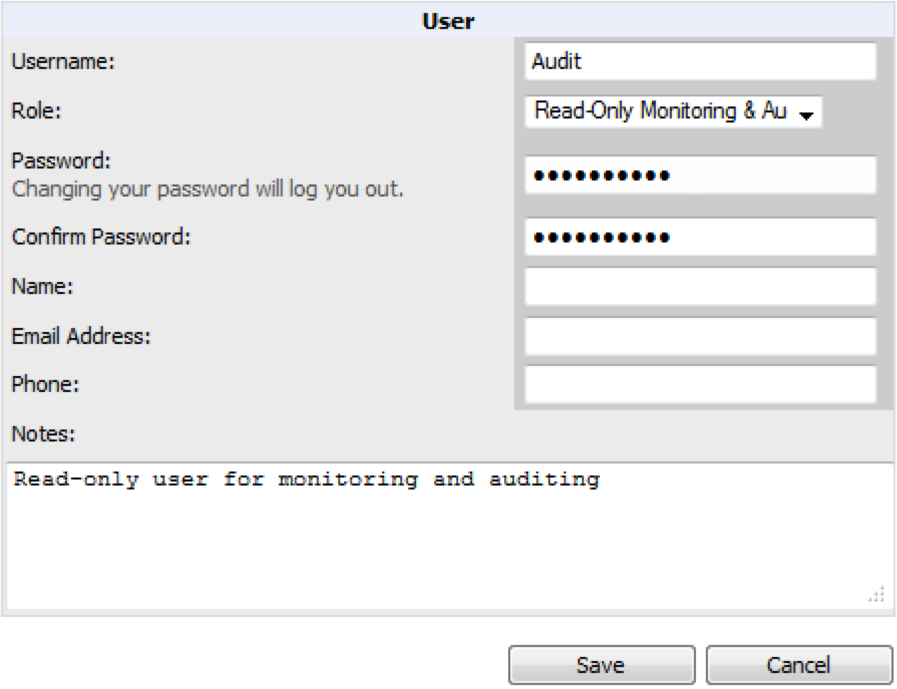
		Username ▲	Role	Role Enabled	Type	Access Level	Top Folder
□	✎	admin	Admin	Yes	AMP Administrator	-	Top

2. Select **Add** to create a new user, select the pencil icon to edit an existing user, or select a user and select **Delete** to remove that user from AMP. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 17.

NOTE

A current user cannot change his/her own role. The **Role** drop-down field is disabled to prevent this.

Figure 17 *AMP Setup > Users > Add/Edit User Page Illustration*



User

Username:	Audit
Role:	Read-Only Monitoring & Au
Password: Changing your password will log you out.	••••••••••
Confirm Password:	••••••••••
Name:	
Email Address:	
Phone:	
Notes:	

```
Read-only user for monitoring and auditing
```

3. Enter or edit the settings on this page. Table 17 describes these settings in additional detail.

Table 17: *AMP Setup > Users > 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 AMP and appears in AMP log files.
Role	None	Specifies the user's **Role**, which defines the Top viewable folder as well as the 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. **NOTE:** Because the default user's password is identical to the name, it is **strongly recommended that you change this password**. Changing your password will log you out.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.

Table 17: *AMP Setup > Users > Add/Edit User Fields and Default Values (Continued)*

Setting	Default	Description
Email Address	None	Allows you to specify a specific email address that will propagate throughout many additional pages in AMP 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.

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

NOTE

AMP 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 AMP deployment, such as help desk or IT staff.

What Next?

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

AMP User Roles

The **AMP Setup** > **Roles** page defines the viewable devices, the operations that can be performed on devices, and general AMP access. User roles can be created that provide users with 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 AMP deployment. You can restrict user roles to multiple folders within the overall hierarchy even if they do not share the same top-level folder. Non-admin users are only able to see data and users for devices within their assigned subset of folders.

User Roles and VisualRF

VisualRF uses the same user roles as defined for AMP. Users can see floor plans that contain an AP to which they have access in AMP, although only visible APs appear on the floor plan. VisualRF users can also see any building that contains a visible floor plan and any campus that contains a visible building.

NOTE

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

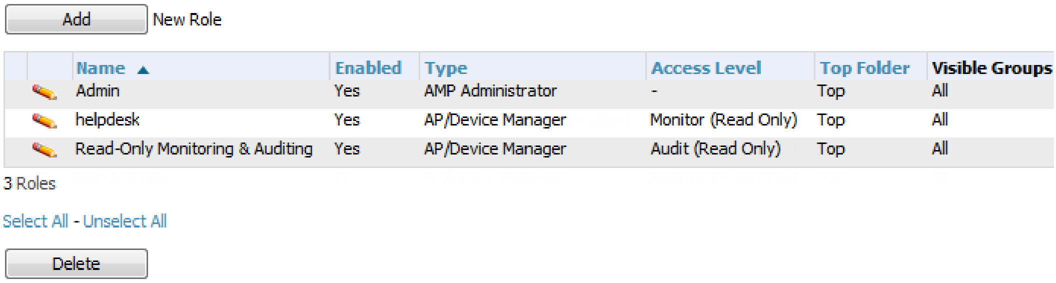
When a new role is added to AMP, VisualRF must be restarted for the new user to be enabled.

Creating AMP User Roles

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

1. Go to the **AMP Setup** > **Roles** page. This page displays all roles currently configured in AMP. Figure 18 illustrates the contents and layout of this page.

Figure 18 *AMP Setup > Roles Page Illustration*



Add New Role

	Name ▲	Enabled	Type	Access Level	Top Folder	Visible Groups
✎	Admin	Yes	AMP Administrator	-	Top	All
✎	helpdesk	Yes	AP/Device Manager	Monitor (Read Only)	Top	All
✎	Read-Only Monitoring & Auditing	Yes	AP/Device Manager	Audit (Read Only)	Top	All

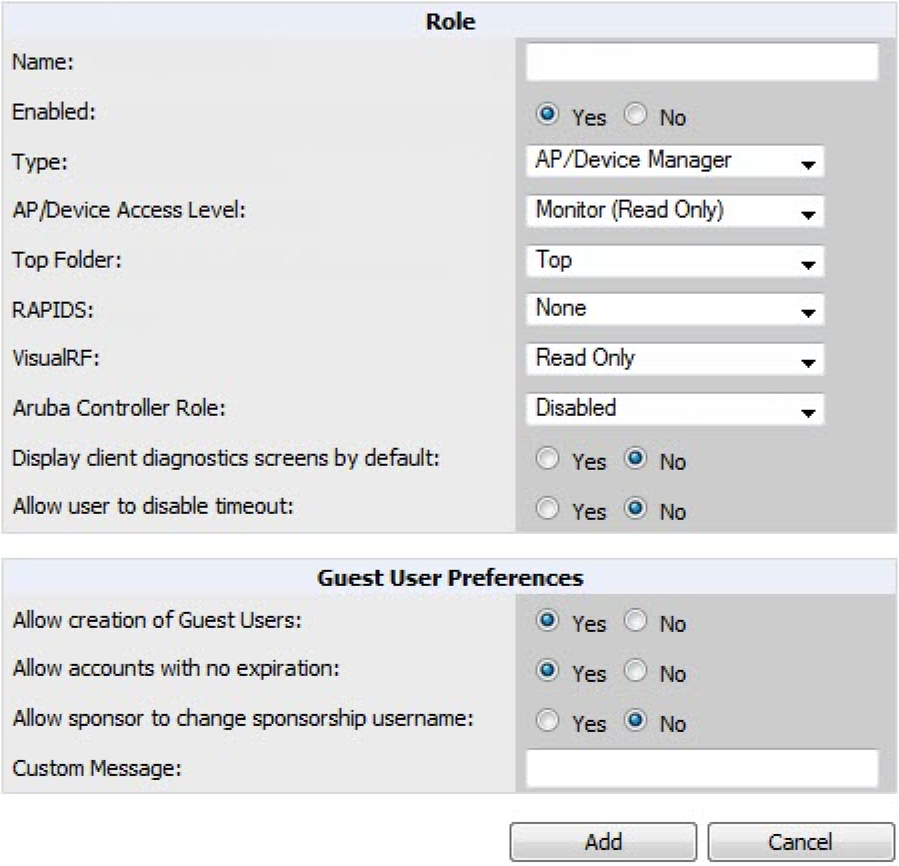
3 Roles

Select All - Unselect All

Delete

2. Select **Add** to create a new role, select the pencil icon to edit an existing role, or select a checkbox and select **Delete** to remove that role from AMP. When you select **Add** or the edit icon, the **Add/Edit Role** page appears, illustrated in Figure 19.

Figure 19 *AMP Setup > Roles > Add/Edit Role Page Illustration*



Role

Name:	
Enabled:	● Yes ○ No
Type:	AP/Device Manager
AP/Device Access Level:	Monitor (Read Only)
Top Folder:	Top
RAPIDS:	None
VisualRF:	Read Only
Aruba Controller Role:	Disabled
Display client diagnostics screens by default:	○ Yes ● No
Allow user to disable timeout:	○ Yes ● No

Guest User Preferences

Allow creation of Guest Users:	● Yes ○ No
Allow accounts with no expiration:	● Yes ○ No
Allow sponsor to change sponsorship username:	○ Yes ● No
Custom Message:	

Add Cancel

3. Enter or edit the settings on this page. 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 AMP. The available configuration options differ for each role type.

NOTE

Most users will see two sections on this page: **Role** and **Guest User Preferences**. The **Guest User Preferences** section will not appear, however, if **Guest User Configuration** is disabled in **AMP Setup > General**.

The following tables describe the available settings and default values for each role type.

Table 18: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for AMP Administrator Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AMP.
Type	AP/Device Manager	Defines the type of role. AMP Administrator–The AMP Administrator has full access to AMP and all of the devices. Only theAMP Administrator can create new users or access the AMP Setup page, the VisualRF > Setup page, VisualRF > Audit Log page, System > Event Log, and System > Performance.
Aruba Controller Role	Disabled	Enables or disables **Single Sign-On** for the role. If enabled, allows the role to directly access Aruba controller UIs from the Quick Links or IP Address hypertext throughout AMP without having to enter credentials for the controller.
Allow user to disable timeout	No	Whether a user can disable AMP's timeout feature.
Custom Message	none	A custom message can also be included.

Table 19: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AMP.
Type	AP/Device Manager	Defines the type of role. **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.
AP/Device Access Level	Monitor (Read Only)	Defines the privileges the role has over the viewable APs. AMP supports three privilege levels, as follows: ● **Manage (Read/Write)**–Manage users can view and modify devices and Groups. Selecting this option causes a new field, **Allow authorization of APs/Devices**, to appear on the page, and is enabled by default. ● **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 and VisualRF. Monitor users cannot view the **APs/Devices > Audit** page which may contain sensitive information, including passwords.

Table 19: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role (Continued)*

Setting	Default	Description
Top Folder	Top	Defines the highest viewable folder for the role. The role is able to view all devices and groups contained by the specified top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** AMP 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 AMP deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow authorization of APs/Devices	Yes	**NOTE:** This option is only available when the **AP/Device Access Level** is specified as **Manage (Read/Write)**.
RAPIDS	None	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: ● **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 edit individual rogues, classification, threat levels and notes, and perform OS scans. ● **Administrator**–Has the same privileges as the Read/Write user, but can also set up RAPIDS rules, override scores and is the only user who can access the **RAPIDS > Setup** page.
VisualRF	Read Only	Sets the VisualRF privileges, which are set separately from the APs/Devices. Options are as follows: ● **Read Only**–The user can view the VisualRF pages but cannot make any changes to floor plans. ● **Read/Write**–The user may edit individual floor plans, buildings, and campuses.
Aruba Controller Role	Disabled	Enables or disables **Single Sign-On** for the role. If enabled, allows the role to directly access Aruba controller UIs from the Quick Links or IP Address hypertext throughout AMP without having to enter credentials for the controller
Display client diagnostics screens by default	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.
Allow user to disable timeout	No	Whether a user can disable AMP’s timeout feature.
Allow creation of Guest Users	Yes	If this option is enabled, users with an assigned role of Monitoring or Audit can be given access to guest user account creation along with the option to allow a sponsor to change its username. **NOTE:** This option is not available if the **AP/Device Access Level** is specified as **Manage (Read/Write)**.

Table 19: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for AP/Device Manager Role (Continued)*

Setting	Default	Description
Allow accounts with no expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow sponsor to change sponsorship username	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

Table 20: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for AirWave Management Client Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AMP.
Type	AP/Device Manager	Defines the type of role. **AirWave Management Client**–The AirWave Management Client (AMC) software allows WiFi-enabled devices to serve as additional sensors to gather data for RAPIDS. Use this role type to set up a client to be treated as a user with the AMC role. The user information defined in AMC must match the user with the AMP Management Client type.
Allow user to disable timeout	No	Whether a user can disable AMP's timeout feature.

Table 21: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for Guest Access Sponsor Role*

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AMP.

Table 21: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for Guest Access Sponsor Role (Continued)*

Setting	Default	Description
Type	AP/Device Manager	Defines the type of role. **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.
Top Folder	Top	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. **NOTE:** AMP 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 AMP deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow user to disable timeout	No	Whether a user can disable AMP's timeout feature.
Allow accounts with no expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow sponsor to change sponsorship username	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

What Next?

- Go to additional tabs in the **AMP Setup** section to continue additional setup configurations. The next section describes how to set up AMP users.
- Complete the required configurations in this chapter before proceeding. Aruba support remains available to you for any phase of AMP configuration.

Configuring Login Message, TACACS+, RADIUS, and LDAP Authentication

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

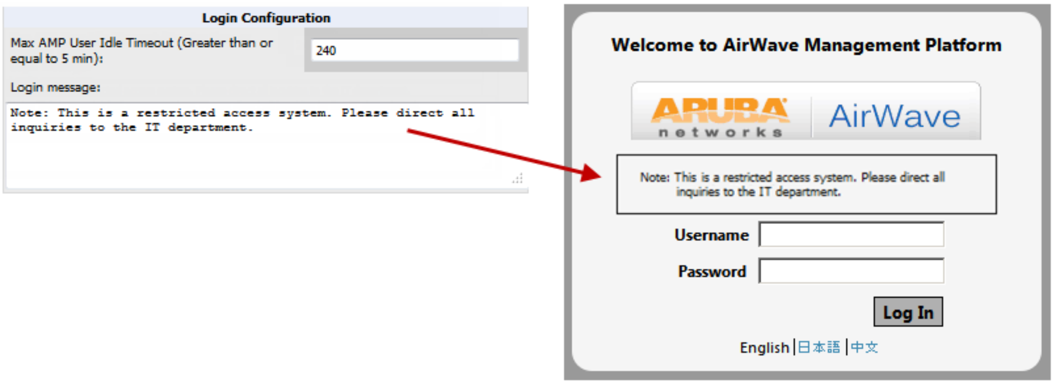
- "Setting Up Login Configuration Options" on page 49
- "Setting Up Certificate Authentication" on page 50
- "Setting Up Single Sign-On" on page 49
- "Specifying the Authentication Priority" on page 50
- "Configuring RADIUS Authentication and Authorization" on page 50

- "Integrating a RADIUS Accounting Server" on page 51
- "Configuring TACACS+ Authentication" on page 52
- "Configuring LDAP Authentication and Authorization" on page 54

Setting Up Login Configuration Options

On the **AMP Setup** > **Authentication** page, administrators can optionally configure the AMP user's idle timeout or a message-of-the-day that appears when a user first logs in, as shown in Figure 20:

Figure 20 *Login configuration field and results in the AMP Login page*



Login Configuration

Max AMP User Idle Timeout (Greater than or equal to 5 min): 240

Login message:

```
Note: This is a restricted access system. Please direct all
inquiries to the IT department.
```

Welcome to AirWave Management Platform

Note: This is a restricted access system. Please direct all inquiries to the IT department.

1. Go to **AMP Setup** > **Authentication.**
2. Complete the fields described on Table 22:

Table 22: *Login Configuration section of AMP Setup > Authentication*

Field	Default	Description
Max AMP User Idle Timeout	60	Number of minutes of idle time until AMP automatically ends the user session. Affects all users of this AMP. The range is 5-240 minutes.
Login message	none	A persistent message that will appear for all of this AMP's users after they log in.

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

Setting Up Single Sign-On

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

Perform the following steps to enable this feature for this AMP.

1. Locate the **Single Sign-On** section in **AMP Setup** > **Authentication**.
2. In the **Enable Single Sign-On** field, select **Yes**.
3. Select **Save** if you are finished or follow the next procedure to specify the authentication priority.

Setting Up Certificate Authentication

On the **AMP Setup** > **Authentication** page, administrators can specify whether to require a certificate during authentication and whether to use two-factor authentication. A PEM-encoded certificate bundle is required for this feature.

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

Perform the following steps to enable this feature for this AMP.

1. Locate the **Certificate Authentication** section in **AMP Setup** > **Authentication**.
2. In the **Enable Certificate Authentication** field, select **Yes**.
3. Specify whether to require a certificate in order to authenticate. If **Yes**, then you can also specify whether to use two-factor authentication.
4. Enter the PEM-encoded CA certificate bundle.
5. Select **Save** if you are finished or follow the next procedure to specify the authentication priority.

Specifying the Authentication Priority

To specify the authentication priority for this AMP, locate the **Authentication Priority** section in **AMP Setup** > **Authentication**, and select either **Local** or **Remote** as the priority.

If **Local** is selected, then remote will be attempted if a user is not available. If **Remote** is selected, then the local database is searched if remote authentication fails. The order of remote authentication is RADIUS first, followed by TACACS, and finally LDAP.

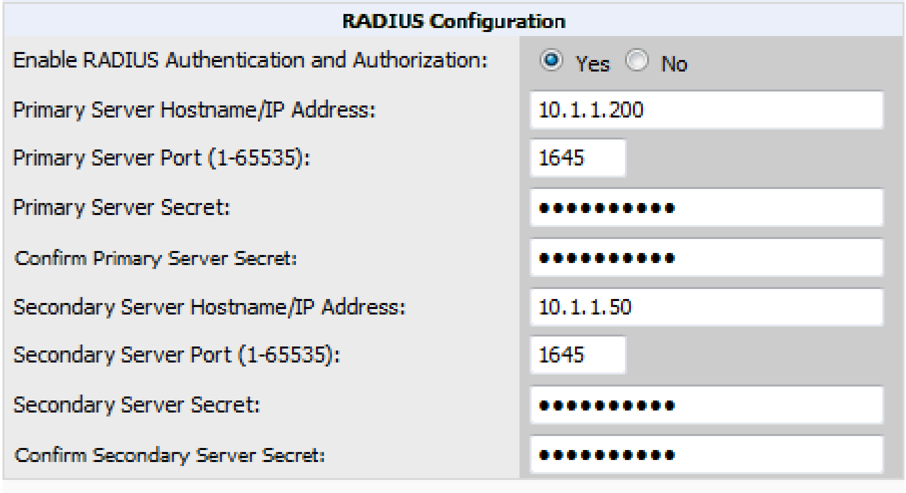
Select **Save** if you are finished or follow the next procedure to configure RADIUS, TACACS+, and LDAP Authentication options.

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 configure RADIUS authentication:

1. Go to the **AMP Setup** > **Authentication** page. This page displays current status of RADIUS. Figure 21 illustrates this page.

Figure 21 *AMP Setup > Authentication Page Illustration for RADIUS*



RADIUS Configuration

Enable RADIUS Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	10.1.1.200
Primary Server Port (1-65535):	1645
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	10.1.1.50
Secondary Server Port (1-65535):	1645
Secondary Server Secret:	••••••••••
Confirm Secondary Server Secret:	••••••••••

2. Select **No** to disable or **Yes** to enable RADIUS authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 23.

Table 23: *AMP Setup > Authentication Fields and Default Values for RADIUS Authentication*

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 (1-65535)	1812	Enter the TCP port for the primary RADIUS server.
Primary Server Secret	N/A	Specify and confirm the primary shared secret for the primary RADIUS server.
Confirm Primary Server Secret	N/A	Re-enter the primary server secret.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or the hostname of the secondary RADIUS server.
Secondary Server Port (1-65535)	1812	Enter the TCP port for the secondary RADIUS server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary RADIUS server.
Confirm Secondary Server Secret	N/A	Re-enter the secondary server secret.

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

NOTE

For instructions on setting up a RADIUS server, please see http://www.airwave.com/support/knowledge-base/?sid=50140000000Mer6 in the AirWave knowledge base.

Integrating a RADIUS Accounting Server

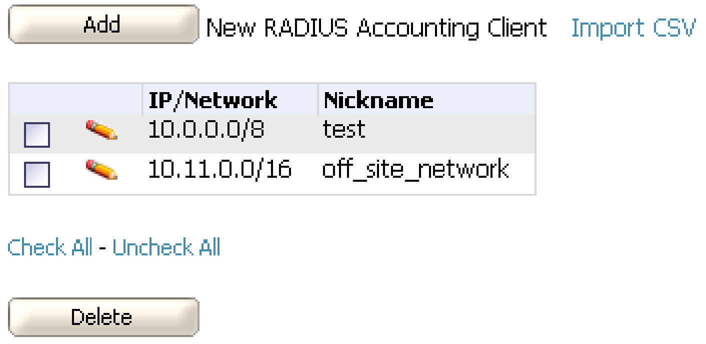
NOTE

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

Optionally, you can configure RADIUS server accounting on **AMP Setup > RADIUS Accounting**. This capability is not required for basic AMP operation, but can increase the user-friendliness of AMP administration in large networks. Figure 22 illustrates the settings of this optional configuration interface.

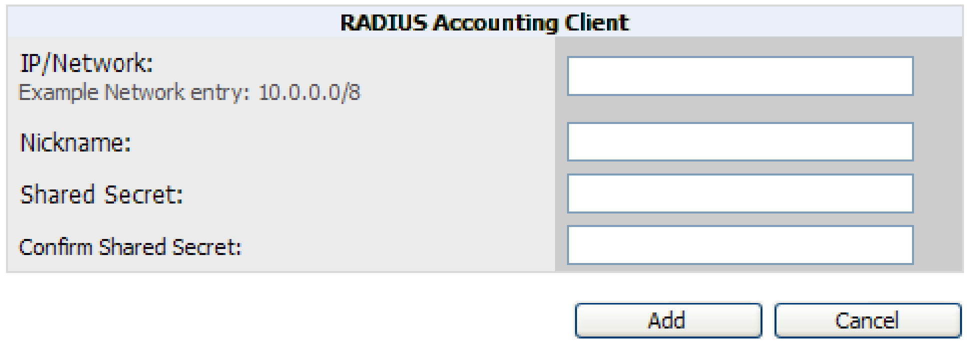
Perform the following steps and configurations to enable AMP to receive accounting records from a separate RADIUS server. Figure 22 illustrates the display of RADIUS accounting clients already configured, and Figure 23 illustrates the **Add RADIUS Accounting Client** page.

Figure 22 *AMP Setup > RADIUS Accounting Page Illustration*



		IP/Network	Nickname
□	✎	10.0.0.0/8	test
□	✎	10.11.0.0/16	off_site_network

Figure 23 *AMP Setup > RADIUS > Add RADIUS Accounting Client Page Illustration*



RADIUS Accounting Client

IP/Network:
Example Network entry: 10.0.0.0/8

Nickname:

Shared Secret:

Confirm Shared Secret:

1. To specify the RADIUS authentication server or network, browse to the **AMP Setup** > **RADIUS Accounting** page, select **Add**, illustrated in Figure 23, and provide the information in Table 24.
2. Complete the following fields:

Table 24: *AMP Setup > Radius Accounting Fields and Default Values for LDAP Authentication*

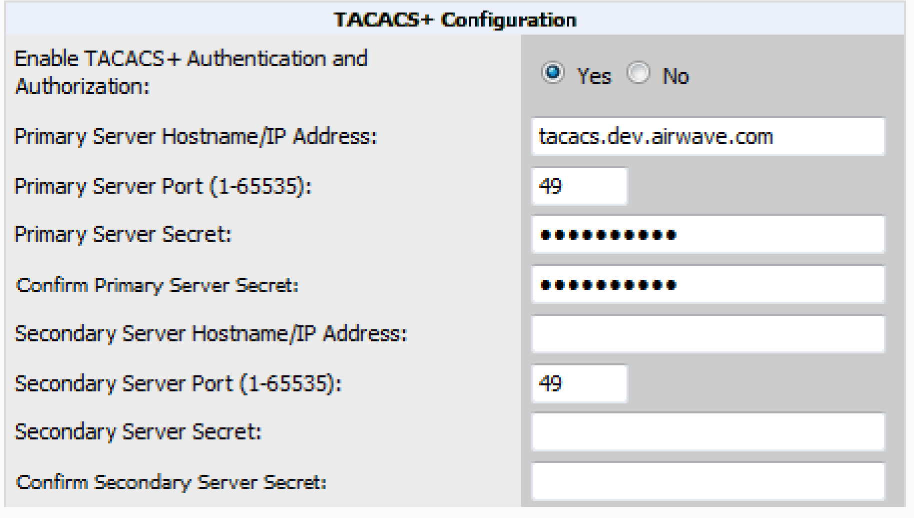
Setting	Default	Description
IP/Network	None	Specify the IP address for the authentication server if you only want to accept packets from one device. To accept packets from an entire network enter the IP/Netmask of the network (for example, 10.51.0.0/24).
Nickname	None	Sets a user-defined name for the authentication server.
Shared Secret (Confirm)	None	Sets the Shared Secret that is used to establish communication between AMP and the RADIUS authentication 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 AMP users and does not affect APs or users logging into APs.

1. Go to the **AMP Setup** > **Authentication** page. This page displays current status of TACACS+. Figure 24 illustrates this page when neither TACACS+, LDAP, nor RADIUS authentication is enabled in AMP.

Figure 24 *AMP Setup > Authentication Page Illustration for TACACS+*



TACACS+ Configuration

Enable TACACS+ Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	tacacs.dev.airwave.com
Primary Server Port (1-65535):	49
Primary Server Secret:	••••••••••
Confirm Primary Server Secret:	••••••••••
Secondary Server Hostname/IP Address:	
Secondary Server Port (1-65535):	49
Secondary Server Secret:	
Confirm Secondary Server Secret:	

2. Select **No** to disable or **Yes** to enable TACACS+ authentication. If you select **Yes**, several new fields appear. Complete the fields described in Table 25.

Table 25: *AMP Setup > Authentication Fields and Default Values for TACACS+ Authentication*

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 (1-65535)	49	Enter the port for the primary TACACS+ server.
Primary Server Secret	N/A	Specify and confirm the primary shared secret for the primary TACACS+ server.
Confirm Primary Server Secret	N/A	Re-enter the primary server secret.
Secondary Server Hostname/IP Address	N/A	Enter the IP address or hostname of the secondary TACACS+ server.
Secondary Server Port (1-65535)	49	Enter the port for the secondary TACACS+ server.
Secondary Server Secret	N/A	Enter the shared secret for the secondary TACACS+ server.
Confirm Secondary Server Secret	N/A	Re-enter the secondary server secret.

3. Select **Save** and continue with additional steps.

Configuring Cisco ACS to Work with AMP

To configure Cisco ACS to work with AMP, you must define a new service named **AMP** that uses https on the ACS server.

1. The AMP https service is added to the **TACACS+** (Cisco) interface under the **Interface Configuration** tab.
2. Select a checkbox for a new service.

3. Enter **AMP** in the service column and **https** in the protocol column.
4. Select **Save**.
5. Edit the existing groups or users in TACACS to use the AMP service and define a role for the group or user.
   - The role defined on the **Group Setup** page in ACS must match the exact name of the role defined on the **AMP Setup** > **Roles** page.
   - The defined role should use the following format: **role=**<*name_of_*AMP*_role*>. One example is as follows:

   role=DormMonitoring

   As with routers and switches, AMP does not need to know usernames.
6. AirWave also needs to be configured as an AAA client.
   - On the **Network Configuration** page, select **Add Entry**.
   - Enter the IP address of AirWave as the **AAA Client IP Address**.
   - The secret should be the same value that was entered on the **AMP Setup** > **TACACS+** page.
7. Select **TACACS+** (Cisco IOS) in the **Authenticate Using** drop down menu and select **submit + restart**.

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

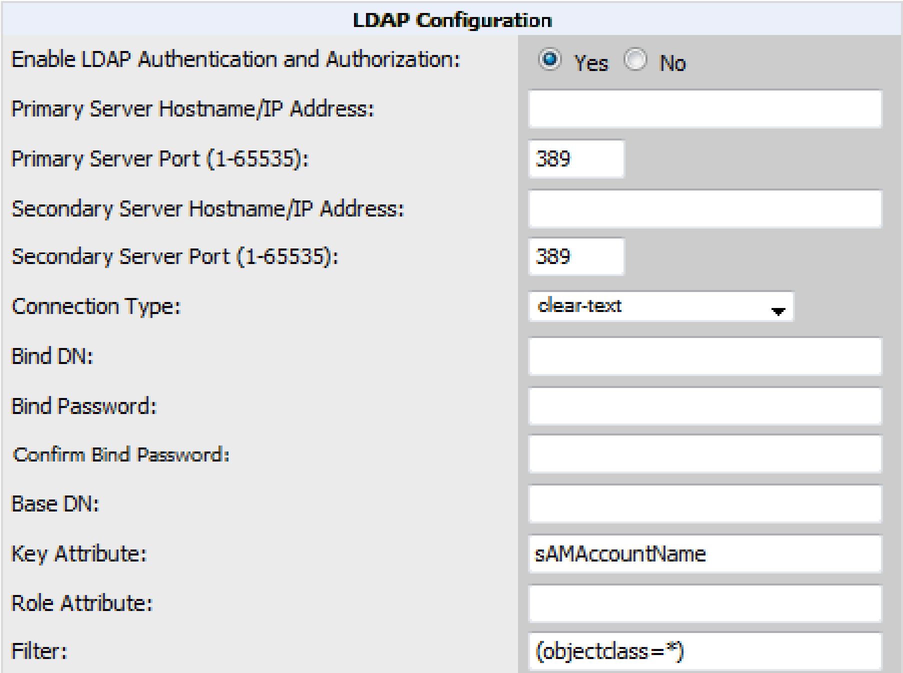
Configuring LDAP Authentication and Authorization

LDAP (Lightweight Directory Access Protocol) provides users with a way of accessing and maintaining distributed directory information services over a network. When LDAP is enabled, a client can begin a session by authenticating against an LDAP server which by default is on TCP port 389.

Perform these steps to configure LDAP authentication:

1. Go to the **AMP Setup> Authentication** page.
2. Select the **Yes** radio button to enable LDAP authentication and authorization. Once enabled, the available LDAP configuration options will display. Figure 25 illustrates this page.

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



LDAP Configuration

Enable LDAP Authentication and Authorization:	● Yes ○ No
Primary Server Hostname/IP Address:	
Primary Server Port (1-65535):	389
Secondary Server Hostname/IP Address:	
Secondary Server Port (1-65535):	389
Connection Type:	clear-text
Bind DN:	
Bind Password:	
Confirm Bind Password:	
Base DN:	
Key Attribute:	sAMAccountName
Role Attribute:	
Filter:	(objectclass=*)

3. Complete the fields described in Table 26.

Table 26: *AMP Setup > Authentication Fields and Default Values for LDAP Authentication*

Field	Default	Description
Primary Server Hostname/IP Address	none	Enter the IP address or the hostname of the primary LDAP server.
Primary Server Port (1-65535)	389	Enter the port where the LDAP server is listening. The default port is 389.
Secondary Server Hostname/IP Address	none	Optionally enter the IP address or hostname of the secondary LDAP server. This server will be contacted in the event that the primary LDAP server is not reachable.
Secondary Server Port (1-65535)	389	Enter the port where the LDAP service is listening on the secondary LDAP server. The default port is 389.
Connection Type	clear-text	Specify one of the following connection types AMP and the LDAP server: ● **clear-text** results in unencrypted communication. ● **ldap-s** results in communication over SSL. ● **start-tls** uses certificates to initiate encrypted communication.
View Server Certificate	none	If **Connection Type** is configured as **start-tls**, then also specify whether the **start-tls** connection type uses a certificate. ● **none** - The server may provide a certificate, but it will not be verified. This may mean that you are connected to the wrong server. ● **optional** - Verifies only when the servers offers a valid certificate. ● **require** - The server must provide a valid certificate.

Table 26: *AMP Setup > Authentication Fields and Default Values for LDAP Authentication (Continued)*

Field	Default	Description
		A valid **LDAP Server CA Certificate** must be provided in case of optional or require. Certificates uploaded on the **Device Setup > Certificates** page with a type of Intermediate CA or Trusted CA are listed in the drop down for **LDAP Server CA Certificate**.
LDAP Server CA Certificate	none	Specify the LDAP server certificate to use to initiate encrypted communication. Only certificates that have been uploaded with a type of Intermediate CA or Trusted CA will appear in this drop down. **NOTE:** This **LDAP Server CA Certificate** drop down menu oly appears if **View Server Certificate** is specified as **optional** or **require**.
Bind DN	none	Specify the Distinguished Name (DN) of the administrator account, such as 'cn=admin01,cn=admin,dn=domain,dn=com'. Note that for the Active directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).
Bind Password	none	Specify the bind DN account password.
Confirm Bind Password	none	Re-enter the bind password.
Base DN	none	The DN of the node in your directory tree from which to start searching for records. Generally, this would be the node that contains all the users who may access AMP, for example cn=users,dc=domain,dc=com.
Key Attribute	sAMAccountName	The LDAP attribute that identifies the user, such as 'sAMAccountName' for Active Directory
Role Attribute	none	The LDAP attribute that contains the AMP role. Users who log in to AMP using this LDAP authentication will be granted permissions based on this role. Refer to "AMP User Roles" on page 43 for more information about AMP User Roles.
Filter	(objectclass=*)	This option limits the object classes in which the key,role attributes would be searched.

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

What Next?

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

Enabling AMP to Manage Your Devices

Once AMP is installed and active on the network, the next task is to define the basic settings that allow AMP to communicate with and manage your devices. Device-specific firmware files are often required or are highly desirable.

Furthermore, the use of Web Auth bundles is advantageous for deployment of Cisco WLC wireless LAN controllers when they are present on the network.

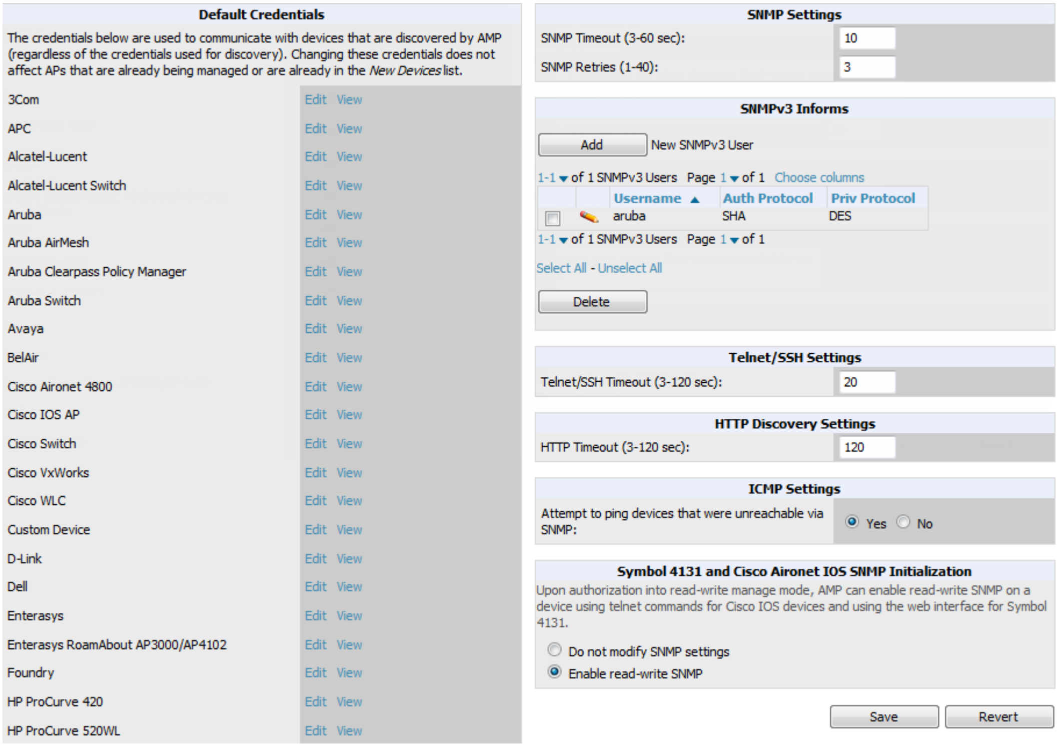
This section contains the following procedures:

- "Configuring Communication Settings for Discovered Devices" on page 57
- "Loading Device Firmware Onto AMP (optional)" on page 59

Configuring Communication Settings for Discovered Devices

To configure AMP 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 26.

Figure 26 *Device Setup > Communication Page Illustration*



Default Credentials

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

3Com	Edit View
APC	Edit View
Alcatel-Lucent	Edit View
Alcatel-Lucent Switch	Edit View
Aruba	Edit View
Aruba AirMesh	Edit View
Aruba Clearpass Policy Manager	Edit View
Aruba Switch	Edit View
Avaya	Edit View
BelAir	Edit View
Cisco Aironet 4800	Edit View
Cisco IOS AP	Edit View
Cisco Switch	Edit View
Cisco VxWorks	Edit View
Cisco WLC	Edit View
Custom Device	Edit View
D-Link	Edit View
Dell	Edit View
Enterasys	Edit View
Enterasys RoamAbout AP3000/AP4102	Edit View
Foundry	Edit View
HP ProCurve 420	Edit View
HP ProCurve 520WL	Edit View

SNMP Settings

SNMP Timeout (3-60 sec): 10

SNMP Retries (1-40): 3

SNMPv3 Informs

Add New SNMPv3 User

1-1 ▾ of 1 SNMPv3 Users Page 1 ▾ of 1 Choose columns

		Username ▲	Auth Protocol	Priv Protocol
□	✎	aruba	SHA	DES

1-1 ▾ of 1 SNMPv3 Users Page 1 ▾ of 1

Select All - Unselect All

Delete

Telnet/SSH Settings

Telnet/SSH Timeout (3-120 sec): 20

HTTP Discovery Settings

HTTP Timeout (3-120 sec): 120

ICMP Settings

Attempt to ping devices that were unreachable via SNMP: ● Yes ○ No

Symbol 4131 and Cisco Aironet IOS SNMP Initialization

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

○ Do not modify SNMP settings

● Enable read-write SNMP

Save Revert

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

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

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

NOTE

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

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

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

Setting	Default	Description
SNMP Timeout (3-60 sec)	3	Sets the time, in seconds, that AMP waits for a response from a device after sending an SNMP request.
SNMP Retries (1-40)	3	Sets the number of times AMP tries to poll a device when it does not receive a response within the **SNMP Timeout Period** or the Group's **Missed SNMP Poll Threshold** setting (1-100). If AMP does not receive an SNMP response from the device after the specified number of retries, AMP classifies that device as **Down**. **NOTE:** Although the upper limit for this value is 40, some SNMP libraries still have a hard limit of 20 retries. In these cases, any retry value that is set above 20 will still stop at 20.

3. Locate the **SNMPv3 Informs** section. Select the **Add** button to reveal configuration options. AMP users will need to configure all v3 users that are configured on the controller. The SNMP Inform receiver in the AMP will be restarted when users are changed or added to the controller.
   - **Username** - Username of the SNMP v3 user as configured on the controller.
   - **Auth Protocol** - Can be MD5 or SHA. The default setting is SHA.
   - **Auth and Priv Protocol Passphrases** - Enter the authentication and privilege protocol passphrases for the user as configured on the controller.
   - **Priv Protocol** - Can be DES or AES. The default setting is DES..

NOTE

This form allows you to edit existing SNMPv3 users by selecting the pencil icon next to the desired user. It also allows you to remove existing users by selecting the user's checkbox and then clicking **Delete**.

4. Locate the **Telnet/SSH Settings** section, and complete or adjust the default value for the field. Table 28 shows the setting and default value.

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

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

5. Locate the **HTTP Discovery Settings** section and adjust the default value. Table 29 shows the setting and default value.

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

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

6. Locate the **ICMP Settings** section and adjust the default value as required. Table 30 shows the setting and default value.

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

Setting	Default	Description
Attempt to ping devices that were unreachable via SNMP	Yes	● When **Yes** is selected, AMP attempts 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. **NOTE:** If ICMP is disabled on the network, select **No** to avoid the performance penalty caused by numerous ping requests.

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

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

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

Loading Device Firmware Onto AMP (optional)

AMP 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 AMP for distribution to devices via the **Device Setup > Upload Firmware & Files** page.

This page lists all firmware files on AMP 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 AMP appear as an option in the drop-down menu on the **Groups > Firmware** page and as a label on individual **APs/Devices > Manage** pages.
- Use the AMP Setup page to configure AMP-wide default firmware options.

Table 32 below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

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

Setting	Default	Description
Type	Aruba Networks Controller(any model)	Displays a drop-down list of the primary AP makes and models that AMP 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

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

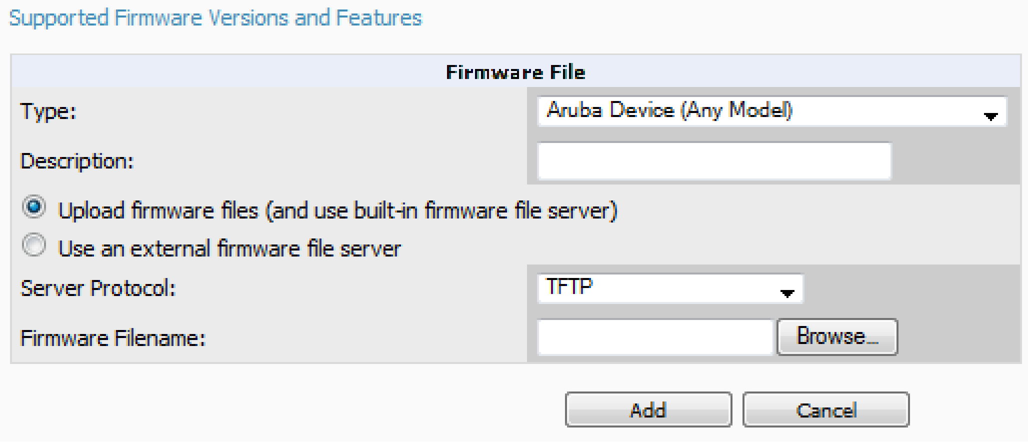
Setting	Default	Description
		obtained from the server. This can be FTP, TFTP, HTTP, or HTTPS.
Use Group File Server	None	If enabled, displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to AMP and to be transferred to an AP when the file is used in an upgrade.
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to AMP. The MD5 checksum is used to verify that the file was uploaded to AMP 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.
Firmware Version	None	Displays the firmware version number. This is a user-configurable field.
HTML Filename	None	Supporting HTML, displays the name of the file that was uploaded to AMP and to be transferred to an AP when the file is used in an upgrade.
HTML MD5 Checksum	None	Supporting HTML, displays the MD5 checksum of the file after it was uploaded to AMP. The MD5 checksum is used to verify that the file was uploaded to AMP 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.
HTML Version	None	Supporting HTML, displays the version of HTML used for file transfer.
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 onto AMP

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

1. Go to the **Device Setup** > **Upload Firmware & Files** page.
2. Select **Add**. The Add Firmware File page appears. Figure 27 illustrates this page.

Figure 27 *Device Setup > Upload Firmware and Files > Add Page Illustration*



Supported Firmware Versions and Features

Firmware File

Type: Aruba Device (Any Model)

Description:

● Upload firmware files (and use built-in firmware file server)

○ Use an external firmware file server

Server Protocol: TFTP

Firmware Filename: [Browse...]

[Add] [Cancel]

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

NOTE

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

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

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

Setting	Default	Description
Type	Aruba Networks controller	Indicates the firmware file is used with the specified type. 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. This open appears if **Use an external firmware file server** is enabled.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware)	Enabled	Allows you to select a firmware from your local machine and upload it via TFTP or FTP.
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.
Server Protocol	TFTP	Specify whether to use a built-in TFTP server or FTP, HTTP,

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

Setting	Default	Description
		or HTTPS to upload a firmware file. TFTP is recommended. If you select FTP, AMP uses an anonymous user for file upload.
Use Group File Server	Disabled	If you opt to use an external firmware file server, this additional option appears. This setting instructs AMP to use the server that is associated with the group instead of defining a server.
Firmware File Server IP Address	None	Provides the IP address of the External TFTP Server (like SolarWinds) used for the firmware upgrade. This option displays when the user selects the **Use an external firmware file** option.
Firmware Filename	None	Enter the name of the firmware file that needs to be uploaded. Ensure that the firmware file is in the TFTP root directory. If you are using a non-external server, you select **Choose File** to find your local copy of the file.
HTML Filename	None	Browse to the HTML file that will accompany the firmware upload. Note that this field is only available for certain Firmware File Types (for example, Symbol 4121).
Patch Filename	None	If you selected Symbol WS5100 as the Firmware File Type, and you are upgrading from version 3.0 to 3.1, then browse to the path where the patch file is located.
Boot Software Version	None	If you specified a Cisco WLC device as the Firmware File Type, then also enter the boot software version.

NOTE

Additional fields may appear for multiple device types. AMP 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 AMP for the firmware to be distributed successfully via AMP.

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

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

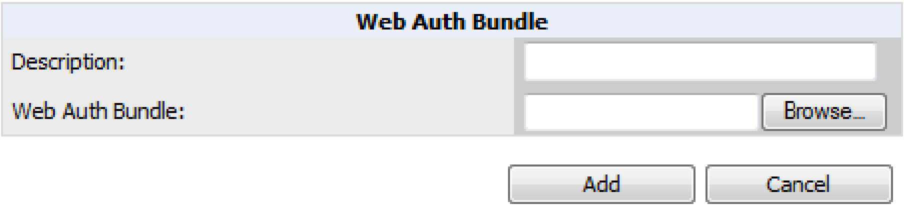
Web authentication bundles are configuration files that support Cisco WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco WLC devices.

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

1. Go to the **Device Setup** > **Upload Firmware & Files** page. This page displays any existing Web Auth bundles that are currently configured in AMP, and allows you to add or delete Web Auth bundles.

2. Scroll to the bottom of the page. Select the **Add New Web Auth Bundle** button to create a new Web Auth bundle (see Figure 28), or select the pencil icon next to an existing bundle to edit. You may also delete Web Auth bundles by selecting that bundle with the checkbox, and selecting **Delete**.

Figure 28 ***Add Web Auth Bundle*** *Page Illustration*



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

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

- Wireless LAN controller Web Authentication Configuration Example, Document ID: 69340
  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008067489f.shtml

Setting Up Device Types

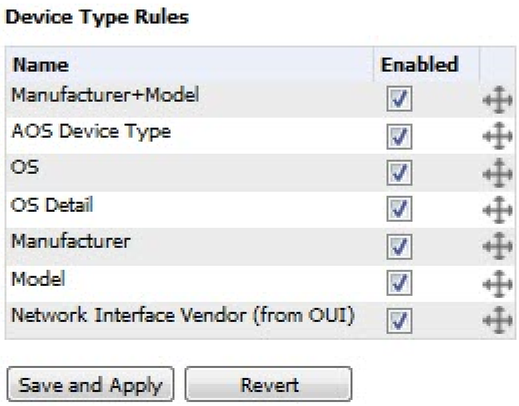
On **AMP Setup > Device Type Setup**, you can define how the Device Type displayed for users on your network is calculated from available data. The first matching property is used. These rules cannot be edited or deleted, but only reordered or enabled.

You can change the priority order of rules by dragging and dropping rows, as shown in Figure 29.

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

Refer to "Monitoring and Supporting WLAN Clients" on page 235 for more information on the **Device Type** column that appears in **Clients** list tables.

Figure 29 *AMP Setup > Device Type Setup Page Illustration*



Device Type Rules

Name	Enabled
Manufacturer+Model	☑
AOS Device Type	☑
OS	☑
OS Detail	☑
Manufacturer	☑
Model	☑
Network Interface Vendor (from OUI)	☑

Configuring Cisco WLSE and WLSE Rogue Scanning

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

- "Introduction to Cisco WLSE" on page 64
- "Initial WLSE Configuration" on page 64
- "Configuring IOS APs for WDS Participation" on page 66
- "Configuring ACS for WDS Authentication" on page 67
- "Configuring Cisco WLSE Rogue Scanning" on page 67

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 AMP to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. Table 34 describes these components.

Table 34: *Cisco SWAN Architecture Components*

SWAN Component	Requirements
WDS (Wireless Domain Services)	● WDS Name ● Primary and backup IP address for WDS devices (IOS AP or WLSM) ● WDS Credentials APs within WDS Group **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.
WLSE (Wireless LAN Solution Engine)	● IP Address ● Login
ACS (Access Control Server)	● IP Address ● Login
APs	● APs within WDS Group

Initial WLSE Configuration

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

- "Adding an ACS Server for WLSE" on page 64
- "Enabling Rogue Alerts for Cisco WLSE" on page 65
- "Configuring WLSE to Communicate with APs" on page 65
- "Discovering Devices" on page 65
- "Managing Devices" on page 65
- "Inventory Reporting" on page 65
- "Defining Access" on page 66
- "Grouping" on page 66

Adding an ACS Server for WLSE

1. Go 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. Select **Save**.

Enabling Rogue Alerts for Cisco WLSE

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

Additional information about rogue device detection is available in "Configuring Cisco WLSE Rogue Scanning" on page 67.

Configuring WLSE to Communicate with APs

1. Go to the **Device Setup > Discover** page.
2. Configure SNMP Information.
3. Configure HTTP Information.
4. Configure Telnet/SSH Credentials
5. Configure HTTP ports for IOS access points.
6. Configure WLCCP credentials.
7. Configure AAA information.

Discovering Devices

The following three methods can be used to discover access points within WLSE:

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

Perform these steps to discover access points.

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

Managing Devices

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

NOTE

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

Use these pages to make such configurations:

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

Inventory Reporting

When new devices are managed, the WLSE generates an inventory report detailing the new APs. AMP 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 AMP, CDP, SNMP scanning, and HTTP scanning discovery for Cisco IOS access points. Perform these steps for inventory reporting.

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

Defining Access

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

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

Grouping

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

1. Go to **Devices** > **Group Management**.
2. Configure **Role** and **User**.

Configuring IOS APs for WDS Participation

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

- Primary WDS
- Backup WDS
- WDS Member

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

NOTE

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

WDS Participation

Perform these steps to configure WDS participation.

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

Primary or Secondary WDS

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

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

8. Select the **ACS server** in the **Priority 1** drop-down menu and select **Apply**.

Configuring ACS for WDS Authentication

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

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

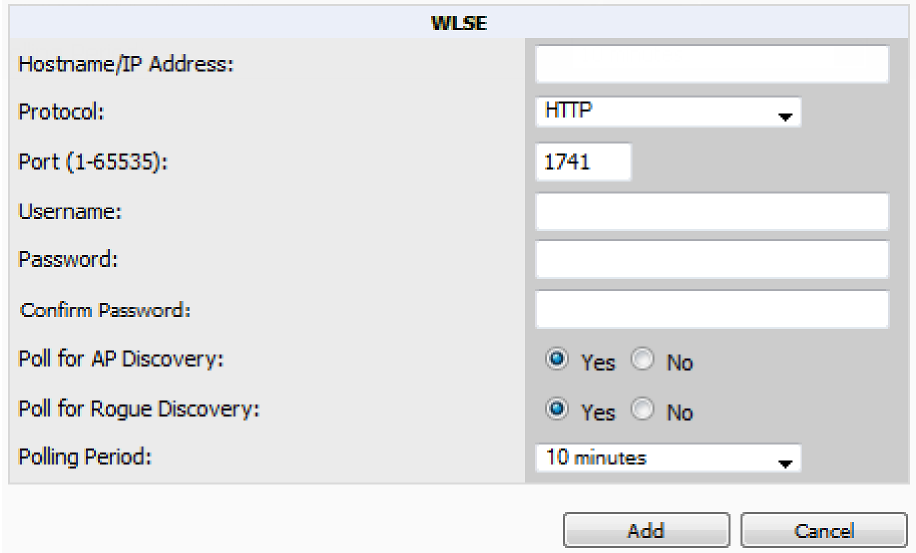
For additional and more general information about ACS, refer to "Configuring ACS Servers" on page 68.

Configuring Cisco WLSE Rogue Scanning

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

Figure 30 illustrates and itemizes the AMP settings for communication that is enabled between AMPand WLSE.

Figure 30 ***AMP Setup > WLSE > Add New WLSE*** *Page Illustration*



WLSE

Hostname/IP Address:	
Protocol:	HTTP
Port (1-65535):	1741
Username:	
Password:	
Confirm Password:	
Poll for AP Discovery:	● Yes ○ No
Poll for Rogue Discovery:	● Yes ○ No
Polling Period:	10 minutes

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

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

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

Setting	Default	Description
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	Specify whether to use HTTP or HTTPS when polling the WLSE.
Port	1741	Defines the port AMP uses to communicate with the WLSE server.
Username	None	Defines the username AMP uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on AMP. 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 AMP to pull the necessary XML APIs.
Password	None	Defines the password AMP uses to communicate with the WLSE server. The username and password must be configured the same way on the WLSE server and on AMP. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow AMP to pull the necessary XML APIs.
Poll for AP Discovery; Poll for Rogue Discovery	Yes	Sets the method by which AMP uses WLSE to poll for discovery of new APs and/or new rogue devices on the network.
Polling Period	10 minutes	Determines how frequently AMP polls WLSE to gather rogue scanning data.

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

What Next?

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

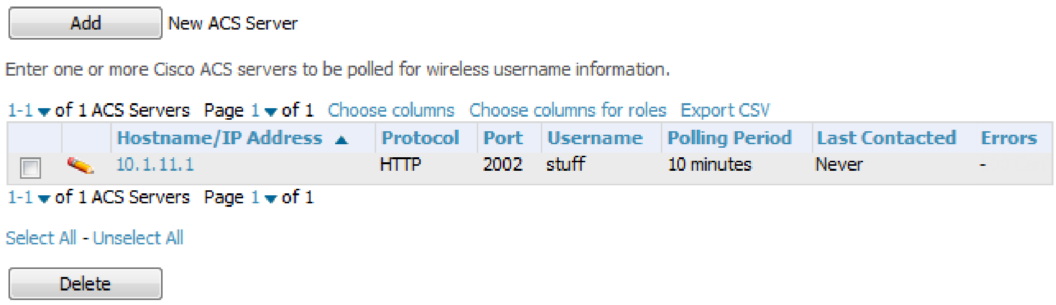
Configuring ACS Servers

This is an optional configuration. The **AMP Setup > ACS** page allows AMP to poll one or more Cisco ACS servers for wireless username information. When you specify an ACS server, AMP gathers information about your wireless users. Refer to "Setting Up Device Types" on page 63 if you want to use your ACS server to manage your AMP users.

Perform these steps to configure ACS servers:

1. Go to the **AMP Setup > ACS** page. This page displays current ACS setup, as illustrated in Figure 31.

Figure 31 *AMP Setup > ACS Page Illustration*



Enter one or more Cisco ACS servers to be polled for wireless username information.

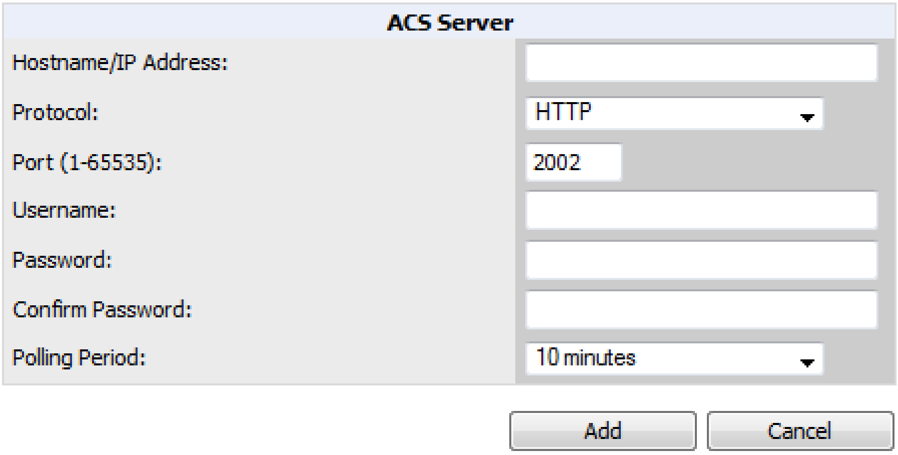
1-1 of 1 ACS Servers Page 1 of 1 Choose columns Choose columns for roles Export CSV

		Hostname/IP Address ▲	Protocol	Port	Username	Polling Period	Last Contacted	Errors
□	✎	10.1.11.1	HTTP	2002	stuff	10 minutes	Never	-

1-1 of 1 ACS Servers Page 1 of 1

2. Select **Add** to create a new ACS server, or select a pencil icon to edit an existing server. To delete an ACS server, select that server and select **Delete**. When selecting **Add** or edit, the **Details** page appears, as illustrated in Figure 32.

Figure 32 *AMP Setup > ACS > Add/Edit Details Page Illustration*



ACS Server

Hostname/IP Address:	
Protocol:	HTTP
Port (1-65535):	2002
Username:	
Password:	
Confirm Password:	
Polling Period:	10 minutes

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

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

Field	Default	Description
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 AMP uses when it polls the ACS server.
Port	2002	Sets the port through which AMP communicates with the ACS. AMP generally communicates over port 2002.
Username	None	Sets the Username of the account AMP uses to poll the ACS server.
Password	None	Sets the password of the account AMP uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently AMP polls the ACS server for username information.

4. Select **Add** to finish creating the new ACS server, or **Save** to finish editing an existing ACS server.

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

What Next?

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

Integrating AMP with an Existing Network Management Solution (NMS)

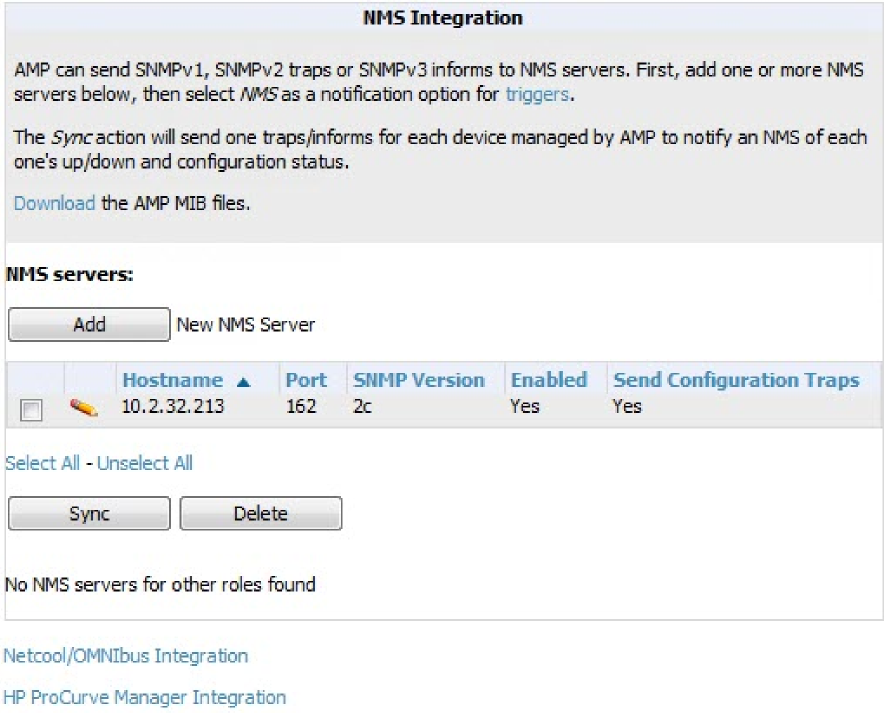
This is an optional configuration. The **AMP Setup** > **NMS** configuration page allows AMP to integrate with other Network Management Solution (NMS) consoles. This configuration enables advanced and interoperable functionality as follows:

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

Perform these steps to configure NMS support in AMP:

1. Go to **AMP Setup** > **NMS**, illustrated in Figure 33.

Figure 33 *AMP Setup > NMS Page Illustration*



NMS Integration

AMP can send SNMPv1, SNMPv2 traps or SNMPv3 informs 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 traps/informs for each device managed by AMP to notify an NMS of each one's up/down and configuration status.

Download the AMP MIB files.

NMS servers:

Add New NMS Server

		Hostname ▲	Port	SNMP Version	Enabled	Send Configuration Traps
□	✎	10.2.32.213	162	2c	Yes	Yes

Select All - Unselect All

No NMS servers for other roles found

Netcool/OMNIbus Integration

HP ProCurve Manager Integration

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

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

Setting	Default	Description
Hostname	None	Cites the DNS name or the IP address of the NMS.
Port	162	Sets the port AMP uses to communicate with the NMS. **NOTE:** AMP generally communicates via SNMP traps on port 162.
Community String	None	Sets the community string used to communicate with the NMS.
SNMP Version	2C	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 to information and instructions. The IBM Tivoli Netcool/OMNIbus operations management software enables automated event correlation and additional features resulting in optimized network uptime.
4. The **NMS Integration Add/Edit** page includes the **HP ProCurve Manager Integration** link. Select this link for additional information, zip file download, and brief instructions for installation with AMP. Select **Add** to finish creating the NMS server or **Save** to configure an existing NMS server.

What Next?

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

Auditing PCI Compliance on the Network

This section describes PCI requirements and auditing functions in AMP. It includes the following topics:

- "Introduction to PCI Requirements" on page 71
- "PCI Auditing" on page 72
- "Enabling or Disabling PCI Auditing" on page 73

Introduction to PCI Requirements

AMP 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.AMP 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 Web site

    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

PCI Auditing in AMP 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 73.
- The **Reports** > **Definitions** page allows you to create custom-configured and custom-scheduled PCI Compliance reports. See "Reports > Definitions Page Overview" on page 271.
- The **Reports** > **Generated** page lists PCI Compliance reports currently available, and allows you to generate the latest daily version of the PCI Compliance Report with a single select. Refer to "Reports > Generated Page Overview" on page 273.
- 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 73.
- The **PCI Compliance Report** offers additional information. Refer to "Using the PCI Compliance Report" on page 304. 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 AMP, AMP grades the network as pass or fail for the respective PCI requirement. Whenever a PCI requirement is not enabled in AMP, AMP does not monitor the network's status in relation to that requirement, and cannot designate Pass or Fail network status. AMP users without RAPIDS visibility enabled will not see the 11.1 PCI requirements in the PCI Compliance Report.

Table 38: *PCI Requirements and Support in AMP*

Requirement	Description
1.1	Monitoring configuration standards for network firewall devices When Enabled: PCI Requirement 1.1 establishes firewall and router configuration standards. A device fails Requirement 1.1 if there are mismatches between the desired configuration and the configuration on the device. When Disabled: firewall router and device configurations are not checked for PCI compliance, and Pass or Fail status is not reported or monitored.
1.2.3	Monitoring firewall installation between any wireless networks and the cardholder data environment When Enabled: A device passes requirement 1.2.3 if it can function as a stateful firewall. When Disabled: firewall router and device installation are not checked for PCI compliance.
2.1	Monitoring the presence of vendor-supplied default security settings When Enabled: PCI Requirement 2 establishes the standard in which all vendor-supplied default passwords are changed prior to a device's presence and operation in the network. A device fails requirement 2.1 if the username, passwords or SNMP credentials being used by AMP to communicate with the device are on a list of forbidden default credentials. The list includes common vendor default passwords, for example.

Table 38: *PCI Requirements and Support in AMP (Continued)*

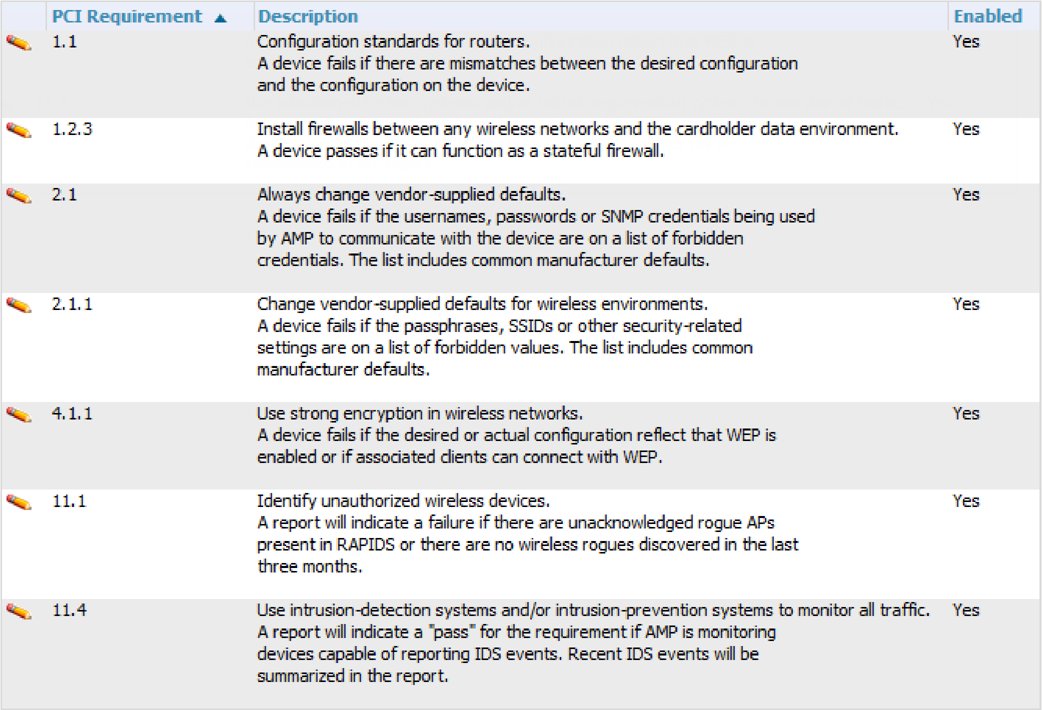
Requirement	Description
	When Disabled: device passwords and other vendor default settings are not checked for PCI compliance.
2.1.1	Changing vendor-supplied defaults for wireless environments When Enabled: A device fails requirement 2.1.1 if the passwords, SSIDs, or other security-related settings are on a list of forbidden values that AMP establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance. When Disabled: network devices are not checked for forbidden information and PCI Compliance is not established.
4.1.1	Using strong encryption in wireless networks 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. When Disabled: AMP cannot establish a pass or fail status with regard to PCI encryption requirements on the network.
11.1	Identifying unauthorized wireless devices. When enabled, 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.
11.4	Using intrusion-detection or intrusion-prevention systems to monitor all traffic When Enabled: AMP 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. When Disabled: AMP 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.

Enabling or Disabling PCI Auditing

Perform these steps to verify status and to enable or disable AMP support for PCI 1.2 requirements. enabling one or all PCI standards on AMP enables real-time information and generated reports that advise on Pass or Fail status. The PCI auditing supported in AMP is reported in Table 1 in the "PCI Auditing" on page 72 section.

1. To determine what PCI Compliance standards are enabled or disabled on AMP, navigate to the **AMP Setup > PCI Compliance** page, illustrated in Figure 34.

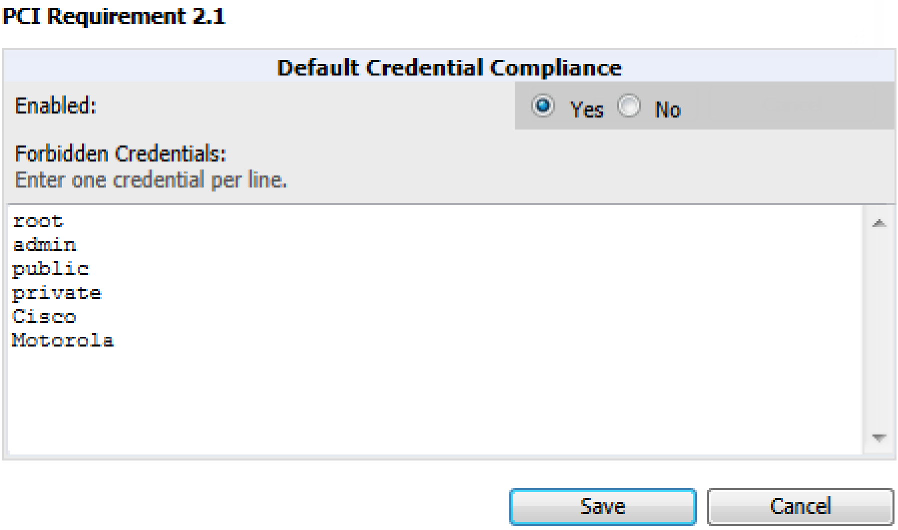
Figure 34 *AMP Setup > PCI Compliance page illustration*



	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 AMP 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 clients can connect with WEP.	Yes
✎	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.	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 AMP 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 AMP, select the pencil icon next to the category. The Default Credential Compliance page displays for the respective PCI standard.
3. Create changes as required. The edit pages will vary based on the PCI Requirement that you select. Figure 35 shows an example of how to edit the PCI 2.1 requirement.

Figure 35 *Default Credential Compliance for PCI Requirements*



PCI Requirement 2.1

Default Credential Compliance

Enabled: ● Yes ○ No

Forbidden Credentials:
Enter one credential per line.

```
root
admin
public
private
Cisco
Motorola
```

4. Select **Save**.
5. To view and monitor PCI auditing on the network, use generated or daily reports. See "Creating, Running, and Emailing Reports" on page 271. In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
   a. Go to the **APs/Devices > List** page.

b. Select a specific device. The **Monitor** page for that device displays. The **APs/Devices** page also displays a **Compliance** subtab in the menu bar.

c. Select **Compliance** to view complete PCI compliance auditing for that specific device.

Deploying WMS Offload

Overview of WMS Offload in AMP

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

- ArubaOS Version 2.5.4 or later
- AirWave Version 6.0 or later

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

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

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

General Configuration Tasks Supporting WMS Offload in AMP

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

1. Configure WLAN switches for optimal AMP monitoring.
   a. Disable debugging.
   b. Ensure the AMP server is a trap receiver host.
   c. Ensure proper traps are enabled.
2. Configure AMP to optimally monitor the AMP infrastructure.
   a. Enable WMS offload on the **AMP Setup** > **General** page.
   b. Configure SNMP communication.
   c. Create a proper policy for monitoring the AMP infrastructure.
   d. Discover the infrastructure.
3. Configure device classification.
   a. Set up rogue classification.
   b. Set up rogue classification override.
   c. Establish user classification override devices.
4. Deploy ArubaOS-specific monitoring features.
   a. Enable remote AP and wired network monitoring.
   b. View controller license information.
5. Convert existing floor plans to VisualRF to include the following elements:
   - ArubaOS
   - RF Plan
6. Use RTLS for increasing location accuracy (optional).

a. Enable RTLS service on the AMP server.

b. Enable RTLS on ArubaOS infrastructure.

Additional Information Supporting WMS Offload

Refer to the *Aruba and AirWave 7.7 Best Practices Guide* for additional information, including detailed concepts, configuration procedures, restrictions, ArubaOS infrastructure, and AMP version differences in support of WMS Offload.

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

Figure 36 *Subtabs under the **Group** tab*

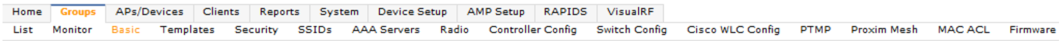


Table 39: *Groups pages*

Menu Item	Description	Refer to
List	This page is the default page in the **Groups** section of AMP. It lists all groups currently configured in AMP and provides the foundation for all group-level configurations.	"Viewing All Defined Device Groups" on page 80
Monitor	This page displays client and bandwidth usage information, lists devices in a given group, provides an **Alert Summary** table for monitoring alerts for the group, and provides a detailed **Audit Log** for group-level activity.	"Viewing Device Monitoring Statistics" on page 136
Basic	This page appears when you create a new group on the **Groups > List** page. Once you define a group name, AMP displays the **Basic** page from which you configure many group-level settings. This page remains available for any device group configured in AMP.	"Configuring Basic Group Settings" on page 81
Templates	This page manages templates for any device group. Templates allow you to manage the configuration of Dell Networking W-Series, 3Com, Alcatel-Lucent, Aruba Networks, Cisco Aironet IOS, Cisco Catalyst switches, Enterasys, HP, Nortel, Symbol and Trapeze devices in a given group using a configuration file. Variables in such templates configure device-specific properties, such as name, IP address and channel. Variables also define group-level properties.	"Creating and Using Templates" on page 178
Security	This page defines general security settings for device groups, to include RADIUS, encryption, and additional security settings on devices.	"Configuring Group Security Settings" on page 91
SSID	This page sets SSIDs, VLANs, and related parameters in device groups.	"Configuring Group SSIDs and VLANs" on page 95

Table 39: *Groups pages (Continued)*

Menu Item	Description	Refer to
AAA Servers	This page configures authentication, authorization, and accounting settings in support of RADIUS servers for device groups.	"Adding and Configuring Group AAA Servers" on page 90
Radio	This page defines general 802.11 radio settings for device groups.	"Configuring Radio Settings for Device Groups" on page 99
Controller Config	This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Aruba devices on the network. Use this page as an alternative to the **Device Setup > Aruba > Configuration** page. The appearance of this page varies depending on whether AMP is configured for global configuration or group configuration.	*Aruba Controller Configuration Guide*
Switch Config	This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Aruba switches on the network.	*Aruba Aruba Switch Configuration Guide*
Instant Config	This page manages Aruba Instant devices on the network.	*Aruba Instant User 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.	"Cisco WLC Group Configuration" on page 103
PTMP	This page defines settings specific to Proxim MP devices when present. As such, this page is only available when a Proxim MP device is added to this group.	"Configuring Group PTMP Settings" on page 110.
Proxim Mesh	This page defines mesh AP settings specific to Proxim devices when present.	"Configuring Proxim Mesh Radio Settings" on page 111
MAC ACL	This page defines MAC-specific settings that apply to Proxim, Symbol, and ProCurve 520 devices when present.	"Configuring Group MAC Access Control Lists" on page 113

Table 39: *Groups pages (Continued)*

Menu Item	Description	Refer to
Firmware	This page manages firmware files for many devices.	"Specifying Minimum Firmware Versions for APs in a Group" on page 114
Compare	This page allows you to compare line item-settings between two device groups. On the **Groups > List** page, select the **Compare two groups** link, select the two groups from the drop-down menus, and then select **Compare**. Refer to	"Comparing Device Groups" on page 115

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

- "Deleting a Group" on page 116
- "Changing Multiple Group Configurations " on page 117
- "Modifying Multiple Devices" on page 118
- "Using Global Groups for Group Configuration" on page 121

AMP Groups Overview

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

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

Typical group configuration variables include the following settings:

- Basic settings - SSID, SNMP polling interval, and so forth
- Security settings - VLANs, WEP, 802.1x, ACLs, and so forth
- Radio settings - data rates, fragmentation threshold, RTS threshold, DTIM, preamble, and so forth.

When configuration changes are applied at a *group level*, they are assigned automatically to every device within that group. Such changes must be applied with every device in **Managed** mode. **Monitor** mode is the more common mode.

CAUTION

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

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

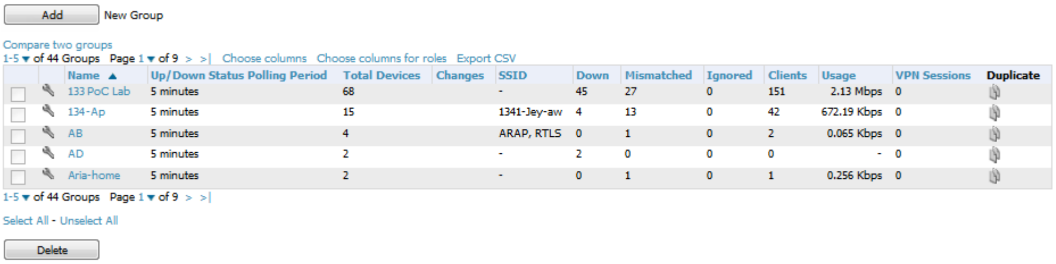
You can create as many different groups as required. Administrators usually establish groups that range in size from five to 100 wireless devices.

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

Viewing All Defined Device Groups

To display a list of all defined groups, browse to the **Groups** > **List** page, illustrated in Figure 37.

Figure 37 *Groups > List Page Illustration (partial view)*


Add
New Group
Compare two groups
1-5 ▾ of 44 Groups Page 1 ▾ of 9 > >| Choose columns Choose columns for roles Export CSV

		Name ▲	Up/Down Status Polling Period	Total Devices	Changes	SSID	Down	Mismatched	Ignored	Clients	Usage	VPN Sessions	Duplicate
□		133 PoC Lab	5 minutes	68		-	45	27	0	151	2.13 Mbps	0	
□		134-Ap	5 minutes	15		1341-Jey-aw	4	13	0	42	672.19 Kbps	0	
□		AB	5 minutes	4		ARAP, RTLS	0	1	0	2	0.065 Kbps	0	
□		AD	5 minutes	2		-	2	0	0	0	-	0	
□		Aria-home	5 minutes	2		-	0	1	0	1	0.256 Kbps	0	

1-5 ▾ of 44 Groups Page 1 ▾ of 9 > >|
Select All - Unselect All
Delete

Table 40 describes the columns in the **Groups** > **List** page.

Table 40: *Groups > List Columns*

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 81.
Manage (wrench icon)	Goes to the **Groups > Basic** configuration page for that group. Hover your mouse over the icon to see a list of shortcuts to group-specific subtabs that would appear across the navigation section if this group is selected. (See Figure 38 in "Configuring Basic Group Settings" on page 81.)
Name	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).
Up/Down Status Polling Period	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.
Total Devices	Total number of devices contained in the group including APs, controllers, routers, or switches.
Changes	Displays when a group has unapplied changes.
Is Global Group	If a group is designated as global, it may not contain APs but it may be used as a template for other groups. This column may also indicate **Yes** if this group has been pushed to AMP from a Master Console.
Global Group	Specifies which group this Subscriber Group is using as its template.

Table 40: *Groups > List Columns (Continued)*

Column	Description
SSID	The SSID assigned to supported device types within the group.
Down	The number of access points within the group that are not reachable via SNMP or are no longer associated to a controller. Note that thin APs are not directly polled with SNMP, but are polled through the controller. That controller may report that the thin AP is down or is no longer on the controller. At this point, AMP classifies the device as down.
Mismatched	The number of devices within the group that are in a mismatched state.
Ignored	The number of ignored devices in that group.
Clients	The number of mobile users associated with all access points within the group. To avoid double counting of clients, clients are only listed in the group of the AP with which they are associated. Note that device groups with only controllers in them report no clients.
Usage	A running average of the sum of bytes in and bytes out for the managed radio page.
VPN Sessions	Number of active (connected) VPN sessions under this group.
Duplicate	Creates a new group with the name **Copy of <Group Name>** with identical configuration settings. (Aruba configuration settings will have to be manually added back.)

NOTE

When you first configure AMP, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to "Configuring Basic Group Settings" on page 81.

Configuring Basic Group Settings

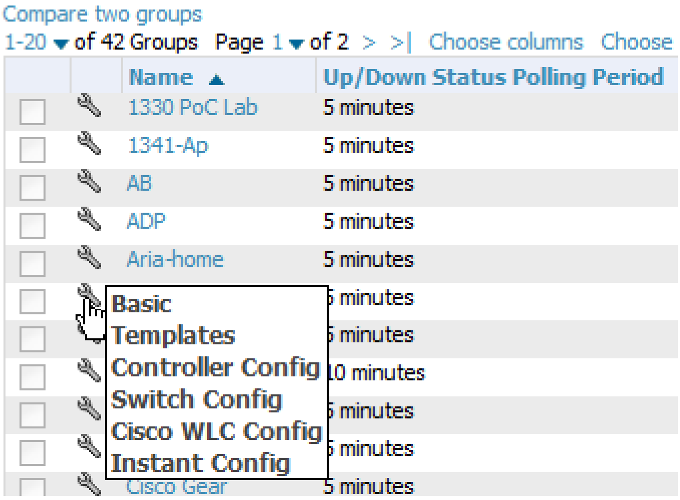
The first default device group that AMP sets up is the **Access Points** group, but you can use this procedure to add and configure any device group. Perform these steps to configure basic group settings, then continue to additional procedures to define additional settings as required.

- To create a new group, select **Add** on the **Groups > List page**. Enter a group name and select **Add**. The **Groups > Basic** page appears.
- To edit an existing device group, select the **manage** (wrench) icon next to the group. The **Groups > Basic** page appears. If you mouse over an existing group’s wrench, a popup menu displays, allowing you to select options such as **Basic**, **Templates**, **Security**, **SSIDs**, **AAA Servers**, **Radio**, **Controller Config**, **Switch Config**, **Instant Config**, and **Cisco WLC Config**. See Figure 38.

NOTE

The mouse-over list can vary based on a group's settings.

Figure 38 *Pop-up When Hovering over Wrench Icon in Groups > List*



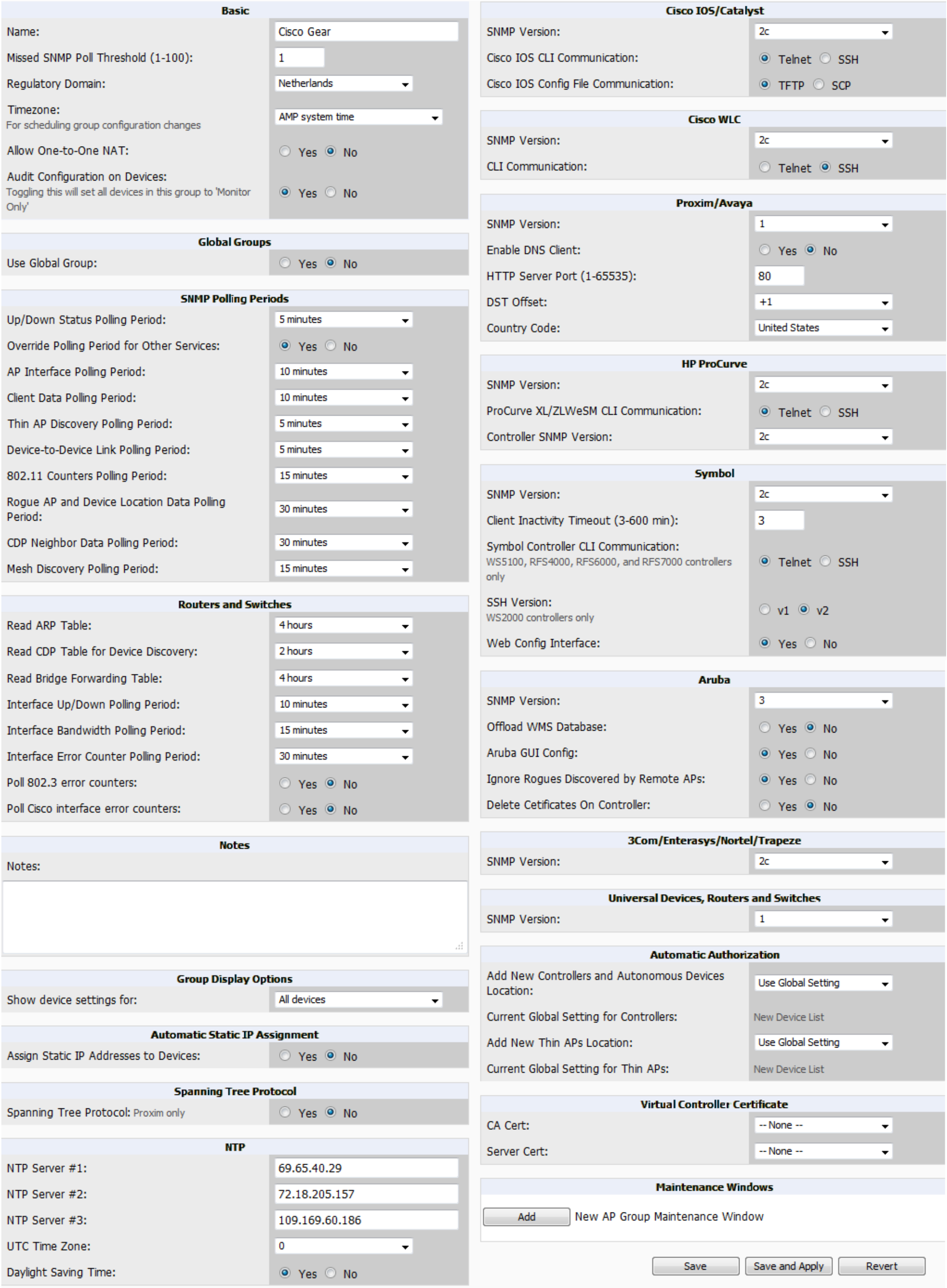
Compare two groups

1-20 ▾ of 42 Groups Page 1 ▾ of 2 > >| Choose columns Choose

		Name ▲	Up/Down Status Polling Period
□		1330 PoC Lab	5 minutes
□		1341-Ap	5 minutes
□		AB	5 minutes
□		ADP	5 minutes
□		Aria-home	5 minutes
□			5 minutes
□			5 minutes
□			10 minutes
□			5 minutes
□			5 minutes
□		Cisco Gear	5 minutes

Figure 39 illustrates one example of the **Groups** > **Basic** page.

Figure 39 *Groups > Basic Page Illustration*



Basic

Name: Cisco Gear

Missed SNMP Poll Threshold (1-100): 1

Regulatory Domain: Netherlands

Timezone: AMP system time
For scheduling group configuration changes

Allow One-to-One NAT: ○ Yes ● No

Audit Configuration on Devices: ● Yes ○ No
Toggling this will set all devices in this group to 'Monitor Only'

Global Groups

Use Global Group: ○ Yes ● No

SNMP Polling Periods

Up/Down Status Polling Period: 5 minutes

Override Polling Period for Other Services: ● Yes ○ No

AP Interface Polling Period: 10 minutes

Client Data Polling Period: 10 minutes

Thin AP Discovery Polling Period: 5 minutes

Device-to-Device Link Polling Period: 5 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

Mesh Discovery Polling Period: 15 minutes

Routers and Switches

Read ARP Table: 4 hours

Read CDP Table for Device Discovery: 2 hours

Read Bridge Forwarding Table: 4 hours

Interface Up/Down Polling Period: 10 minutes

Interface Bandwidth Polling Period: 15 minutes

Interface Error Counter Polling Period: 30 minutes

Poll 802.3 error counters: ○ Yes ● No

Poll Cisco interface error counters: ○ Yes ● No

Notes

Notes:

Group Display Options

Show device settings for: All devices

Automatic Static IP Assignment

Assign Static IP Addresses to Devices: ○ Yes ● No

Spanning Tree Protocol

Spanning Tree Protocol: Proxim only ○ Yes ● No

NTP

NTP Server #1: 69.65.40.29

NTP Server #2: 72.18.205.157

NTP Server #3: 109.169.60.186

UTC Time Zone: 0

Daylight Saving Time: ● Yes ○ No

Cisco IOS/Catalyst

SNMP Version: 2c

Cisco IOS CLI Communication: ● Telnet ○ SSH

Cisco IOS Config File Communication: ● TFTP ○ SCP

Cisco WLC

SNMP Version: 2c

CLI Communication: ○ Telnet ● SSH

Proxim/Avaya

SNMP Version: 1

Enable DNS Client: ○ Yes ● No

HTTP Server Port (1-65535): 80

DST Offset: +1

Country Code: United States

HP ProCurve

SNMP Version: 2c

ProCurve XL/ZLWeSM CLI Communication: ● Telnet ○ SSH

Controller SNMP Version: 2c

Symbol

SNMP Version: 2c

Client Inactivity Timeout (3-600 min): 3

Symbol Controller CLI Communication: ● Telnet ○ SSH
WS5100, RFS4000, RFS6000, and RFS7000 controllers only

SSH Version: ○ v1 ● v2
WS2000 controllers only

Web Config Interface: ● Yes ○ No

Aruba

SNMP Version: 3

Offload WMS Database: ○ Yes ● No

Aruba GUI Config: ● Yes ○ No

Ignore Rogues Discovered by Remote APs: ● Yes ○ No

Delete Certificates On Controller: ○ Yes ● No

3Com/Enterasys/Nortel/Trapeze

SNMP Version: 2c

Universal Devices, Routers and Switches

SNMP Version: 1

Automatic Authorization

Add New Controllers and Autonomous Devices Location: Use Global Setting

Current Global Setting for Controllers: New Device List

Add New Thin APs Location: Use Global Setting

Current Global Setting for Thin APs: New Device List

Virtual Controller Certificate

CA Cert: -- None --

Server Cert: -- None --

Maintenance Windows

New AP Group Maintenance Window

1. Define the settings in the **Basic** and **Global Group** sections. Table 41 describes several typical settings and default values of this **Basic** section.

Table 41: *Basic and Global Groups 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 name to uniquely identify the group by location, vendor, department, or any other identifier (such as Accounting APs, Cisco devices, 802.1x APs, and so forth).
Missed SNMP Poll Threshold (1-100)	1	Sets the number of Up/Down SNMP polls that must be missed before AMP considers a device to be down. The number of SNMP retries and the SNMP timeout of a poll can be set on the **Device Setup > Communication** page.
Regulatory Domain	United States	Sets the regulatory domain in AMP, 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	No	Allows AMP 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.
Is Global Group	No	If specified as **Yes**, then this group can be selected in the Use Global Group drop down menu for future group configurations.
Use Global Group	No	When enabled, this field allows you to define the device group to be a Global Group. Refer to "Using Global Groups for Group Configuration" on page 121.

2. Complete the **SNMP Polling Periods** section. The information in this section overrides default settings. Table 42 describes the SNMP polling settings.

Table 42: *SNMP Polling Periods 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** page. An initial polling interval of **5** minutes is best for most networks.
Override Polling Period for Other Services	No	Enables or disables overriding the base SNMP Polling Period. If you select **Yes**, the other settings in the SNMP Polling Periods section are activated, and you can override default values.
AP Interface Polling	10	Sets the interval at which AMP polls for radio monitoring and

Table 42: *SNMP Polling Periods Fields and Default Values (Continued)*

Setting	Default	Description
Period	minutes	bandwidth being used by a device.
Client Data Polling Period	10 minutes	Sets time between SNMP polls for client data for devices in the group.
Thin AP Discovery Polling Period	15 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.
802.11 Counters Polling Period	15 minutes	Sets time between SNMP polls for 802.11 Counter information.
Rogue AP and Device Location Data Polling Period	30 minutes	Sets time between SNMP polls for Rogue AP and Device Location Data polling.
CDP Neighbor Data Polling Period	30 minutes	Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors.
Mesh Discovery Polling Period	15 minutes	Sets time between SNMP polls for Mesh Device Discovery.

3. To configure support for routers and switches in the group, locate the **Routers and Switches** section and adjust these settings as required. This section defines the frequency in which all devices in the group polled. These settings can be disabled entirely as desired. Table 43 describes the SNMP polling settings.

Table 43: *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	For Cisco devices, sets the frequency in which devices poll routers and switches for Cisco Discovery Protocol (CDP) information. This setting can be disabled, or set to poll for CDP neighbor information in a range from every 15 seconds to 12 hours.
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 Up/Down Polling Period	5 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll from switches in a range from every 15 seconds to 30 minutes.

Table 43: *Routers and Switches Fields and Default Values (Continued)*

Setting	Default	Description
Interface Bandwidth Polling Period	15 minutes	Sets the frequency in which network interfaces are polled for bandwidth usage. This setting can be disabled, or set to poll from switches in a range from every 5 minutes to 30 minutes.
Interface Error Counter Polling Period	30 minutes	Sets the frequency in which network interfaces are polled for up/down status. This setting can be disabled, or set to poll bridge forwarding tables from switches in a range from every 5 minutes to 30 minutes.
Poll 802.3 error counters	No	Sets whether 802.3 error counters should be polled.
Poll Cisco interface error counters	No	Sets whether the interface error counters for Cisco devices should be polled.

4. Record additional information and comments about the group in the **Notes** section.
5. To configure which options and tabs are visible for the group, complete the settings in the **Group Display Options** section. Table 44 describes the settings and default values.

Table 44: *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: ● **All Devices**–AMP displays all Group tabs and setting options. ● **Only devices in this group**–AMP hides all options and tabs that do not apply to the devices in the group. If you use this setting, then to get the group list to display the correct SSIDs for the group, you must **Save and Apply** on the group. ● **Only devices on this AMP**– hides all options and tabs that do not apply to the APs and devices currently on AMP. ● **Use system defaults**–Use the default settings on **AMP Setup > General** ● **Selected device types**–Allows you to specify the device types for which AMP displays Group settings.
Selected Device Types	N/A	This option appears if you chose to display selected device types, allowing you to select the device types to display group settings. Use **Select devices in this group** to display only devices in the group being configured.

6. 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 45 describes the settings and default values This section is only relevant for a small number of device types, and will appear when they are present.

Table 45: *Automatic Static IP Assignment Fields and Default Values*

Setting	Default	Description
Assign Static IP Addresses to Devices	No	Specify whether to enable AMP to statically assign IP addresses from a specified range to all devices in the Group. If this value is set to **Yes**, then the additional configuration fields described in this table will become available.
Start IP	none	Sets the first address AMP assigns to the devices in the Group.

Table 45: *Automatic Static IP Assignment Fields and Default Values (Continued)*

Setting	Default	Description
Address		
Number of Addresses	none	Sets the number of addresses in the pool from which AMP can assign IP addresses.
Subnet Mask	none	Sets the subnet mask to be assigned to the devices in the Group.
Subnet Gateway	none	Sets the gateway to be assigned to the devices in the Group.
Next IP Address	none	Defines the next IP address queued for assignment. This field is disabled for the initial Access Points group.

7. To configure Spanning Tree Protocol on WLC devices and Proxim APs, locate the **Spanning Tree Protocol** section on the **Groups** > **Basic** configuration page. Adjust these settings as required. Table 46 describes the settings and default values.

Table 46: *Spanning Tree Protocol Fields and Default Values*

Setting	Default	Description
Spanning Tree Protocol	No	Specify wehther to enable or disables Spanning Tree Protocol on Proxim APs.If this value is set to **Yes**, then the additional configuration fields described in this table will become available.
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.

8. To configure Network Time Protocol (NTP) settings locate the **NTP** section and adjust these settings as required. Table 47 describes the settings and default values.

Table 47: *NTP Fields and Default Values*

Setting	Default	Description
NTP Server #1,2,3	None	Sets the IP address of the NTP servers 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 AMP graphs and logs use the time set on the AMP server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim section of the **Groups > Basic** configuration page.

9. To configure settings specific to Cisco IOS/Catalyst, locate the **Cisco IOS/Catalyst** section and adjust these settings as required. Table 48 describes the settings and default values.

Table 48: *Cisco IOS/Catalyst Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by AMP to communicate to the AP.
Cisco IOS CLI Communication	Telnet	The protocol AMP uses to communicate with Cisco IOS devices. Selecting **SSH** uses the secure shell for command line page (CLI) communication and displays an **SSH Version** option. Selecting **Telnet** sends the data in clear text via Telnet.
Cisco IOS Config File Communication	TFTP	The protocol AMP uses to communicate with Cisco IOS devices. Selecting **SCP** uses the secure copy protocol for file transfers and displays an **SCP Version** option. 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.

10. To configure settings specific to Cisco WLC, locate the **Cisco WLC** section and adjust these settings as required. Table 49 describes the settings and default values.

Table 49: *Cisco WLC Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Sets the version of SNMP used by AMP to communicate to WLC controllers.
CLI Communication	SSH	Sets the protocol AMP 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 to "Configuring Wireless Parameters for Cisco Controllers" on page 109.

11. To configure settings specific to Aruba locate the **Aruba** section and adjust these settings as required. Table 50 describes the settings and default values of this section.

Table 50: *Aruba Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by AMP to communicate to the AP.
Offload WMS Database	No	Configures commands previously documented in the AirWave 7.7 *Best Practices Guide*. When enabled, this feature allows AMP 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 **AMP Setup > General** is changed to **Yes**.

Table 50: *Aruba Fields and Default Values (Continued)*

Setting	Default	Description
Aruba GUI Config	Yes	This setting selects whether you'd like to configure your devices using the **Groups > Controller** method (either global or group) or using Templates.
Ignore Rogues Discovered by Remote APs	No	Configures whether to turn off RAPIDS rogue classification and rogue reporting for RAPs in this group.
Delete Certificates On Controller	No	Specifies whether to delete the current certificates on an ArubaOS controller.

12. To configure settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **3Com/Enterasys/Nortel/Trapeze** section and define the version of SNMP to be supported.
13. 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.
14. To control the conditions by which devices are automatically authorized into this group, locate the **Automatic Authorization** settings section and adjust these settings as required. Table 51 describes the settings and default values.

Table 51: *Automatic Authorization Fields and Default Values*

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

15. The specify the **Virtual Controller Certificates** to be applied to this group, locate the Virtual Controller Certificates settings section and adjust these settings as desired. Table 52 describes the settings and default values.

Table 52: *Virtual Controller Certificate Fields and Default Values*

Setting	Default	Description
CA Cert	None	Specify a CA certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Intermediate CA** or **Trusted CA** is added in the **Device Setup > Certificates** page.
Server Cert	None	Specify a server certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Server Cert** is added in the **Device Setup > Certificates** page.

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

What Next?

- Continue to additional sections in this chapter to create new groups or to edit existing groups.
- Once general group-level configurations are complete, continue to later chapters in this document to add or edit additional device-level configurations and to use several additional AMP functions.

Adding and Configuring Group AAA Servers

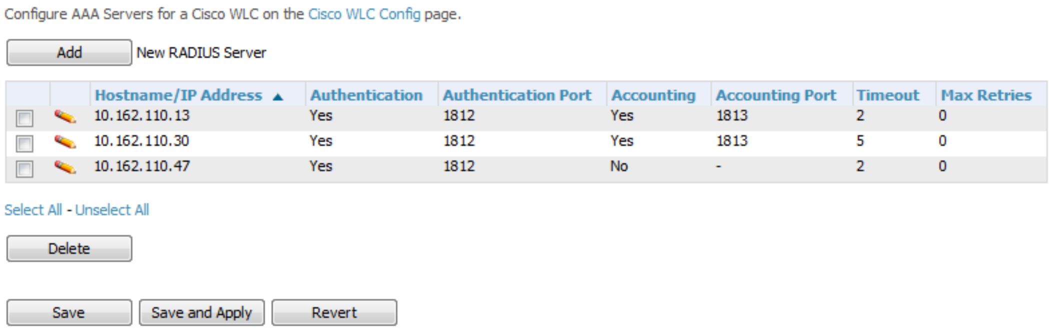
Configure RADIUS servers on the **Groups > AAA Servers** page.

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

> NOTE
>
> TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Cisco WLC Security Parameters and Functions" on page 109.

1. Go to the **Groups > List** page and select the group for which to define AAA servers by selecting the group name. The **Monitor** page appears.
2. Select the **AAA Servers** page. The **AAA Servers** page appears, enabling you to add a RADIUS server. Figure 40 illustrate this page for AAA RADIUS Servers:

Figure 40 *Groups > AAA Servers Page Illustration*



Configure AAA Servers for a Cisco WLC on the Cisco WLC Config page.

Add New RADIUS Server

		Hostname/IP Address ▲	Authentication	Authentication Port	Accounting	Accounting Port	Timeout	Max Retries
□	✎	10.162.110.13	Yes	1812	Yes	1813	2	0
□	✎	10.162.110.30	Yes	1812	Yes	1813	5	0
□	✎	10.162.110.47	Yes	1812	No	-	2	0

Select All - Unselect All

3. To add a RADIUS server or edit an existing server, select **Add New RADIUS Server** or the corresponding pencil icon to edit an existing server. Table 53 describes the settings and default values of the **Add/Edit** page.

Table 53: *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.

Table 53: *Adding a RADIUS Server Fields and Default Values (Continued)*

Setting	Default	Description
Secret and Confirm Secret	None	Sets the shared secret that is used to establish communication between AMP and the RADIUS server. **NOTE:** The shared secret entered in AMP must match the shared secret on the server.
Authentication	No	Sets the RADIUS server to perform authentication when this setting is enabled with **Yes**.
Authentication Port (1-65535)	1812	Appears when **Authentication** is enabled. 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 (1-65535)	1813	Appears when **Accounting** is enabled.Sets the port used for communication between the AP and the RADIUS server.
Timeout (0-86400)	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. Select **Add** to complete the creation of the RADIUS server, or select **Save** if editing an existing RADIUS server. The **Groups** > **AAA Servers** page displays this new or edited server. You can now reference this server on the **Groups** > **Security** page.

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

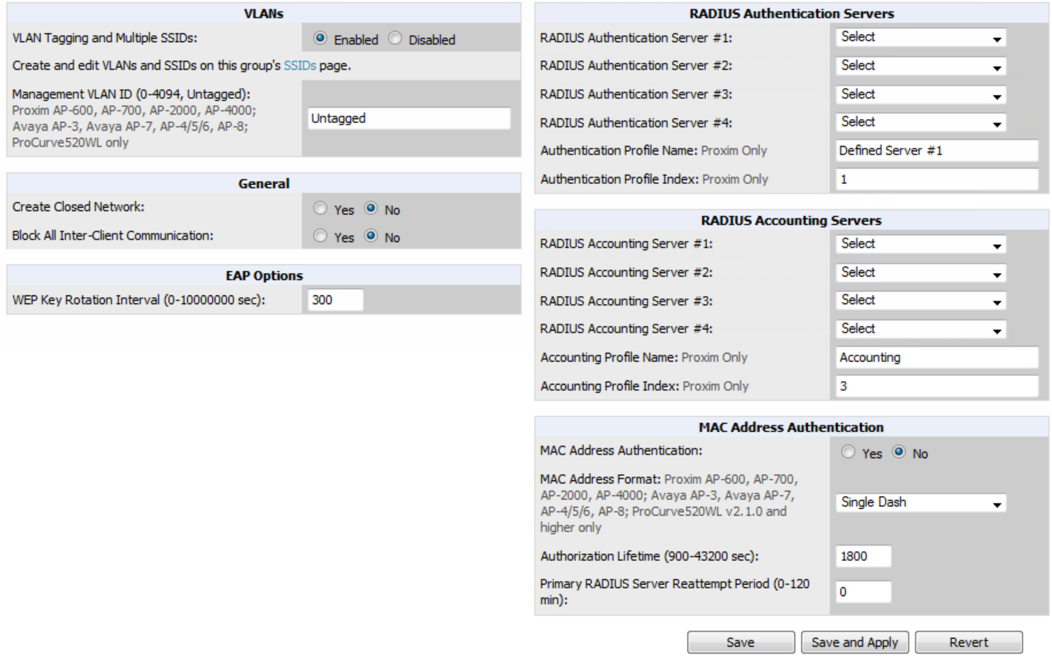
5. To make additional RADIUS configurations for device groups, use the **Groups** > **Security** page and continue to the next topic.

Configuring Group Security Settings

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

1. Select the device group for which to define security settings from the **Groups** > **List** page.
2. Go to **Groups** > **Security**. Some controls on this page interact with additional AMP pages. Figure 41 illustrates this page and Table 54 explains the fields and default values.

Figure 41 *Groups > Security Page Illustration*



VLANs

VLAN Tagging and Multiple SSIDs: ● Enabled ○ Disabled

Create and edit VLANs and SSIDs on this group's SSIDs page.

Management VLAN ID (0-4094, Untagged): Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL only: Untagged

General

Create Closed Network: ○ Yes ● No

Block All Inter-Client Communication: ○ Yes ● No

EAP Options

WEP Key Rotation Interval (0-10000000 sec): 300

RADIUS Authentication Servers

RADIUS Authentication Server #1: Select

RADIUS Authentication Server #2: Select

RADIUS Authentication Server #3: Select

RADIUS Authentication Server #4: Select

Authentication Profile Name: Proxim Only: Defined Server #1

Authentication Profile Index: Proxim Only: 1

RADIUS Accounting Servers

RADIUS Accounting Server #1: Select

RADIUS Accounting Server #2: Select

RADIUS Accounting Server #3: Select

RADIUS Accounting Server #4: Select

Accounting Profile Name: Proxim Only: Accounting

Accounting Profile Index: Proxim Only: 3

MAC Address Authentication

MAC Address Authentication: ○ Yes ● No

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

Authorization Lifetime (900-43200 sec): 1800

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

Table 54: *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 95. If this setting is disabled, then you can specify the **Encryption Mode** in the **Encryption** section that displays. Refer to "Groups > Security Encryption Mode settings" on page 94 for information on configuring Encryption.
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in AMP . This setting is supported only for the following devices: ● Proxim AP-600, AP-700, AP-2000, AP-4000 ● Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8 ● ProCurve520WL
General Section		
Create Closed Network	No	If enabled, the APs in the Group do not broadcast their SSIDs. **NOTE:** Creating a closed network will 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		

Table 54: *Groups > Security Page Fields and Default Values (Continued)*

Setting	Default	Description
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.
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.
Authentication Profile Name		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: ● 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
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

The **Encryption** options display on the **Groups** > **Security** page when the **VLAN Tagging and Multiple SSIDs** option is set to **Disabled**. This setting defaults to **No Encryption**. Refer to Table 55 for information regarding configuring encryption.

Table 55: *Groups > Security Encryption Mode settings*

Setting	Default	Description
Encryption Modes: Require 802.1X, Optional WEP, Require WEP, Require 802.1X, Require LEAP, 802.1X + WEP, 802.1X + WEP, LEAP + WEP,		
Encryption Mode	Require 802.1X	
Transmit Key	1	Select the Transmit Key value. This can be a value from 1 through 4. Note that 802.1X + WEP mode sets this key value to 1.
Key #1	None	Enter 40/64-bit Keys in 5 alphanumeric or 10 hexadecimal digits, or enter 104/128-bit Keys in 13 alphanumeric or 26 hexadecimal digits.
Key #2	None	
Key #3	None	
Key #4	None	
Encryption Mode Static CKIP		
CKIP Static Key (hex) and Confirm	None	Enter and confirm the Cisco Key Integrity Protocol (CKIP) static key, specified in hexadecimal digits.
CKIP Key Index	1	Select the CKIP Key Index value. This can be a value from 1 through 4.
CKIP Key Permutation	No	Specify whether to use Key Permutation.
CKIP MMH Mode	No	Specify whether to use Multi-Module Has (MMH) mode.
Encryption Mode WPA		
Unicast Cipher (Cisco only)	AES	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
Encryption Mode WPA/PSK		
Unicast Cipher (Cisco only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
WPA Preshared Key (Alphanumeric)	None	Enter an alphanumeric value for the preshared key.
Encryption Mode WPA2		
WPA2 WPA Compatibility Mode	Yes	Specify whether to enable WPA2 WPA Compatibility Mode.
WPA1 Cipher (Cisco WLC Only)	TKIP	Specify the WPA1 Cipher. Values include AES, TKIP, and AES/TKIP. **NOTE:** This drop down is only available if WPA2 WPA Compatibility Mode is **Yes**.

Table 55: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
Unicast Cipher (Cisco Only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
Encryption Mode WPA2/PSK		
WPA2 WPA Compatibility Mode	Yes	Specify whether to enable WPA2 WPA Compatibility Mode.
WPA1 Cipher (Cisco WLC Only)	TKIP	Specify the WPA1 Cipher. Values include AES, TKIP, and AES/TKIP. **NOTE:** This drop down is only available if WPA2 WPA Compatibility Mode is **Yes**.
Unicast Cipher (Cisco Only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
WPA Preshared Key (Alphanumeric)	None	Enter an alphanumeric value for the preshared key.
Encryption Mode xSec		
This indicates to use xSec encryption. No other configuration options are available.		

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

Configuring Group SSIDs and VLANs

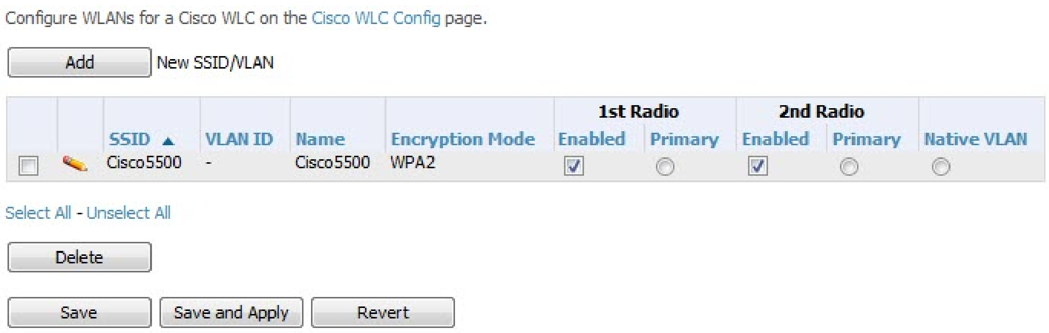
The **Groups** > **SSIDs** configuration page allows you to create and edit SSIDs and VLANs that apply to a device group. Perform these steps to create or edit VLANs and to set SSIDs.

NOTE

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

Figure 42 illustrates an example of the **Groups** > **SSIDs** page.

Figure 42 *Groups > SSIDs Page Illustration*



Configure WLANs for a Cisco WLC on the Cisco WLC Config page.

						1st Radio		2nd Radio		
		SSID ▲	VLAN ID	Name	Encryption Mode	Enabled	Primary	Enabled	Primary	Native VLAN
□	✎	Cisco5500	-	Cisco5500	WPA2	☑	○	☑	○	○

> **NOTE** AMP reports users by radio and by SSID. Graphs on the AP and controller monitoring pages display bandwidth in and out based on SSID. AMP reports can also be run and filtered by SSID. An option on the **AMP Setup > General** page can age out inactive SSIDs and their associated graphical data.

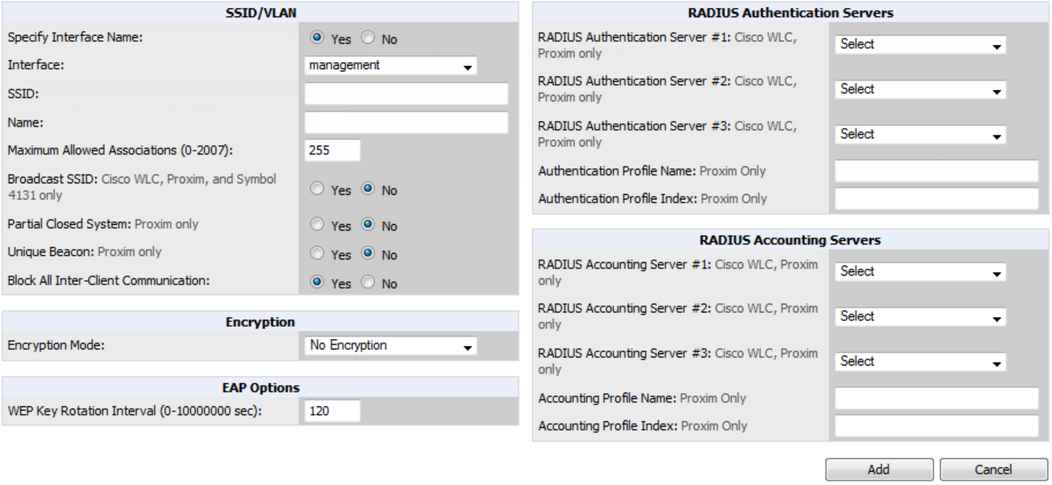
1. Go to **Groups** > **List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups** > **SSIDs** configuration page. Table 56 describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 56: *Groups > SSIDs Fields and Descriptions*

Field	Description
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	Enables the VLAN, SSID and Encryption Mode on the radio control.
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 the **Create Closed Network** setting below) in which the APs broadcast an SSID, the primary SSID is broadcast.
Native VLAN	Sets this VLAN to be the native VLAN. Native VLANs are untagged and typically used for management traffic only. AMP requires a Native VLAN to be set. For AP types do not require a native VLAN, create a dummy VLAN, disable it on both radio controls, and ensure that it has the highest VLAN ID.

3. Select **Add** to create a new SSID or VLAN, or select the pencil icon next to an existing SSID/VLAN to edit that existing SSID or VLAN. The **Add SSID/VLAN** configuration page appears as illustrated in Figure 43 and explained in Table 57.

Figure 43 *Add SSID/VLAN Page Illustration*



SSID/VLAN

Specify Interface Name:	● Yes ○ No
Interface:	management
SSID:	
Name:	
Maximum Allowed Associations (0-2007):	255
Broadcast SSID: Cisco WLC, Proxim, and Symbol 4131 only	○ Yes ● No
Partial Closed System: Proxim only	○ Yes ● No
Unique Beacon: Proxim only	○ Yes ● No
Block All Inter-Client Communication:	● Yes ○ No

Encryption

Encryption Mode:	No Encryption

EAP Options

WEP Key Rotation Interval (0-10000000 sec):	120

RADIUS Authentication Servers

RADIUS Authentication Server #1: Cisco WLC, Proxim only	Select
RADIUS Authentication Server #2: Cisco WLC, Proxim only	Select
RADIUS Authentication Server #3: Cisco WLC, Proxim only	Select
Authentication Profile Name: Proxim Only	
Authentication Profile Index: Proxim Only	

RADIUS Accounting Servers

RADIUS Accounting Server #1: Cisco WLC, Proxim only	Select
RADIUS Accounting Server #2: Cisco WLC, Proxim only	Select
RADIUS Accounting Server #3: Cisco WLC, Proxim only	Select
Accounting Profile Name: Proxim Only	
Accounting Profile Index: Proxim Only	

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

Table 57: *SSID/VLAN Section Fields and Default Values*

Setting	Default	Description
Specify Interface Name	Yes	Enables or disables an interface name for the VLAN interface. Selecting **No** for this option displays the **Enable VLAN Tagging** and **VLAN ID** options.
Enable VLAN Tagging (Cisco WLC, Proxim, Symbol only)		Enables or disables VLAN tagging. Displays if **Specify Interface Name** is set to **No**.
VLAN ID (1-4094)	None	Indicates the number of the VLAN designated as the **Native VLAN**, typically for management purposes. Displays if **Specify Interface Name** is set to **No** and **Enable VLAN Tagging** is set to **Yes**.
Interface	management	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.
Name	None	Sets a user-definable name associated with SSID/VLAN combination.
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.
Broadcast SSID (Cisco WLC, Proxim and Symbol 4131 only)	No	For specific devices as cited, this setting enables the AP to broadcast the SSID for the specified VLAN/SSID. This setting works in conjunction with the **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	This setting blocks communication between client devices based on SSID.

5. Locate the **Encryption** area on the **Groups** > **SSIDs** page and adjust these settings as required. Table 58 describes the available encryption modes. Table 55 in "Configuring Group Security Settings" on page 91 describes configuration settings for each mode.

Table 58: *Encryption Section Field 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: ● No Encryption ● **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**–Based on the WEP algorithm ● **Require LEAP**–Lightweight Extensible Authentication Protocol ● **802.1x+WEP**–Combines the two encryption types shown ● **802.1x+LEAP**–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 ● **xSec**–FIPS-compliant encryption including Layer 2 header info

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

Table 59: *EAP Options Section Field and Default Value*

Setting	Default	Description
WEP Key Rotation Interval (0-10000000 sec)	120	Time (in seconds) between WEP key rotation on the AP.

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

Table 60: *RADIUS Authentication Servers Fields and Default Values*

Setting	Default	Description
RADIUS Authentication Server 1-3 (Cisco WLC, Proxim only)	None	Drop-down menu to select RADIUS Authentication servers previously entered on the **Groups > 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.
Authentication Profile Index (Proxim Only)	None	Sets the Authentication Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

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

NOTE

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

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

Table 61: *Radius Accounting Servers Fields and Default Values*

Setting	Default	Description
RADIUS Accounting Server 1-3 (Cisco WLC, Proxim Only)	None	Pull-down menu selects RADIUS Accounting servers previously entered on the **Groups > 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.
Accounting Profile Index (Proxim Only)	None	Sets the Accounting Profile Index for Proxim AP-600, AP-700, AP-2000, AP-4000.

10. Select **Add** when you have completed all sections. This returns you to the **Groups** > **SSIDs** page.
11. Select **Save** to retain these **SSID** configurations for the group, select **Save and Apply** to make the changes permanent, or select **Revert** to discard all unapplied changes.

What Next?

- Continue with additional Group procedures in this document as required.

Configuring Radio Settings for Device Groups

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

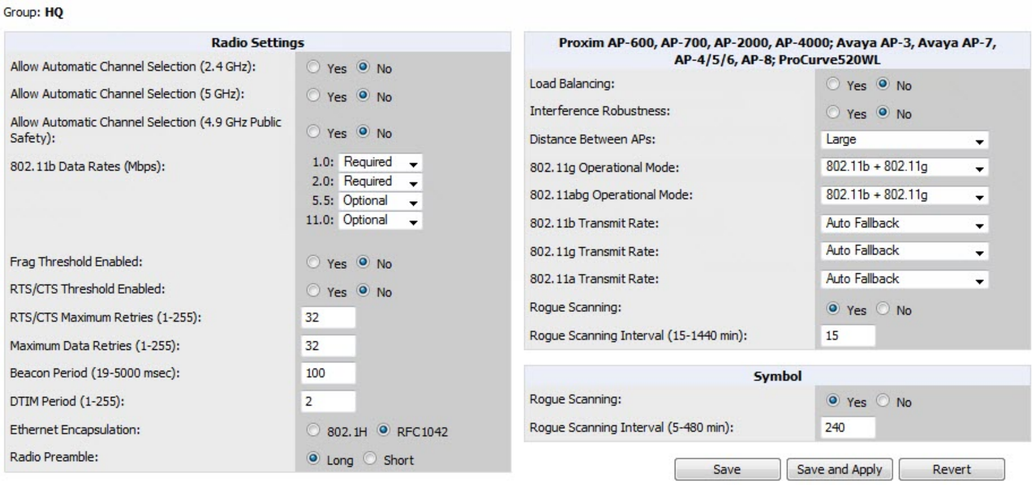
NOTE

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. Go to the **Groups** > **List** page and select the group for which to define radio settings by selecting the group name. Alternatively, select **Add** from the **Groups** > **List** page to create a new group, define a group name. In either case, the **Monitor** page appears.
2. Go to the **Groups** > **Radio** page. Figure 44 illustrates this page.

Figure 44 *Groups > Radio Page Illustration*



Group: **HQ**

Radio Settings

Allow Automatic Channel Selection (2.4 GHz): ○ Yes ● No

Allow Automatic Channel Selection (5 GHz): ○ Yes ● No

Allow Automatic Channel Selection (4.9 GHz Public Safety): ○ Yes ● No

802.11b Data Rates (Mbps): 1.0: Required; 2.0: Required; 5.5: Optional; 11.0: Optional

Frag Threshold Enabled: ○ Yes ● No

RTS/CTS Threshold Enabled: ○ Yes ● No

RTS/CTS Maximum Retries (1-255): 32

Maximum Data Retries (1-255): 32

Beacon Period (19-5000 msec): 100

DTIM Period (1-255): 2

Ethernet Encapsulation: ○ 802.1H ● RFC1042

Radio Preamble: ● Long ○ Short

Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL

Load Balancing: ○ Yes ● No

Interference Robustness: ○ Yes ● No

Distance Between APs: Large

802.11g Operational Mode: 802.11b + 802.11g

802.11abg Operational Mode: 802.11b + 802.11g

802.11b Transmit Rate: Auto Fallback

802.11g Transmit Rate: Auto Fallback

802.11a Transmit Rate: Auto Fallback

Rogue Scanning: ● Yes ○ No

Rogue Scanning Interval (15-1440 min): 15

Symbol

Rogue Scanning: ● Yes ○ No

Rogue Scanning Interval (5-480 min): 240

3. Locate the **Radio Settings** area and adjust these settings as required. Table 62 describes the settings and default values.

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

Setting	Default	Description
Allow Automatic Channel Selection (2.4, 5, and 4.9GHz Public Safety)	No	If enabled, whenever the AP is rebooted it uses its radio to scan the airspace and select its optimal RF channel based on observed signal strength from other radios. **NOTE:** If you enable this feature, AMP automatically reboots the APs in the group when the change is implemented.
802.11b Data Rates (Mbps)	Required: ● 1.0 ● 2.0 Optional: ● 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: ● **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, leave this option disabled.
Threshold Value (256-2347 bytes)	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, leave this option disabled.
RTS/CTS Threshold Value (0-2347 bytes)	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.

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

Setting	Default	Description
RTS/CTS Maximum Retries (1-255)	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 (1-255)	32	The maximum number of attempts the AP makes to send a packet before giving up and dropping the packet. Acceptable values range from **1** to **255**.
Beacon Period (19-5000 msec)	100	Time between beacons (in 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.

4. 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.

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

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

Setting	Default	Description
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.

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

Setting	Default	Description
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 APs in the group (with the appropriate firmware) will passively scan for rogue access points at the specified interval. This rogue scan will not break users' association to the network. **NOTE:** This feature can affect the data performance of the access point.
Rogue Scanning Interval (15-1440 min)	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.

6. To configure settings specific to Proxim 4900M, locate the **Proxim 4900M** section and define the required fields. Table 64 describes the settings and default values.

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

Setting	Default	Description
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.

7. To configure Symbol-only settings, locate the **Symbol** section and define the required fields. Table 65 describes the settings and default values.

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

Setting	Default	Description
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.

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

Cisco WLC Group Configuration

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

Accessing Cisco WLC Configuration

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

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

Navigating Cisco WLC Configuration

The navigation pane on the left side of the **Groups** > **Cisco WLC Config** page is expandable, and displays the Cisco configurations supported and deployed. Figure 45 and Figure 46 illustrate this navigation pane.

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

Figure 45 *Groups > Cisco WLC Config Page Illustration, collapsed view*

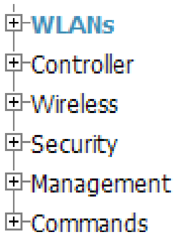
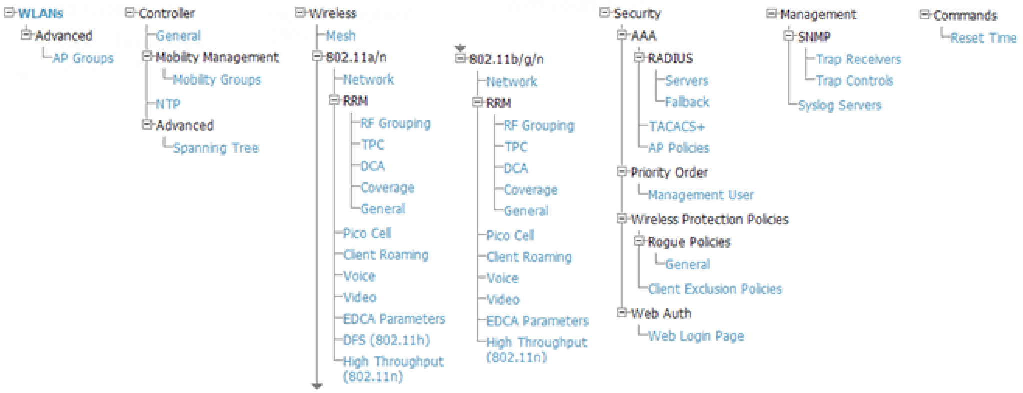


Figure 46 *Groups > Cisco WLC Config Page Illustration, expanded view*

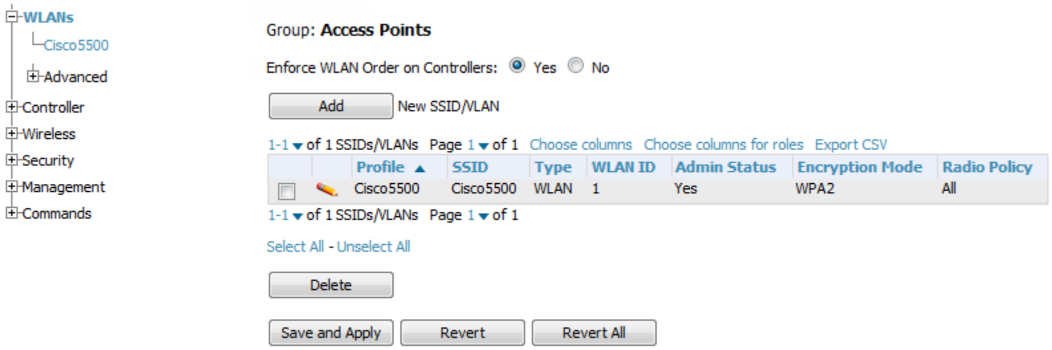


Configuring WLANs for Cisco WLC Devices

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

1. Go to the **Groups** > **Cisco WLC Config** page, and select **WLANs** in the navigation pane at left. This page displays the SSIDs or VLANs that are available for use with Cisco WLC devices and enables you to define new SSIDs or VLANs. Figure 47 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 config and device config differ only on the order.

Figure 47 *Groups > Cisco WLC Config > WLANS page illustration*



Group: **Access Points**

Enforce WLAN Order on Controllers: ● Yes ○ No

New SSID/VLAN

1-1 of 1 SSIDs/VLANs Page 1 of 1 Choose columns Choose columns for roles Export CSV

		Profile ▲	SSID	Type	WLAN ID	Admin Status	Encryption Mode	Radio Policy
□	✎	Cisco5500	Cisco5500	WLAN	1	Yes	WPA2	All

1-1 of 1 SSIDs/VLANs Page 1 of 1

Select All - Unselect All

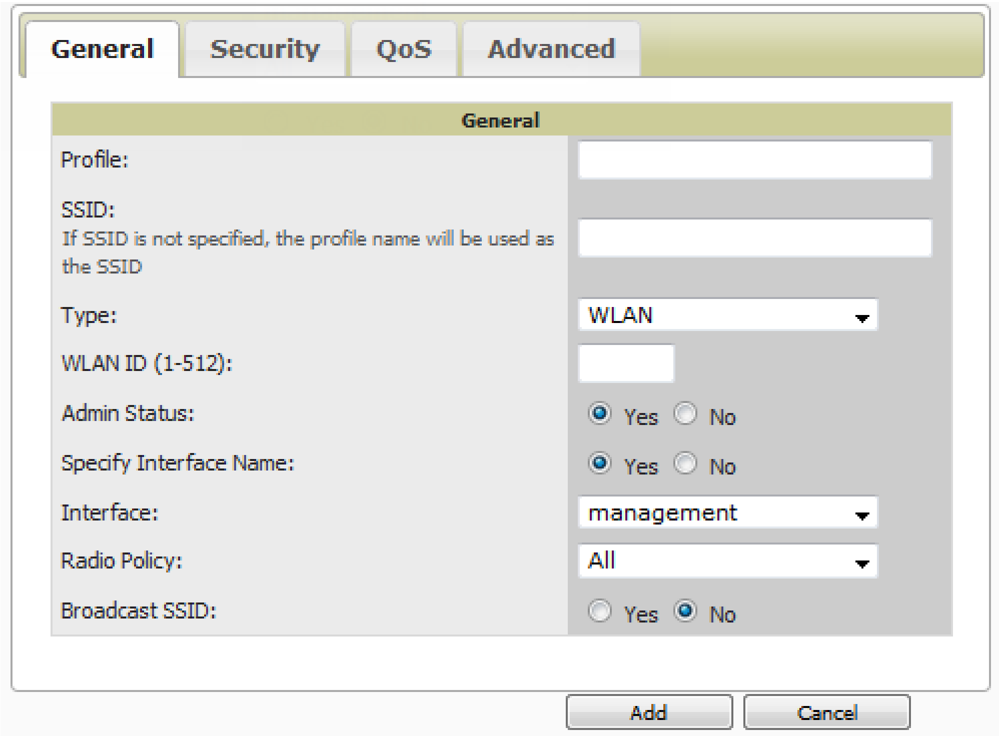
3. To add or edit SSIDs or VLANs that are dedicated to Cisco WLC devices, either select the **Add** button, or select the pencil icon for an existing SSID/VLAN. A new page appears comprised of four tabs, as follows:

- **General**—Defines general administrative parameters for the Cisco WLC WLAN.
- **Security**—Defines encryption and RADIUS servers.
- **QoS**—Defines quality of service (QoS) parameters for the Cisco WLC WLAN.
- **Advanced**—Defines advanced settings that are available only with Cisco WLC devices, for example, AAA override, coverage, DHCP and DTIM period.

NOTE

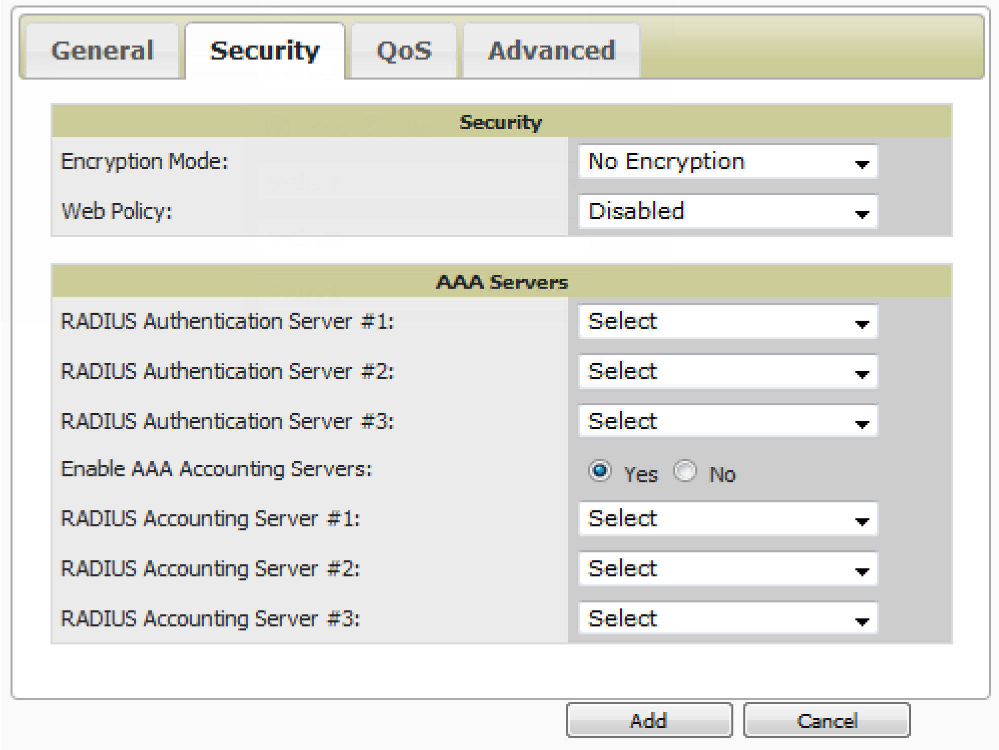
Refer to Cisco documentation for additional information about Cisco WLC devices and related features.

Figure 48 *Add New SSID/VLAN > General Tab Illustration*



General	
Profile:	
SSID: If SSID is not specified, the profile name will be used as the SSID	
Type:	WLAN
WLAN ID (1-512):	
Admin Status:	● Yes ○ No
Specify Interface Name:	● Yes ○ No
Interface:	management
Radio Policy:	All
Broadcast SSID:	○ Yes ● No

Figure 49 *Add New SSID/VLAN > Security Tab Illustration*



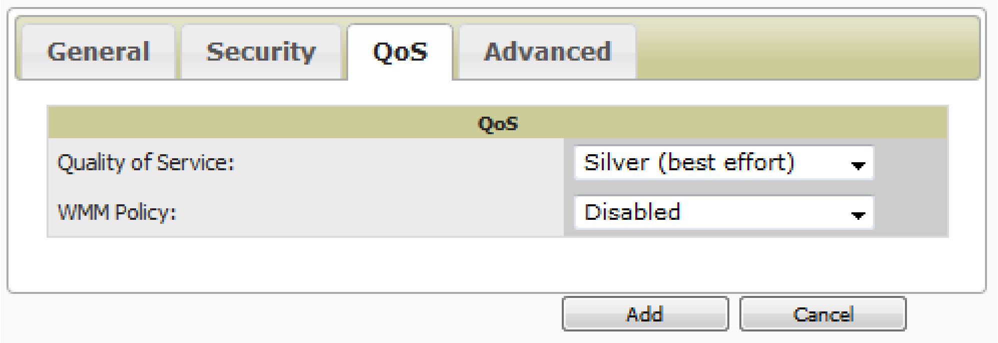
Security

Encryption Mode:	No Encryption
Web Policy:	Disabled

AAA Servers

RADIUS Authentication Server #1:	Select
RADIUS Authentication Server #2:	Select
RADIUS Authentication Server #3:	Select
Enable AAA Accounting Servers:	● Yes ○ No
RADIUS Accounting Server #1:	Select
RADIUS Accounting Server #2:	Select
RADIUS Accounting Server #3:	Select

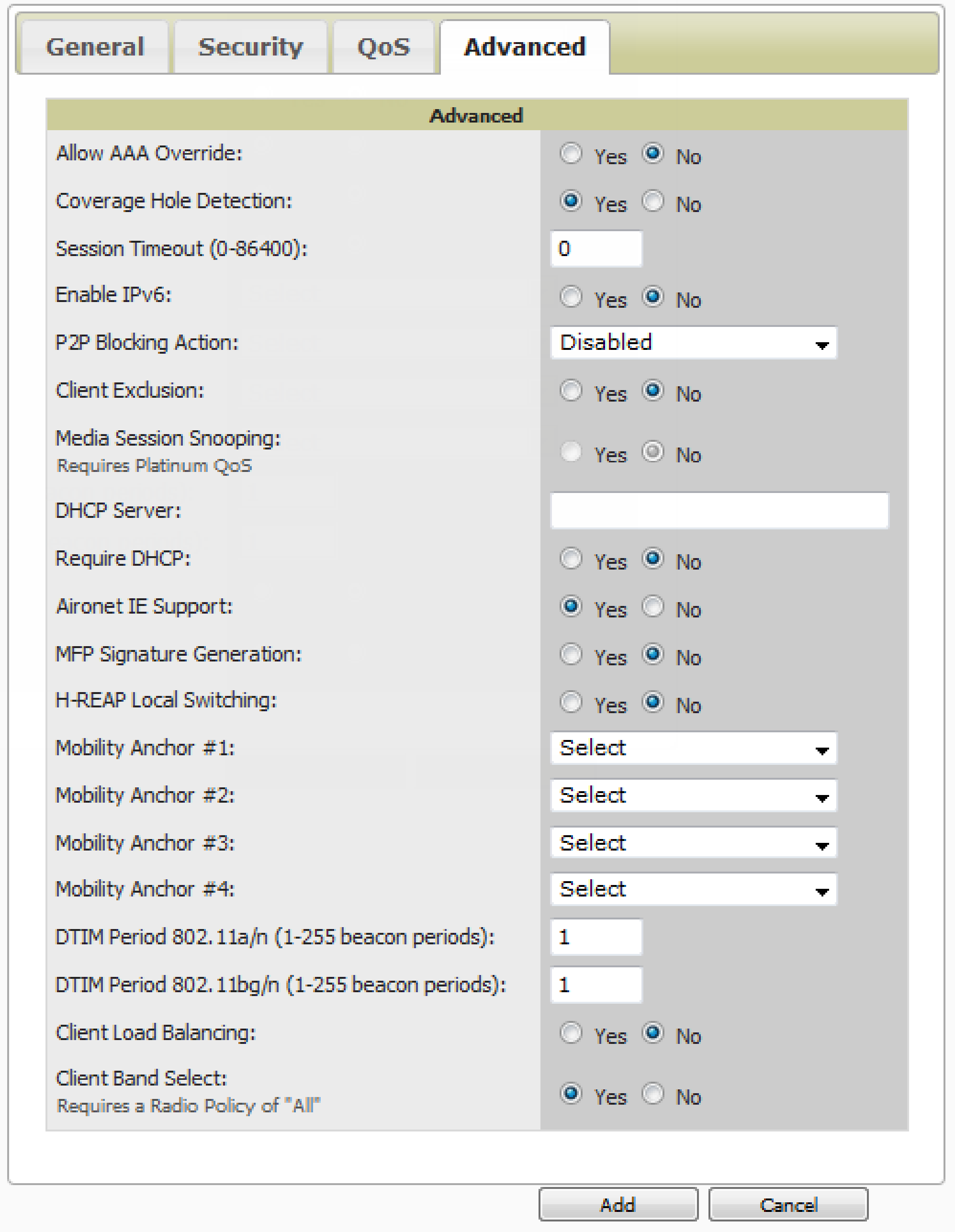
Figure 50 *Add New SSID/VLAN > QoS Tab Illustration*



QoS

Quality of Service:	Silver (best effort)
WMM Policy:	Disabled

Figure 51 *Add New SSID/VLAN > Advanced Tab Illustration*



General | Security | QoS | Advanced

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

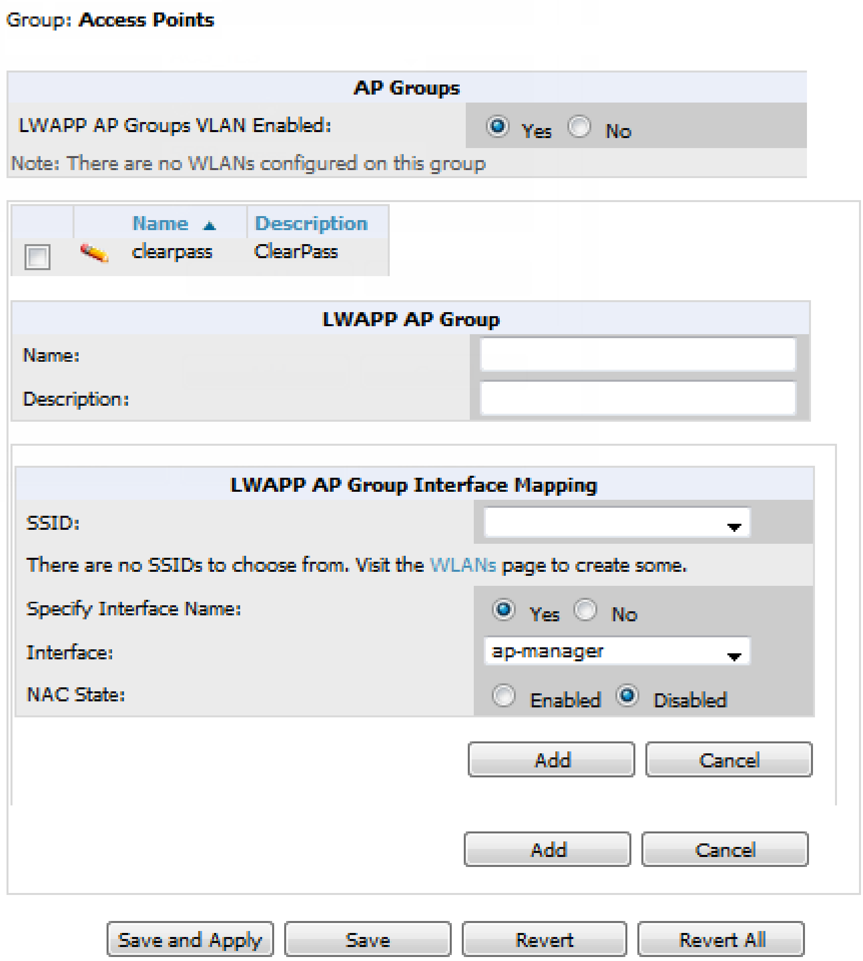
Defining and Configuring LWAPP AP Groups for Cisco Devices

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

Viewing and Creating Cisco AP Groups

1. Go to the **Groups** > **Cisco WLC Config** page, and select **WLANs** > **Advanced** > **AP Groups** in the navigation pane on the left side. This page displays the configured LWAPP APs. Figure 52 illustrates this page.

Figure 52 *Groups > Cisco WLC Config > WLANS > Advanced > AP Groups Page Illustration*



Group: **Access Points**

AP Groups

LWAPP AP Groups VLAN Enabled: ● Yes ○ No

Note: There are no WLANs configured on this group

		Name ▲	Description
☐	✎	clearpass	ClearPass

LWAPP AP Group

Name:	
Description:	

LWAPP AP Group Interface Mapping

SSID:

There are no SSIDs to choose from. Visit the WLANs page to create some.

Specify Interface Name: ● Yes ○ No

Interface: ap-manager

NAC State: ○ Enabled ● Disabled

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

Configuring Cisco Controller Settings

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

Go to the **Groups > Cisco WLC Config > Controller** page. This navigation is illustrated in Figure 53.

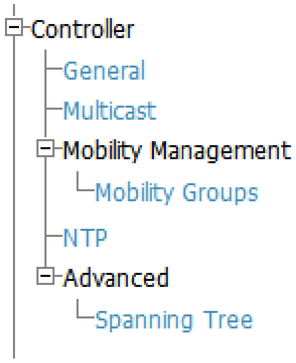
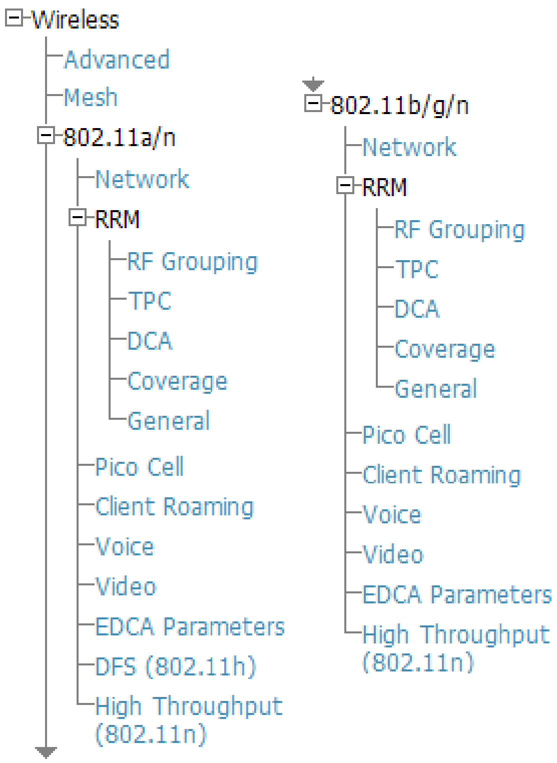


Figure 53 *Groups > Cisco WLC Config > Controller Navigation*

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 54.

Figure 54 *Groups > Cisco WLC Config > Wireless Navigation Illustration*



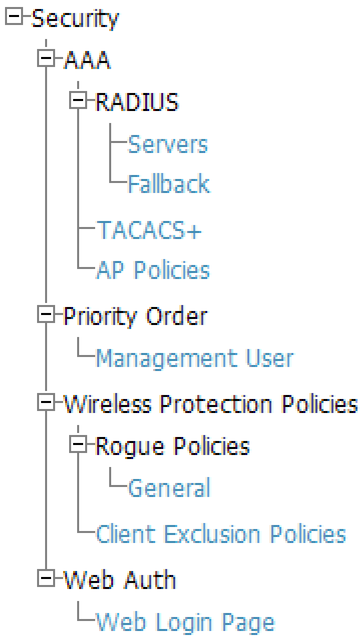
Configuring Cisco WLC Security Parameters and Functions

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

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

Figure 55 illustrates these components and this navigation:

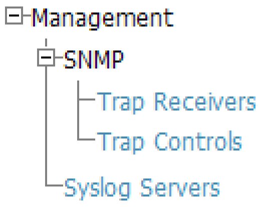
Figure 55 *Groups > Cisco WLC Config > Security Navigation Illustration*



Configuring Management Settings for Cisco WLC Controllers

AMP allows you to configure of SNMP and Syslog Server settings for Cisco WLC controllers. You can configure up to four trap receivers on the Cisco WLC including the AMP IP that can be used in Global Groups. To define SNMP and server settings, go to the **Groups** > **Cisco WLC Config** > **Management** page, illustrated in Figure 56.

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



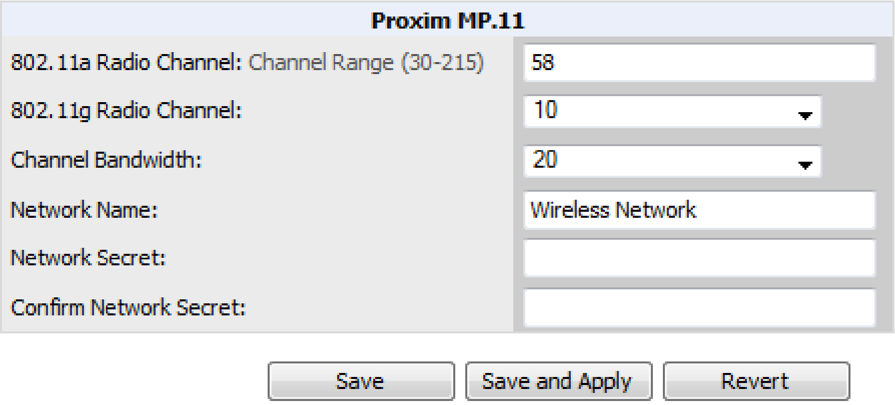
Configuring Group PTMP Settings

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

Perform the following steps to configure these functions.

1. Go to the **Groups** > **List** page and select the group for which to define PTMP settings by selecting the group that supports Proxim MP.11. Alternatively, select **Add** from the **Groups** > **List** page to create a new group.
2. Select the **Groups** > **PTMP** tab. Figure 57 illustrates this page.

Figure 57 *Groups > PTMP Page Illustration*



Proxim MP.11

802.11a Radio Channel: Channel Range (30-215)	58
802.11g Radio Channel:	10
Channel Bandwidth:	20
Network Name:	Wireless Network
Network Secret:	
Confirm Network Secret:	

3. Define the settings on this page. Table 66 describes the settings and default values.

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

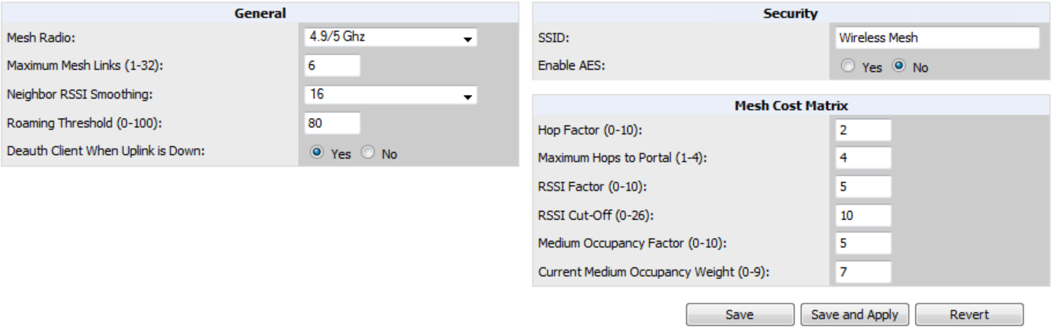
Setting	Default	Description
802.11a Radio Channel	58	Selects the channel used for 802.11a radios by the devices in this group.
802.11g Radio Channel	10	Selects the channel used for 802.11g radios by the devices in this group.
Channel Bandwidth	20	Defines the channel bandwidth used by the devices in this 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.

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

Configuring Proxim Mesh Radio Settings

1. Go to the **Groups > Proxim Mesh** configuration page to configure Mesh-specific radio settings.
2. Define the settings as required for your network. Figure 58 illustrates this page. The tables that follow describe the settings and default values.

Figure 58 *Groups > Proxim Mesh Page Illustration*



General

Mesh Radio:	4.9/5 Ghz
Maximum Mesh Links (1-32):	6
Neighbor RSSI Smoothing:	16
Roaming Threshold (0-100):	80
Deauth Client When Uplink is Down:	● Yes ○ No

Security

SSID:	Wireless Mesh
Enable AES:	○ Yes ● No

Mesh Cost Matrix

Hop Factor (0-10):	2
Maximum Hops to Portal (1-4):	4
RSSI Factor (0-10):	5
RSSI Cut-Off (0-26):	10
Medium Occupancy Factor (0-10):	5
Current Medium Occupancy Weight (0-9):	7

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

Table 67: *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.
Maximum Mesh Links (1-32)	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 (0-100)	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.
Deauth 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 68: *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.
Shared Secret	None	Specify a shared secret if **Enable AES** is **Yes**.

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

Table 69: *Mesh Cost Matrix Fields and Default Values*

Setting	Default	Description
Hop Factor (1-10)	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 (1-4)	4	Set the maximum number of hops for the AP to reach the Portal AP.
RSSI Factor (0-10)	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.
RSSI Cutoff (0-26)	10	Specifies the minimum RSSI needed to become a mesh neighbor.
Medium Occupancy Factor (0-10)	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 (0-9)	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.

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

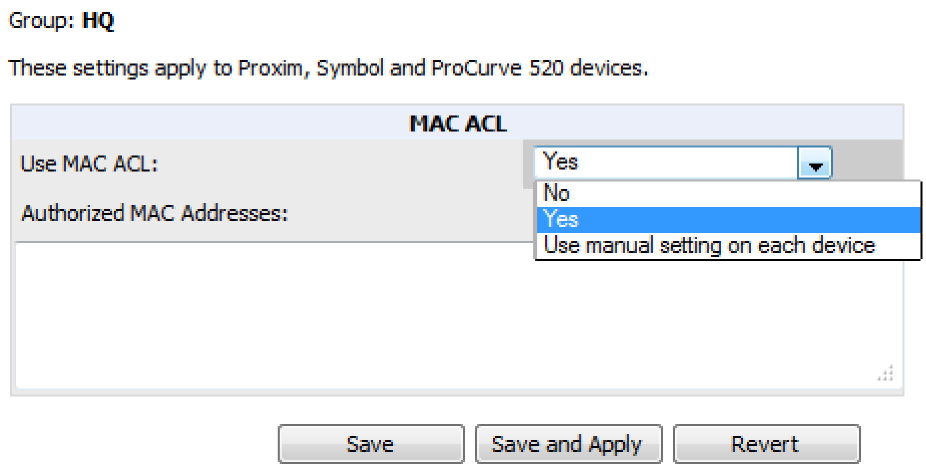
Configuring Group MAC Access Control Lists

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

Perform the following steps to use the MAC ACL function.

1. Browse to the **Groups** > **MAC ACL** configuration page. Figure 59 illustrates this page.

Figure 59 *Groups > MAC ACL Page Illustration*



Group: **HQ**

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

MAC ACL

Use MAC ACL: Yes

Authorized MAC Addresses:

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

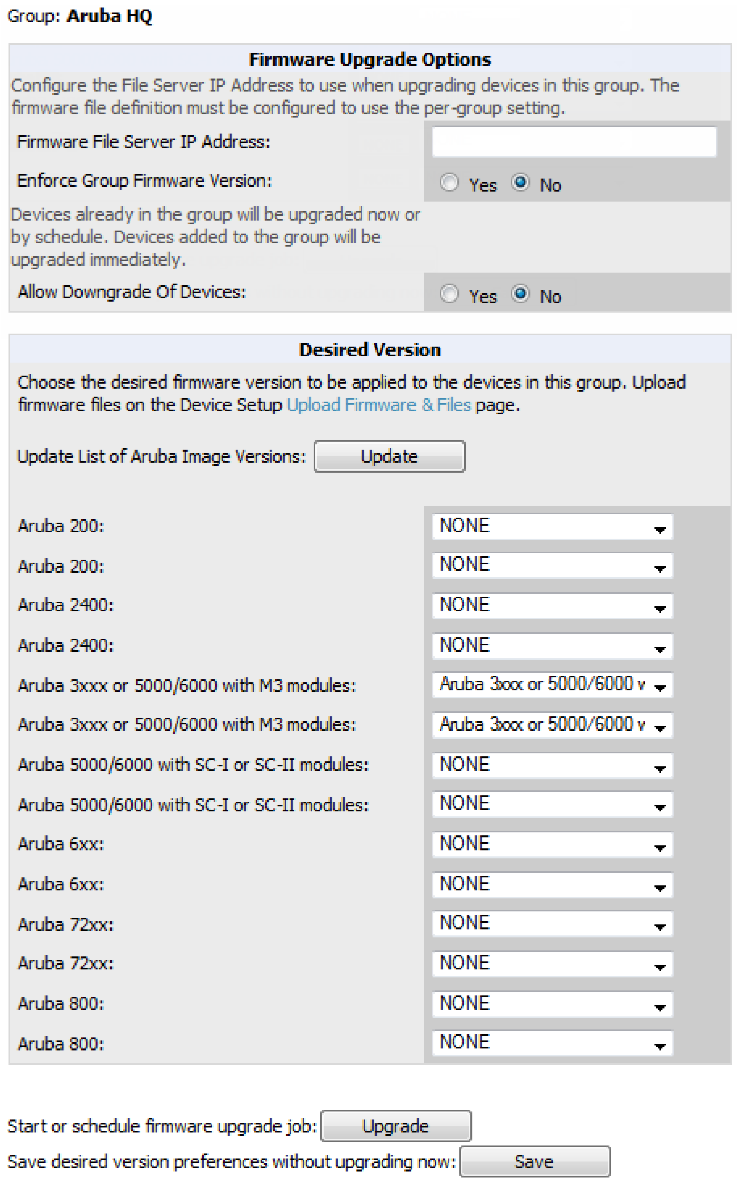
Specifying Minimum Firmware Versions for APs in a Group

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

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

1. Browse to the **Groups** > **Firmware** configuration page. Figure 60 illustrates this page.

Figure 60 *Groups > Firmware Page Illustration*



Group: **Aruba HQ**

Firmware Upgrade Options

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

Firmware File Server IP Address:	
Enforce Group Firmware Version:	○ Yes ● No

Devices already in the group will be upgraded now or by schedule. Devices added to the group will be upgraded immediately.

Allow Downgrade Of Devices:	○ Yes ● No

Desired Version

Choose the desired firmware version to be applied to the devices in this group. Upload firmware files on the Device Setup Upload Firmware & Files page.

Update List of Aruba Image Versions: Update

Aruba 200:	NONE
Aruba 200:	NONE
Aruba 2400:	NONE
Aruba 2400:	NONE
Aruba 3xxx or 5000/6000 with M3 modules:	Aruba 3xxx or 5000/6000 v
Aruba 3xxx or 5000/6000 with M3 modules:	Aruba 3xxx or 5000/6000 v
Aruba 5000/6000 with SC-I or SC-II modules:	NONE
Aruba 5000/6000 with SC-I or SC-II modules:	NONE
Aruba 6xx:	NONE
Aruba 6xx:	NONE
Aruba 72xx:	NONE
Aruba 72xx:	NONE
Aruba 800:	NONE
Aruba 800:	NONE

Start or schedule firmware upgrade job: Upgrade

Save desired version preferences without upgrading now: Save

2. For each device type in the group, specify the minimum acceptable firmware version. If no firmware versions are listed, go to the **Device Setup > Upload Firmware & Files** configuration page to upload the firmware files to AMP.
3. Select **Upgrade** to apply firmware preferences to devices in the group. The device types that display will vary based on the device types that were selected on the **Groups > Basic** page.
4. Select **Save** to save the firmware file as the desired version for the group.
5. If you have opted to assign an external TFTP server on a per-group basis on the **Device Setup > Upload Firmware & Files** configuration page, you can enter the IP address in the **Firmware Upgrade Options** field on the top of this configuration page.
6. Once you have defined your first group, you can configure that group to be the default group on your network. When AMP discovers new devices that need to be assigned to a management group, the default group appears at the top of all drop-down menus and lists. Newly discovered devices are place automatically in the default group if AMP is set to automatically monitor/manage new devices.
7. Browse to the **AMP Setup > General** page.
8. In the General section, select the desired group from the **Default Group** drop down menu to make it the default.

Comparing Device Groups

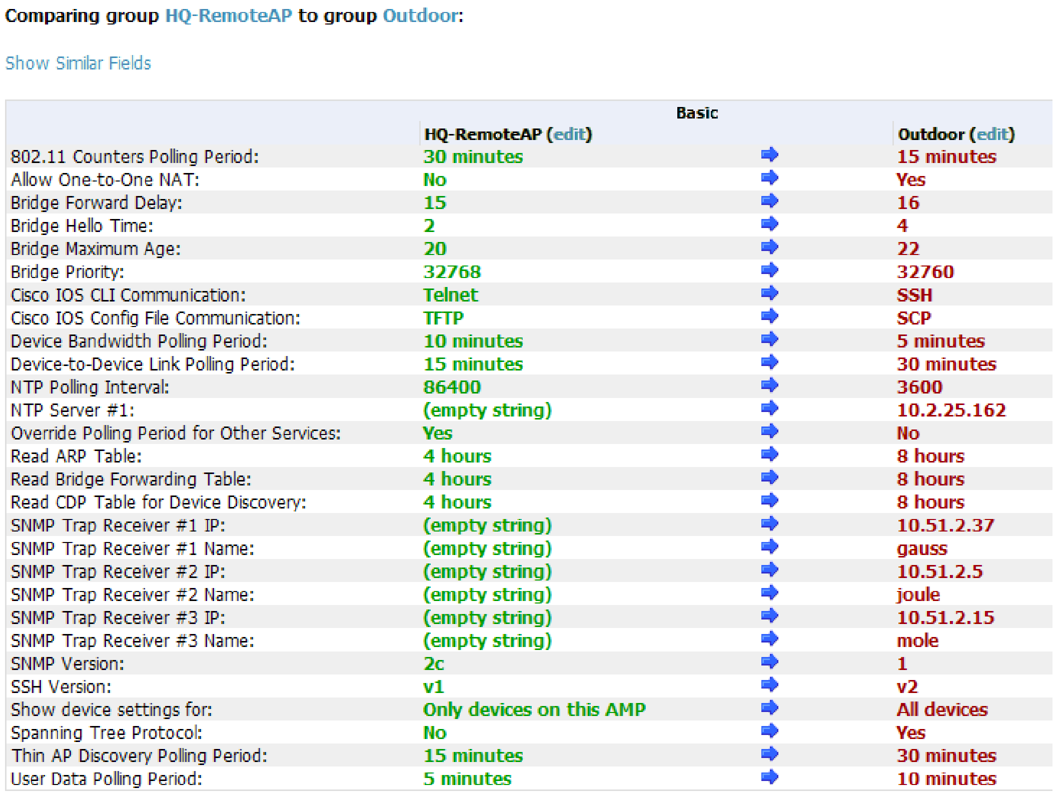
You can compare two existing device groups with a detailed line-item comparison. Group comparison allows several levels of analysis including the following:

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

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

1. From the **Groups > List** page, select the **Compare two groups** link. Two drop-down menus appear.
2. Select the two groups to compare in the drop-down menus, and select **Compare**. The **Compare** page appears, displaying some or many configuration categories. Figure 61 illustrates this page.

Figure 61 *Comparing Two Devices Groups on the* ***Groups > List > Compare*** *Page (Partial View)*



Comparing group HQ-RemoteAP to group Outdoor:

Show Similar Fields

	Basic		
	HQ-RemoteAP (edit)		**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

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

Deleting a Group

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

1. Browse to the **Groups** > **List** configuration page.
2. Ensure that the group you wish to delete is not marked as the **default** group. (See the **AMP Setup** > **General** page.) AMP does not permit you to delete the current default group.

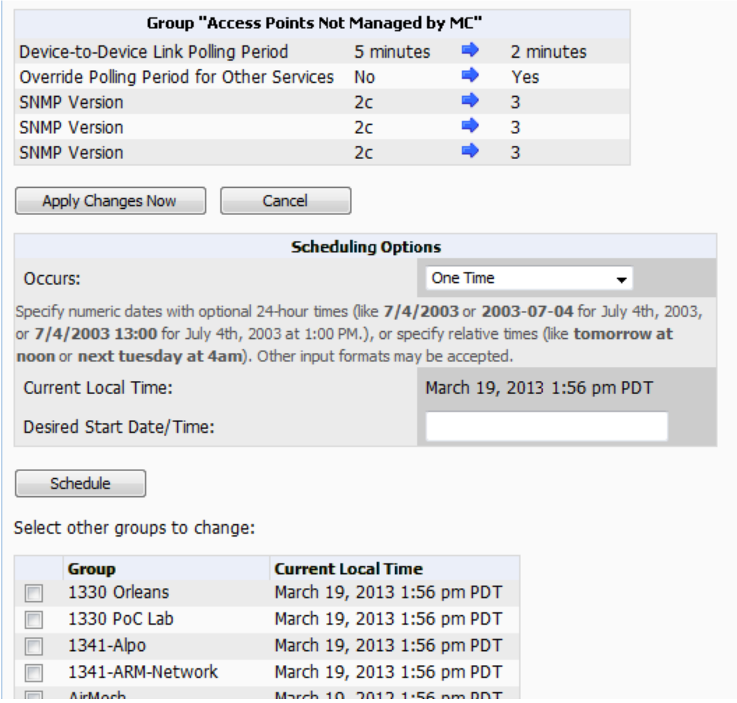
3. Ensure that there are no devices in the group that you want to delete. AMP does not permit you to delete a group that still contains managed devices. You must move all devices to other groups before deleting a group.
4. Ensure that the group is not a global group that has subscriber groups, and is not a group that was pushed from a Master Console. AMP will not delete a group in which either of those cases is true.
5. Select the checkbox, and click the **Delete** button.

Changing Multiple Group Configurations

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

1. Browse to the **Groups** > **List** configuration page.
2. Select the **Modify** button (the wrench icon) for the group you wish to edit. The **Groups** > **Basic** configuration page appears.
3. Select the fields to be edited on the **Basic** configuration page or go to **Radio**, **Security**, **VLANs**, or **MAC ACL** configuration page and edit the fields. Use the **Save** button to store the changes prior to applying them.
4. When all changes for the group are complete select the **Save and Apply** button to make the changes permanent. Figure 62 illustrates the confirmation message that appears.

Figure 62 *Groups > Basic Configuration Change Confirmation Page Illustration*



Group "Access Points Not Managed by MC"			
Device-to-Device Link Polling Period	5 minutes	→	2 minutes
Override Polling Period for Other Services	No	→	Yes
SNMP Version	2c	→	3
SNMP Version	2c	→	3
SNMP Version	2c	→	3

Scheduling Options	
Occurs:	One Time

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

Current Local Time:	March 19, 2013 1:56 pm PDT
Desired Start Date/Time:	

Select other groups to change:

	Group	Current Local Time
□	1330 Orleans	March 19, 2013 1:56 pm PDT
□	1330 PoC Lab	March 19, 2013 1:56 pm PDT
□	1341-Alpo	March 19, 2013 1:56 pm PDT
□	1341-ARM-Network	March 19, 2013 1:56 pm PDT
□	AirMesh	March 19, 2013 1:56 pm PDT

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

NOTE

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

   - **Scheduling Options** — Schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time field**. You can also specify if this is a one-time schedule or a recurring schedule.

Recurring options are **Daily**, **Weekly**, **Monthly**, and **Annually**. AMP takes the time zone into account for the group if a time zone other than AMP System Time has been configured on the **Groups > Basic** configuration page.

- **Cancel** — Cancels the application of changes (immediately or scheduled).

NOTE

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

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

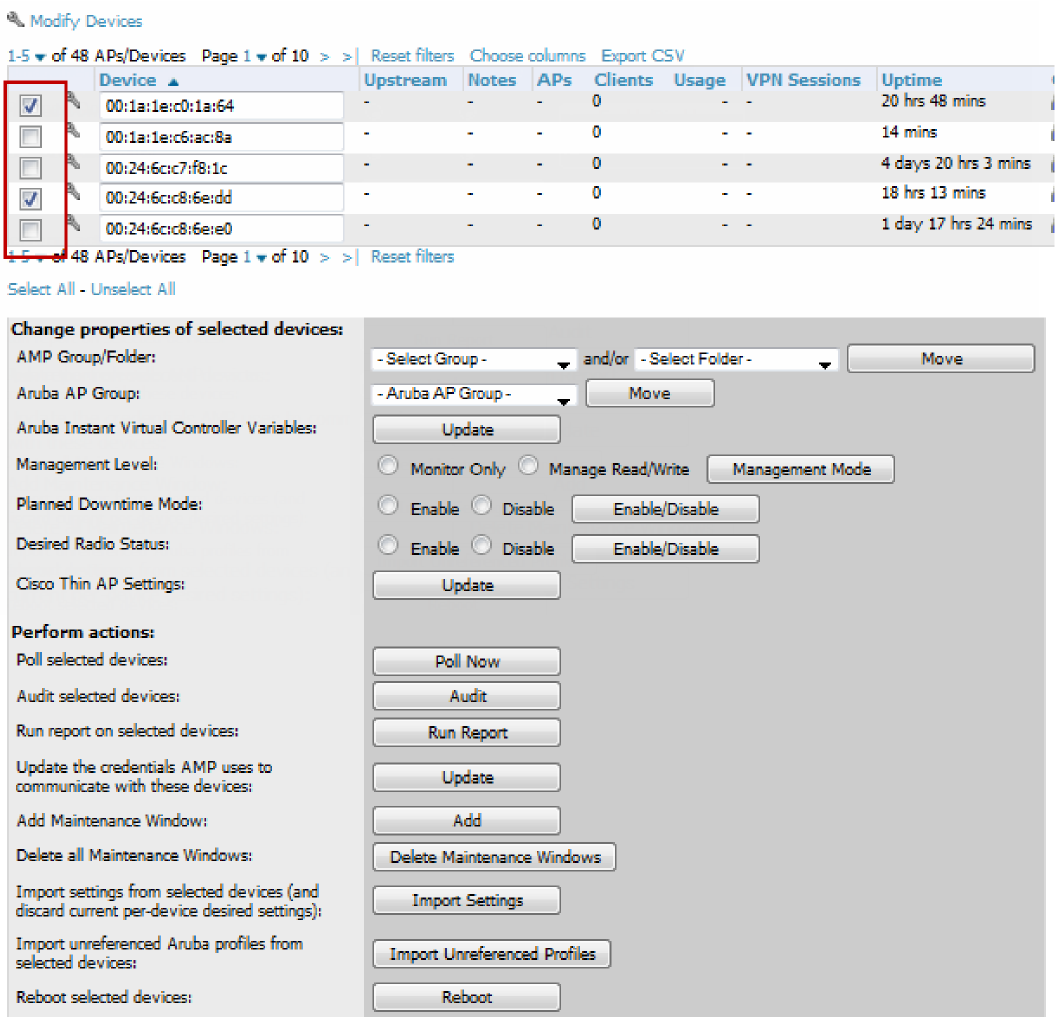
Modifying Multiple Devices

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

1. To modify multiple devices, go to one of the following pages with a device list:
   - **APs/Devices > List**
   - **APs/Devices > Up**
   - **APs/Devices > Down**
   - **APs/Devices > Mismatched**
   - **Groups > Monitor**

   Each of these pages displays a list of devices. Controller monitoring pages also have lists of their thin APs which can be modified using **Modify Devices**.
2. Select **Modify Devices** to make the checkboxes at the left of all devices appear. In addition, a new section appears in this page location to display various settings that can be configured for multiple devices at one time (some operations cannot be performed on the selected devices). Figure 63 illustrates this page.

Figure 63 *Modify Multiple Devices Section Illustration*



Modify Devices

1-5 ▾ of 48 APs/Devices Page 1 ▾ of 10 > >| Reset filters Choose columns Export CSV

	Device ▲	Upstream	Notes	APs	Clients	Usage	VPN Sessions	Uptime
☑	00:1a:1e:c0:1a:64	-	-	-	0	-	-	20 hrs 48 mins
□	00:1a:1e:c6:ac:8a	-	-	-	0	-	-	14 mins
□	00:24:6c:c7:f8:1c	-	-	-	0	-	-	4 days 20 hrs 3 mins
☑	00:24:6c:c8:6e:dd	-	-	-	0	-	-	18 hrs 13 mins
□	00:24:6c:c8:6e:e0	-	-	-	0	-	-	1 day 17 hrs 24 mins

1-5 ▾ of 48 APs/Devices Page 1 ▾ of 10 > >| Reset filters

Select All - Unselect All

Change properties of selected devices:	
AMP Group/Folder:	- Select Group - ▾ and/or - Select Folder - ▾ [Move]
Aruba AP Group:	- Aruba AP Group - ▾ [Move]
Aruba Instant Virtual Controller Variables:	[Update]
Management Level:	○ Monitor Only ○ Manage Read/Write [Management Mode]
Planned Downtime Mode:	○ Enable ○ Disable [Enable/Disable]
Desired Radio Status:	○ Enable ○ Disable [Enable/Disable]
Cisco Thin AP Settings:	[Update]
Perform actions:	
Poll selected devices:	[Poll Now]
Audit selected devices:	[Audit]
Run report on selected devices:	[Run Report]
Update the credentials AMP uses to communicate with these devices:	[Update]
Add Maintenance Window:	[Add]
Delete all Maintenance Windows:	[Delete Maintenance Windows]
Import settings from selected devices (and discard current per-device desired settings):	[Import Settings]
Import unreferenced Aruba profiles from selected devices:	[Import Unreferenced Profiles]
Reboot selected devices:	[Reboot]

3. Select one or more devices that are to share the configurations. Select the checkbox for each device to modify.
4. In the **Modify Multiple Devices** section, select any button or use any drop-down menu for the supported changes. Any action you take applies to all selected devices. Each action you take will direct you to a new configuration page, or prompt you with a confirmation page to confirm your changes.
5. You are taken to a confirmation configuration page that allows you to schedule the change for a time in the future. Enter a start date and time in the scheduling field and select when the change should occur from the drop-down menu (one time is the default, but you may select recurring options for many of the actions). Scheduled jobs can be viewed and edited in the **System > Configuration Change Jobs** tab.
6. Using the neighbor lists, AMP is able to optimize channel selection for APs. Select the APs to optimize. AMP minimizes the channel interference while giving channel priority to the most heavily used APs. Table 70 describes these actions and controls.

Table 70: *Modify Multiple Devices Section Fields and Default Values*

Action	Description
AMP 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 70: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Aruba 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.
Aruba Instant Virtual Controller Variables	Opens the Variable Editor page for selected Aruba Instant APs.
Management Level	Move the selected devices into **Monitor Only** or **Manage Read/Write** Mode.
Planned Downtime Mode	Puts the selected devices into Planned Maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up.
Desired Radio Status	Enables or disables the radios on the selected device. Does *not* apply Cisco IOS APs.
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.
Poll selected devices	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 AMP server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired AMP configuration. The audit action updates the Configuration Status. **NOTE:** In versions of AMP prior to 7.3, the **Audit** button appeared on **Groups > List** for groups with audit disabled. Now, if a group has audit disabled for its devices, AMP does not show the **Audit** button in the **Modify devices** list.
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 282.
Update the credentials AMP uses to communicate with these devices	**Update** changes the credentials AMP uses to communicate with the device. It does *not* change the credentials on the AP.
Add Maintenance Window	Automate the manual action of putting the selected devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode. Maintenance windows can be set as a one-time or recurring event.
Delete all Maintenance Windows	Deletes all maintenance windows set for these devices.
Import settings from	Audit updates a number of the AP-specific settings that AMP initially read off of the

Table 70: *Modify Multiple Devices Section Fields and Default Values (Continued)*

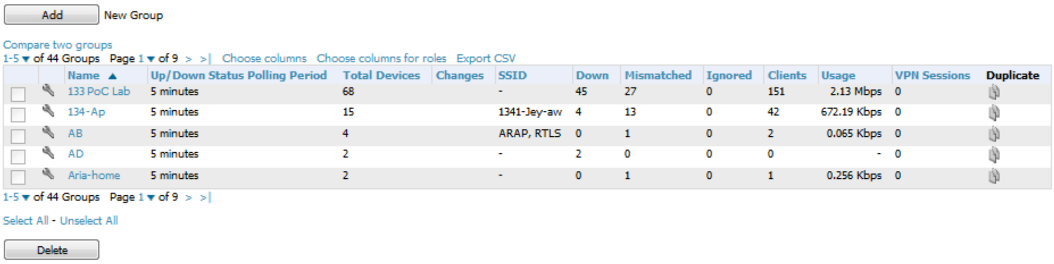
Action	Description
selected devices (and discard current pre-device desired settings)	AP including channel, power, antenna settings and SSL certifications. AMP recommends using this setting if APs have been updated outside of AMP. Most settings on the **APs/Devices Manage** configuration page are set to the values currently read off of the devices.
Import unreferenced Aruba profiles from selected devices	Select the devices that include unreferenced profiles, then click this button to import those profiles from the selected devices.
Reboot selected devices	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
Reprovision selected Aruba 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.
Replace Hardware	Select the down device that will be replaced and view the list of AMP devices that match the name or IP address of the selected device. The down devices can be replaced with any device in the **New Devices** list or in the current folder or group.
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.
Rename devices	Rename all the selected devices in bulk. Note that you can also rename the devices one at a time using the editable Name fields in each row.
Delete selected devices from AMP	Removes the selected APs from AMP. The deletes will be performed in the background and may take a minute to be removed from the list.

Using Global Groups for Group Configuration

To apply group configurations using the AMP Global Groups feature, first go to the **Groups > List** configuration page. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group. Select the **Duplicate** icon (usually near the last column of the list) to create a new group with identical configuration to an existing group.

- To have Global Group status, a group must contain no devices; accordingly, access points can never be added to a Global Group. Global groups are visible to users of all roles, so they may not contain devices, which can be made visible only to certain roles. Figure 64 illustrates the **Groups > List** page.

Figure 64 *Groups > List Page Illustration*



Add New Group

Compare two groups

1-5 ▾ of 44 Groups Page 1 ▾ of 9 > >| Choose columns Choose columns for roles Export CSV

		Name ▲	Up/Down Status Polling Period	Total Devices	Changes	SSID	Down	Mismatched	Ignored	Clients	Usage	VPN Sessions	Duplicate
□		133 PoC Lab	5 minutes	68		-	45	27	0	151	2.13 Mbps	0	
□		134-Ap	5 minutes	15		1341-Jey-aw	4	13	0	42	672.19 Kbps	0	
□		AB	5 minutes	4		ARAP, RTLS	0	1	0	2	0.065 Kbps	0	
□		AD	5 minutes	2		-	2	0	0	0	-	0	
□		Aria-home	5 minutes	2		-	0	1	0	1	0.256 Kbps	0	

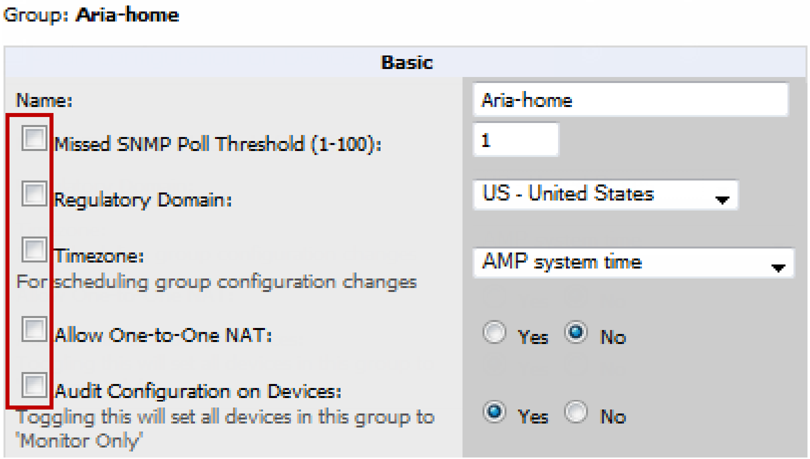
1-5 ▾ of 44 Groups Page 1 ▾ of 9 > >|

Select All - Unselect All

Delete

- To set a group as a Global Group, go to the **Groups > Basic** configuration page for an existing or a newly created group. Select **Yes** for the **Is Global Group** field under the Global Group section.
- When the change is saved and applied, the group will have a checkbox next to fields. Figure 65 illustrates this configuration page.

Figure 65 *Groups > Basic Page for a Global Group (partial view)*



Group: **Aria-home**

Basic

Name: Aria-home

□ Missed SNMP Poll Threshold (1-100): 1

□ Regulatory Domain: US - United States

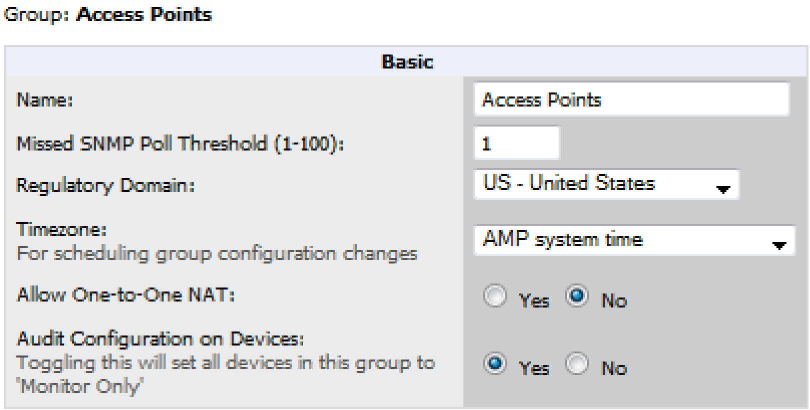
□ Timezone: AMP system time
For scheduling group configuration changes

□ Allow One-to-One NAT: ○ Yes ● No

□ Audit Configuration on Devices: ● Yes ○ No
Toggling this will set all devices in this group to 'Monitor Only'

- When a Global Group configuration is pushed to Subscriber Groups, all settings are static except for settings with the checkbox selected; for fields with checkboxes selected, the value or setting can be changed on the corresponding tab for each managed group. In the case of the **Groups > SSIDs** configuration page, override options are available only on the **Add** configuration page (go to the **Groups > SSIDs** configuration page and select **Add**). Global templates are also configurable as part of Global Groups; for more information, see "Creating and Using Templates" on page 178.
- Once Global Groups have been configured, groups may be created or configured to subscribe to a particular Global Group. Go to the **Groups > Basic** configuration page of a group and locate the **Use Global Groups** section. Select the **Yes** radio button and select the name of the Global Group from the drop-down menu. Then select **Save and Apply** to make the changes permanent. Figure 66 illustrates this page.

Figure 66 *Groups > Basic > Managed Page Illustration*



Group: **Access Points**

Basic	
Name:	Access Points
Missed SNMP Poll Threshold (1-100):	1
Regulatory Domain:	US - United States
Timezone: For scheduling group configuration changes	AMP system time
Allow One-to-One NAT:	○ Yes ● No
Audit Configuration on Devices: Toggling this will set all devices in this group to 'Monitor Only'	● Yes ○ No

- Once the configuration is pushed, the unchecked fields from the Global Group appears on the Subscriber Group as static values and settings. Only fields that had the override checkbox selected in the Global Group appear as fields that can be set at the level of the Subscriber Group. Any changes to a static field must be made on the Global Group.
- If a Global Group has Subscriber Groups, it cannot be changed to a non-Global Group. A Global Group without Subscriber Groups can be changed to a regular Group by updating the setting on the **Groups** > **Basic** configuration interface. The Global Groups feature can also be used with the **Master Console**. For more information about this feature, refer to "Supporting AMP Servers with the Master Console" on page 265.

Chapter 4

Discovering, Adding, and Managing Devices

This section describes how to add, configure, and monitor wired and wireless devices, and contains the following sections corresponding to features of the **Device Setup** and **APs/Devices** tabs:

- "Device Discovery Overview" on page 124
- "Discovering and Adding Devices" on page 124
- "Monitoring Devices" on page 136
- "Configuring and Managing Devices" on page 156
- "Troubleshooting a Newly Discovered Down Device" on page 172
- "Using AMP to Set up Spectrum Analysis" on page 174

Device Discovery Overview

After you have deployed AMP on the network, the next step is to discover all existing devices connected to your network.

AMP allows device discovery in the following ways, all of which are described in the sections that follow:

- **SNMP/HTTP discovery scanning**—This is the primary method to discover devices on your network, configured in the **Device Setup > Discover** page. See "SNMP/HTTP Scanning" on page 124.
- **Cisco Discovery Protocol (CDP)**—AMP enhances support for CDP by discovering a Cisco device’s CDP neighbors. See "The Cisco Discovery Protocol (CDP)" on page 129.
- **Manual device entry**—This admin-supported method of discovery applies when you know of devices that are already on your network. See the following sections for information and procedures:
  - "Manually Adding Individual Devices" on page 129
  - "Manually Adding Individual Devices" on page 129
  - "Manually Adding Individual Devices" on page 129
- **Controller-driven device discovery**—Thin APs will automatically be discovered in the network and added to the **New Devices** list when you add their controller to AMP. To add the thin APs, refer to "Authorizing Devices to AMP from APs/Devices > New Page" on page 129.

Discovering and Adding Devices

This section describes the following topics:

- "SNMP/HTTP Scanning" on page 124
- "The Cisco Discovery Protocol (CDP)" on page 129
- "Authorizing Devices to AMP from APs/Devices > New Page" on page 129
- "Manually Adding Individual Devices" on page 129

SNMP/HTTP Scanning

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

NOTE

This page is only visible to users with the AMP Administrator role or roles that have **Allow authorization of APs/Devices** enabled in **AMP Setup > Roles.**

SNMP/HTTP scanning information is provided in these sections:

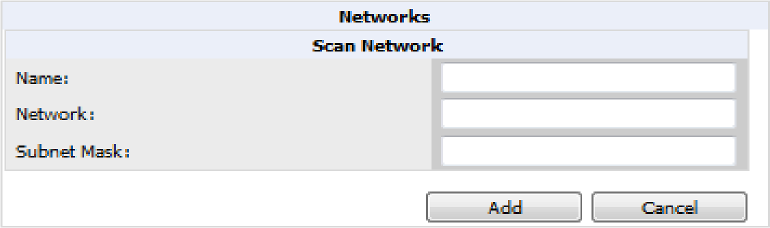
- "Adding Networks for SNMP/HTTP Scanning" on page 125—explains how to enable networks that have been defined for scanning.
- "Adding Credentials for Scanning" on page 125—explains how to define network credentials for scanning. Credentials must be defined before using them in scan sets.
- "Defining a Scan Set" on page 126—explains how to create a scan set by combining networks and credentials when scanning for devices.
- "Running a Scan Set" on page 127—provides a procedure for running a scan set.

Adding Networks for SNMP/HTTP Scanning

The first step when enabling SNMP/HTTP scanning for devices is to define the network segments to be scanned. Perform these steps.

1. Go to the **Device Setup** > **Discover** page, and scroll down to the **Networks** section.
2. In the **Networks** section, select the **Add button to add a new scan network**. The **Scan Network** page appears, as shown in Figure 67. (Note that you may have to scroll down the page again to view this section.) Alternatively, you can edit an existing scan network by selecting the corresponding pencil icon. The **New/Edit Networks** page also appears in this instance.

Figure 67 *Device Setup > Discover > New Network Section Illustration*



Networks

Scan Network

Name:	
Network:	
Subnet Mask:	

3. In the **Name** field, provide a name for the network to be scanned (for example, **Accounting Network**).
4. In the **Network** field, define the IP network range, or the first IP address on the network, to be scanned. One example would be 10.52.0.0.
5. Enter the **Subnet Mask** for the network to be scanned (for example, 255.255.252.0). The largest subnet AMP supports is 255.255.255.0.
6. Select **Add**.
7. Repeat these steps to add as many networks for which to enable device scanning. All network segments configured in this way appear in the **Network** section of the **Device Setup > Discover** page.
8. Complete the configuration of scan credentials, then combine scan networks and scan credentials to create scan sets. The next two procedures in this section describe these tasks: "Adding Credentials for Scanning" on page 125 and "Defining a Scan Set" on page 126.

Adding Credentials for Scanning

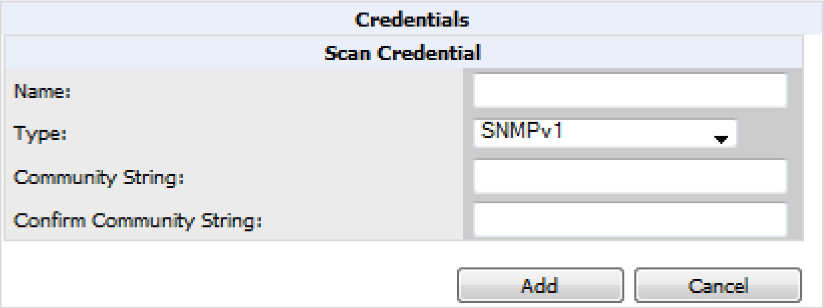
The next step in SNMP/HTTP device discovery is to define the scan credentials that govern scanning of a given network. New APs inherit scan credentials from the System Credentials that you configure on the **Device Setup** > **Communications** page.

Perform these steps to define scan credentials for SNMP/HTTP scanning:

1. Locate the **Credentials** section on the **Device Setup > Discover** page. (Scroll down if necessary.) This page displays scan sets, networks, and credentials that have been configured so far, and allows you to define new elements for device scanning.

2. To create a new scan credential, select the **Add button to add a new scan credential**. Figure 68 illustrates this page. (Note that you may have to scroll down the page again to view this section.)

Figure 68 *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*



Credentials

Scan Credential

Name:	
Type:	SNMPv1
Community String:	
Confirm Community String:	

3. Enter a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters (both upper and lower case), blank spaces, hyphens, and underscore characters.
4. Choose the type of scan to be completed (**SNMPv1, SNMPv2,** or **HTTP**). In most cases, perform scans using SNMP for device discovery, but consider the following factors in your decision:
   - SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.
   - HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.

   a. If you selected SNMPv1 or SNMPv2, then 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 because AMP only uses it for discovering APs. To bring APs under management, AMP uses the credentials supplied in the **Device Setup > Communication SNMP** section. Once the device is authorized, it will use the non-scanning credentials.

   b. If you selected HTTP for the type, then enter a **Username** and **Password** for the scan credentials.

NOTE

AMP automatically appends the type of scan (SNMP or HTTP) to the Label.

5. Select **Add** after you have completed the previous steps. The **Device Setup** > **Discover** page displays the new scan credential or credentials just created or edited.
6. Repeat these steps to add as many credentials as you require.
7. Once scan networks and scan credentials are defined, combine them by creating scan sets using the next procedure: "Defining a Scan Set" on page 126.

Defining a Scan Set

Once you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery. Perform these steps to create a scan set.

1. Locate the **Scan Set** area at the top of the **Device Setup** > **Discover** page.
2. Select **Add New Scan Set** to see all scan components configured so far. If you wish to create a new network, or new scanning credentials, you can select **Add** in either of these fields to create new components prior to creating a scan set.
3. Select the network(s) to be scanned and the Credential(s) to be used. AMP defines a unique scan for each Network-Credential combination.

4. In the **Automatic Authorization** section, select whether to override the global setting in **AMP Setup > General** and have New Devices be automatically authorized into the New Device List, the same Group/Folder as the discovering devices, the same Group/Folder as the closest IP neighbor, and/or a specified auto-authorization group and folder.
5. Select **Add** to create the selected scans, which then appear in a list at the top of the **Device Setup > Discover** page.
6. To edit an existing scan, select the **pencil** icon next to the scan on the **Device Setup > Discover** page.
7. When ready, proceed to the next task, "Running a Scan Set" on page 127.

NOTE

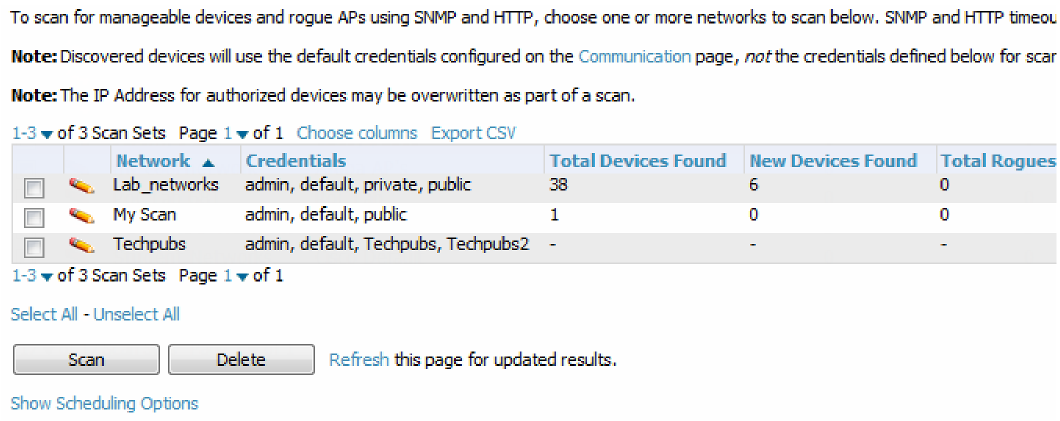
Scheduling an HTTP scan to run daily on your network can help you to discover rogues. Some consumer APs, like most D-Link, Linksys, and NetGear models, do not support SNMP and are found only on the wired side with an HTTP scan. These devices are discovered only if they have a valid IP address. Proper credentials are not required to discover these APs. Wireless scans and the AMC discover these rogues without any special changes.

Running a Scan Set

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

1. Browse to the **Device Setup > Discover** page and locate the list of all scan sets that have been defined so far. Figure 69 illustrates this page.

Figure 69 *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 timeou

Note: Discovered devices will use the default credentials configured on the Communication page, *not* the credentials defined below for scar

Note: The IP Address for authorized devices may be overwritten as part of a scan.

1-3 ▾ of 3 Scan Sets Page 1 ▾ of 1 Choose columns Export CSV

		Network ▲	Credentials	Total Devices Found	New Devices Found	Total Rogues
□	✎	Lab_networks	admin, default, private, public	38	6	0
□	✎	My Scan	admin, default, public	1	0	0
□	✎	Techpubs	admin, default, Techpubs, Techpubs2	-	-	-

1-3 ▾ of 3 Scan Sets Page 1 ▾ of 1

Select All - Unselect All

Refresh this page for updated results.

Show Scheduling Options

2. Check the box next to the scan(s) that you would like to execute.
3. Select **Scan** to execute the selected scans, and the scan immediately begins. The **Stop** column indicates the scan is **In Progress**. Clicking this column heading will stop the scan(s).
4. For future scans, select the **Show Scheduling Options** link and enter the desired date and time to schedule a future scan.
5. After several minutes have passed, refresh the browser page and view the results of the scan. When the **Start** and **Stop** columns display date and time information, the scan is available to display the results.
6. Select the **pencil** icon for the scan to display the results. Table 71 describes the scan results and related information.

Table 71: *Device Setup > Discover > Discovery Execution Fields*

Column	Description
Network	Displays the network to be scanned.
Credentials	Displays the credentials used in the scan.
Total Devices	Displays the total number of APs detected during the scan that AMP can configure and

Table 71: *Device Setup > Discover > Discovery Execution Fields (Continued)*

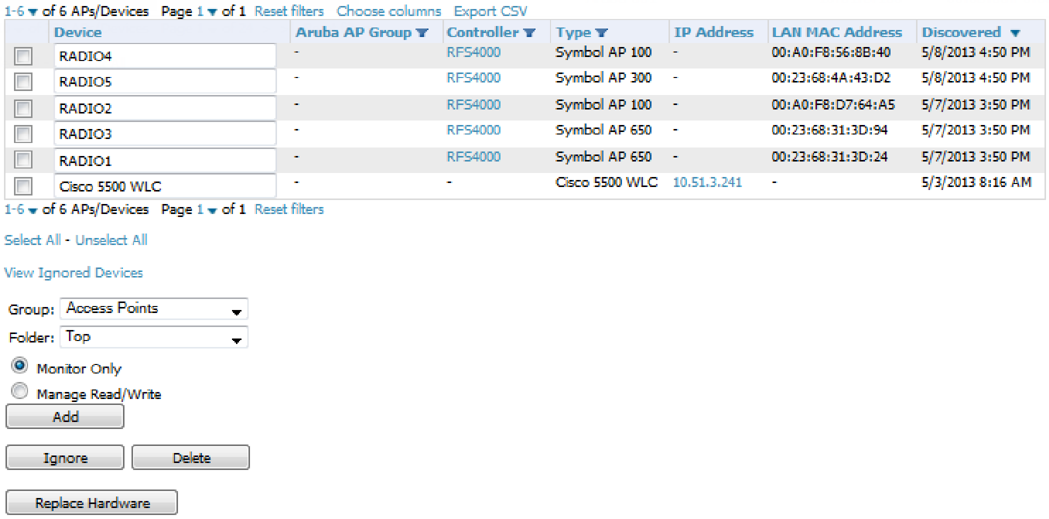
Column	Description
Found	monitor. **Total** includes both APs that are currently being managed by AMP as well as newly discovered APs that are not yet being managed.
New Devices Found	Displays the number of discovered APs that are not yet managed, but are available.
Total Rogues Found	Displays the total number of APs detected during the scan that AMP 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. Go to the **APs/Devices** > **New** page to see a full list of the newly discovered devices that the scan detected. Figure 70 illustrates this page.

NOTE

This page is only visible to users with the AMP Administrator role or roles that have **Allow authorization of APs/Devices** enabled in **AMP Setup > Roles**.

Figure 70 *APs/Devices > New Page Illustration*



1-6 ▾ of 6 APs/Devices Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Device	Aruba AP Group	Controller	Type	IP Address	LAN MAC Address	Discovered
□	RADIO4	-	RFS4000	Symbol AP 100	-	00:A0:F8:56:8B:40	5/8/2013 4:50 PM
□	RADIO5	-	RFS4000	Symbol AP 300	-	00:23:68:4A:43:D2	5/8/2013 4:50 PM
□	RADIO2	-	RFS4000	Symbol AP 100	-	00:A0:F8:D7:64:A5	5/7/2013 3:50 PM
□	RADIO3	-	RFS4000	Symbol AP 650	-	00:23:68:31:3D:94	5/7/2013 3:50 PM
□	RADIO1	-	RFS4000	Symbol AP 650	-	00:23:68:31:3D:24	5/7/2013 3:50 PM
□	Cisco 5500 WLC	-	-	Cisco 5500 WLC	10.51.3.241	-	5/3/2013 8:16 AM

1-6 ▾ of 6 APs/Devices Page 1 ▾ of 1 Reset filters

Select All - Unselect All

View Ignored Devices

Group: Access Points

Folder: Top

● Monitor Only

○ Manage Read/Write

What Next?

- To authorize one or more devices to a group, see "Authorizing Devices to AMP from APs/Devices > New Page" on page 129.
- To delete a device altogether from AMP, select the corresponding check box for each device, and select **Delete**.
- Aruba thin APs can have Aruba AP Groups specified, and Cisco thin APs can have LWAPP AP Groups specified when they are authorized.

The Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual Cisco switch or router on the **Groups** > **List** page. AMP requires read-only access to a router or switch for all subnets that contain wired or wireless devices. The polling interval is specified on the **Groups** > **Basic** page.

Authorizing Devices to AMP from APs/Devices > New Page

Once you have discovered devices on your network, add these devices to a group and specify whether the device is to be placed in **Manage Read/Write** or **Monitor Only** mode. To configure a new group, refer to "Configuring and Using Device Groups" on page 77.

In **Manage Read/Write** mode, AMP compares the device's current configuration settings with the Group configuration settings and automatically updates the device's configuration to match the Group policy.

In **Monitor Only** mode, AMP updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **APs/Devices** > **Audit** page, but does not change the configuration of the device.

CAUTION

Put devices in Monitor Only mode when they are added to a newly established device group. This avoids overwriting any important existing configuration settings.

Once you have added several devices to the Group, and verified that no unexpected or undesired configuration changes will be made to the devices, you can begin to put the devices in **Manage Read/Write** mode using the **APs/Devices** > **Manage** or the **Modify these devices** link on any list page.

Perform the following steps to add a newly discovered device to a group:

1. Browse to the **APs/Devices** > **New** page. The **APs/Devices** > **New** page displays all newly discovered devices, the related controller (when known/applicable) and the device vendor, model, LAN MAC Address, IP Address, and the date/time of discovery.
2. Select the group and folder to which the device will be added from the drop-down menu (the default group appears at the top of the **Group** listing). Devices cannot be added to a Global Group; groups designated as Global Groups cannot contain access points.
3. Select either the **Monitor Only** or the **Manage Read/Write** radio button and select **Add**.

   At this point, you can go to the **APs/Devices** > **List** page and select the folder(s) to which you have assigned one or more devices to verify that your device has been properly assigned. If you want to assign a device to the **Ignored** page or delete it entirely from AMP, go to step 4 on page 129.

NOTE

If you select **Manage Select Devices**, AMP automatically overwrites existing device settings with the specified group settings. Placing newly discovered devices in Monitor mode is strongly recommended until you can confirm that all group configuration settings are appropriate for that device.

4. If you do not want to manage or monitor a discovered device, you may select the device(s) from the list and select either **Ignore** or **Delete**. If you choose to **Ignore** the devices, they will not be displayed in the **APs/Devices** > **New** list, even if they are discovered in subsequent scans. You can view a list of all Ignored devices on the **APs/Devices** > **Ignored** page. If you choose to **Delete** the device, it will be listed on the **APs/Devices** > **New** list if discovered by AMP in a subsequent scan. Refer to "Assigning Devices to the Ignored Page" on page 134.

Manually Adding Individual Devices

Some deployment situations may require that you manually add devices to AMP. You can add devices manually by uploading a CSV file, or from the **Device Setup** > **Add** page.

This section describes the following procedures:

- "Adding Devices with the Device Setup > Add Page" on page 130
- "Adding Multiple Devices from a CSV File" on page 133

- "Adding Universal Devices" on page 134

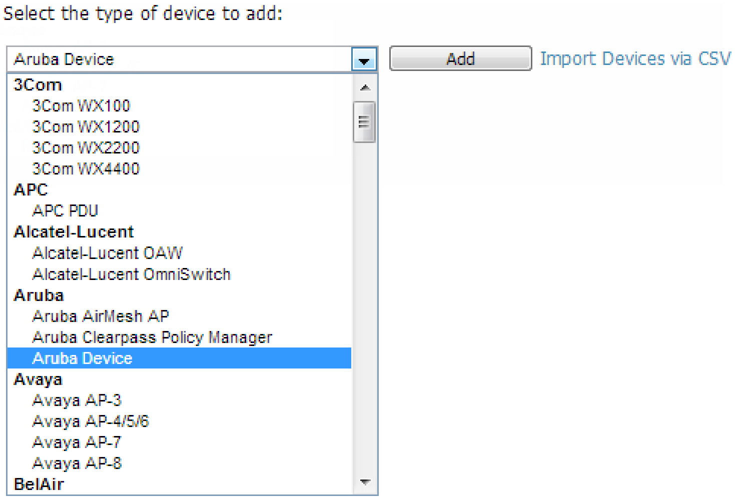
Adding Devices with the Device Setup > Add Page

Manually adding devices from the **Device Setup** > **Add** page to AMP is an option for adding all device types. You only need to select device vendor information from a drop down menu for Cisco and Aruba devices, and AMP automatically finds and adds specific make and model information into its database.

Perform these steps to manually add devices to AMP:

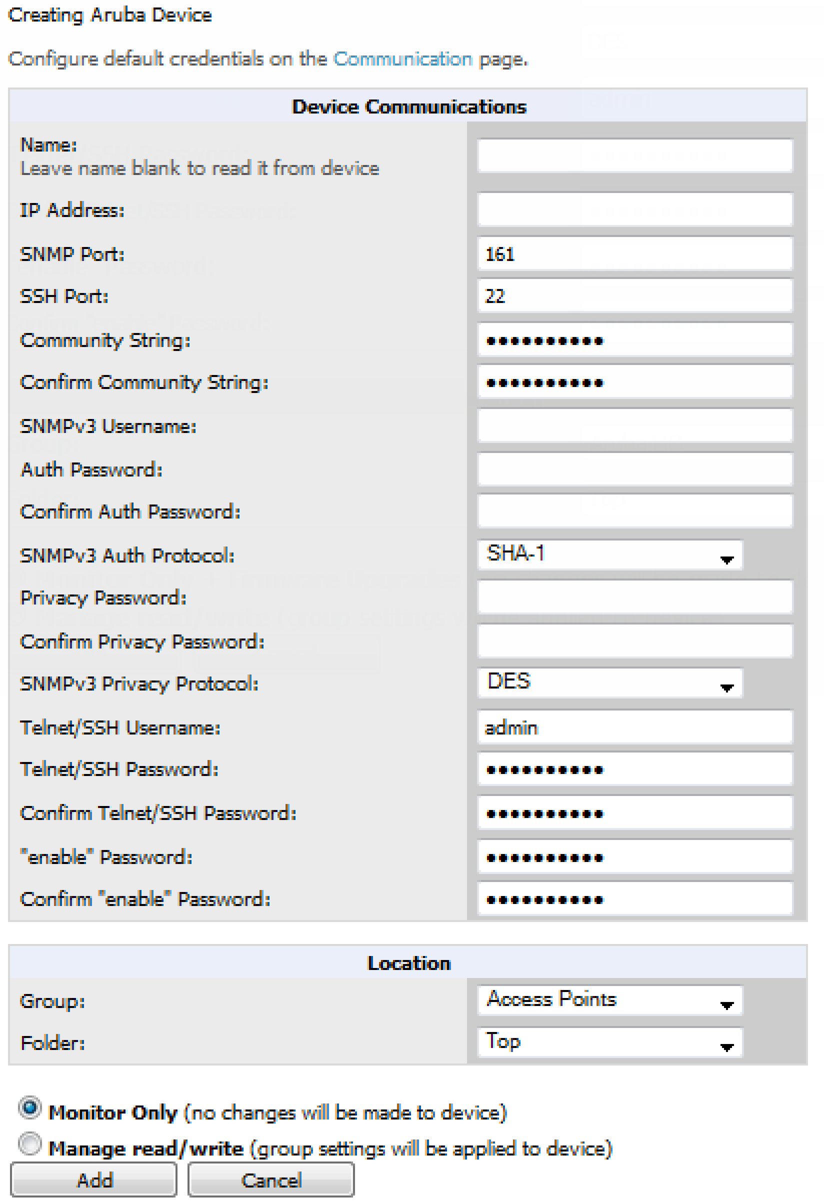
1. The first step to add a device manually is to select the vendor and model. Browse to the **Device Setup** > **Add** page and select the vendor and model of the device to add. Figure 71 illustrates this page.

Figure 71 *Device Setup > Add Page Illustration*



2. Select **Add**. The **Device Communications** and **Location** sections appear, illustrated in Figure 72.

Figure 72 *Device Setup > Add > Device Communications and Location Sections*



Creating Aruba Device

Configure default credentials on the Communication page.

Device Communications

Name: Leave name blank to read it from device	
IP Address:	
SNMP Port:	161
SSH Port:	22
Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••

Location

Group:	Access Points
Folder:	Top

● **Monitor Only** (no changes will be made to device)

○ **Manage read/write** (group settings will be applied to device)

3. Complete these **Device Communications** and **Location** settings for the new device. Table 72 further describes the contents of this page. Settings may differ from device to device based on the type of device and the features that the device supports. In several cases, the default values from any given device derive from the **Device Setup** > **Communication** page.

Table 72: *Device Communication and Location Fields and Default Values*

Setting	Default	Description
Name	None	User-configurable name for the AP (maximum of 20 characters).
IP Address	None	IP address of the device. This field is required.
SNMP Port	161	The port AMP uses to communicate with the AP using SNMP.

Table 72: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
SSH Port	22	For devices that support SSH, specify the SSH port number.
Community String (Confirm)	Taken from **Device Setup > Communication**	Community string used to communicate with the AP. **NOTE:** The **Community String** should have RW (Read-Write) capability. New, out-of-the-box Cisco devices typically have SNMP disabled and a blank username and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.
SNMPv3 Username	Taken from **Device Setup > Communication**	If you are going to manage configuration for the device, this field provides a read-write user account (SNMP, HTTP, and Telnet) within the Cisco Security System for access to existing APs. AMP initially uses this username and password combination to control the Cisco AP. AMP creates a user-specified account with which to manage the AP if the **User Creation Options** are set to **Create** and user Specified as User
Auth Password	Taken from **Device Setup > Communication**	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. AMP currently only supports authentication and encryption.
Privacy Password (Confirm)	Taken from **Device Setup > Communication**	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. AMP currently only supports authentication and encryption.
SNMPv3 Auth Protocol	Taken from **Device Setup > Communication**	Drop-down menu that allows you to enable the SNMPv3 authentication protocol to the device being added.
SNMPv3 Privacy Protocol	Taken from **Device Setup > Communication**	Drop-down menu that allows you to enable SNMPv3 privacy protocol to the device being added.
Telnet/SSH Username	Taken from **Device Setup > Communication**	Telnet username for existing Cisco IOS APs. AMP 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.
Telnet/SSH Password (Confirm)	Taken from **Device Setup > Communication**	Telnet password for existing Cisco IOS APs. AMP 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 **Device Setup > Communication**	Password that allows AMP to enter **enable** mode on the device.

4. In the **Location** field, select the appropriate Group and Folder for the device.

NOTE

When adding an Aruba device, be sure to add controllers and switches to separate groups.

5. At the bottom of the page, select either the **Monitor Only** or **Management read/write** radio button. The choice depends on whether or not you wish to overwrite the **Group** settings for the device being added. For more information and a detailed procedure, see "Authorizing Devices to AMP from APs/Devices > New Page" on page 129.

NOTE

If you select **Manage read/write**, AMP overwrites existing device settings with the **Groups** settings. Place newly discovered devices in **Monitor read/only** mode to enable auditing of actual settings instead of Group Policy settings.

6. Select **Add** to finish adding the devices to the network.

Adding Multiple Devices from a CSV File

You can add devices in bulk from a CSV file to AMP. Here you also have the option of specifying vendor name only, and AMP will automatically determine the correct type while bringing up the device. If your CSV file includes make and model information, AMP will add the information provided in the CSV file as it did before. It will not override what you have specified in this file in any way.

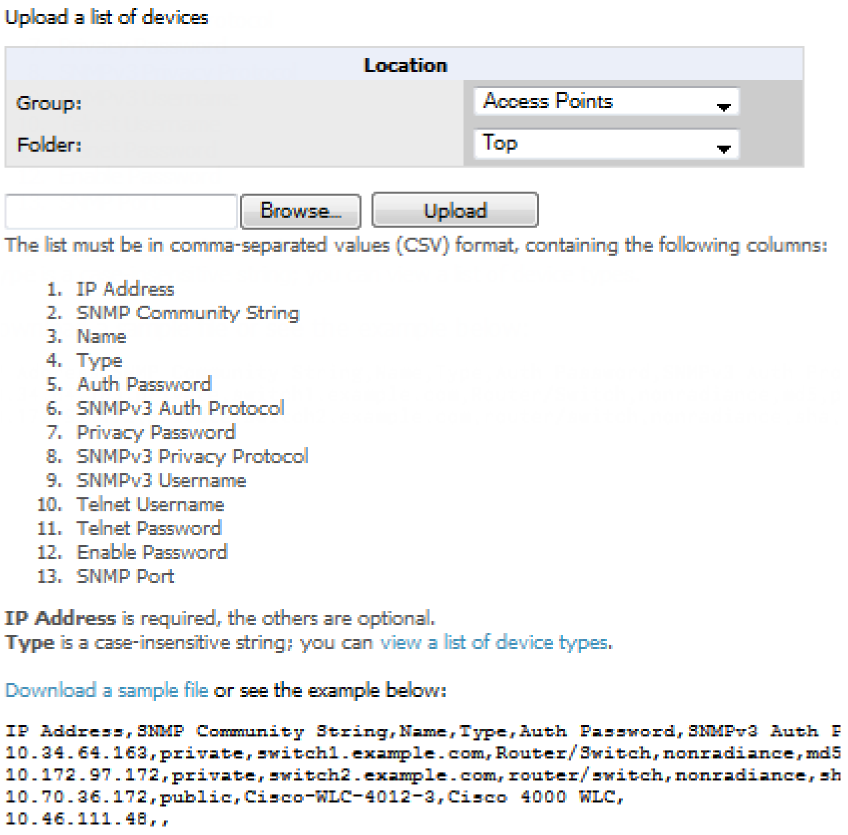
The CSV list must contain the following columns:

- IP Address
- SNMP Community String
- Name
- Type
- Auth Password
- SNMPv3 Auth Protocol
- Privacy Password
- SNMPv3 Privacy Protocol
- SNMPv3 Username
- Telnet Username
- Telnet Password
- Enable Password
- SNMP Port

You can download a CSV file and customize it as you like.

1. To import a CSV file, go to the **Device Setup** > **Add** page.
2. Select the **Import Devices via CSV link**. The **Upload a list of devices** page displays. See Figure 73.

Figure 73 *Device Setup > Add > Import Devices via CSV Page Illustration*



Upload a list of devices

Location	
Group:	Access Points
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 P
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sh
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 select the CSV list file on your computer.
5. Click the **Upload** button to add the list of devices into AMP.

Adding Universal Devices

AMP gets basic monitoring information from any device including switches, routers and APs whether or not they are supported devices. Entering SNMP credentials is optional. If no SNMP credentials are entered, AMP will provide ICMP monitoring of universal devices. This allows you to monitor key elements of the wired network infrastructure, including upstream switches, RADIUS servers and other devices. While AMP can manage most leading brands and models of wireless infrastructure, universal device support also enables basic monitoring of many of the less commonly used devices.

Perform the same steps to add universal devices to AMP that were detailed in "Adding Devices with the Device Setup > Add Page" on page 130.

AMP collects basic information about universal devices including name, contact, uptime and location. Once you have added a universal device, you can view a list of its interfaces on **APs/Devices > Manage**.

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

Assigning Devices to the Ignored Page

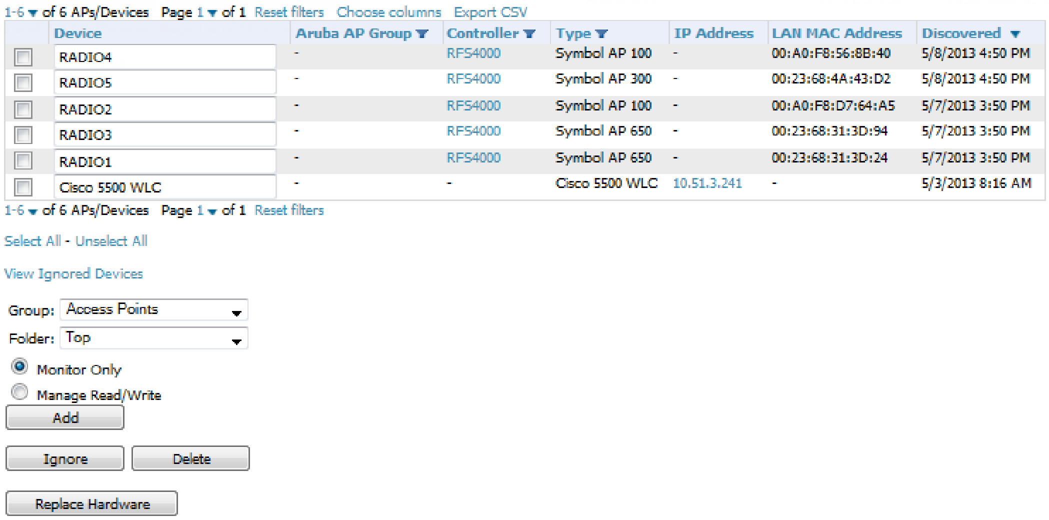
A device can be assigned to the **Ignored** page from the **APs/Devices > New** page. The advantage of having the device be designated in this way, as in the case of a device that is temporarily down for a known reason, is that when you take it off the ignored list, it returns immediately to the location in AMP where it had resided before it was marked **Ignored**.

- Ignored devices are *not* displayed in **APs/Devices** > **New** if discovered in subsequent scans.
- Deleted devices *will* be listed on the **APs/Devices** > **New** if discovered in subsequent scans.

Perform these steps to further process or return an ignored device to a managed status.

1. Go to the **APs/Devices** > **New** page to view all newly discovered devices. See Figure 74.

Figure 74 *APs/Devices > New Page Illustration*



1-6 ▾ of 6 APs/Devices Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Device	Aruba AP Group ▾	Controller ▾	Type ▾	IP Address	LAN MAC Address	Discovered ▾
□	RADIO4	-	RFS4000	Symbol AP 100	-	00:A0:F8:56:8B:40	5/8/2013 4:50 PM
□	RADIO5	-	RFS4000	Symbol AP 300	-	00:23:68:4A:43:D2	5/8/2013 4:50 PM
□	RADIO2	-	RFS4000	Symbol AP 100	-	00:A0:F8:D7:64:A5	5/7/2013 3:50 PM
□	RADIO3	-	RFS4000	Symbol AP 650	-	00:23:68:31:3D:94	5/7/2013 3:50 PM
□	RADIO1	-	RFS4000	Symbol AP 650	-	00:23:68:31:3D:24	5/7/2013 3:50 PM
□	Cisco 5500 WLC	-	-	Cisco 5500 WLC	10.51.3.241	-	5/3/2013 8:16 AM

1-6 ▾ of 6 APs/Devices Page 1 ▾ of 1 Reset filters

Select All - Unselect All

View Ignored Devices

Group: Access Points

Folder: Top

● Monitor Only

○ Manage Read/Write

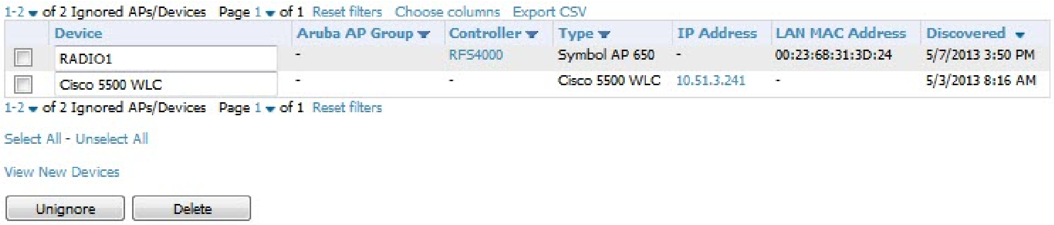
2. Select the checkbox beside the device or devices that you want to ignore, and then select the **Ignore** button.

Unignoring a Device

Perform these steps to further process a device or to return an ignored device to a managed status.

1. To view all devices that are ignored, go to the **APs/Devices** > **Ignored** page, illustrated in Figure 75.

Figure 75 *APs/Devices > Ignored Page Illustration*



1-2 ▾ of 2 Ignored APs/Devices Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Device	Aruba AP Group ▾	Controller ▾	Type ▾	IP Address	LAN MAC Address	Discovered ▾
□	RADIO1	-	RFS4000	Symbol AP 650	-	00:23:68:31:3D:24	5/7/2013 3:50 PM
□	Cisco 5500 WLC	-	-	Cisco 5500 WLC	10.51.3.241	-	5/3/2013 8:16 AM

1-2 ▾ of 2 Ignored APs/Devices Page 1 ▾ of 1 Reset filters

Select All - Unselect All

View New Devices

This page provides the following information for any ignored device:

- device name or MAC address, when known
- controller associated with that device
- device type
- device IP address
- LAN MAC address for the LAN on which the device is located
- date and time of device discovery

2. To change the device parameters for a given device, select its checkbox and adjust group, folder, monitor, and manage settings as desired.
3. Select **Add** to add the device to AMP so that it appears on the **APs/Devices** > **New** list.

4. The **Unignore** button will either return the device to its regular folder or group or send it to the **APs/Devices > New** page.

Monitoring Devices

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

- "Viewing Device Monitoring Statistics" on page 136
- "Understanding the APs/Devices > Monitor Pages for All Device Types" on page 137
- "Monitoring Data Specific to Wireless Devices" on page 138
- "Evaluating Radio Statistics for an AP" on page 145
- "Monitoring Data for Mesh Devices" on page 150
- "Monitoring Data for Wired Devices (Routers and Switches)" on page 151
- "Understanding the APs/Devices > Interfaces Page" on page 153
- "Auditing Device Configuration" on page 154
- "Using Device Folders (Optional)" on page 155

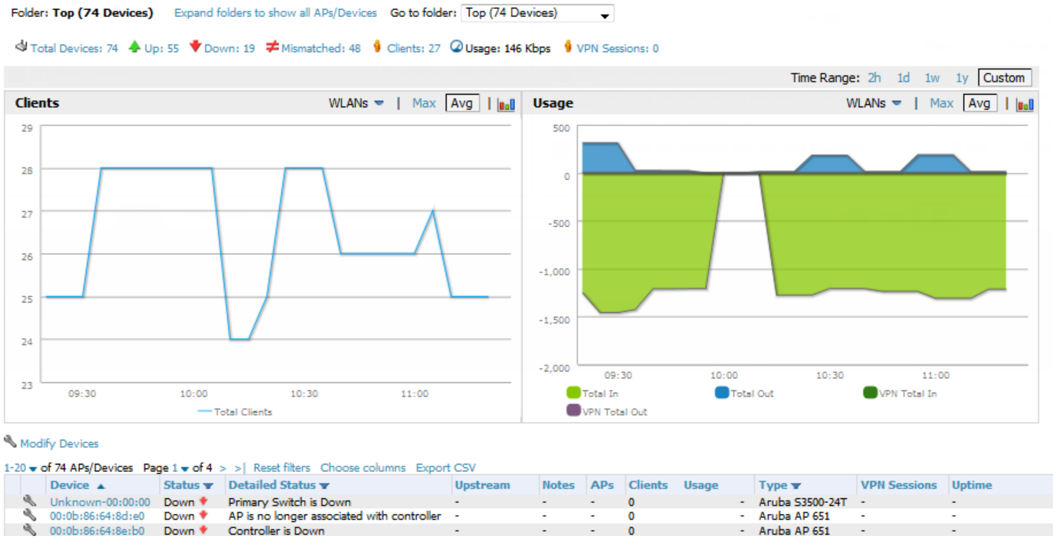
Viewing Device Monitoring Statistics

You can view many useful device monitoring statistics in the **APs/Devices > List** page. The **APs/Devices > List** page displays Clients and Usage interactive graphs (formerly Users and Bandwidth prior to 7.4) and lists all devices that are managed or monitored by AMP.

To see only the Up devices, you can click the **Up** link in the Top Header Stats bar (next to the green arrow). This displays the **APs/Devices > Up** page with the same information, but only containing active devices. You can do the same with the **Down** and **Mismatched** top header stats links.

Use the **Go to folder** field to filter the list by folder, or click **Expand folders to show all APs/Devices** if you are looking at a filtered device list. A lock icon in the **Configuration** column indicates that the device in that row is in **Monitor only** mode. Figure 76 illustrates this page.

Figure 76 *APs/Devices > List (partial view)*



Folder: **Top (74 Devices)** Expand folders to show all APs/Devices Go to folder: Top (74 Devices)

Total Devices: 74 Up: 55 Down: 19 Mismatched: 48 Clients: 27 Usage: 146 Kbps VPN Sessions: 0

1-20 of 74 APs/Devices Page 1 of 4 > >| Reset filters Choose columns Export CSV

	Device ▲	Status ▼	Detailed Status ▼	Upstream	Notes	APs	Clients	Usage	Type ▼	VPN Sessions	Uptime
	Unknown-00:00:00	Down	Primary Switch is Down	-	-	-	0	-	Aruba S3500-24T	-	-
	00:0b:86:64:8d:e0	Down	AP is no longer associated with controller	-	-	-	0	-	Aruba AP 651	-	-
	00:0b:86:64:8e:b0	Down	Controller is Down	-	-	-	0	-	Aruba AP 651	-	-

Verify that the devices you added are now appearing in the **APs/Devices > Up** page.

NOTE

Newly added devices will have a status of **Down** until they have been polled the first time. Their configuration status will remain **Unknown** until they have finished verification. The **Up** status is not contingent on verification.

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

The **Alert Summary** section of **APs/Devices** > **List** cites the number of events that have occurred in the last two hours, the last 24 hours, and total. There are three categories of alerts as listed below:

- AMP Alerts
- IDS Events
- RADIUS Authentication Issues

NOTE

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

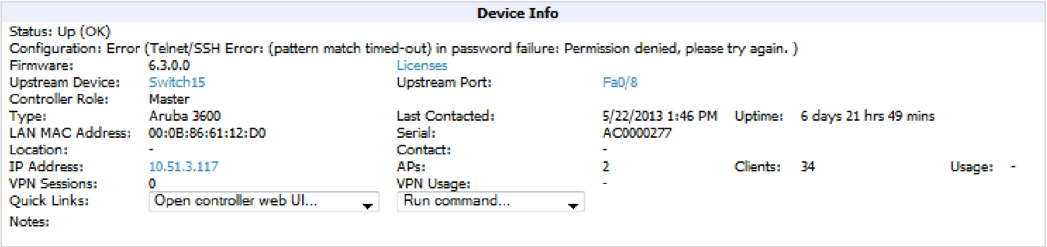
For more information on the **Alert Summary** table, refer to "Viewing Alerts" on page 227.

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

You can quickly go to any device’s monitoring page once you go to its specific folder or group on the **APs/Devices** > **List** page by selecting its hyperlinked name in the **Device** column.

All **Monitor** pages include a section at the top displaying information such as monitoring/configuration status, serial number, total clients, firmware version, and so on, as shown in Figure 77.

Figure 77 *Monitoring Page Top Level Data Common to All Device Types*



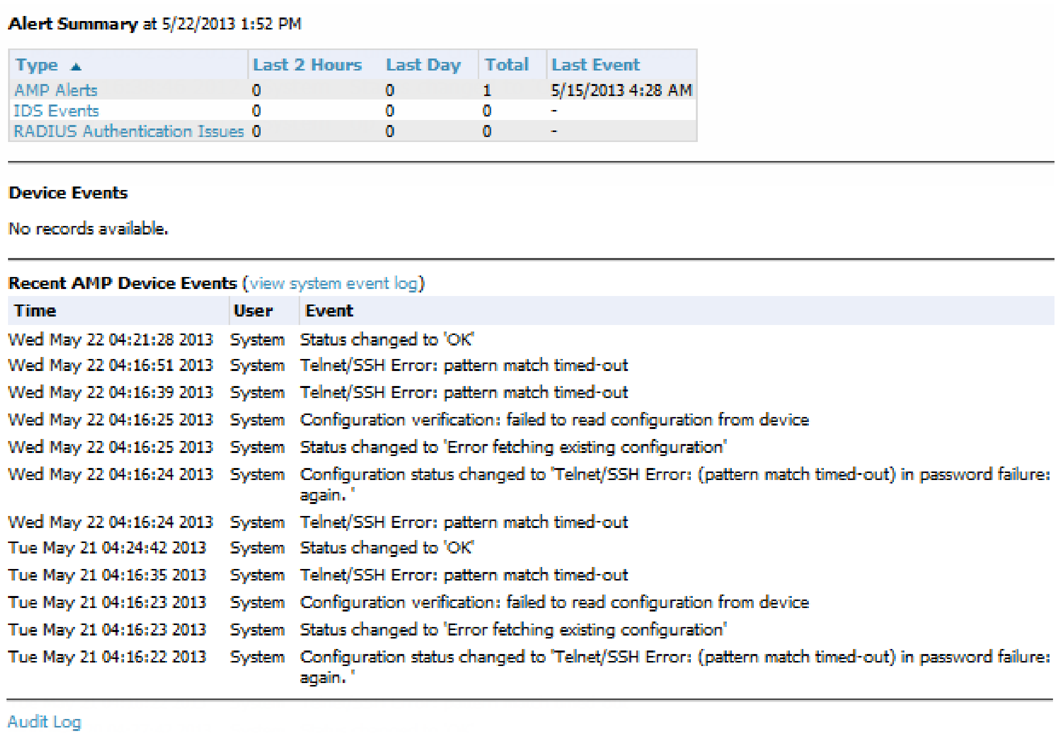
Device Info

Status: Up (OK)
Configuration: Error (Telnet/SSH Error: (pattern match timed-out) in password failure: Permission denied, please try again.)

Firmware:	6.3.0.0	Licenses					
Upstream Device:	Switch15	Upstream Port:	Fa0/8				
Controller Role:	Master						
Type:	Aruba 3600	Last Contacted:	5/22/2013 1:46 PM	Uptime:	6 days 21 hrs 49 mins		
LAN MAC Address:	00:0B:86:61:12:D0	Serial:	AC0000277				
Location:	-	Contact:	-				
IP Address:	10.51.3.117	APs:	2	Clients:	34	Usage:	-
VPN Sessions:	0	VPN Usage:	-				
Quick Links:	Open controller web UI...	Run command...					
Notes:							

The alert summary and recent events sections are also the same regardless of the device type, and these sections appear toward the bottom of these pages. In addition, a link to the Audit Log is available on the bottom of this page. A portion of this page is shown in Figure 78.

Figure 78 *Monitoring Page Bottom Level Data Common to All Device Types (partial view)*



Alert Summary at 5/22/2013 1:52 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	1	5/15/2013 4:28 AM
IDS Events	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Device Events

No records available.

Recent AMP Device Events (view system event log)

Time	User	Event
Wed May 22 04:21:28 2013	System	Status changed to 'OK'
Wed May 22 04:16:51 2013	System	Telnet/SSH Error: pattern match timed-out
Wed May 22 04:16:39 2013	System	Telnet/SSH Error: pattern match timed-out
Wed May 22 04:16:25 2013	System	Configuration verification: failed to read configuration from device
Wed May 22 04:16:25 2013	System	Status changed to 'Error fetching existing configuration'
Wed May 22 04:16:24 2013	System	Configuration status changed to 'Telnet/SSH Error: (pattern match timed-out) in password failure: again. '
Wed May 22 04:16:24 2013	System	Telnet/SSH Error: pattern match timed-out
Tue May 21 04:24:42 2013	System	Status changed to 'OK'
Tue May 21 04:16:35 2013	System	Telnet/SSH Error: pattern match timed-out
Tue May 21 04:16:23 2013	System	Configuration verification: failed to read configuration from device
Tue May 21 04:16:23 2013	System	Status changed to 'Error fetching existing configuration'
Tue May 21 04:16:22 2013	System	Configuration status changed to 'Telnet/SSH Error: (pattern match timed-out) in password failure: again. '

Audit Log

Monitoring pages vary according to whether they are wired routers/switches, controllers/WLAN switches, or thin or fat APs; whether the device is a Mesh device; and whether Spectrum is enabled. These differences are discussed in the sections that follow.

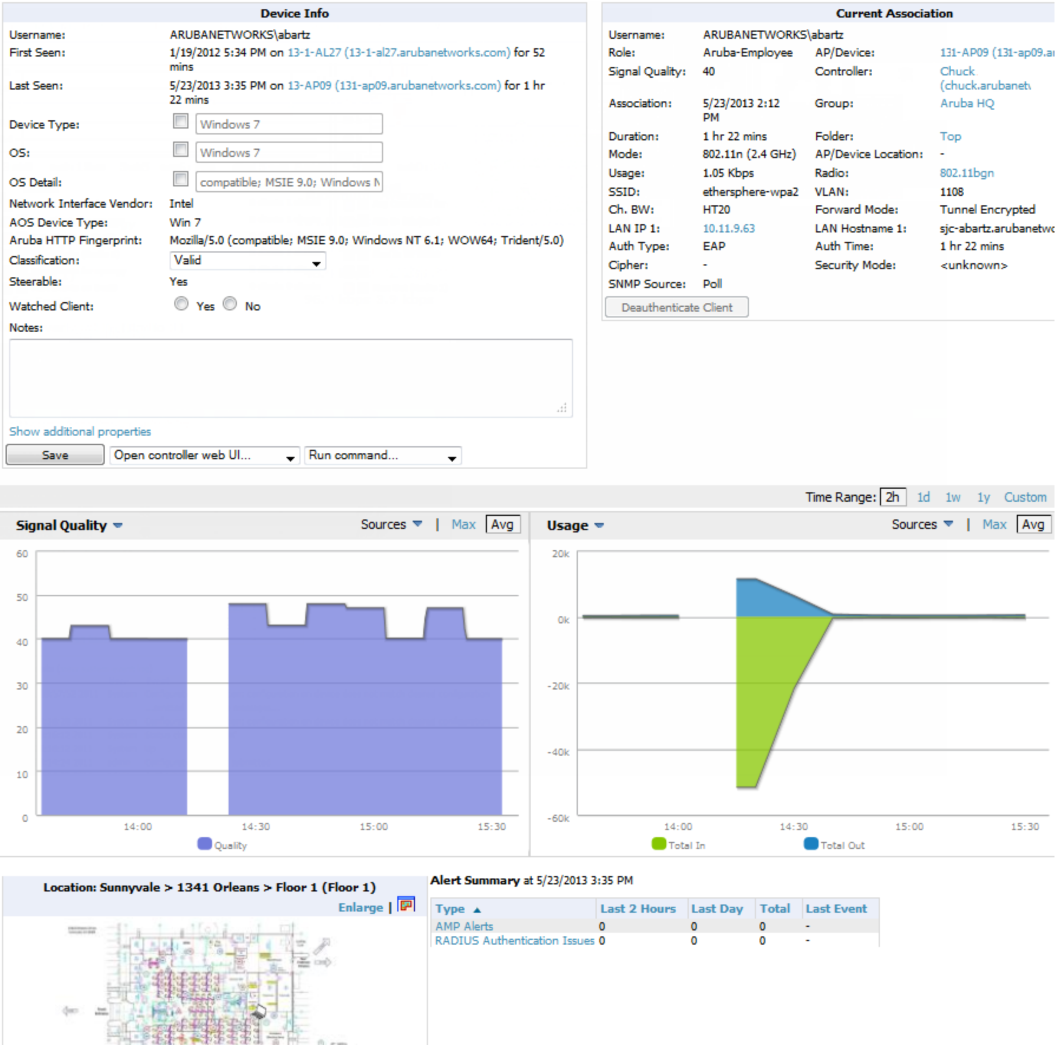
Monitoring Data Specific to Wireless Devices

The **APs/Devices** > **Monitor** page for controllers and APs include a graph for users and bandwidth. The controller graph lists the APs connected to it, while the APs include a list of users it has connected.

When available, lists of CDP and RF neighbors are also listed.

A sample monitoring page for wireless devices is shown in Figure 79.

Figure 79 *APs/Devices > Monitor Page for Wireless Devices (partial view of an AP)*



Device Info

Username: ARUBANETWORKS\abartz

First Seen: 1/19/2012 5:34 PM on 13-1-AL27 (13-1-al27.arubanetworks.com) for 52 mins

Last Seen: 5/23/2013 3:35 PM on 13-AP09 (131-ap09.arubanetworks.com) for 1 hr 22 mins

Device Type: □ Windows 7

OS: □ Windows 7

OS Detail: □ compatible; MSIE 9.0; Windows N

Network Interface Vendor: Intel

AOS Device Type: Win 7

Aruba HTTP Fingerprint: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

Classification: Valid

Steerable: Yes

Watched Client: ○ Yes ○ No

Notes:

Show additional properties

Save | Open controller web UI... | Run command...

Current Association

Username: ARUBANETWORKS\abartz

Role: Aruba-Employee

AP/Device: 131-AP09 (131-ap09.ar

Signal Quality: 40

Controller: Chuck (chuck.arubanet

Association: 5/23/2013 2:12 PM

Group: Aruba HQ

Duration: 1 hr 22 mins

Folder: Top

Mode: 802.11n (2.4 GHz)

AP/Device Location: -

Usage: 1.05 Kbps

Radio: 802.11bgn

SSID: ethersphere-wpa2

VLAN: 1108

Ch. BW: HT20

Forward Mode: Tunnel Encrypted

LAN IP 1: 10.11.9.63

LAN Hostname 1: sjc-abartz.arubanetwo

Auth Type: EAP

Auth Time: 1 hr 22 mins

Cipher: -

Security Mode: <unknown>

SNMP Source: Poll

Deauthenticate Client

Location: Sunnyvale > 1341 Orleans > Floor 1 (Floor 1)

Enlarge |

Alert Summary at 5/23/2013 3:35 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Table 73 describes the fields and information displayed in the **Device Info** section. The displayed fields vary from device to device.

Table 73: *APs/Devices > Monitor > Device Info Fields and Default Values*

Field	Description
Poll Now	Button above the **Device Info** section that, when pressed, immediately polls the individual AP or the controller for a thin AP; this overrides the group's preset polling intervals to force an immediate update of all data except for rogue information. Shows attempt status and last polling times.
Status	Displays ability of AMP to connect to the AP. **Up** (no issue) means everything is working as it should. **Down** (SNMP get failed) means AMP can get to the device but not speak with it using SNMP. Check the SNMP credentials AMP is using the view secrets link on the **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 AMP is unable to connect to the AP using SNMP and is unable to ping the AP. This usually means AMP is blocked from connecting to the AP or the AP needs to be rebooted or reset.

Table 73: *APs/Devices > Monitor > Device Info Fields and Default Values (Continued)*

Field	Description
Configuration	● **Good** means all the settings on the AP agree with the settings AMP wants them to have. ● **Mismatched** means there is a configuration mismatch between what is on the AP and what AMP wants to push to the AP. The **Mismatched** link directs you to this specific **APs/Devices > Audit** page where each mismatch is highlighted. ● **Unknown** means the device configuration has not yet been fetched (possible issue with credentials). ● **Verifying** means that the device is fetching a configuration that will be compared to the desired settings. ● **Error** indicates a problem with the device. This configuration is accompanied with a description of the error.
Firmware	Displays the firmware version running on the AP. Newer AirMesh APs include the new bootloader APBoot. AMP helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Licenses (Appears for Aruba controllers)	Selecting this link opens a pop-up window that lists the built-in licenses as well as other installed licenses for this controller. This also shows whether any license has expired.
Controller (Appears for APs)	Displays the controller for the associated AP device as a link. Select the link to display the **APs/Devices > Monitor** page for that controller.
Mesh Gateway *	Specifies the mesh AP acting as the wired connection to the network.
Mesh Mode*	Specifies whether the AP is a portal device or a mesh node. The portal device is connected to the network over a wired connection. A node is a device downstream of the portal that uses wireless connections to reach the portal device.
Mesh ID *	The name of the mesh device.
Google Earth*	Selecting the Google Earth icon opens the mesh network view in Google Earth.
Type	Displays the make and model of the device.
Last Contacted	Displays the most recent time AMP 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 AMP.
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. This field is not available for all APs.
Location	Displays the SNMP location of the device.
Contact	Displays the SNMP contact of the device.

Table 73: *APs/Devices > Monitor > Device Info Fields and Default Values (Continued)*

Field	Description
IP Address	Displays the IP address that AMP uses to communicate to the device. This number is also a link to the AP web interface. When the link is moused over a pop-up menu will appear allowing you to http, https, telnet or SSH to the device. For Aruba controllers, if Single Sign-On is enabled for your role in this AMP and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link.
Outer IP	Public IP address for a RAP device.
Remote LAN IP	LAN IP address for a RAP. This address is useful for troubleshooting from the local network.
Quick Links	**Open controller web UI:** A drop-down menu that allows you to jump to the controller's UI in a new window. For Aruba controllers, if Single Sign-On is enabled for your role in this AMP and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link. **Run a command:** A drop-down menu with a list of CLI commands you can run directly from the **APs/Devices > Monitor** page.
APs	For controllers, displays the number of APs managed by this device at the time of the last polling.
Clients	Displays the total number of users associated to the device or its APs regardless of which radio they are associated to, at the time of the last polling.
Usage	Combined bandwidth through the device at time of polling.

*These fields are only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Data for Mesh Devices" on page 150.

Table 74 describes the information in the **Radio** table for APs:

Table 74: *APs/Devices > Monitor > Radio Fields and Descriptions*

Field	Description
Index	The number of the radio, used to distinguish radios that may be of the same type on a device.
Name	The Radio type (802.11a/b/g/n) as a link to the **Radio Statistics** page for that radio.
MAC address	The MAC address of the corresponding radio in the AP.
Clients	The number of users associated to the corresponding radio at the time of the last polling.
Usage (Kbps)	The amount of bandwidth being pushed through the corresponding radio interface or device at the time of the last polling.
Channel	The channel of the corresponding radio.
Tx Power	Some devices report transmit power reduction rather than transmit power; no value is reported for those devices.

Table 74: *APs/Devices > Monitor > Radio Fields and Descriptions (Continued)*

Field	Description
Antenna Type	Indicates **Internal** or **External** radio. For devices where antenna type is defined per AP, the same antenna type will be listed for each radio.
Channel Width*	The bandwidth of the channel used by 802.11 stations. Legacy devices use **20 MHz** channels, and newer devices that support the 802.11n standard can use **40 MHz** channels to increase throughput.
Mesh Links *	The total number of mesh links to the device including uplinks and downlinks.
Role	Whether the radio acts as a Mesh Node or Access
Active SSIDs	The SSID(s) of the radio.

*These fields are only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Data for Mesh Devices" on page 150.

Devices with wired interfaces (other than Aruba Instant APs) will display the **Wired Interfaces** table, which is described in Table 75:

Table 75: *APs/Devices > Monitor > Wired Interfaces Fields and Descriptions*

Field	Description
Name	Displays the name of the interface.
MAC Address	Displays the MAC address of the corresponding interface in the device.
Clients	Displays the number of users associated to the corresponding interface at the time of the last polling.
Type	Indicates the type of interface - gigabit Ethernet or fast Ethernet for wired interfaces.
Admin Status	The administrator setting that determined whether the port is on or off.
Operational Status	Displays the current status of the interface. If an interface is **Up**, then AMP is able to ping it and fetch SNMP information. If the AP is listed as **Down**, then AMP is either unable to ping the interface or unable to read the necessary SNMP information from the device.
Duplex	Duplex mode of the link, full or half.
Aruba Port Mode	Either Active Standby (which provides redundancy so that when an active interface fails, the user traffic can failover to the standby interface) or one of the forwarding modes (Split, Bridge).
Input Capacity	The input capacity of the interface.
Output Capacity	The output capacity of the interface.

Figure 80 illustrates the interactive graphs. Use the drop down button next to the graph title to select a different graph.

Figure 80 *Interactive graphs for an Arubacontroller*

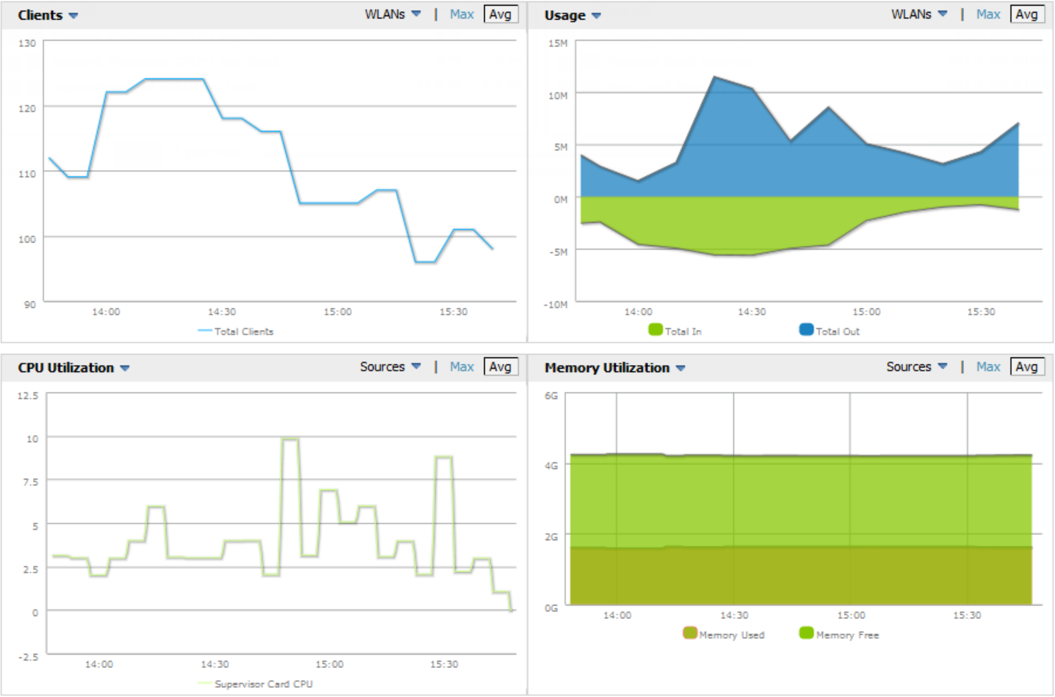


Table 76 describes the graphs on this page.

Table 76: *APs/Devices > Monitor Graphical Data*

Graph	Description
Clients	Formerly Users. Shows the max and average client count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Check boxes below the graph can be used to limit the data displayed.
Usage	Formerly Bandwidth. Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Check boxes below the graph can be used to limit the data displayed.
CPU Utilization (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only)	Reports overall CPU utilization (not on a per-CPU basis) of the device.
Memory Utilization (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only	Reports average used and free memory and average max memory for the device.

Table 77 describes the fields and information displayed for the **Connected Clients** display.

Table 77: *APs/Devices > Monitor > Connected Clients Fields and Default Values*

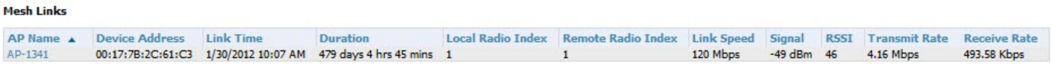
Field	Description
Username	Provides the name of the User associated to the AP. AMP gathers this data in a variety of ways. It can be taken from RADIUS accounting data or traps.
Device Type	The type of device the user is using as determined by the Device Type Rules set up by an administrator in **AMP Setup > Device Type Setup**. For more information, refer to "Setting Up Device Types" on page 63.
Role	The role of the connected client such as employee, perforce, or logon (captive portal).
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 AMP 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. Supported auth types include: ● **EAP**–Extensible Authentication Protocol. ● **RADIUS accounting**–RADIUS accounting servers integrated with AMP provide the RADIUS Accounting Auth type ● **WPA2**–Wi-Fi Protected Access 2 encryption ● No Encryption AMP considers all other types as not authenticated. The information AMP displays in **Auth Type** and **Cipher** columns depends on what information the server receives from the devices it is monitoring. The client devices may all be similar, but if the APs to which they are associated are of different models, or if security is set up differently between them, then different **Auth Type** or **Cipher** values may be reported to AMP. 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**.
Cipher	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 AMP.
Auth Time	Shows how long the user has been authenticated, in minutes. A negative number (such as -17 min) indicates that the user has not authenticated for the duration displayed.
Signal Quality	Displays the average signal quality the user experienced.
Usage	Displays the average bandwidth consumed by the MAC address.
Goodput	The ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes. Note that this information is not available for Instant devices.

Table 77: *APs/Devices > Monitor > Connected Clients Fields and Default Values (Continued)*

Field	Description
Speed	The packet and byte counts of data frames successfully transmitted to and received from associated stations. Note that this information is not available for Instant devices.
Location	Displays the QuickView box allows users to view features including heatmap for a device and location history for a user.
LAN IP Addresses	Displays the IP assigned to the user MAC. This information is not always available. AMP can gather it from the ARP cache of switches discovered by AMP. This column can accommodate multiple IP addresses for a client if it has both IPv4 and IPv6.
LAN Hostnames	The DNS hostname(s) broadcast by the client. This column can accommodate multiple hostnames for a client if it has both IPv4 and IPv6.

If you are viewing an Aruba AirMesh device's monitoring page, the **Mesh Links** table lists the mesh devices linked to this device, as shown in Figure 81:

Figure 81 *Mesh Links Table on APs/Devices > Monitor Illustration*



Mesh Links

AP Name ▲	Device Address	Link Time	Duration	Local Radio Index	Remote Radio Index	Link Speed	Signal	RSSI	Transmit Rate	Receive Rate
AP-1341	00:17:7B:2C:61:C3	1/30/2012 10:07 AM	479 days 4 hrs 45 mins	1	1	120 Mbps	-49 dBm	46	4.16 Mbps	493.58 Kbps

The **Recent Events** area lists the most recent events specific to the device. This information also appears on the **System > Events** Log page (refer to "Using the System > Event Log Page" on page 218). Table 78 describes the fields in this page that display in the **Recent Events** table.

Table 78: *APs/Devices > Monitor > Recent Events Fields and Default Values*

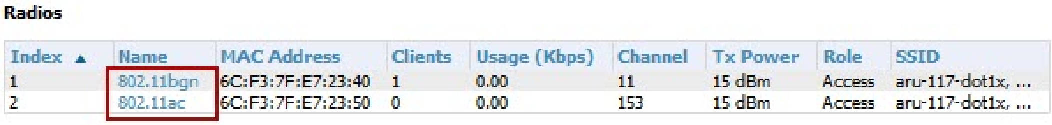
Field	Description
Time	Displays the day and time the event was recorded.
User	Displays the user that triggered the event. Configuration changes are logged as the AMP user that submitted them. Automated AMP events are logged as the **System** user.
Event	Displays a short text description of the event.

Evaluating Radio Statistics for an AP

The **APs/Devices** > **Monitor** > **Radio Statistics** page contains useful data for pinpointing network issues at the AP radio level for Aruba APs and Cisco WLC thin APs (firmware 4.2 or greater).

To see radio statistics details, navigate to the **APs/Devices** > **Monitoring** page for a supported AP and select the linked radio under the **Name** column in the **Radios** list table, as illustrated in Figure 82.

Figure 82 *Links to the Radio Statistics page on APs/Devices > Monitoring for an AP*



Radios

Index ▲	Name	MAC Address	Clients	Usage (Kbps)	Channel	Tx Power	Role	SSID
1	802.11bgn	6C:F3:7F:E7:23:40	1	0.00	11	15 dBm	Access	aru-117-dot1x, ...
2	802.11ac	6C:F3:7F:E7:23:50	0	0.00	153	15 dBm	Access	aru-117-dot1x, ...

Overview of the Radio Statistics Page

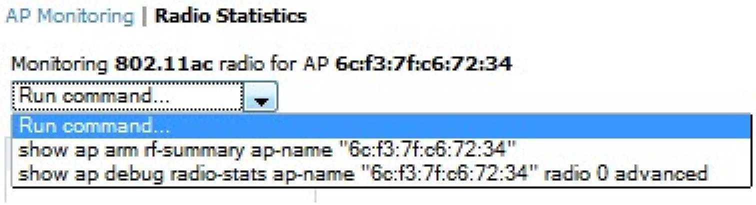
The Radio Statistics page displays transmit and receive statistics about the communication quality of individual radios. Depending on the AP, assigned group profiles, and recent activity on this radio, this data gives visibility into recent and historical changes in the network, fetches real-time statistics from the AP's controller, indicates actively interfering devices (requires Aruba set to Spectrum mode), and summarizes major issues.

Viewing Real-Time ARM Statistics

Aruba AP Groups that have the **Adaptive Radio Management** (**ARM**) feature enabled continuously optimize each AP to use the best channel and transmission power settings available. An AP configured with ARM will automatically adjust to a better channel if it reaches a configured threshold for noise, MAC errors, or PHY errors; additionally, it can attenuate transmit power and switch between radio modes as needed. For more information, refer to the ARM chapter in the *ArubaOS User Guide*.

Complete ARM statistics from Aruba controllers can be retrieved from the Radio Statistics page by selecting the **Run a command** drop-down menu and choosing button, as illustrated in Figure 83.

Figure 83 *Fetch additional radio stats by running a show command*



AP Monitoring | Radio Statistics

Monitoring 802.11ac radio for AP 6c:f3:7f:c6:72:34

```
show ap arm rf-summary ap-name "6c:f3:7f:c6:72:34"
show ap debug radio-stats ap-name "6c:f3:7f:c6:72:34" radio 0 advanced
```

When this button is selected, a new browser window launches with the statistics in plain text. Other ARM-tracked metrics are visible in the **Radio Statistics** page for Aruba APs.

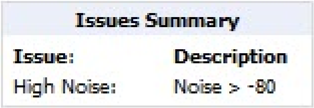
Issues Summary section

The **Issues Summary** section only displays when noise, client count, non-802.11 interfering devices, channel utilization, usage, and MAC and PHY errors reach a certain threshold of concern, as described in Table 79 and illustrated in Figure 84:

Table 79: *Issues Summary labels and thresholds*

Issue	Triggering Threshold
High Noise	> -80
High Number of Clients	> 15
High Channel Utilization	> 75%
High Usage	> 75% of max
Interfering Devices Detected	Detected within the last 5 minutes
High MAC/Phy Errors	> 1000 frames/sec

Figure 84 *Issues Summary Section Illustration*



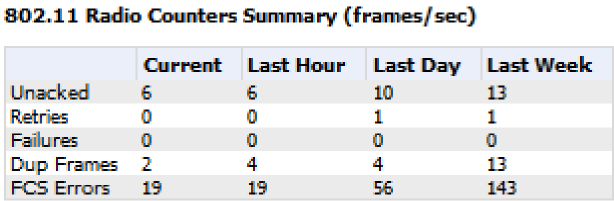
Issues Summary	
Issue:	**Description**
High Noise:	Noise > -80

These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the "Radio Statistics Interactive Graphs" on page 147 section of this chapter for details.

802.11 Radio Counters Summary

This table appears for radios with 802.11 counters and summarizes the number of times an expected acknowledgment frame was not received, the number of duplicate frames, the number of frames containing Frame Check Sequence (FCS) errors, and the number of frame/packet transmission retries and failures. These aggregate error counts are broken down by Current, Last Hour, Last Day, and Last Week time frames, as illustrated in Figure 85.

Figure 85 ***802.11 Radio Counters Summary*** *table*



802.11 Radio Counters Summary (frames/sec)

	Current	Last Hour	Last Day	Last Week
Unacked	6	6	10	13
Retries	0	0	1	1
Failures	0	0	0	0
Dup Frames	2	4	4	13
FCS Errors	19	19	56	143

The frame- per-second rate of these and other 802.11 errors over time are tracked and compared in the **802.11 Counters** graph on the same page.

Radio Statistics Interactive Graphs

Time-series graphs for the radio show changes recorded at every polling interval over time when polling with either SNMP or AMON. Clients and Usage data are polled based on the AP's group's **User Data Polling Period**. Channel, Noise, and Power are based on **AP Interface Polling Period**. 802.11 Counters data are based on the APs group's **802.11 Counters Polling Period**.

The two graph panes enable simultaneous display of two different information sets, as detailed in the following table:

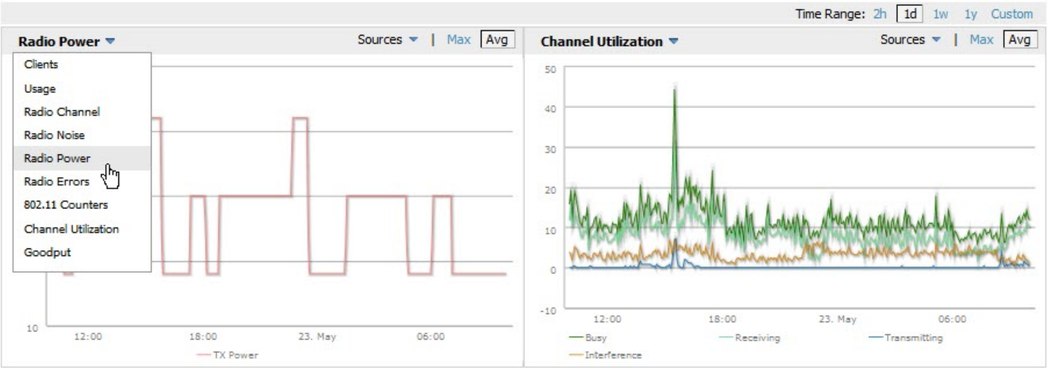
Table 80: *Radio Statistics Interactive Graphs Descriptions*

Graph Title	Description
Clients	A line graph that displays the maximum users associated to the corresponding radio at polling intervals over the time range set in the slider. Select **Show All** for other metrics such as average users and max users for various individual devices.
Usage	An area graph displaying the average bandwidth in each direction for the radio. Select **Show All** for other metrics such as max bandwidth in and out, average and max mesh/overhead or overhead bandwidth, and average/max Enet0.
Radio Channel	An area graph that displays the channel changes (if any) of the radio over time. Frequent, regular channel changes on an Aruba or Cisco WLC AP radio usually indicate that the Adaptive Radio Management feature (ARM) in ArubaOS is compensating for high noise levels from interfering devices.

Table 80: *Radio Statistics Interactive Graphs Descriptions (Continued)*

Graph Title	Description
Radio Noise	An area graph that displays signal interference (noise floor) levels in units of dBm. Noise from interfering devices above your AP's noise threshold can result in dropped packets. For ARM-enabled Aruba APs, crossing the noise threshold triggers an automatic channel change.
Radio Power	A line graph that displays the average and maximum radio transmit power, between 0 and 30 dBm, over the time range set in the slider. You can adjust the transmit power manually in the **APs/Devices > Manage** page for this radio's AP, or enable ARM on Aruba APs to dynamically adjust the power toward your acceptable Coverage Index as needed. For more information, see the Adaptive Radio Management chapter of the *ArubaOS User Guide*.
Radio Errors	A line graph displaying the frame reception rate, physical layer error rate (resulting from poor signal reception or broken antennas), and the data link (MAC) layer (corrupt frames, driver decoding issues) for the radio.
802.11 Counters	A line graph that displays statistics such as frame rate, fragment rate, retry rate, duplicate frame rate, and other metrics tracked by 802.11 counters.
Utilization (Aruba and Cisco WLC thin APs on supported firmware versions only)	Displays max and average percentages on this radio for busy, interfering receiving and transmitting signals. Special configuration on the controller is required to enable this data. Consult the *Aruba and AirWave Best Practices Guide* in **Home > Documentation** for details.
Goodput (Aruba and Cisco WLC thin APs on supported firmware versions only)	Displays the max and average goodput values. Goodput is the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes. The air time includes the retransmission time taken for both successful and dropped frames.

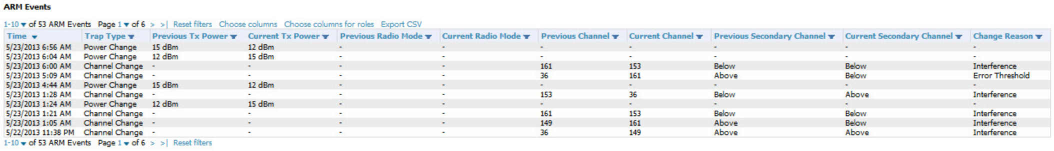
Figure 86 *Radio Statistics Interactive Graphs Illustration – Radio Power and Channel Utilization displayed*



Recent ARM Events Log

If this radio references an active and enabled ARM profile, and if your AMP is enabled as a trap host (see the *Aruba and AirWave Best Practices Guide* in **Home > Documentation** for instructions), ARM-initiated events such as automatic channel changes, power changes, and mode changes are displayed in the ARM Events table with the original and modified values; these values can be selected for filtering the results. You can export the table in CSV format. The columns and values are illustrated in Figure 87.

Figure 87 *ARM Events Table Illustration*



ARM Events

1-10 ▾ of 53 ARM Events Page 1 ▾ of 6 > >| Reset filters Choose columns Choose columns for roles Export CSV

Time ▾	Trap Type ▾	Previous Tx Power ▾	Current Tx Power ▾	Previous Radio Mode ▾	Current Radio Mode ▾	Previous Channel ▾	Current Channel ▾	Previous Secondary Channel ▾	Current Secondary Channel ▾	Change Reason ▾
5/23/2013 6:56 AM	Power Change	15 dBm	12 dBm	-	-	-	-	-	-	-
5/23/2013 6:04 AM	Power Change	12 dBm	15 dBm	-	-	-	-	-	-	-
5/23/2013 6:00 AM	Channel Change	-	-	-	-	161	153	Below	Below	Interference
5/23/2013 5:09 AM	Channel Change	-	-	-	-	36	161	Above	Below	Error Threshold
5/23/2013 4:44 AM	Power Change	15 dBm	12 dBm	-	-	-	-	-	-	-
5/23/2013 1:28 AM	Channel Change	-	-	-	-	153	36	Below	Above	Interference
5/23/2013 1:24 AM	Power Change	12 dBm	15 dBm	-	-	-	-	-	-	-
5/23/2013 1:21 AM	Channel Change	-	-	-	-	161	153	Below	Below	Interference
5/23/2013 1:05 AM	Channel Change	-	-	-	-	149	161	Above	Below	Interference
5/22/2013 11:38 PM	Channel Change	-	-	-	-	36	149	Above	Above	Interference

1-10 ▾ of 53 ARM Events Page 1 ▾ of 6 > >| Reset filters

The columns and values are described in Table 81.

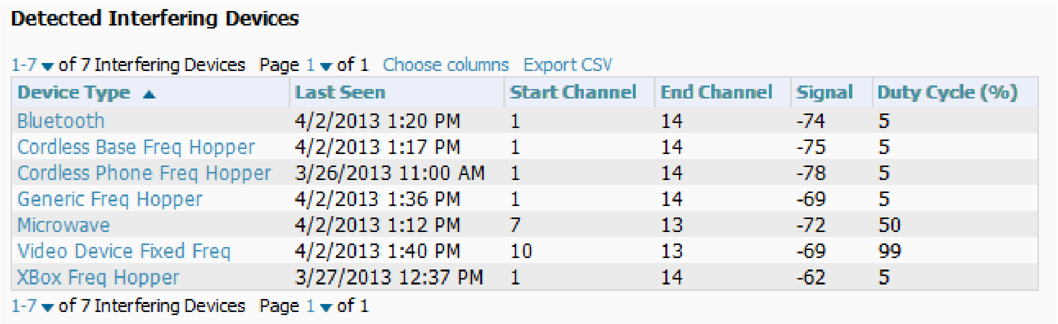
Table 81: *ARM Events table Columns and Values*

Column	Description
Time	The time of the ARM event.
Trap Type	The type of trap that delivered the change information. Current ARM trap types that display in AMP are: ● Power Change ● Mode Change ● Channel Change Values that display in the following columns depend on the Trap Type.
Previous Tx Power	Old value for transmit power before the Power Change event took place.
Current Tx Power	New transmit power value after the change.
Previous Radio Mode	Old value for radio mode before the Mode Change event took place.
Current Radio Mode	New radio mode value after the change.
Previous Channel	Old primary channel value before the Channel Change event took place.
Current Channel	New primary channel value after the change.
Previous Secondary Channel	Old secondary channel value (for 40Mhz channels on 802.11n devices) before the Channel Change event took place.
Current Secondary Channel	New secondary channel value after the change.
Change Reason	If the noise and interference cause for the change can be determined, they will be displayed here. Mode change reasons are not yet tracked.

Detected Interfering Devices Table

For Aruba APs running in Spectrum mode, the same non-802.11 interfering devices identified in the **Issues Summary** section are classified in the **Detected Interfering Devices** table along with the timestamp of its last detection, the start and end channels of the interference, the signal to noise ratio, and the percentage of time the interference takes place (duty cycle), as illustrated in Figure 88. This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

Figure 88 *Detected Interfering Devices Table Illustration*



Detected Interfering Devices

1-7 ▾ of 7 Interfering Devices Page 1 ▾ of 1 Choose columns Export CSV

Device Type ▲	Last Seen	Start Channel	End Channel	Signal	Duty Cycle (%)
Bluetooth	4/2/2013 1:20 PM	1	14	-74	5
Cordless Base Freq Hopper	4/2/2013 1:17 PM	1	14	-75	5
Cordless Phone Freq Hopper	3/26/2013 11:00 AM	1	14	-78	5
Generic Freq Hopper	4/2/2013 1:36 PM	1	14	-69	5
Microwave	4/2/2013 1:12 PM	7	13	-72	50
Video Device Fixed Freq	4/2/2013 1:40 PM	10	13	-69	99
XBox Freq Hopper	3/27/2013 12:37 PM	1	14	-62	5

1-7 ▾ of 7 Interfering Devices Page 1 ▾ of 1

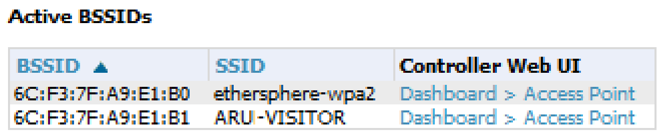
Possible device types for the **Detected Interfering Devices** table include:

- Audio Device Fixed Freq
- Bluetooth
- Cordless Base Freq Hopper
- Cordless Phone Fixed Freq
- Cordless Phone Freq Hopper
- Generic Fixed Freq
- Generic Freq Hopper
- Microwave
- Microwave Inverter
- Unknown
- Video Device Fixed Freq
- Wi-Fi
- XBox Freq Hopper

Active BSSIDs Table

The Active BSSIDs table maps the BSSIDs on a radio with the SSID it broadcasts to the network, as illustrated in Figure 89. This table appears only for Aruba AP radios.

Figure 89 ***Active BSSIDs*** *Table Illustration*



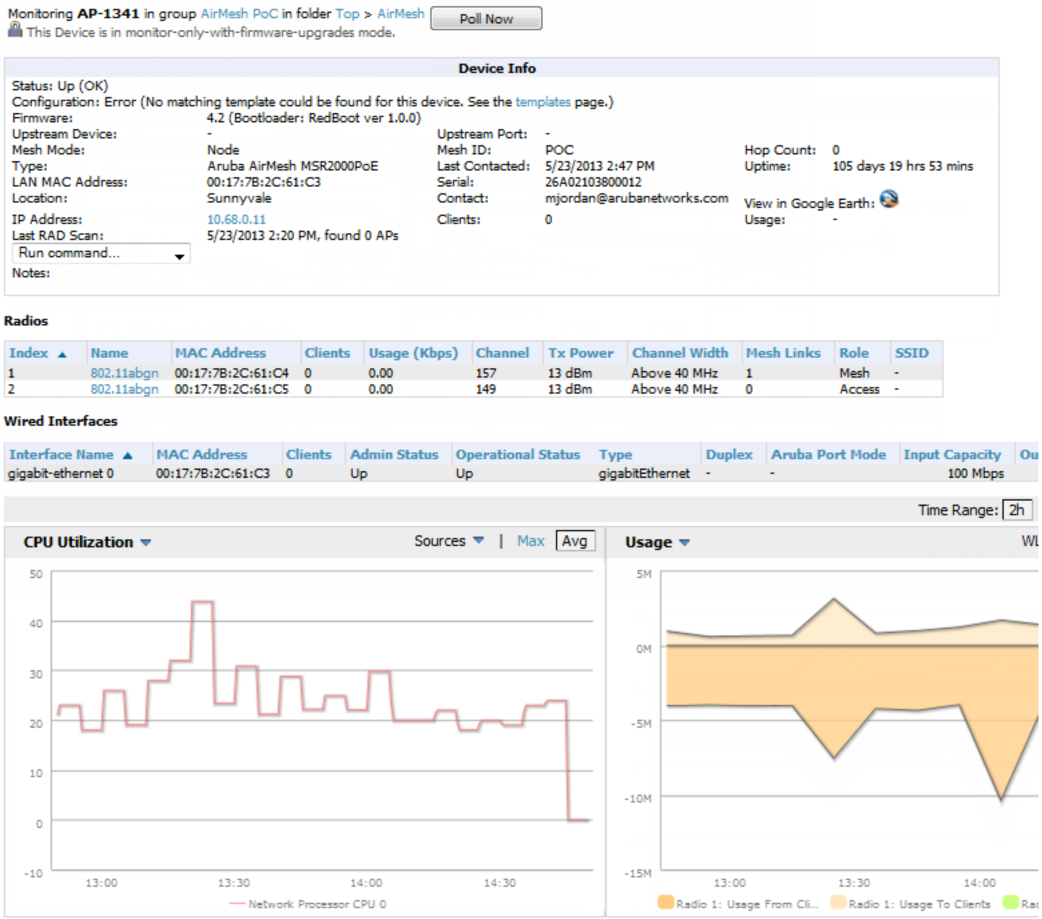
Active BSSIDs

BSSID ▲	SSID	Controller Web UI
6C:F3:7F:A9:E1:B0	ethersphere-wpa2	Dashboard > Access Point
6C:F3:7F:A9:E1:B1	ARU-VISITOR	Dashboard > Access Point

Monitoring Data for Mesh Devices

The monitoring page for mesh devices includes basic device information at the top, two tables for Radios and Wired Interfaces, and Clients, Usage, CPU Utilization, and Memory Utilization graphs. Under these graphs are a list of associated Clients, Mesh Links, RF Neighbors, and other common event logs and information.

Figure 90 *APs/Devices > Monitor page for a Mesh Device*



Monitoring **AP-1341** in group AirMesh PoC in folder Top > AirMesh Poll Now
This Device is in monitor-only-with-firmware-upgrades mode.

Device Info

Status: Up (OK)
Configuration: Error (No matching template could be found for this device. See the templates page.)

Firmware:	4.2 (Bootloader: RedBoot ver 1.0.0)				
Upstream Device:	-	Upstream Port:	-		
Mesh Mode:	Node	Mesh ID:	POC	Hop Count:	0
Type:	Aruba AirMesh MSR2000PoE	Last Contacted:	5/23/2013 2:47 PM	Uptime:	105 days 19 hrs 53 mins
LAN MAC Address:	00:17:7B:2C:61:C3	Serial:	26A02103800012		
Location:	Sunnyvale	Contact:	mjordan@arubanetworks.com	View in Google Earth:	
IP Address:	10.68.0.11	Clients:	0	Usage:	-
Last RAD Scan:	5/23/2013 2:20 PM, found 0 APs				

Run command...
Notes:

Radios

Index ▲	Name	MAC Address	Clients	Usage (Kbps)	Channel	Tx Power	Channel Width	Mesh Links	Role	SSID
1	802.11abgn	00:17:7B:2C:61:C4	0	0.00	157	13 dBm	Above 40 MHz	1	Mesh	-
2	802.11abgn	00:17:7B:2C:61:C5	0	0.00	149	13 dBm	Above 40 MHz	0	Access	-

Wired Interfaces

Interface Name ▲	MAC Address	Clients	Admin Status	Operational Status	Type	Duplex	Aruba Port Mode	Input Capacity	Ou
gigabit-ethernet 0	00:17:7B:2C:61:C3	0	Up	Up	gigabitEthernet	-	-	100 Mbps	

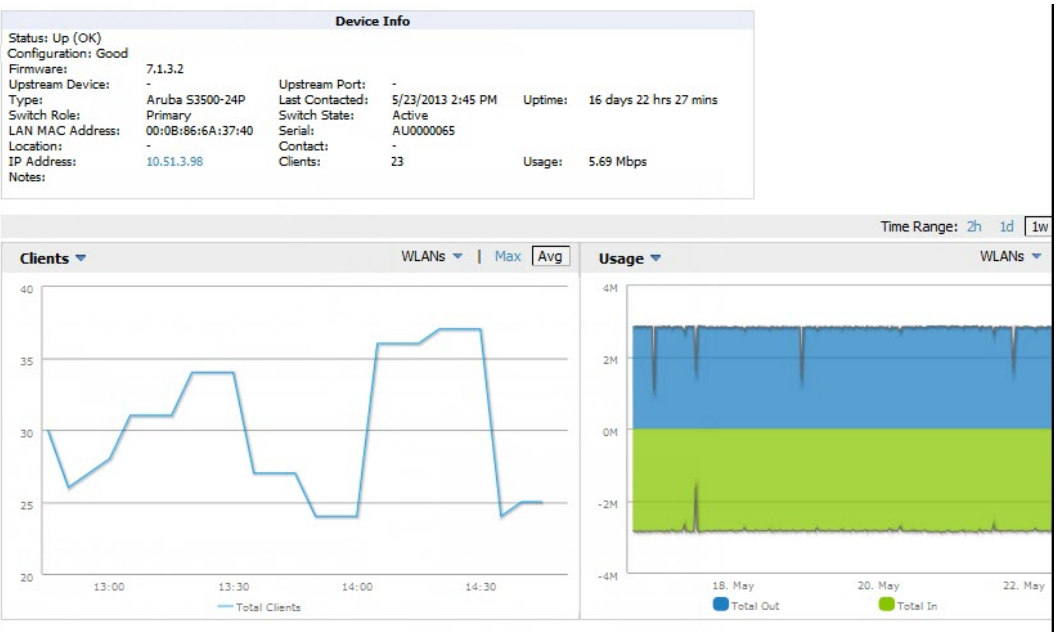
Time Range: 2h

These fields are described in detail in "Viewing Device Monitoring Statistics" on page 136.

Monitoring Data for Wired Devices (Routers and Switches)

The monitoring page for routers and switches includes basic device information at the top, a bandwidth graph depicting the sum of all the physical interfaces, and beneath that, CPU/Memory utilization graphs as shown in Figure 91.

Figure 91 *APs/Devices > Monitor Page for a Mobility Access Switch*



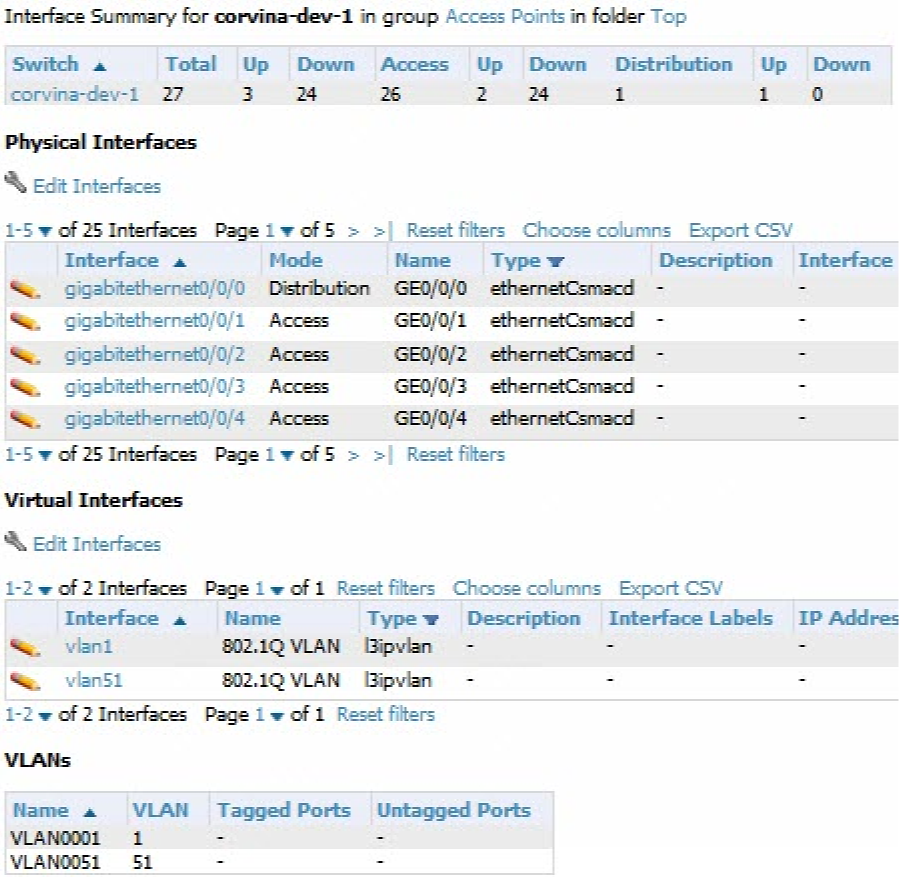
Device Info

Status: Up (OK)
Configuration: Good

Firmware:	7.1.3.2				
Upstream Device:	-	Upstream Port:	-		
Type:	Aruba S3500-24P	Last Contacted:	5/23/2013 2:45 PM	Uptime:	16 days 22 hrs 27 mins
Switch Role:	Primary	Switch State:	Active		
LAN MAC Address:	00:0B:86:6A:37:40	Serial:	AU0000065		
Location:	-	Contact:	-		
IP Address:	10.51.3.98	Clients:	23	Usage:	5.69 Mbps
Notes:					

All managed wired devices also include an **Interfaces** subtab, as shown in Figure 92.

Figure 92 *APs/Devices > Interfaces Page for Wired Devices (partial view)*



Interface Summary for **corvina-dev-1** in group Access Points in folder Top

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution	Up	Down
corvina-dev-1	27	3	24	26	2	24	1	1	0

Physical Interfaces

Edit Interfaces

1-5 ▾ of 25 Interfaces Page 1 ▾ of 5 > >| Reset filters Choose columns Export CSV

	Interface ▲	Mode	Name	Type ▾	Description	Interface
	gigabitethernet0/0/0	Distribution	GE0/0/0	ethernetCsmacd	-	-
	gigabitethernet0/0/1	Access	GE0/0/1	ethernetCsmacd	-	-
	gigabitethernet0/0/2	Access	GE0/0/2	ethernetCsmacd	-	-
	gigabitethernet0/0/3	Access	GE0/0/3	ethernetCsmacd	-	-
	gigabitethernet0/0/4	Access	GE0/0/4	ethernetCsmacd	-	-

1-5 ▾ of 25 Interfaces Page 1 ▾ of 5 > >| Reset filters

Virtual Interfaces

Edit Interfaces

1-2 ▾ of 2 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CSV

	Interface ▲	Name	Type ▾	Description	Interface Labels	IP Addres
	vlan1	802.1Q VLAN	l3ipvlan	-	-	-
	vlan51	802.1Q VLAN	l3ipvlan	-	-	-

1-2 ▾ of 2 Interfaces Page 1 ▾ of 1 Reset filters

VLANs

Name ▲	VLAN	Tagged Ports	Untagged Ports
VLAN0001	1	-	-
VLAN0051	51	-	-

The **Interfaces** page includes a summary of all the interfaces at the top. In case of the stacked switches, the master includes the interfaces of all the members including its own. The physical and the virtual interfaces are displayed in separate tables, labeled **Physical Interfaces** and **Virtual Interfaces**. VLANs are listed below the interface.

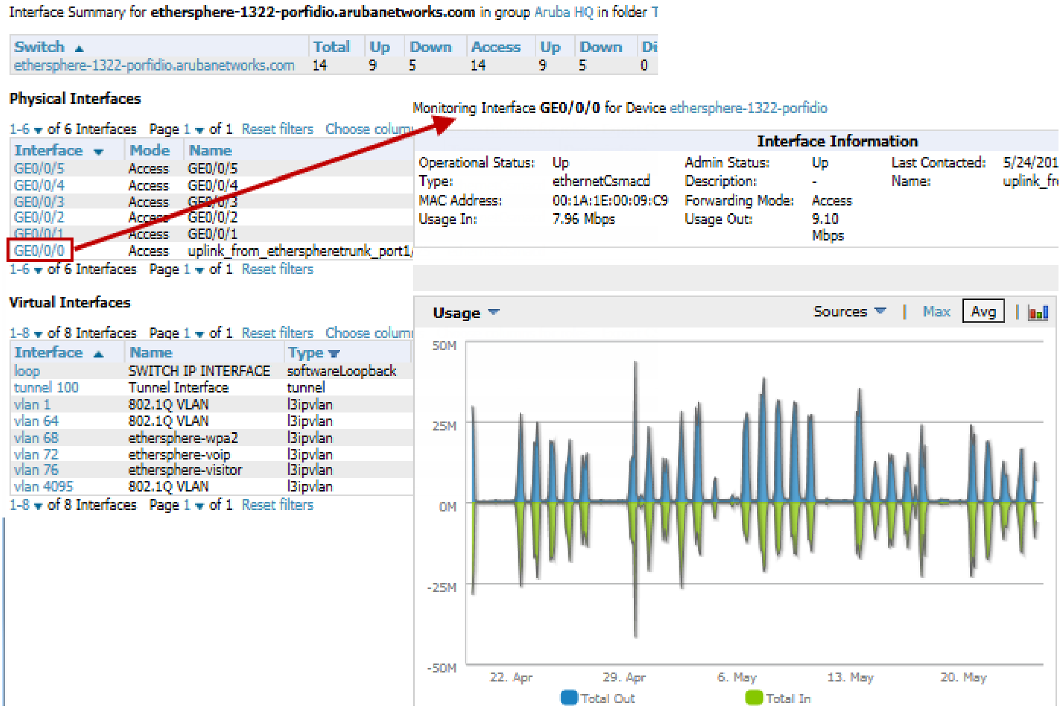
> NOTE
>
> The Interfaces page for AirMesh APs includes VLANs as part of the Virtual Interfaces. When no management interface is specified, VLAN1 will be treated as management interface. If VLAN1 does not exist, then ethernet 0 will be treated as the management interface

AMP monitors **Up/Down** status and bandwidth information on all interfaces. You can edit multiple interfaces concurrently by selecting one of the two **Edit Interfaces** hyperlinks. Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers.

Understanding the APs/Devices > Interfaces Page

"Monitoring Data for Wired Devices (Routers and Switches)" on page 151 showed you how to view high- level interface information for all physical and virtual interfaces on an entire router or switch. Select any interface hotlink in the **Interface** column of the Physical or Virtual Interfaces tables on the stacked switches to go to an **Interface Monitoring** page displaying data relevant to that specific interface, as shown Figure 93.

Figure 93 *Interface Monitoring Page for a Wired Device*



Interface Summary for **ethersphere-1322-porfidio.arubanetworks.com** in group Aruba HQ in folder T

Switch ▲	Total	Up	Down	Access	Up	Down	Di
ethersphere-1322-porfidio.arubanetworks.com	14	9	5	14	9	5	0

Physical Interfaces

1-6 ▾ of 6 Interfaces   Page 1 ▾ of 1   Reset filters   Choose colum

Interface ▾	Mode	Name
GE0/0/5	Access	GE0/0/5
GE0/0/4	Access	GE0/0/4
GE0/0/3	Access	GE0/0/3
GE0/0/2	Access	GE0/0/2
GE0/0/1	Access	GE0/0/1
GE0/0/0	Access	uplink_from_ethersphere trunk_port1/

1-6 ▾ of 6 Interfaces   Page 1 ▾ of 1   Reset filters

Virtual Interfaces

1-8 ▾ of 8 Interfaces   Page 1 ▾ of 1   Reset filters   Choose colum

Interface ▲	Name	Type ▾
loop	SWITCH IP INTERFACE	softwareLoopback
tunnel 100	Tunnel Interface	tunnel
vlan 1	802.1Q VLAN	l3ipvlan
vlan 64	802.1Q VLAN	l3ipvlan
vlan 68	ethersphere-wpa2	l3ipvlan
vlan 72	ethersphere-voip	l3ipvlan
vlan 76	ethersphere-visitor	l3ipvlan
vlan 4095	802.1Q VLAN	l3ipvlan

1-8 ▾ of 8 Interfaces   Page 1 ▾ of 1   Reset filters

Monitoring Interface **GE0/0/0** for Device ethersphere-1322-porfidio

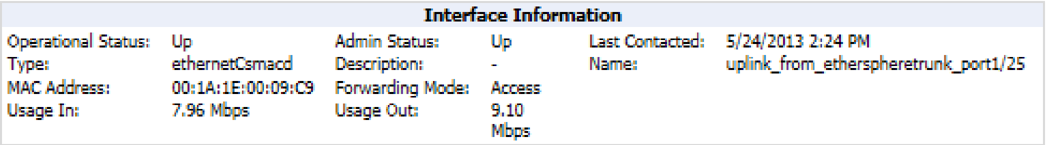
Interface Information

Operational Status:	Up	Admin Status:	Up	Last Contacted:	5/24/201
Type:	ethernetCsmacd	Description:	-	Name:	uplink_fr
MAC Address:	00:1A:1E:00:09:C9	Forwarding Mode:	Access		
Usage In:	7.96 Mbps	Usage Out:	9.10 Mbps		

An **Interface Monitoring** page is comprised of three sections: Interface Information, Usage and Interface Frame Counters graphs, and Connected Clients.

Specifics of the interface are in the Interface Information section, as depicted in Figure 94.

Figure 94 *Individual Interface Information Section*



Interface Information

Operational Status:	Up	Admin Status:	Up	Last Contacted:	5/24/2013 2:24 PM
Type:	ethernetCsmacd	Description:	-	Name:	uplink_from_ethersphere trunk_port1/25
MAC Address:	00:1A:1E:00:09:C9	Forwarding Mode:	Access		
Usage In:	7.96 Mbps	Usage Out:	9.10 Mbps		

Bandwidth, and various standard and enterprise specific error counting information is displayed in the lower section in a tabbed graph, which are shown in "Interface Monitoring Page for a Wired Device" on page 153 above.

Connected Clients, if any, are listed in a table below the interactive graphs.

What Next?

All device lists in AirWave act as portals to management pages if you have the proper read/write privileges. Selecting the wrench or pencil icon next to a device table entry, or selecting **Modify Devices** where appropriate above a device table, will take you to the appropriate Management page (**APs/Devices > Manage**). For more information, see "Configuring and Managing Devices" on page 156.

Auditing Device Configuration

When you have added a newly discovered device successfully to a Group in **Monitor** mode, the next step is to verify device configuration status. Determine whether any changes will be applied to that device when you convert it to **Managed read/write** mode.

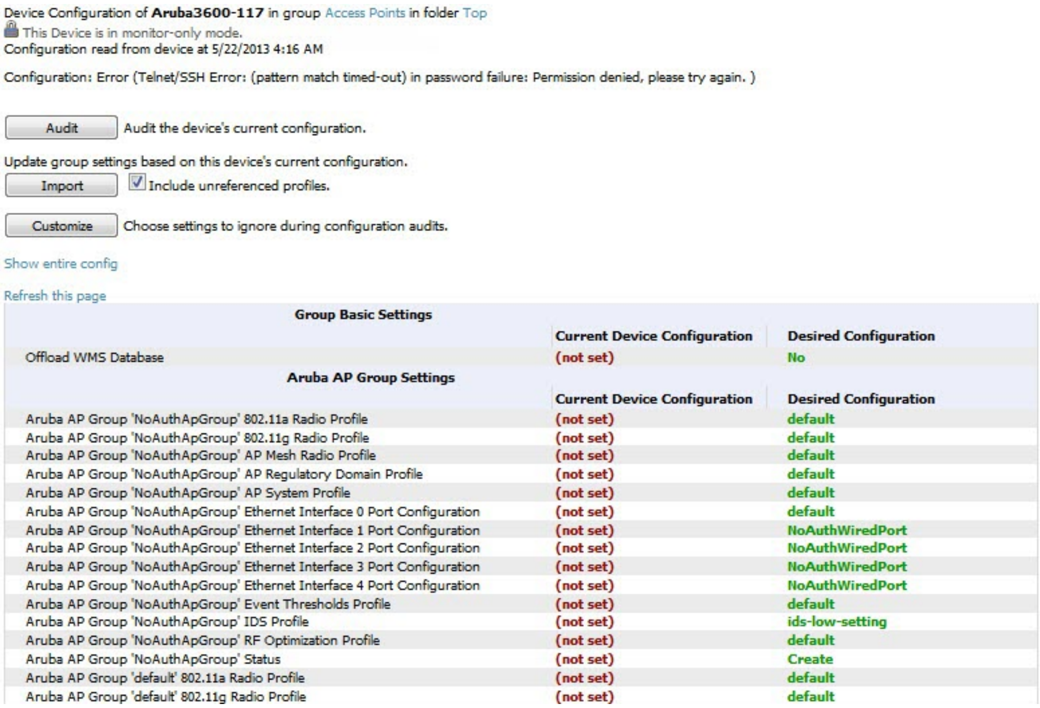
AMP uses SNMP or Telnet to read a device’s configuration. SNMP is used for Cisco controllers. Aruba devices and wired routers and switches use Telnet/SSH to read device configuration. See "Individual Device Support and Firmware Upgrades" on page 169 for more details.

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 AMP.
4. Verify the additional information in the **Configuration** column for that device.
    - A status of **Good** indicates that all of the device's current settings match the group policy settings and that no changes will be applied when the device is shifted to **Manage** mode.
    - A status of **Mismatched** indicates that at least one of the device's current configuration settings does not match the group policy and will be changed when the device is shifted to **Manage** mode.
5. If the device configuration is **Mismatched**, select the **Mismatched** link to go to the **APs/Devices > Audit** page. This page lists detailed information for all existing configuration parameters and settings for an individual device.

    The group configuration settings are displayed on the right side of the page. If the device is moved from **Monitor** to **Manage** mode, the settings on the right side of the page overwrite the settings on the left. "APs/Devices > Audit Page Illustration" on page 155 illustrates this page.

Figure 95 *APs/Devices > Audit Page Illustration*



Device Configuration of **Aruba3600-117** in group Access Points in folder Top
This Device is in monitor-only mode.
Configuration read from device at 5/22/2013 4:16 AM

Configuration: Error (Telnet/SSH Error: (pattern match timed-out) in password failure: Permission denied, please try again.)

Audit the device's current configuration.

Update group settings based on this device's current configuration.
☑ Include unreferenced profiles.

Choose settings to ignore during configuration audits.

Group Basic Settings		
	Current Device Configuration	Desired Configuration
Offload WMS Database	(not set)	No
Aruba AP Group Settings		
	Current Device Configuration	**Desired Configuration**
Aruba AP Group 'NoAuthApGroup' 802.11a Radio Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' 802.11g Radio Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' AP Mesh Radio Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' AP Regulatory Domain Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' AP System Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' Ethernet Interface 0 Port Configuration	(not set)	default
Aruba AP Group 'NoAuthApGroup' Ethernet Interface 1 Port Configuration	(not set)	NoAuthWiredPort
Aruba AP Group 'NoAuthApGroup' Ethernet Interface 2 Port Configuration	(not set)	NoAuthWiredPort
Aruba AP Group 'NoAuthApGroup' Ethernet Interface 3 Port Configuration	(not set)	NoAuthWiredPort
Aruba AP Group 'NoAuthApGroup' Ethernet Interface 4 Port Configuration	(not set)	NoAuthWiredPort
Aruba AP Group 'NoAuthApGroup' Event Thresholds Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' IDS Profile	(not set)	ids-low-setting
Aruba AP Group 'NoAuthApGroup' RF Optimization Profile	(not set)	default
Aruba AP Group 'NoAuthApGroup' Status	(not set)	Create
Aruba AP Group 'default' 802.11a Radio Profile	(not set)	default
Aruba AP Group 'default' 802.11g Radio Profile	(not set)	default

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** page include **List, Up, Down,** and **Mismatched** fields. These devices are arranged in groups called folders. Folders provide a logical organization of devices unrelated to the configuration groups of the devices. Using folders, you can quickly view basic statistics about devices. You *must* use folders if you want to limit the APs and devices AMP users can see.

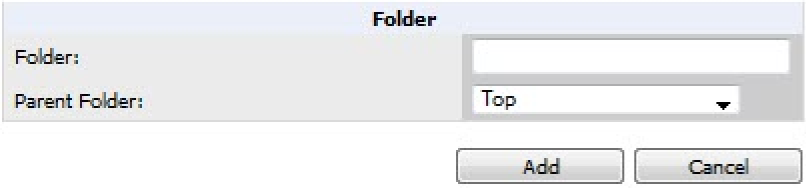
Folder views are persistent in AMP. If you select the **Top** folder and then select the **Down** link at the top of the page, you are taken to all of the down devices in the folder.

If you want to see every **down** device, select the **Expand folders to show all devices** link. When the folders are expanded, you see all of the devices on AMP that satisfy the criteria of the page. You also see an additional column that lists the folder containing the AP.

Perform the following steps to add a device folder to AMP.

1. To add a folder, select the **Add New Folder** link at the bottom of **APs/Devices > List**, **> Up**, **> Down**, or **> Mismatched** pages. Figure 96 illustrates the page.

Figure 96 *Folder Creation Page Illustration*



Folder	
Folder:	
Parent Folder:	Top

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

4. Select **Add**.

Once a new folder has been created, devices can be moved into it using the **Modify Devices** link or when **New Devices** are added into AMP.

Configuring and Managing Devices

This section contains the following topics describing individual device configuration within device groups:

- "Moving a Device from Monitor Only to Manage Read/Write Mode" on page 156
- "Configuring AP Settings" on page 157
- "Setting a Maintenance Window for a Device" on page 164
- "Configuring Device Interfaces for Switches" on page 165
- "Individual Device Support and Firmware Upgrades" on page 169

While most device configuration settings can be efficiently managed by AMP at a Group level, certain settings must be managed at the individual device level. For example, because devices within a Group are often contiguous with one another, and have overlapping coverage areas, it makes sense to manage these devices individually to avoid RF interference.

NOTE

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

AMP automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **APs/Devices > Audit** page and identified by name. By default, configuration is tracked by the date and time it was created; device configurations are also archived by date.

It is not possible to push archived configurations to devices, but archived configurations can be compared to the current configuration, the desired configuration, or to other archived configurations using the drop-down menus on the **APs/Devices > Audit** page. This applies to startup or to running configuration files.

Compare two configurations to highlight the specific lines that are mismatched. The Audit page provides links to AMP 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 in the *AirWave 7.7 Installation Guide*.

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.

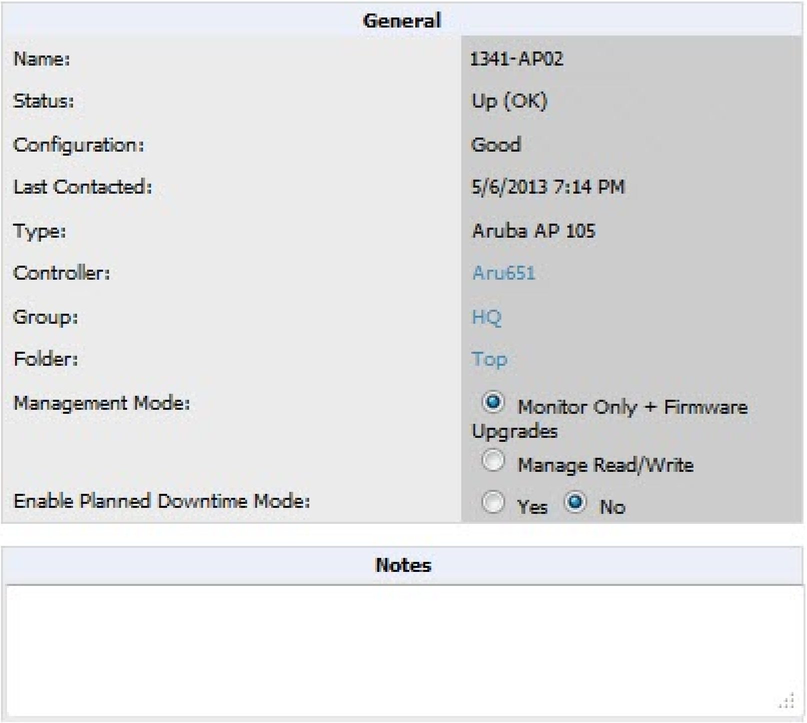
NOTE

When a device is in Manage mode, AMP will push a new configuration to the device in the event that the actual device configuration does not match the AMP configuration for that device.

To move a device from **Monitor Only** to **Manage Read/Write** mode, perform the following steps.

1. Go to the **APs/Devices > List** page and select the **wrench** icon next to the name of the AP to be shifted from **Monitor Only** mode to **Manage Read/Write** mode. This directs you to the **APs/Devices > Manage** page.
2. Locate the **General** area as shown in Figure 97.

Figure 97 *APs/Devices > Manage > General Section Illustration*



General	
Name:	1341-AP02
Status:	Up (OK)
Configuration:	Good
Last Contacted:	5/6/2013 7:14 PM
Type:	Aruba AP 105
Controller:	Aru651
Group:	HQ
Folder:	Top
Management Mode:	● Monitor Only + Firmware Upgrades ○ Manage Read/Write
Enable Planned Downtime Mode:	○ Yes ● No

Notes

3. Select **Manage Read/Write** on the **Management Mode** field.
4. Select **Save and Apply**, then **Confirm Edit** on the confirmation page to retain these settings and to push configuration to the device.
5. For device configuration changes that require the device to reboot, use the **Schedule** function to push the changes at a time when WLAN users will not be affected.
6. To move multiple devices into managed mode at once, use the **Modify Devices** link on an AP list page. For more information, refer to "Modifying Multiple Devices" on page 118.

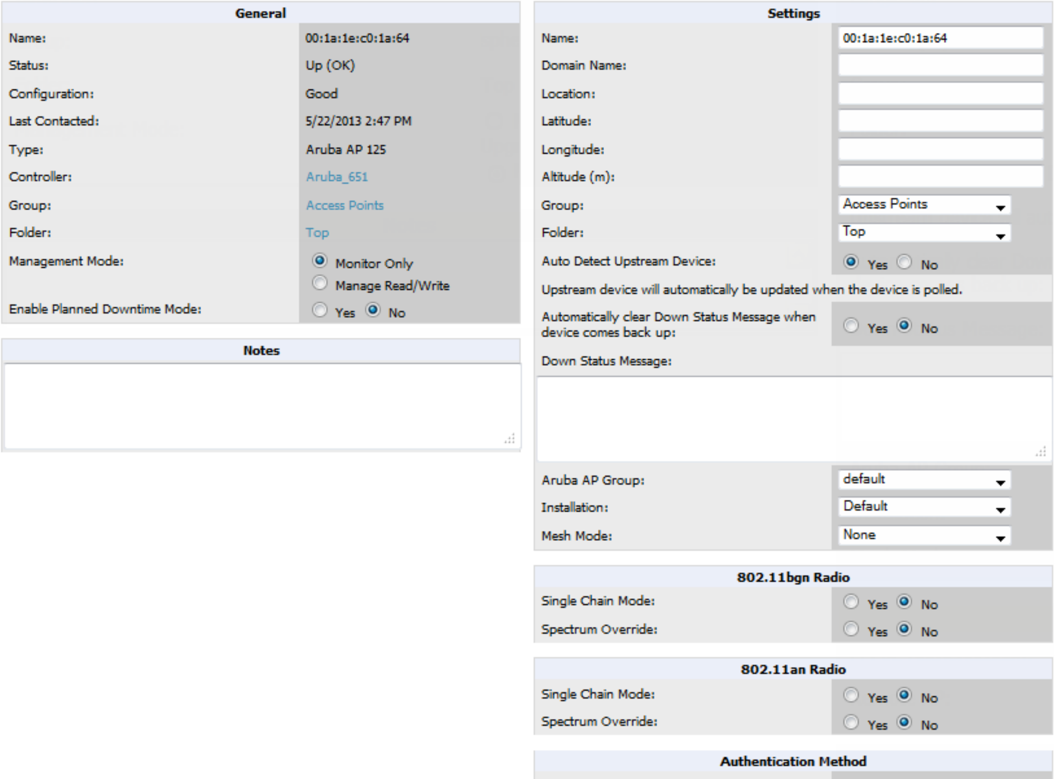
NOTE

Use the **Enable Planned Maintenance Mode** field in **APs/Devices > Manage > General** to put this device into planned maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page.

Configuring AP Settings

1. Browse to the **APs/Devices > List** page and select the wrench icon next to the device whose AP settings you want to edit. This directs you to the **Manage** page for that device. Figure 98 illustrates one example of this page. (Note that the page and fields vary based on the device type.)

Figure 98 *APs/Devices > Manage Page Illustration (partial view)*



General

Name:	00:1a:1e:c0:1a:64
Status:	Up (OK)
Configuration:	Good
Last Contacted:	5/22/2013 2:47 PM
Type:	Aruba AP 125
Controller:	Aruba_651
Group:	Access Points
Folder:	Top
Management Mode:	● Monitor Only ○ Manage Read/Write
Enable Planned Downtime Mode:	○ Yes ● No

Notes

Settings

Name:	00:1a:1e:c0:1a:64
Domain Name:	
Location:	
Latitude:	
Longitude:	
Altitude (m):	
Group:	Access Points
Folder:	Top
Auto Detect Upstream Device:	● Yes ○ No

Upstream device will automatically be updated when the device is polled.

Automatically clear Down Status Message when device comes back up:	○ Yes ● No
Down Status Message:	
Aruba AP Group:	default
Installation:	Default
Mesh Mode:	None

802.11bgn Radio

Single Chain Mode:	○ Yes ● No
Spectrum Override:	○ Yes ● No

802.11an Radio

Single Chain Mode:	○ Yes ● No
Spectrum Override:	○ Yes ● No

Authentication Method

If any changes are scheduled for this AP, they appear in a **Scheduled Changes** section at the top of the page above the other fields. The linked name of the job takes you to its **System** > **Configuration Change Job Detail** page.

2. Locate the **General** section for information about the AP's current status. Table 82 describes the fields, information, and settings.

Table 82: *APs/Devices > Manage > General Fields and Descriptions*

Field	Description
Name	Displays the name currently set on the device.
Status	Displays the current status of an AP. If an AP is **Up**, then AMP is able to ping it and fetch SNMP information from the AP. If the AP is listed **Down** then AMP 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, select **Audit** on the **APs/Devices > Audit** page.
Last Contacted	Displays the last time AMP successfully contacted the AP.
Type	Displays the type of AP.
Controller	Links to the controller that is monitoring this device. **NOTE:** This field is visible for APs.
Firmware	Shows the device firmware version. **NOTE:** This field is visible for controllers and switches.

Table 82: *APs/Devices > Manage > General Fields and Descriptions (Continued)*

Field	Description
Group	Links to the **Group > Monitoring** page for the AP.
Template	Displays the name of the group template currently configuring the AP. This also displays a link to the **Groups > Template** page. **NOTE:** This field is only visible for APs that are managed by 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. AMP pushes configurations and makes changes to an AP when it is in **Manage Read/Write** mode.
Enable Planned Maintenance Mode	Put this device into planned maintenance. During the maintenance mode, no AP Down triggers will be deployed on these devices. Users will not be able to delete folders that contain devices in Planned Maintenance. The devices in Planned Maintenance will show the Up status, but will not be tracked in historical graphs and logs as Up. You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page.
Notes	Provides a free-form text field to describe device information.

3. Review and provide the following information in the **Settings** area. Devices with dual radios display radio-specific settings in the Slot A and Slot B area. If a device is dual-radio capable but only has one device installed, AMP manages that device as if it were a single slot device.

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 83 describes field settings, default values, and information for the **Settings** section of this page.

Table 83: *APs/Devices > Manage > Settings Fields and Default Values*

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain Name	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.
Mesh ID	None	Mesh	Text field for entering the Mesh ID.
Timezone	None	Instant	Drop-down menu for specifying the controller timezone.

Table 83: *APs/Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
Syslog Server	None	Instant	Text field for specifying the a syslog server for the controller.
RADIUS Server	None	Instant	Text field for specifying the a RADIUS server for the controller.
RF Band Selection	All	Instant	Drop-down menu for specifying the RF Band on the controller.
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.
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.
Automatically clear Down Status Message when device comes back up	None	All	Whether the message entered in the **Down Status Message** field should be removed after the device returns to the Up status.
Down Status Message	None	All	Enter a text message that provides information to be conveyed if the device goes down.
Organization	Read from Device	Instant	The Organization string of the IAP.
Aruba AP Group	default	All	Specifies the Aruba AP Group in which this devices resides.

Table 83: *APs/Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
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: ● Local ● H-REAP ● Monitor ● Rogue Detector ● Sniffer

4. Complete additional settings on the **APs/Devices** > **Manage** page, to include H-REAP, certificates, radio settings, and network settings. Table 84 describes many of the possible fields.

NOTE

For complete listing and discussion of settings applicable only to *Aruba* devices, see the Aruba *Device Configuration Guide.*

Table 84: *Additional Settings*

Setting	Default	Device Type	Description
Mesh Mode	Mesh AP	Mesh Devices	Drop-down menu specifies the mesh role for the AP as shown: ● **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. ● **Remote Portal AP** –The AP will become a remote portal AP. It will use a wireless 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 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.
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 receive and transmit.

Table 84: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
			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	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.
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage radius of the access point by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the AP will interfere with neighboring APs. Supported values are: **Cisco (100mW, 50mW, 30mW, 20mW, 5mW, 1mW) Symbol (Full or 50mW, 30mW, 15mW, 5mW, 1mW)**

Table 84: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
Radio Enabled	Yes	All	The Radio Enabled option allows you to disable the radio's ability to transmit or receive data while still maintaining Ethernet connectivity to the network. AMP will still monitor the Ethernet page and ensure the AP stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at an AP level or Group level. **NOTE:** You cannot disable radios unless rogue scanning is disabled in **Groups > Radio**.
Use DHCP	Yes	All	If enabled, the AP will be assigned a new IP address using DHCP. If disabled, the AP will use a static IP address. For improved security and manageability, disable DHCP and using static IP addresses.
LAN IP	None	All	The IP Address of the AP Ethernet interface. If One-to-One NAT is enabled, AMP will communicate with the AP on a different address (the IP Address defined in the **Device Communication** section). If DHCP is enabled, the current assigned address will appear grayed out and the field cannot be updated in this area.
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 **Template Options** area on the **APs/Devices** > **Manage** page.

NOTE

This section only appears for IOS APs, Symbol devices, and Aruba controllers in groups with Aruba GUI Config disabled.

Table 85 describes field settings, default values, and additional information for this page.

Table 85: *APs/Devices > Manage > Template Options Fields and Default Values*

Setting	Default	Device Type	Description
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.

Table 85: *APs/Devices > Manage > Template Options Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
SSL Certificate	None	Cisco IOS	AMP will read the SSL Certificate off of the AP when it comes UP in AMP. The information in this field will defines what will be used in place of %certificate%.
Extra Device 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 Catalyst switches	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.

6. For Cisco WLC devices, go to the interfaces section of the **APs/Devices** > **Manage** page. Select **Add new Interface** to add another controller interface, or select the **pencil** icon to edit an existing controller interface. Table 86 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by AMP, refer to the Cisco WLC product documentation.

Table 86: *APs/Devices > Manage > Interface Fields and Descriptions for Cisco WLC Devices*

Field	Default	Description
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 VLAN ID	Disabled	Enabled indicates it is a quarantine VLAN; used only for H-REAP-associated clients.
Dynamic Device Management	Enabled	When enabled, makes the interface an AP-manager interface. Cisco calls this feature Dynamic AP Management.

Setting a Maintenance Window for a Device

AMP can automate the manual action of putting multiple devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode.

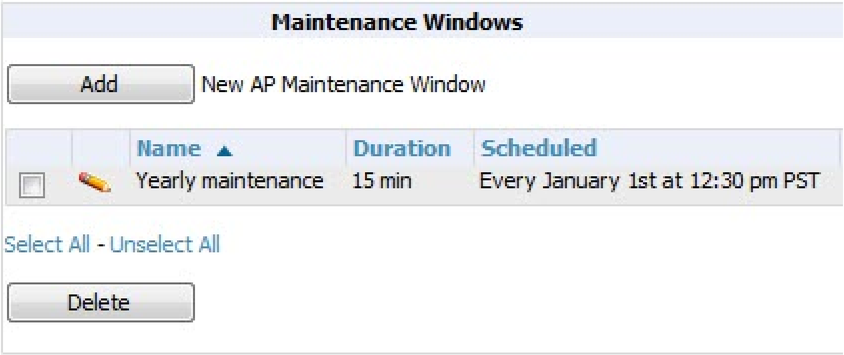
Maintenance windows can be set as a one-time or recurring event on the **APs/Devices > Manage** and **Groups > Basic** pages. You can also use the **Modify Devices** link to add or delete maintenance windows to or from multiple selected devices at once. Additionally, this feature can be used on the Master Console to set maintenance windows for multiple AMPs.

> NOTE
>
> When a maintenance window is configured, AMP automatically moves the devices into Manage mode so that the changes can be applied. After the maintenance period is over, the devices automatically revert to Monitor-Only mode.

To set a maintenance window for a single device, follow these steps:

1. Select a device and navigate to the **APs/Devices > Manage** page for a device.
2. At the bottom of the page, locate the Maintenance Windows section.
3. Click the **Add New AP Maintenance Window** button.

Figure 99 *Add New Maintenance Window in APs/Devices > Manage page*



Maintenance Windows

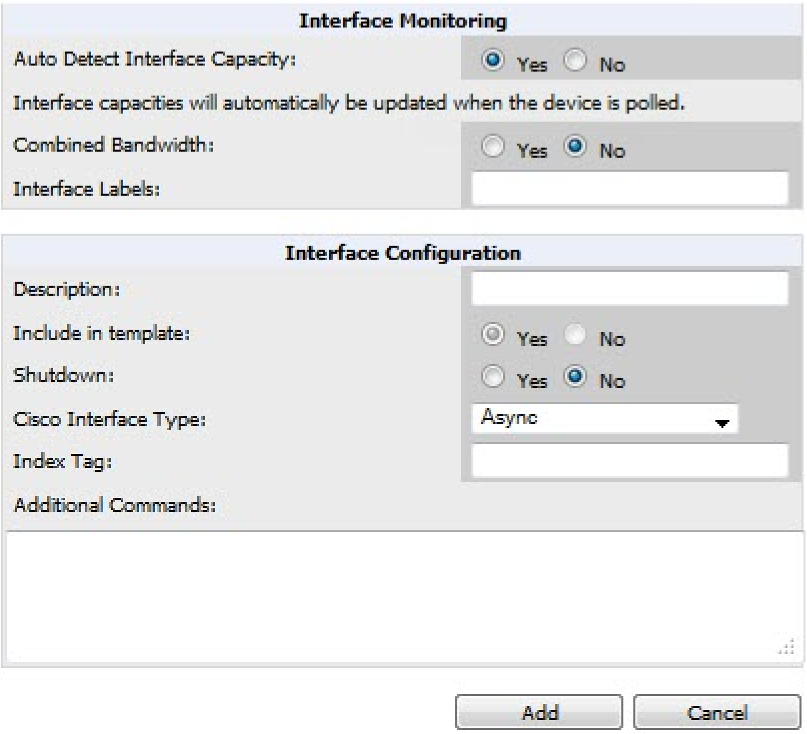
		Name ▲	Duration	Scheduled
☐	✎	Yearly maintenance	15 min	Every January 1st at 12:30 pm PST

4. Enter a name for the maintenance window.
5. In the **Occurs** field, specify whether the maintenance window should occur one time, or daily, weekly, monthly, or annually. Additional options may display based on the selected value. For example, if you select monthly, the you will be prompted to specify the day of the month for the recurrence.
6. Set the desired start time and the duration (in minutes) of the maintenance window.
7. Click the **Add** button.

Configuring Device Interfaces for Switches

When you go to the **APs/Devices > Interfaces** page for a switch, you can add a Virtual interface by selecting **Add** and entering the appropriate information in the page that appears, as shown in Figure 100.

Figure 100 *Add Virtual Interfaces Page for Wired Devices*



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:

Interface Configuration

Description:

Include in template: ○ Yes ○ No

Shutdown: ○ Yes ● No

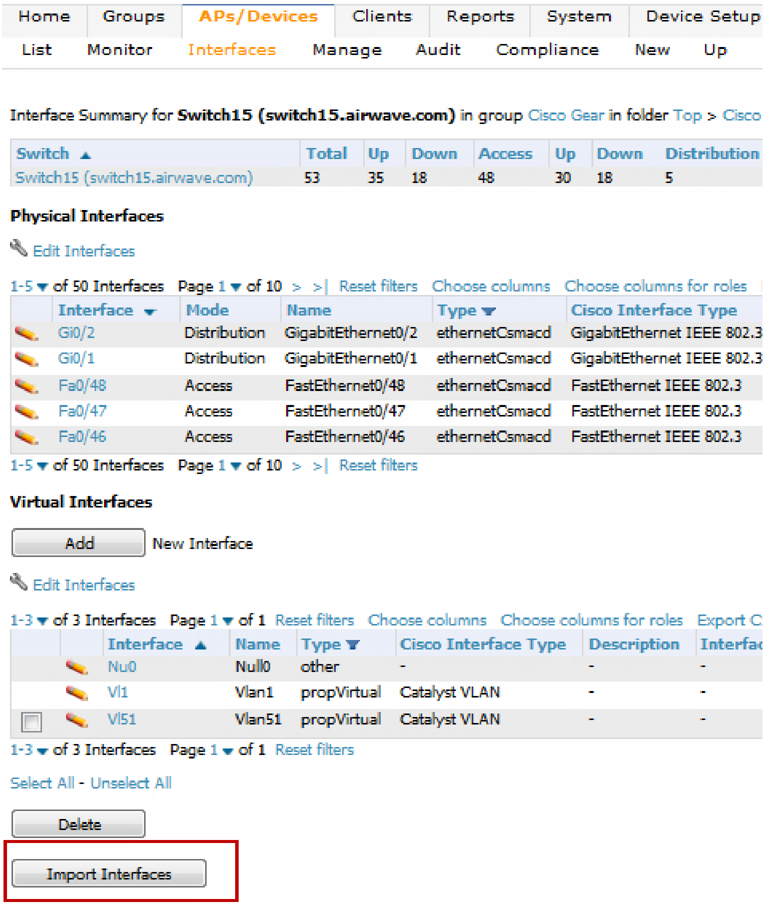
Cisco Interface Type: Async

Index Tag:

Additional Commands:

New physical and virtual interfaces are discovered using SNMP polling as described in "SNMP/HTTP Scanning" on page 124. To refresh and reload all current interface information from a device, select **Import Interfaces** on the bottom of the page as shown in Figure 101.

Figure 101 *Import Interfaces for Refresh and Reload (lower portion of page)*



Interface Summary for **Switch15 (switch15.airwave.com)** in group Cisco Gear in folder Top > Cisco

Switch ▲	Total	Up	Down	Access	Up	Down	Distribution
Switch15 (switch15.airwave.com)	53	35	18	48	30	18	5

Physical Interfaces

Edit Interfaces

1-5 ▾ of 50 Interfaces Page 1 ▾ of 10 > >| Reset filters Choose columns Choose columns for roles

	Interface ▾	Mode	Name	Type ▾	Cisco Interface Type
✎	Gi0/2	Distribution	GigabitEthernet0/2	ethernetCsmacd	GigabitEthernet IEEE 802.3
✎	Gi0/1	Distribution	GigabitEthernet0/1	ethernetCsmacd	GigabitEthernet IEEE 802.3
✎	Fa0/48	Access	FastEthernet0/48	ethernetCsmacd	FastEthernet IEEE 802.3
✎	Fa0/47	Access	FastEthernet0/47	ethernetCsmacd	FastEthernet IEEE 802.3
✎	Fa0/46	Access	FastEthernet0/46	ethernetCsmacd	FastEthernet IEEE 802.3

1-5 ▾ of 50 Interfaces Page 1 ▾ of 10 > >| Reset filters

Virtual Interfaces

Add New Interface

Edit Interfaces

1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Choose columns for roles Export C

		Interface ▲	Name	Type ▾	Cisco Interface Type	Description	Interfac
	✎	Nu0	Null0	other	-	-	-
	✎	Vl1	Vlan1	propVirtual	Catalyst VLAN	-	-
□	✎	Vl51	Vlan51	propVirtual	Catalyst VLAN	-	-

1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters

Select All - Unselect All

Delete

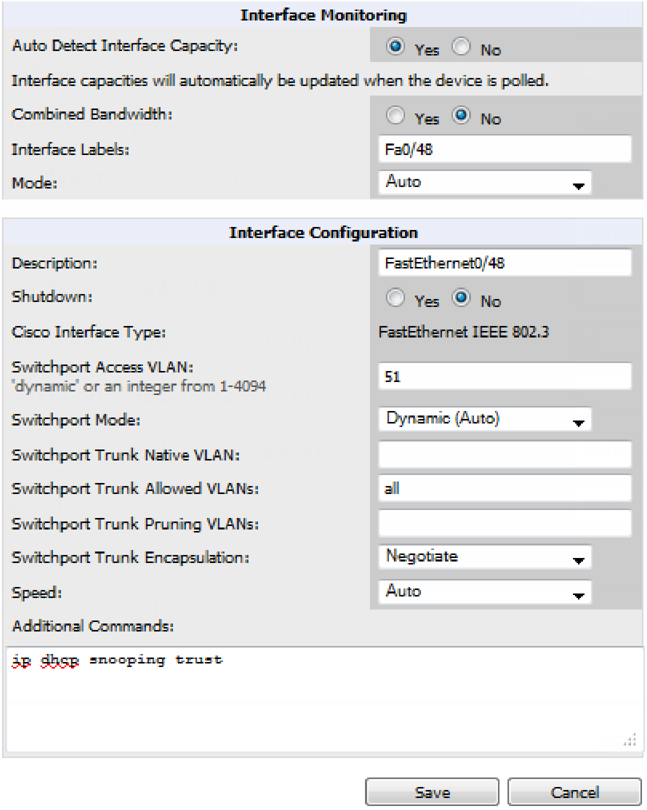
Import Interfaces

You can view details for each interface on a wired device from its individual interface page as well. For details, see "Understanding the APs/Devices > Interfaces Page" on page 153.

You can configure interface settings individually or in groups. For individual settings, select the pencil icon next the interface name in **AP/Devices > Interfaces**.

This takes you to the **Interfaces Monitoring and Configuration** window which has a slightly different appearance depending on whether you are configuring a physical or virtual interface, as shown in Figure 102 and Figure 103.

Figure 102 *Physical Interfaces Monitoring and Configuration Sections*



Interface Monitoring

Auto Detect Interface Capacity:	● Yes ○ No
Interface capacities will automatically be updated when the device is polled.	
Combined Bandwidth:	○ Yes ● No
Interface Labels:	Fa0/48
Mode:	Auto

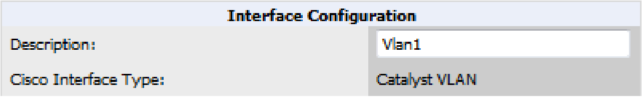
Interface Configuration

Description:	FastEthernet0/48
Shutdown:	○ Yes ● No
Cisco Interface Type:	FastEthernet IEEE 802.3
Switchport Access VLAN: 'dynamic' or an integer from 1-4094	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
```

Figure 103 *Virtual Individual Interfaces Configuration Section*

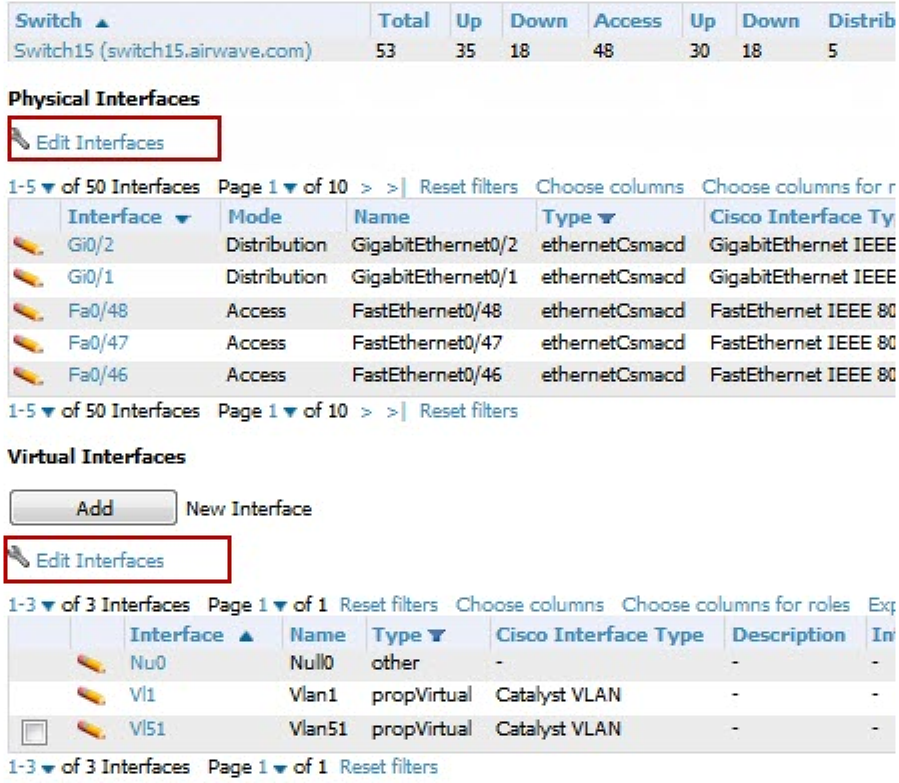


Interface Configuration

Description:	Vlan1
Cisco Interface Type:	Catalyst VLAN

To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 104.

Figure 104 *Edit Multiple Interfaces*



Switch ▲	Total	Up	Down	Access	Up	Down	Distrib
Switch15 (switch15.airwave.com)	53	35	18	48	30	18	5

Physical Interfaces

Edit Interfaces

1-5 ▾ of 50 Interfaces Page 1 ▾ of 10 > >| Reset filters Choose columns Choose columns for r

	Interface ▾	Mode	Name	Type ▾	Cisco Interface Ty
✎	Gi0/2	Distribution	GigabitEthernet0/2	ethernetCsmacd	GigabitEthernet IEEE
✎	Gi0/1	Distribution	GigabitEthernet0/1	ethernetCsmacd	GigabitEthernet IEEE
✎	Fa0/48	Access	FastEthernet0/48	ethernetCsmacd	FastEthernet IEEE 80
✎	Fa0/47	Access	FastEthernet0/47	ethernetCsmacd	FastEthernet IEEE 80
✎	Fa0/46	Access	FastEthernet0/46	ethernetCsmacd	FastEthernet IEEE 80

1-5 ▾ of 50 Interfaces Page 1 ▾ of 10 > >| Reset filters

Virtual Interfaces

Add New Interface

Edit Interfaces

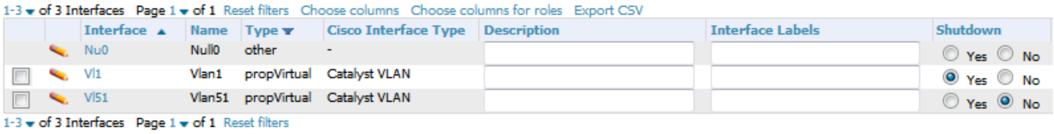
1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Choose columns for roles Exp

		Interface ▲	Name	Type ▾	Cisco Interface Type	Description	In
	✎	Nu0	Null0	other	-	-	-
	✎	Vl1	Vlan1	propVirtual	Catalyst VLAN	-	-
☐	✎	Vl51	Vlan51	propVirtual	Catalyst VLAN	-	-

1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters

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 105.

Figure 105 *Multiple Interface Editing Page Illustration*



1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Choose columns for roles Export CSV

		Interface ▲	Name	Type ▾	Cisco Interface Type	Description	Interface Labels	Shutdown
	✎	Nu0	Null0	other	-			○ Yes ○ No
☐	✎	Vl1	Vlan1	propVirtual	Catalyst VLAN			● Yes ○ No
☐	✎	Vl51	Vlan51	propVirtual	Catalyst VLAN			○ Yes ● No

1-3 ▾ of 3 Interfaces Page 1 ▾ of 1 Reset filters

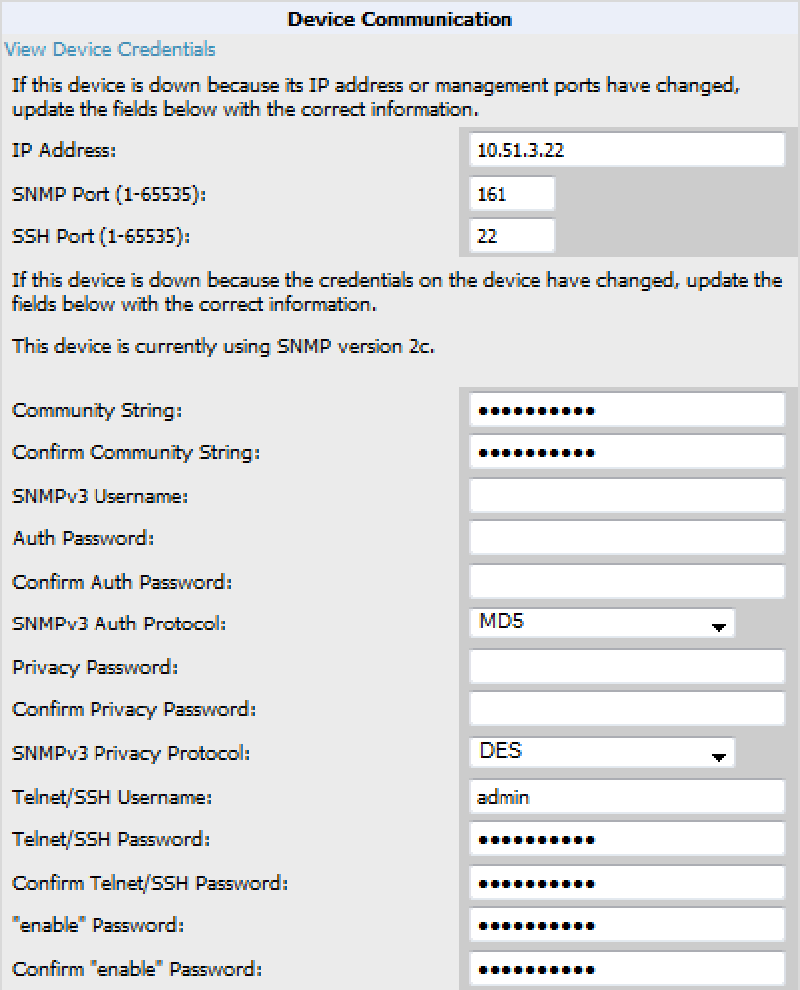
AMP assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on templates, see "Creating and Using Templates" on page 178.

Individual Device Support and Firmware Upgrades

Perform the following steps to configure AP communication settings for individual Aruba controllers.

1. Locate the **Device Communication** area on the **APs/Devices > Manage** page.
2. Specify the credentials to be used to manage the AP. Figure 106 illustrates this page.

Figure 106 *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:	10.51.3.22
SNMP Port (1-65535):	161
SSH Port (1-65535):	22

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 2c.

Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
SNMPv3 Auth Protocol:	MD5
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••

NOTE

The **Device Communication** area may appear slightly different depending on the particular vendor and model of the APs being used.

3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. You can disable the **View Device Credentials** link in AMP if you are the root user. Contact Aruba support for detailed instructions to disable the link.
5. (Optional.) Enter the appropriate SSH and Telnet credentials if you are configuring Dell, Aruba Networks, Alcatel-Lucent or any Cisco device except Cisco WLAN controllers.
6. Select **Apply**, then **Confirm Edit** to apply the changes to the AP immediately, **Schedule** to schedule the changes during a specific time, or **Cancel** to return to **APs/Devices > Manage**.

NOTE

Some AP configuration changes may require the AP to be rebooted. Use the **Schedule** function to schedule these changes to occur at a time when WLAN users will not be affected.

Click the **Update Firmware** button at the bottom right of the page to upgrade the device's firmware. This button is not available if your device is in Monitor Only mode.

NOTE

The **Update Firmware** button only appears if 1) the AMP Administrator has enabled **Allow firmware upgrades in monitor-**

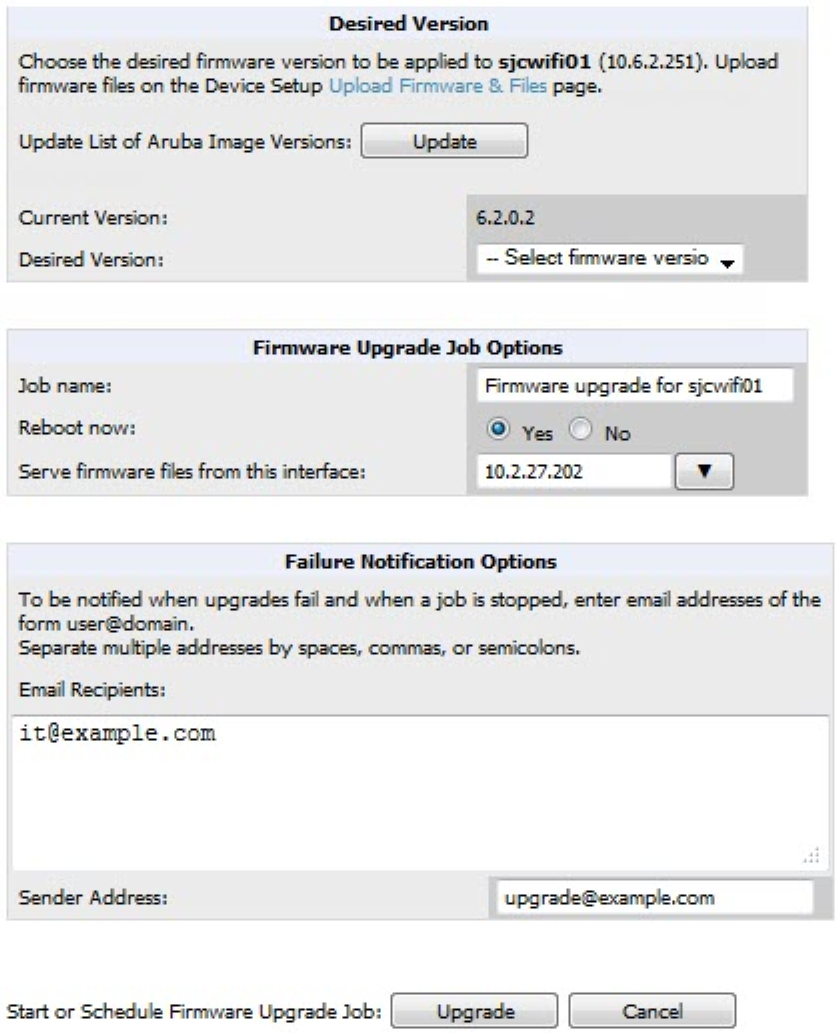
only mode in **AMP Setup > General** or 2) if you are looking at an **APs/Devices > Manage** page for a controller or autonomous AP that supports firmware upgrades in AMP. See the Supported Infrastructure Devices document on the **Home > Documentation** page for a list of the AMP-supported devices that can perform firmware upgrades. In most cases, you cannot upgrade firmware directly on thin APs.

Figure 107 illustrates the page that opens and Table 87 describes the settings and default values.

Table 87: *APs/Devices > Manage > Update Firmware Fields and Default Values*

Setting	Default	Description
Desired Version	None	Specifies the firmware to be used in the upgrade. Firmware can be added to this drop-down menu on the **Device Setup > Upload Firmware & Files** page.
Job Name	None	Sets a user-defined name for the upgrade job. Use 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.

Figure 107 *APs/Devices > Manage Firmware Upgrades*



Desired Version

Choose the desired firmware version to be applied to **sjcwifi01** (10.6.2.251). Upload firmware files on the Device Setup Upload Firmware & Files page.

Update List of Aruba Image Versions: Update

Current Version:	6.2.0.2
Desired Version:	-- Select firmware versio

Firmware Upgrade Job Options

Job name:	Firmware upgrade for sjcwifi01
Reboot now:	● Yes ○ No
Serve firmware files from this interface:	10.2.27.202

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:

it@example.com

Sender Address: upgrade@example.com

Start or Schedule Firmware Upgrade Job: Upgrade Cancel

Initiating a firmware upgrade will change the **Firmware Status** column for the device to Pending in **APs/Devices** > **List**. You can review the status of all recent firmware upgrade jobs in **System** > **Firmware Upgrade Jobs**.

Troubleshooting a Newly Discovered Down Device

If the device status on the **APs/Devices** > **List** page remains **Down** after it has been added to a group, the most likely source of the problem is an error in the SNMP community string being used to manage the device. Perform the following steps to troubleshoot this scenario.

1. Select the **Name** of the down device in the list of devices on the **APs/Devices** > **List** or **APs/Devices** > **Down** page. This automatically directs you to the **APs/Device** > **Monitor** page for that device.
2. Locate the **Status** field in the **Device Info** section. If the Status is **Down**, it includes a description of the cause of the problem. Some of the common system messages are as follows in Table 88:

Table 88: *Common System Messages for Down Status*

Message	Meaning
AP is no longer	This means the AP no longer shows up in any controller's AP list (on the AMP server).

Table 88: *Common System Messages for Down Status (Continued)*

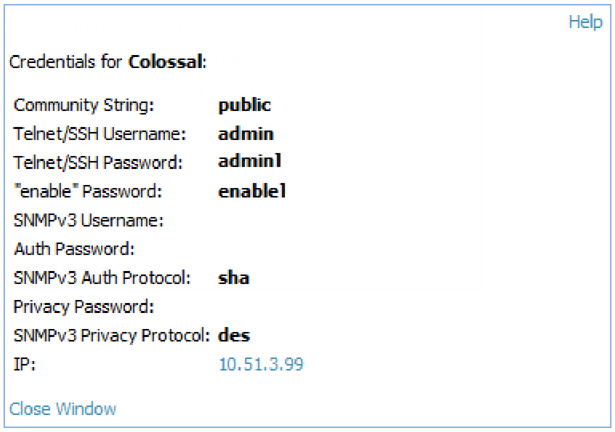
Message	Meaning
associated with controller	Either the AP was removed from the controller, or it has roamed to another controller that AMP does not have visibility to, or it is offline.
Controller is Down	When a controller goes down, AMP automatically marks all associated thin APs down This is because communication to thin APs are via the controller, and AMP assumes that if the Controller has gone offline, then all associated APs are down as well until they are reassociated with another Controller).
Downloading	The AP is in the process of downloading firmware or configuration. (This only applies to Cisco WLC thin APs and some Symbol APs.)
Error fetching existing configuration	AMP could not fetch a config for the AP. Usually this is because AMP has incorrect credentials and was not able to log in.
ICMP Ping Failed (after SNMP Get Failed)	The device is not responding and is likely offline.
SNMP Get Failed	SNMP credentials and/or configuration may be incorrect. Verify that SNMP is enabled and that credentials and access ports are configured correctly on both the target device and in AMP.
SNMP Trap	AMP received an SNMP trap from the controller indicating that the AP is no longer associated to the controller.
Telnet Error: command timed out	Telnet/SSH username and password specified for that device is incorrect.
Unexpected LAN MAC Address found at this device's IP address	If AMP detects that the LAN MAC address of a device has changed this error message will appear. This usually indicates that a physical hardware change has occurred (while reusing the same IP Address) without using the **Replace Hardware** feature in AMP. This error may also indicate an IP address conflict between two or more devices. When an unexpected LAN MAC address is seen in a device's IP address, its **APs/Devices > Manage** page displays the message Click **Replace Hardware** (preferred) or **Reset MAC Address** to reset the LAN MAC address if this device has been replaced with new hardware at the top of the page. Use the **Replace Hardware** button at the bottom of that page in order to avoid this message.

NOTE

To view the detailed status of all your down devices at once, navigate to **APs/Devices > Down** (try the **Down** top header stats link) and look at the **Detailed Status** column for the list of down devices. This column can be sorted using the **Filter** icon (▼).

3. If the **SNMP Get Failed** message appears, select the **APs/Devices > Manage** tab to go to the management page for that device.
4. If visible, select the **View Device Credentials** link in the **Device Communications** section of **APs/Devices > Manage**. This displays the credentials AMP is using unsuccessfully to communicate with the device. This link can be removed from AMP for security reasons by setting a flag in AMP. Only users with root access to the AMP command line can show or hide this link. To disable this feature, please contact Aruba support. Figure 108 illustrates this page.

Figure 108 *View Device Credentials Window*



Help

Credentials for **Colossal**:

Community String:	**public**
Telnet/SSH Username:	**admin**
Telnet/SSH Password:	**admin1**
"enable" Password:	**enable1**
SNMPv3 Username:	
Auth Password:	
SNMPv3 Auth Protocol:	**sha**
Privacy Password:	
SNMPv3 Privacy Protocol:	**des**
IP:	10.51.3.99

Close Window

NOTE

The **View Device Credentials** message may appear slightly different depending on the vendor and model.

5. If the credentials are incorrect, return to the **Device Communications** area on the **APs/Devices > Manage** page. Enter the appropriate credentials, and select **Apply**.
6. Return to the **APs/Devices > List** page to see if the device appears with a Status of **Up**.

Using AMP to Set up Spectrum Analysis

The spectrum analysis software modules on Aruba AP models AP-105, RAP-5WN, the AP-12x series, the AP-13x series, and the AP-9x series can examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources.

The spectrum analyzer is used in conjunction with Aruba's Adaptive Radio Management (ARM) technology. While the spectrum analyzer identifies and classifies Wi-Fi and non-Wi-Fi sources of interference, ARM automatically ensures that APs serving clients will stay clear of interference.

Individual APs or groups of APs can be converted to dedicated spectrum monitors through the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile.

Each 802.11a and 802.11g radio profile references a spectrum profile, which identifies the spectrum band the radio will monitor and analyze, and defines the default ageout times for each monitored device type. By default, an 802.11a radio profile references a spectrum profile named **default-a** (which configures the radio to monitor the upper channels of the 5 GHz radio band), and an 802.11g radio profile references a spectrum profile named **default-g** (which configures the radio to monitor all channels the 2.4 GHz radio band).

Most interference will occur in the 2.4 GHz radio band.

For more information about Spectrum analysis and ARM technology, refer to the *ArubaOS User Guide*.

Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in Spectrum mode in AMP:

- The AP must be in **Manage Read/Write** mode.
- The AP's associated controller must have an RFprotect license and must be running ArubaOS 6.0 or later.
- Aruba GUI Config must be enabled for that AP's group in the **Groups > Basic** page.

There are three main situations in which you would set one or more devices to Spectrum mode in AMP:

- Aruba AP Groups running permanently with the default Spectrum profile

- Individual APs running temporarily in Spectrum mode while part of an Aruba AP Group set to ap-mode
- Controller-level Spectrum Overrides (an alternative to creating new Aruba AP groups or new radio profiles for temporary changes)

Setting up a Permanent Spectrum Aruba AP Group

If you have multiple supported Aruba APs in multiple controllers that you want to run in Spectrum mode over the long run, you create a special Aruba AP group and set up a profile that is set to **spectrum-mode** and references the default **Spectrum** profile. Set up more than one profile if you want to utilize both radio bands in Spectrum mode.

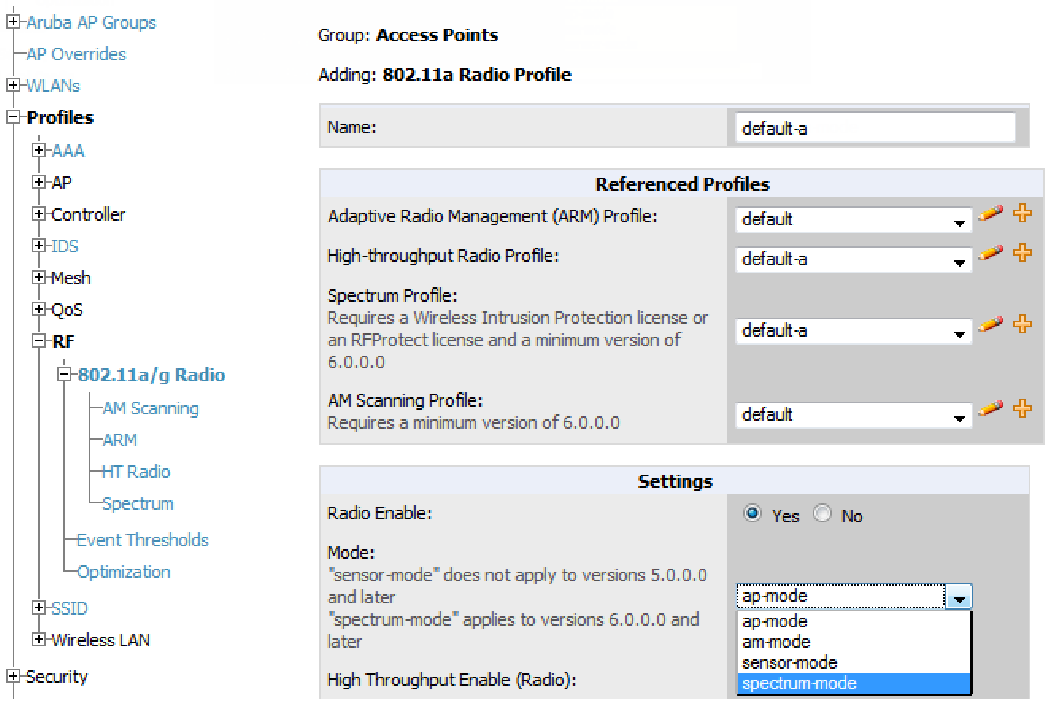
If you use an 802.11a or 802.11g radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile will be set to spectrum mode. Therefore, best practices are to create a new 802.11a or 802.11g radio profile just for spectrum monitors.

If **Use Global Aruba Configuration** is enabled in **AMP Setup** > **General**, create the configuration below, then go to the controller group's **Controller Config** page and select the newly created Aruba AP Group.

Perform these steps to set the AP group to use the default Spectrum profile settings:

1. On the **Groups** > **Controller Config** page, click the **Add New Aruba Group** button.
2. Give the new Group a name (such as Spectrum APs), and select the plus sign next to the **802.11a Radio Profile** field to create a new radio profile.
3. Enter a name under the General Settings section of **Profiles** > **RF** > **802.11a/g Radio**.
4. In the **Other Settings** section, change the **Mode** field from **ap-mode** to **spectrum-mode**, as illustrated in Figure 109, and then select **Save**.

Figure 109 *Spectrum mode in Controller Config*



Group: **Access Points**

Adding: **802.11a Radio Profile**

Name: default-a

Referenced Profiles

Adaptive Radio Management (ARM) Profile: default

High-throughput Radio Profile: default-a

Spectrum Profile: Requires a Wireless Intrusion Protection license or an RFProtect license and a minimum version of 6.0.0.0 — default-a

AM Scanning Profile: Requires a minimum version of 6.0.0.0 — default

Settings

Radio Enable: ● Yes ○ No

Mode: "sensor-mode" does not apply to versions 5.0.0.0 and later "spectrum-mode" applies to versions 6.0.0.0 and later — ap-mode

High Throughput Enable (Radio):

The above steps will use the defaults in the referenced **Spectrum Profile**. In most cases, you should not change the settings in the default profile. If you must change the defaults, however, navigate to **Groups** > **Controller Config** > **Profiles** > **RF** > **802.11a/g Radio** > **Spectrum** page, and create a new Spectrum profile with non-default settings.

If all of the devices in this Aruba AP Group are managed by the same controller and you want to temporarily override one or more profile settings in your spectrum-mode APs, you can set up a controller override.

To disable spectrum mode in this group, change the referenced radio profile back to **default**.

Configuring an Individual AP to run in Spectrum Mode

If you want to temporarily set an individual radio in an AP to run in Spectrum mode without creating or changing Aruba AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Aruba AP:

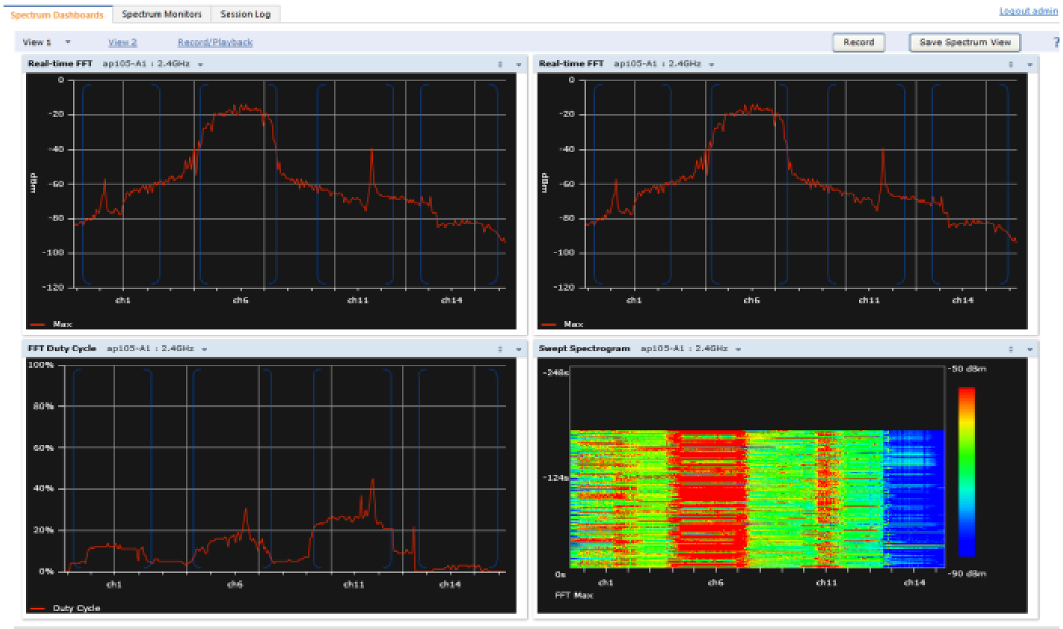
1. Go to the **APs/Devices > Manage** page for a Spectrum-supported AP.
2. After checking the Audit page, set the AP to **Manage Read/Write** mode.
3. Select **Yes** on the **Spectrum Override** field for one or both radios, depending on the band and channels you want it to analyze.
4. Select the band that should run in spectrum. If you selected the 5GHz band in the 802.11an Radio section, choose the lower, middle, or upper range of channels that you want to be analyzed by this radio.
5. Select **Save and Apply** and confirm your edit.

This overrides the current **Mode** setting for that AP (ap-mode or am-mode).

After making this change, you can view the **Radio Role** field that will appear in the **Radios** section of the **APs/Devices > Monitor** page.

The new role, **Spectrum Sensor**, is a link to the Spectrum Analysis page for the controller that manages this AP, as illustrated in Figure 110.

Figure 110 *Spectrum Analysis on Controller Dashboard*



NOTE

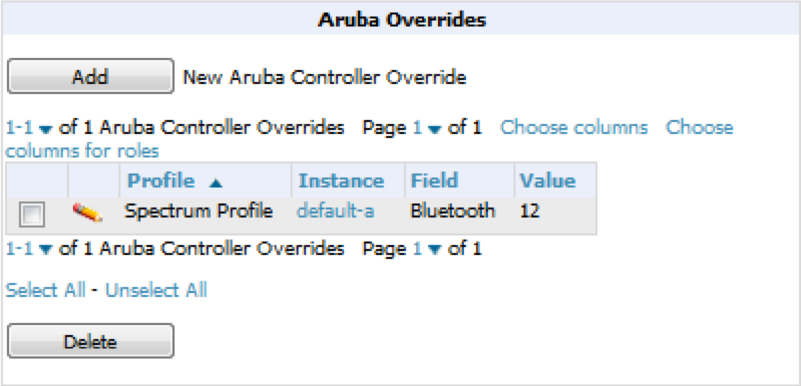
This chart is only available for AP-105, AP-90, and the AP-130 Series.

To disable Spectrum mode on this individual AP after it has collected data, return to the **APs/Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

Configuring a Controller to use the Spectrum Profile

You can use AMP to customize individual fields in the profile instance used by a particular controller without having to create new Aruba AP groups and new radio profiles. To do this, you can set a controller-level override for its referenced Spectrum profile, as illustrated in Figure 111. This will affect all Spectrum-supported APs managed by this controller.

Figure 111 *Override Section of a Supported Controller's Manage Page*



1-1 ▾ of 1 Aruba Controller Overrides Page 1 ▾ of 1 Choose columns Choose columns for roles

		Profile ▲	Instance	Field	Value
□	✎	Spectrum Profile	default-a	Bluetooth	12

1-1 ▾ of 1 Aruba Controller Overrides Page 1 ▾ of 1

Perform these steps to override individual profile settings for an Aruba controller that is part of a spectrum-mode Aruba AP group:

1. Select a Spectrum-supported Aruba controller that is referencing a Spectrum profile, and go to its **APs/Devices > Manage** page. Set it to **Manage Read/Write** mode.
2. Under the Aruba Overrides section, click the **Add New Aruba Controller Override** button.
3. In the **Profile** drop-down menu, select the **Spectrum Profile** type.
4. In the **Profile Instance** drop-down menu, select the instance of the Spectrum profile used by the controller.
5. In the **Field** drop-down menu, select the setting you would like to change (such as an Age-Out setting or a Spectrum Band), and enter the overriding value below it.
6. Select **Add** to save your changes.
7. Repeat this process to create additional overrides for this controller.
8. When you have finished, select **Save and Apply**.

You can also use the above procedure to turn on Spectrum mode for radio profiles on one particular controller, or use the overrides to point your radio profile to a non-default Spectrum profile for just this controller.

This section provides an overview and several tasks supporting the use of device configuration templates in AMP, and contains the following topics:

Group Templates

Supported Device Templates

Templates are helpful configuration tools that allow AMP to manage virtually all device settings. A template uses variables to adjust for minor configuration differences between devices.

The **Groups** > **Templates** configuration page allows you to create configuration templates for the following types of devices:

- Dell Networking W-Series
- Aruba
- Alcatel-Lucent

NOTE

Use the graphical Aruba config feature in support of Aruba devices, particularly for ArubaOS 3.3.2.x and later. Refer to the *AirWave 7.7 Controller Configuration Guide* for additional information.

- Cisco Aironet IOS autonomous APs
- Cisco Catalyst switches
- HP ProCurve 530 and WeSM controllers
- Nomadix
- Symbol
- Trapeze
  - 3Com
  - Nortel
  - Enterasys

It is also possible to create local templates in a subscriber group—using global groups does not mean that global templates are mandatory

Template Variables

Variables in templates configure device-specific properties, such as name, IP address and channel. Variables can also be used to configure group-level properties, such as SSID and RADIUS server, which may differ from one group to the next. The AMP template understands many variables including the following:

- `%allowed_aps%`
- `%ams_identity%`
- `%antenna_receive%`
- `%antenna_transmit%`
- `%ap_include_1%` through `%ap_include_10%`
- `%ca_cert_checksum%`
- `%cck_power%`
- `%certificate%`
- `%cert_psk%`
- `%channel%`
- `%channel_width%`
- `%chassis_id%`
- `%clock_timezone%`
- `%contact%`
- `%controller_ip%`
- `%custom_variable_1% through %custom_variable_10%`
- `%domain%`
- `%enabled%`
- `%gateway%`
- `%guid%`
- `%hostname%`
- `%if interface=Dot11Radio0%`
- `%if interface=Dot11Radio1%`
- `%if ip=dhcp%`
- `%if ip=static%`
- `%if radio_type=a%`
- `%if radio_type=an%`
- `%if radio_type=b%`
- `%if radio_type=bgn%`
- `%if radio_type=g%`
- `%if wds_role=backup%`
- `%if wds_role=client%`
- `%if wds_role=master%`
- `%ip_address%`
- `%ip_address_a%`
- `%ip_address_b%`
- `%ip_address_c%`
- `%manager_ip_address%`
- `%master_ip%`
- `%netmask%`
- `%ofdmpower%`
- `%organization%`

- %password%
- %power%
- %radius_server_ip%
- %rf_band%
- %server_cert_checkstum%
- %syslocation%
- %syslog_server%

The variable settings correspond to device-specific values on the **APs/Devices** > **Manage** configuration page for the specific AP that is getting configured.

NOTE

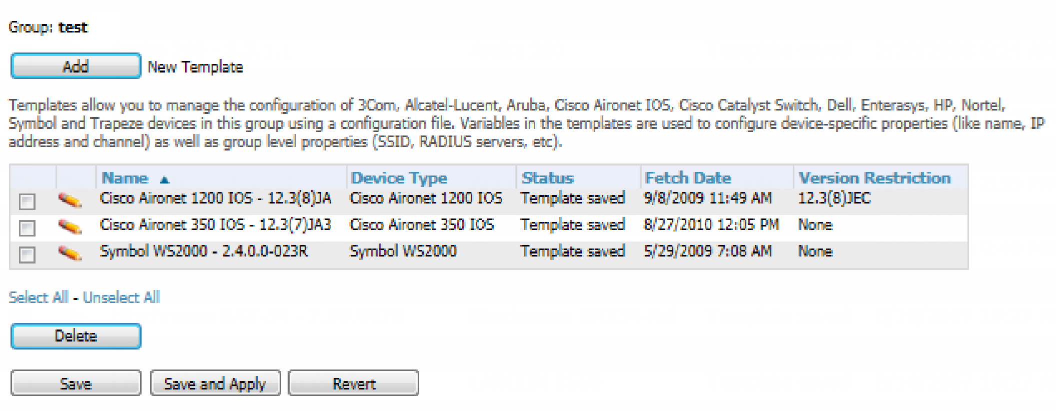
Changes made on the other **Group** pages (Radio, Security, VLANs, SSIDs, and so forth) are not applied to any APs that are configured by templates.

Viewing and Adding Templates

Perform these steps to display, add, or edit templates.

1. Go to the **Groups** > **List** page, and select a group for which to add or edit templates. This can be a new group, created with the **Add** button, or you can edit an existing group by selecting the corresponding pencil icon. The **Groups** > **Basic** page for that group appears.Additional information about adding and editing groups is described in "Configuring and Using Device Groups" on page 77.
2. From the AMP navigation pane, select **Templates**. The **Templates** page appears. Figure 112 illustrates the **Groups** > **Templates** configuration page.

Figure 112 *Groups > Templates Page Illustration for a Sample Device Group*



Group: **test**

Templates allow you to manage the configuration of 3Com, Alcatel-Lucent, Aruba, Cisco Aironet IOS, Cisco Catalyst Switch, Dell, Enterasys, HP, 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 servers, etc).

		Name ▲	Device Type	Status	Fetch Date	Version Restriction
□	✎	Cisco Aironet 1200 IOS - 12.3(8)JA	Cisco Aironet 1200 IOS	Template saved	9/8/2009 11:49 AM	12.3(8)JEC
□	✎	Cisco Aironet 350 IOS - 12.3(7)JA3	Cisco Aironet 350 IOS	Template saved	8/27/2010 12:05 PM	None
□	✎	Symbol WS2000 - 2.4.0.0-023R	Symbol WS2000	Template saved	5/29/2009 7:08 AM	None

Table 89 describes the columns in this image.

Table 89: *Groups > Templates Fields and Default Values*

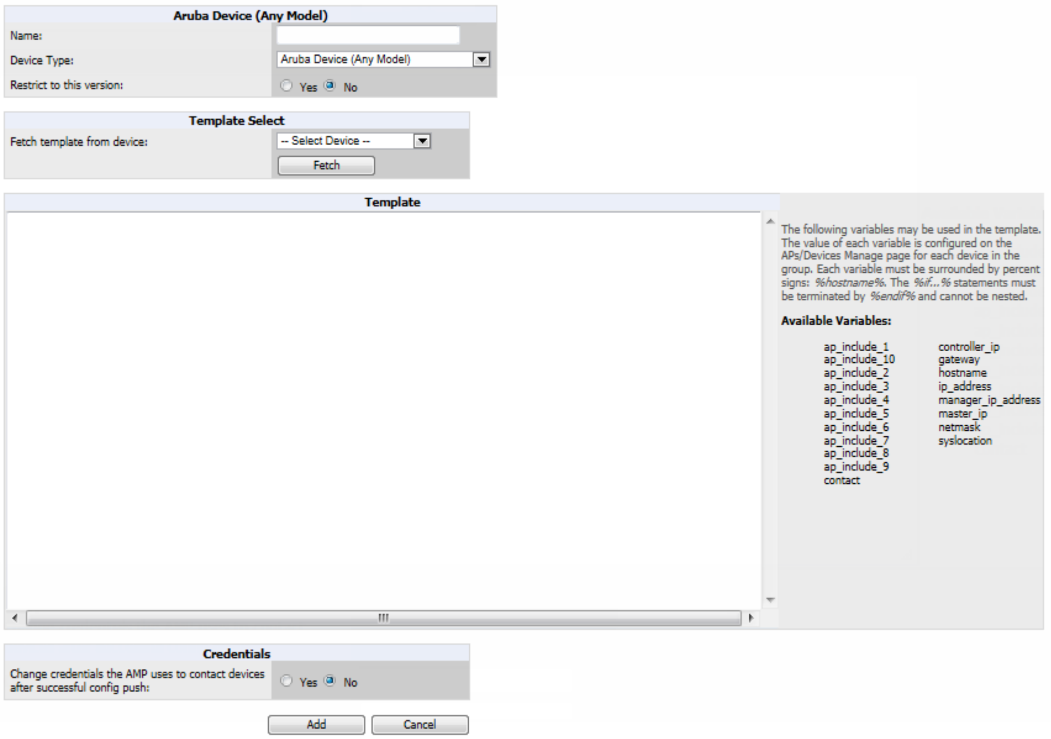
Setting	Description
Notes	When applicable, this section lists devices that are active on the network with no template available for the respective firmware. Select the link from this note to launch the **Add Template** configuration page for that device.
Name	Displays the template name.

Table 89: *Groups > Templates Fields and Default Values (Continued)*

Setting	Description
Device Type	Displays the template that applies to APs or devices of the specified type. If **(Any Model)** is selected for a vendor, then 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.
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 AMP template inventory, go to the **Groups > List** page, and select the group name. The **Details** page appears.
4. Select **Templates**, and then **Add**.
5. Complete the configurations illustrated in Figure 113.

Figure 113 *Groups > Templates > Add Template Page Illustration*



Aruba Device (Any Model)

Name:	
Device Type:	Aruba Device (Any Model)
Restrict to this version:	○ Yes ● No

Template Select

Fetch template from device:	-- Select Device -- Fetch

Template

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: *%hostname%*. The *%if...%* statements must be terminated by *%endif%* and cannot be nested.

Available Variables:

ap_include_1
ap_include_10
ap_include_2
ap_include_3
ap_include_4
ap_include_5
ap_include_6
ap_include_7
ap_include_8
ap_include_9
contact
controller_ip
gateway
hostname
ip_address
manager_ip_address
master_ip
netmask
syslocation

Credentials

Change credentials the AMP uses to contact devices after successful config push:	○ Yes ● No

The settings for the **Add a Template** page are described in Table 90. Note that the fields can vary based on the Group.

Table 90: *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 "Configuring a Global Template" on page 194.
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 AMP applies the template, copied from the new configuration file to the startup configuration file on the AP. If **No** is selected, AMP 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. 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.
Fetch Template from Device	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** page for each AP.
Template Variables	None	Add variables to be used in the template for the group. Refer to "Configuring General Template Files and Variables" on page 183 for more information.
Group Template Variables		Add variables to be used for a Group Template.
Thin AP Groups		Configure a template for selected Thin AP groups.
AP Template		Specify template variables specifically for APs.
Change credentials the AMP uses to contact devices after successful config push:	No	Specify whether to change the credentials that AMP uses to contact devices after the configuration has been pushed. If this option is enabled, then new credential information fields display.

Table 90: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
Community String	None	If the template is updating the community strings on the AP, enter the new community string AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Username	None	If the template is updating the Telnet/SSH Username on the AP, enter the new username AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
Telnet/SSH Password	None	If the template is updating the Telnet/SSH password on the AP, enter the new Telnet/SSH password AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
enable Password	None	If the template is updating the enable password on the AP, enter the new enable password AMP should use here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Username	None	If the template is updating the SNMPv3 Username on the AP, enter the new SNMP Username here. AMP 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 SNMPv3 auth password on the AP, enter the new SNMP Username password here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Auth Protocol	MD5	Specifies the SNMPv3 auth protocol, either **MD5** or **SHA-1**.
Privacy Password	None	If the template is updating the Privacy Password on the AP, enter the new password here. AMP updates the credentials it is using to communicate to the device after the device has been managed.
SNMPv3 Privacy Protocol	DES	Specifies the SNMPv3 Privacy protocol as either **DES** or **AES**. This option is not available for all devices.

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" on page 184
- "Using Template Syntax" on page 185, including the following sections:
  - "Using AP-Specific Variables" on page 185
  - "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 185
  - "Using Conditional Variables in Templates" on page 186
  - "Using Substitution Variables in Templates" on page 187

Configuring General Templates

Perform the following steps to configure Templates within a Group.

1. Select a Group to configure.

NOTE

Start with a small group of access points and placing these APs in Monitor Only mode, which is read-only. Do this using the **Modify Devices** link until you are fully familiar with the template configuration process. This prevents configuration changes from being applied to the APs until you are sure you have the correct configuration specified.

2. Select an AP from the Group to serve as a *model* AP for the others in the Group. You should select a device that is configured currently with all the desired settings. If any APs in the group have two radios, make sure to select a model AP that has two radios and that both are configured in proper and operational fashion.
3. Go to the **Groups > Templates** configuration page. Select **Add** to add a new template.
4. Select the type of device that will be configured by this template.
5. Select the model AP from the drop-down list, and select **Fetch**.
6. AMP automatically attempts to replace some values from the configuration of that AP with *variables* to enable AP-specific options to be set on an AP-by-AP basis. Refer to "Using Template Syntax" on page 185

   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 Aruba customer support before proceeding.
7. Specify the device types for the template. The templates only apply to devices of the specified type.
   - Specify whether AMP should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then AMP instructs the AP to copy the configuration from AMP to the startup configuration file of the AP and reboot the AP.
   - If the **Reboot Devices after Configuration Changes** option is not selected, then AMP instructs the AP to copy the configuration to the startup configuration file and then tell the AP to copy the startup configuration file to the running configuration file.
   - Use the **reboot** option when there are changes requiring reboot to take effect, for example, removing a new SSID from a Cisco IOS device. Copying the configuration from startup configuration file to running configuration file merges the two configurations and can cause undesired configuration lines to remain active on the AP.
8. Restrict the template to apply only to the specified version of firmware. If the template should only apply to a specific version of firmware, select **Yes** and enter the firmware version in the **Template Firmware Version** text field.
9. Select **Save and Apply** to push the configuration to all of the devices in the group. If the devices are in monitor-only mode (which is recommended while you are crafting changes to a template or creating a new one), then AMP will audit the devices and compare their current configuration to the one defined in the template.

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 **APs/Devices > Audit** configuration page, use the **Modify Devices** link on the **Groups > Monitor** configuration page to place the desired devices into **Management** mode. This removes the APs from Monitor mode (read-only) and instructs the AP to pull down its new startup configuration file from AMP.

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" on page 185
- "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 185
- "Using Conditional Variables in Templates" on page 186
- "Using Substitution Variables in Templates" on page 187

Using AP-Specific Variables

When a template is applied to an AP all variables are replaced with the corresponding settings from the **APs/Devices** > **Manage** configuration page. This enables AP-specific settings (such as Channel) to be managed effectively on an AP-by-AP basis. The list of used and available variables appears on the template detail configuration page. Variables are always encapsulated between % signs. The following example illustrates this usage:

```
hostname %hostname%
…
interface Dot11Radio0
…
  power local cck %CCK_POWER%
  power local ofdm %OFDM_POWER%
  channel %CHANNEL%
…
```

The `hostname` line sets the AP hostname to the hostname stored in AMP.

The `power` lines set the power local `cck` and `ofdm` values to the numerical values that are stored in AMP.

Using Directives to Eliminate Reporting of Configuration Mismatches

AMP is designed to audit AP configurations to ensure that the actual configuration of the access point exactly matches the Group template. When a configuration mismatch is detected, AMP generates an automatic alert and flags the AP as having a **Mismatched** configuration status on the user page.

However, when using the templates configuration function, there will be times when the running-config file and the startup-config file do not match under normal circumstances. For example, the `ntp clock-period` setting is almost never identical in the running-config file and the startup-config file. You can use directives such as `<ignore_and_do_not_push>` to customize the template to keep AMP from reporting mismatches for this type of variance.

AMP provides two types of directives that can be used within a template to control how AMP constructs the startup-config file to send to each AP and whether it reports variances between the running-config file and the startup-config file as "configuration mismatches." Lines enclosed in `<push_and_exclude>` are included in the AP startup-config file but AMP ignores them when verifying configurations. Lines enclosed in `<ignore_and_do_not_push>` cause AMP to ignore those lines during configuration verification.

Ignore_and_do_not_push Command

The `ignore and do not push` directive should typically be used when a value cannot be configured on the device, but always appears in the running-config file. Lines enclosed in the ignore and do not push directive will not be included in the startup-config file that is copied to each AP.

When AMP is comparing the running-config file to the startup-config file for configuration verification, it will ignore any lines in the running-config file that start with the text within the directive. Lines belonging to an ignored and unpushed line, the lines immediately below the line and indented, are ignored as well. In the example below, if you were to bracket the NTP server, the NTP clock period would behave as if it were bracketed because it belongs with 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 AMP 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 91:

```
%if variable=value%
```

```
…
%endif%
```

Table 91: *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 dropdown 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 92 are substituted with values specified on each access point's **APs/Devices > Manage** configuration page within the AMP User page.

Sometimes, the running-config file on the AP does not include the command for one of these variables because the value is set to the default. For example, when the **transmission power** is set to maximum (the default), the line **power local maximum** will not appear in the AP running-config file, although it will appear in the startup-config file. AMP would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent AMP from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, AMP suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way AMP suppresses lines enclosed in parentheses, which is explained below). A list of the default values that causes lines to be suppressed when reporting configuration mismatches is shown in Table 92.

Table 92: *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
hostname	Name	hostname %hostname%	-
channel	Channel	channel %channel%	-
ip_address netmask	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp …	-

Table 92: *Substitution Variables in Templates (Continued)*

Variable	Meaning	Command	Suppressed Default
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%	-
chassis id	serial number of the device	%chassis_id%	-
domain	dns-domain of the device	%domain%	-
interfaces	Interfaces of the device	%interfaces%	-

Configuring Templates for Aruba Instant

The first Instant network that is added to AMP automatically includes the default configuration that is used as a template to provision other Instant networks. Refer to the documentation that accompanies Aruba Instant for more information.

Be sure that the default configuration is validated and has been pre-tested in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will follow the same process each time and will be applied to other Instant networks as described in this document.

AMP enables you to control Instant configuration settings via the **Groups** > **Templates** configuration page. A sample configuration is provided below.

```
virtual-controller-country US
virtual-controller-key %guid%
virtual-controller-ip %ip_address_a_b_c%.3
name %hostname%
%if organization%
organization %organization%
%endif%
syslog-server 216.31.249.235
syslog-level debug
terminal-access
clock timezone Pacific-Time -08 00
rf-band 5.0
ams-ip %manager_ip_address%
ams-key %password%
allow-new-aps
%allowed_aps%
snmp-server engine-id undefined
arm
 wide-bands 5ghz
 min-tx-power 18
 max-tx-power 127
 band-steering-mode prefer-5ghz
 air-time-fairness-mode fair-access
syslog-level warn ap-debug
syslog-level warn network
syslog-level warn security
syslog-level warn system
syslog-level warn user
syslog-level warn user-debug
syslog-level warn wireless
mgmt-user admin 446f8a8ddacdb735dd42a9873a2e80e2
wlan ssid-profile remote-node-guest
 index 0
 type employee
 essid %ssid%
 wpa-passphrase a804e1744c137371943bdeed410e720a58eca75717ff714b
 opmode wpa2-psk-aes
 rf-band all
 captive-portal disable
 dtim-period 1
 inactivity-timeout 1000
 broadcast-filter none
enet-vlan guest
wlan external-captive-portal
 server localhost
 port 80
 url "/"
 auth-text "%venue%"
ids classification
ids
 wireless-containment none
```

Configuring Templates for AirMesh

AirMesh devices can be configured using templates in AMP. AMP automatically adds a template for the first AirMesh AP in a group. The configurations are pushed using CLI commands. The sample code below includes Mesh configuration options.

```
mesh
 mesh-id %mesh_id%
 %preferred_link%
 neighbor-list-type %neighbor_list_type%
  authentication open key-management wpa2
    psk ascii 5d4f50485e4f5048ed1da60b85f2784d6bbf16442fdcbfc06aeb4460d98263f5
 neighbor-list
  %neighbor_list%
service avt
  %avt_ingress_interface%
  %avt_ingress_ip%
  buffer_time 200
  mode %avt_mode%
```

NOTE

AMP displays a warning if AirMesh APs attempting to either upgrade or push configurations lack the necessary write permissions.

Configuring Cisco IOS Templates

Cisco IOS access points have hundreds of configurable settings. AMP enables you to control them via the **Groups > Templates** configuration page. This page defines the startup-config file of the devices rather than using the AMP normal **Group** configuration pages. AMP no longer supports making changes for these devices via the browser-based page, but rather uses templates to configure all settings, including settings that were controlled formerly on the AMP Group configuration pages. Perform these steps to configure a Cisco IOS Template for use with one or more groups, and the associated devices.

This section includes the following topics:

- "Applying Startup-config Files" on page 190
- "WDS Settings in Templates" on page 190
- "SCP Required Settings in Templates" on page 191
- "Supporting Multiple Radio Types via a Single IOS Template" on page 191
- "Configuring Single and Dual-Radio APs via a Single IOS Template" on page 192

Applying Startup-config Files

Each of the APs in the Group copies its unique startup-config file from AMP via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then AMP instructs the AP to copy the configuration from AMP to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then AMP instructs the AP to copy the configuration to the startup-config file and then tell the AP to copy the startup config file to the running-config file. Use the reboot option when possible. Copying the configuration from startup to running merges the two configurations and can cause undesired configuration lines to remain active on the AP.

NOTE

Changes made on the standard AMP Group configuration pages, to include Basic, Radio, Security, VLANs, and so forth, are not applied to any template-based APs.

WDS Settings in Templates

A group template supports Cisco WDS settings. APs functioning in a WDS environment communicate with the Cisco WLSE via a WDS master. IOS APs can function in Master or Slave mode. Slave APs report their rogue findings to the WDS Master (AP or WLSM which reports the data back to the WLSE. On the **APs/Devices** > **Manage** configuration page, select the proper role for the AP in the WDS Role drop down menu.

The following example sets an AP as a WDS Slave with the following lines:

```
%if wds_role=client%
wlccp ap username wlse password 7 XXXXXXXXXX
%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 AMP to login to the AP must have level 15 privileges. Without them, AMP is not able to communicate with the AP via SCP. The line "`aaa authorization exec default local`" must be in the APs configuration file and the AP must have the SCP server enabled. These three settings correspond to the following lines in the AP's configuration file:

```
username Cisco privilege 15 password 7 0802455D0A16
aaa authorization exec default local
ip scp server enable
```

The `username` line is a guideline and will vary based on the username being set, in this case Cisco, and the password and encoding type, in this case 0802455D0A16 and 7 respectively.

These values can be set on a group wide level using Templates and TFTP. Once these lines are set, SCP can be enabled on the **Groups** > **Basic** configuration page without problems.

Supporting Multiple Radio Types via a Single IOS Template

Some lines in an IOS configuration file should only apply to 802.11g vs. 802.11b. For instance, lines related to speed rates that mention rates above 11.0Mb/s do not work for 802.11b radios that cannot support these speeds. Use the "`%IF` *`variable=value`*`% … %ENDIF%`" construct to allow a single IOS configuration template to configure APs with different radio types within the same Group as illustrated below:

```
interface Dot11Radio0
…
%IF radio_type=g%
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
%ENDIF%
%IF radio_type=b%
speed basic-1.0 2.0 5.5 11.0
%ENDIF%
%IF radio_type=g%
power local cck %CCK_POWER%
power local ofdm %OFDM_POWER%
%ENDIF%
…
```

Configuring Single and Dual-Radio APs via a Single IOS Template

To configure single and dual-radio APs using the same IOS config template, you can use the interface variable within the %IF…% construct. The below example illustrates this usage:

```
%IF interface=Dot11Radio1%
interface Dot11Radio1
 bridge-group 1
 bridge-group 1 block-unknown-source
 bridge-group 1 spanning-disabled
 bridge-group 1 subscriber-loop-control
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 no ip address
 no ip route-cache
 rts threshold 2312
 speed basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 36.0 48.0 54.0
 ssid decibel-ios-a
   authentication open
   guest-mode
   station-role root
      %ENDIF%
```

Configuring Cisco Catalyst Switch Templates

Cisco Catalyst Switch templates are configured much like Cisco IOS templates with the addition of the `interfaces` and `switch_command` (for stacked switches) variables. Interfaces can be configured on the Device Interface pages, as shown in "Configuring Device Interfaces for Switches" on page 165. 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 184.

Just one template is used for any type of Cisco IOS device, and another is used for any type of Catalyst Switch regardless of individual model.

Configuring Symbol Controller / HP WESM Templates

This section describes the configuration of templates for Symbol controllers and HP WESM devices.

Symbol controllers (RFS x000, 5100 and 2000) can be configured in AMP using templates. AMP supports Symbol thin AP firmware upgrades from the controller's manage page.

A sample running-configuration file template is provided in this topic for reference. A template can be fetched from a model device using the Cisco IOS device procedure described in "Configuring Cisco IOS Templates" on page 190. Cisco IOS template directives such as `ignore_and_do_not_push` can also be applied to Symbol templates.

Certain parameters such as `hostname` and `location` are turned into variables with the `%` tags so that device-specific values can be read from the individual manage pages and inserted into the template. They are listed in Available Variable boxes on the right-hand side of the template fields.

Certain settings have integrated variables, including `ap-license` and `adoption-preference-id`. The radio preamble has been template-integrated as well. An option on the **Group** > **Templates** page reboots the device after pushing a configuration to it.

A sample Symbol controller partial template is included below for reference.

```
!
! configuration of RFS4000 version 4.2.1.0-005R
!
version 1.4
!
!
aaa authentication login default local none
```

```
service prompt crash-info
!
network-element-id RFS4000
!
username admin password 1 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 100 permit ip 192.168.0.0/24 any rule-precedence 10
!
spanning-tree mst cisco-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 255.2
55.255.255 dst-start-port 3333 dst-end-port 3334 rule 1
%redundancy_config%
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b45674b30f176
snmp-server location %location%
snmp-server contact %contact%
snmp-server sysname %hostname%
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpmanager v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpoperator v3 encrypted auth md5 0xb03b1ebfa0e3d02f50e2b1c092ab7c9f
```

A sample Symbol Smart RF template is provided below for reference:

```
radio %radio_index% radio-mac %radio_mac%
%if radio_type=11a%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11an%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11b%
  radio %radio_index% coverage-rate  5p5
%endif%
%if radio_type=11bg%
  radio %radio_index% coverage-rate  6
%endif%
%if radio_type=11bgn%
  radio %radio_index% coverage-rate  18
%endif%
```

A sample Symbol thin AP template is provided below for reference and for the formatting of **`if`** statements.

```
   radio add %radio_index% %lan_mac% %radio_type% %ap_type%
    radio %radio_index% radio-number %radio_number%
    radio %radio_index% description %description%
    %if radio_type=11a%
    radio %radio_index% speed  basic6 9 basic12 18 basic24 36 48 54
    radio %radio_index% antenna-mode primary
```

```
 radio %radio_index% self-heal-offset 1
 radio %radio_index% beacon-interval 99
 radio %radio_index% rts-threshold 2345
 radio %radio_index% max-mobile-units 25
 radio %radio_index% admission-control voice max-perc 76
 radio %radio_index% admission-control voice res-roam-perc 11
 radio %radio_index% admission-control voice max-mus 101
 radio %radio_index% admission-control voice max-roamed-mus 11
 %endif%
 %if radio_type=11an%
 radio %radio_index% speed  basic11a 9 18 36 48 54 mcs 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
 %endif%
 %if radio_type=11b%
 radio %radio_index% speed  basic1 basic2 basic5p5 basic11
 %endif%
 %if radio_type=11bg%
 radio %radio_index% speed  basic1 basic2 basic5p5 6 9 basic11 12 18 24 36 48 54
 radio %radio_index% on-channel-scan
 radio %radio_index% adoption-pref-id 7
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% enhanced-probe-table
 %endif%
 %if radio_type=11bgn%
 radio %radio_index% speed  basic11b2 6 9 12 18 24 36 48 54 mcs 0,1,2,3,4,5,6,7,8,9,10,11,12,
13,14,15
 %endif%
 radio %radio_index% channel-power indoor %channel% %transmit_power% %channel_attribute%
 %detector%
%adoption_pref_id%
 radio %radio_index% enhanced-beacon-table
 radio %radio_index% on-channel-scan
%ap_include_4%
```

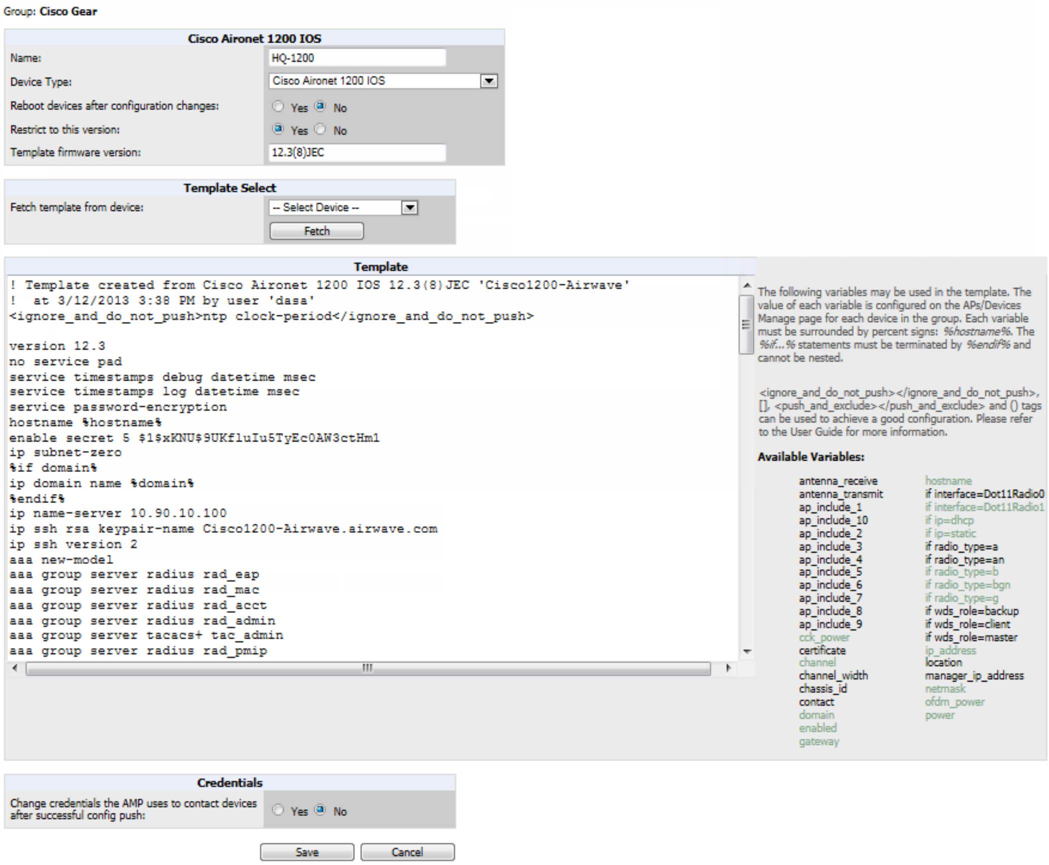
Configuring a Global Template

Global templates allow AMP users to define a single template in a global group that can be used to manage APs in subscriber groups. They turn settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

Perform the following steps to create a global template, or to view or edit an existing global template:

1. Go to the **Group > Templates** configuration page for the global group that owns it.
2. Select **Add** to add a new template, or select the **pencil** icon next to an existing template to edit it.
3. Examine the configurations illustrated in Figure 114.

Figure 114 *Group > Templates > Add Page Illustration*



Group: **Cisco Gear**

Cisco Aironet 1200 IOS

Name:	HQ-1200
Device Type:	Cisco Aironet 1200 IOS
Reboot devices after configuration changes:	○ Yes ● No
Restrict to this version:	● Yes ○ No
Template firmware version:	12.3(8)JEC

Template Select

Fetch template from device: -- Select Device --

Template

```
! Template created from Cisco Aironet 1200 IOS 12.3(8)JEC 'Cisco1200-Airwave'
!  at 3/12/2013 3:38 PM by user 'dasa'
<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 $1$xKNU$9UKfluIu5TyEc0AW3ctHm1
ip subnet-zero
%if domain%
ip domain name %domain%
%endif%
ip name-server 10.90.10.100
ip ssh rsa keypair-name Cisco1200-Airwave.airwave.com
ip ssh version 2
aaa new-model
aaa group server radius rad_eap
aaa group server radius rad_mac
aaa group server radius rad_acct
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
```

The following variables may be used in the template. The value of each variable is configured on the APs/Devices Manage page for each device in the group. Each variable must be surrounded by percent signs: *%hostname%*. The *%if...%* statements must be terminated by *%endif%* and cannot be nested.

<ignore_and_do_not_push></ignore_and_do_not_push>, [], <push_and_exclude></push_and_exclude> and () tags can be used to achieve a good configuration. Please refer to the User Guide for more information.

Available Variables:

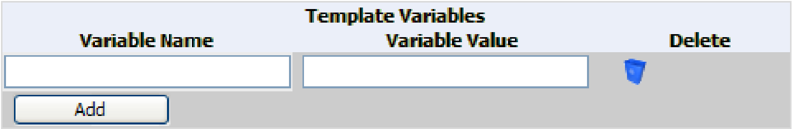
antenna_receive
antenna_transmit
ap_include_1
ap_include_10
ap_include_2
ap_include_3
ap_include_4
ap_include_5
ap_include_6
ap_include_7
ap_include_8
ap_include_9
cck_power
certificate
channel
channel_width
chassis_id
contact
domain
enabled
gateway
hostname
if interface=Dot11Radio0
if interface=Dot11Radio1
if ip=dhcp
if ip=static
if radio_type=a
if radio_type=an
if radio_type=b
if radio_type=bgn
if radio_type=g
if wds_role=backup
if wds_role=client
if wds_role=master
ip_address
location
manager_ip_address
netmask
ofdm_power
power

Credentials

Change credentials the AMP uses to contact devices after successful config push: ○ Yes ● No

4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The menus are populated with all devices that are contained in any group that subscribes to the global group. The fetched configuration populates the template field. Global template variables can be configured with the **Add** button in the **Template Variables** box, illustrated in Figure 115.

Figure 115 *Template Variables Illustration*



Template Variables

Variable Name	Variable Value	Delete

The variable name cannot have any spaces or non-alphanumeric characters. The initial variable value entered is the default value, but can be changed on a per-group basis later. You can also populate global template variables by uploading a CSV file (see below).

5. Once you have configured your global template, select **Add**. You are taken to a confirmation configuration page where you can review your changes.
6. If you want to add the global template, select **Apply Changes Now**. If you do not want to add the template, select **Cancel and Discard Changes**. Canceling from the confirmation configuration page causes the template and all of the template variables to be lost.
7. Once you have added a new global template, you can use a CSV upload option to configure global template variables. Go to the **Groups** > **Templates** configuration page and select the **CSV** upload icon for the template. The CSV file must contain columns for **Group Name** and **Variable Name**. All fields must be completed.

- **Group Name**—the name of the subscriber group that you wish to update.
- **Variable Name**—the name of the group template variable you wish to update.
- **Variable Value**—the value to set.

For example, for a global template with a variable called "ssid_1", the CSV file might resemble what follows:

```
Group Name, ssid_1
Subscriber 1, Value 0
```

8. Once you have defined and saved a global template, it is available for use by any local group that subscribes to the global group. Go to the **Groups > Template** configuration page for the local group and select the pencil icon next to the global template in the list.
9. To make template changes, go to the **Groups > Template** configuration page for the global group and select the **pencil** icon next to the template you wish to edit. Note that you cannot edit the template itself from the subscriber group's **Groups > Templates** tab.
10. If group template variables have been defined, you are able to edit the value for the group on the **Groups > Templates > Add** configuration page in the **Group Template Variables** box. For Symbol devices, you are also able to define the template per group of APs.

Using RAPIDS and Rogue Classification

This chapter provides an overview to rogue device and IDS event detection, alerting, and analysis using RAPIDS, and contains the following sections:

Introduction to RAPIDS

Rogue device detection is a core component of wireless security. With RAPIDS rules engine and containment options, you can create a detailed definition of what constitutes a rogue device, and quickly act on a rogue AP for investigation, restrictive action, or both. Once rogue devices are discovered, RAPIDS alerts your security team of the possible threat and provides essential information needed to locate and manage the threat.

RAPIDS discovers unauthorized devices in your WLAN network in the following ways:

- Over the Air, using your existing enterprise APs or the optional AMP Management Client (AMC).
- On the Wire
  - Polling routers and switches to identify, classify, and locate unknown APs
  - Using the controller’s wired discovery information
  - Using HTTP and SNMP scanning

NOTE

To set up a scan, refer to "Discovering and Adding Devices" on page 124.

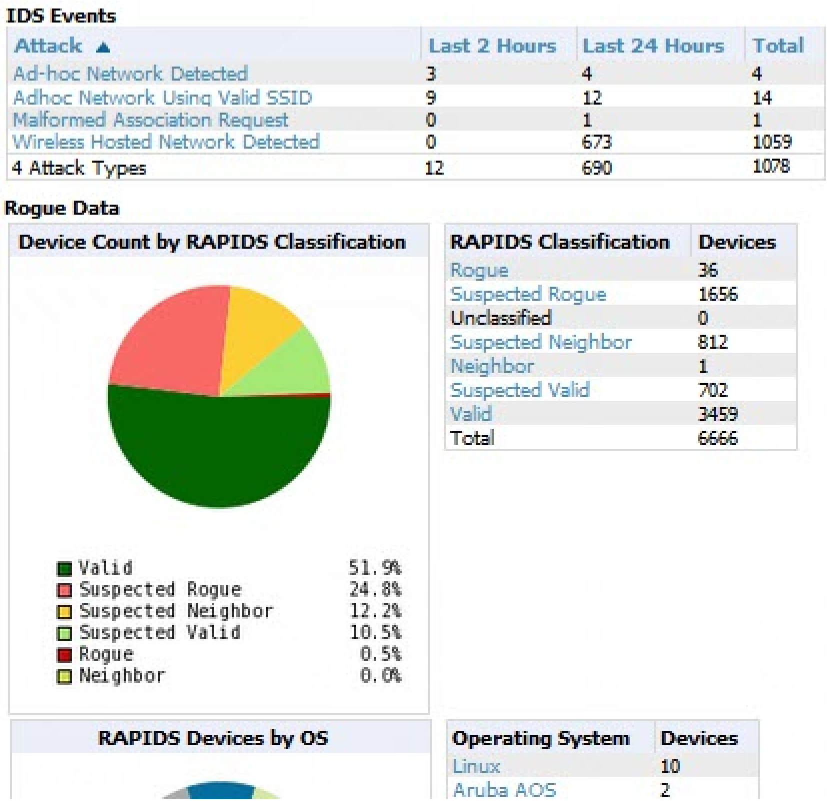
Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Aruba WIP**—Wireless Intrusion Protection (WIP) module integrates wireless intrusion protection into the mobile edge infrastructure. The WIP module provides wired and wireless AP detection, classification and containment; detects DoS and impersonation attacks; and prevents client and network intrusions.
- **Cisco WLSE** (1100 and 1200 IOS)—AMP fetches rogue information from the HTTP interface and gets new AP information from SOAP API. This system provides wireless discovery information rather than rogue detection information.
- **AirMagnet Enterprise**—Retrieves a list of managed APs from AMP.
- **AirDefense**—Uses the AMP XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from AMP.

Viewing Overall Network Health on RAPIDS > Overview

The **RAPIDS** > **Overview** page displays a page of RAPIDS summary information (see Figure 116). Table 93 defines the summary information that appears on the page.

Figure 116 *RAPIDS > Overview Page Illustration (partial view)*



IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Ad-hoc Network Detected	3	4	4
Adhoc Network Using Valid SSID	9	12	14
Malformed Association Request	0	1	1
Wireless Hosted Network Detected	0	673	1059
4 Attack Types	12	690	1078

Rogue Data

Device Count by RAPIDS Classification

🟩	Valid	51.9%
🟥	Suspected Rogue	24.8%
🟨	Suspected Neighbor	12.2%
🟩	Suspected Valid	10.5%
🟥	Rogue	0.5%
🟩	Neighbor	0.0%

RAPIDS Classification	Devices
Rogue	36
Suspected Rogue	1656
Unclassified	0
Suspected Neighbor	812
Neighbor	1
Suspected Valid	702
Valid	3459
Total	6666

RAPIDS Devices by OS

Operating System	Devices
Linux	10
Aruba AOS	2

Table 93: *RAPIDS > Overview Fields and Descriptions*

Summary	Description
IDS Events	Displays a list of attack types for the designated folder and subfolders. Field displays events from the past two hours, the past 24 hours, and total IDS events. Names of attacks link to summary pages with more details. **NOTE:** AMP should be configured as the SNMP trap receiver on the controllers to receive IDS traps. See the *Aruba and AirWave Best Practices Guide* for details.
Device Count by RAPIDS Classification	A pie chart of rogue device percentages by RAPIDS classification.
RAPIDS Classification	A summary list with details of the statistics depicted in the Device Count by RAPIDS Classification pie chart. Click the linked classification name to be taken to a filtered rogue list.
RAPIDS Devices by OS	A pie chart of RAPIDS percentages by the detected operating system.
Operating System	Detected operating systems represented in this summary listing. Click on the linked Operating System name to see the rogues list filtered by that classification. OS scans can be run manually or enabled to run automatically on the **RAPIDS > Setup** page.

Table 93: *RAPIDS > Overview Fields and Descriptions (Continued)*

Summary	Description
Acknowledged RAPIDS Devices	A color coded pie chart comparing the number of acknowledged devices to the unacknowledged devices.
RAPIDS Changes	Tracks every change made to RAPIDS including changes to rules, manual classification, and components on the **RAPIDS > Setup** page. A link at the top of the list directs you to the **RAPIDS > Audit Log** page.

Setting Up RAPIDS

The **RAPIDS** > **Setup** page allows you to configure your AMP server for RAPIDS. Complete the settings on this page as desired, and select **Save**. Most of the settings are internal to the way that AMP will process rogues.

Refer to the following sections:

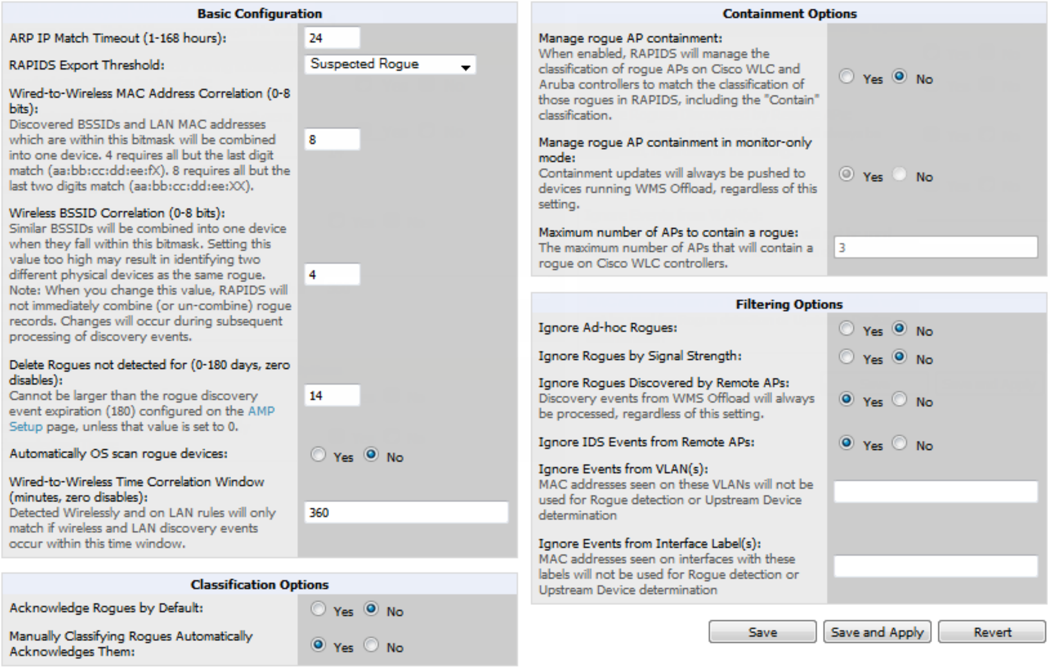
- "RAPIDS Setup" on page 199
- "Additional Settings" on page 202

RAPIDS Setup

Basic Configuration

On the **RAPIDS** > **Setup** page, the **Basic Configuration** section allows you to define RAPIDS behavior settings. The figure below illustrates this page, and the tables that follow describe the fields.

Figure 117 *RAPIDS > Setup Page Illustration*



Basic Configuration

ARP IP Match Timeout (1-168 hours):	24
RAPIDS Export Threshold:	Suspected Rogue
Wired-to-Wireless MAC Address Correlation (0-8 bits): Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).	8
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.	4
Delete Rogues not detected for (0-180 days, zero disables): Cannot be larger than the rogue discovery event expiration (180) configured on the AMP Setup page, unless that value is set to 0.	14
Automatically OS scan rogue devices:	○ Yes ● No
Wired-to-Wireless Time Correlation Window (minutes, zero disables): Detected Wirelessly and on LAN rules will only match if wireless and LAN discovery events occur within this time window.	360

Classification Options

Acknowledge Rogues by Default:	○ Yes ● No
Manually Classifying Rogues Automatically Acknowledges Them:	● Yes ○ No

Containment Options

Manage rogue AP containment: When enabled, RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS, including the "Contain" classification.	○ Yes ● No
Manage rogue AP containment in monitor-only mode: Containment updates will always be pushed to devices running WMS Offload, regardless of this setting.	● Yes ○ No
Maximum number of APs to contain a rogue: The maximum number of APs that will contain a rogue on Cisco WLC controllers.	3

Filtering Options

Ignore Ad-hoc Rogues:	○ Yes ● No
Ignore Rogues by Signal Strength:	○ Yes ● No
Ignore Rogues Discovered by Remote APs: Discovery events from WMS Offload will always be processed, regardless of this setting.	● Yes ○ No
Ignore IDS Events from Remote APs:	● Yes ○ No
Ignore Events from VLAN(s): MAC addresses seen on these VLANs will not be used for Rogue detection or Upstream Device determination	
Ignore Events from Interface Label(s): MAC addresses seen on interfaces with these labels will not be used for Rogue detection or Upstream Device determination	

Table 94: *RAPIDS > Setup > Basic Configuration Fields and Default Values*

Field	Default	Description
ARP IP Match Timeout (1-168 hours)	24	If you have routers and switches on AMP, and it's scanning them for ARP tables, this can assign a rogue IP address information. This timeout specifies how recent that information needs to be for the IP address to be considered valid. Note that the default ARP poll period is long (several hours).
RAPIDS Export Threshold	Suspected Rogue	Exported rogues will be sent to VisualRF for location calculation.
Wired-to-Wireless MAC Address Correlation (0-8 bits)	4	Discovered BSSIDs and LAN MAC addresses which are within this bitmask will be combined into one device. 4 requires all but the last digit match (aa:bb:cc:dd:ee:fX). 8 requires all but the last two digits match (aa:bb:cc:dd:ee:XX).
Wireless BSSID Correlation (0-8 bits)	4	Similar BSSIDs will be combined into one device when they fall within this bitmask. Setting this value too high may result in identifying two different physical devices as the same rogue. **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.
Delete Rogues not detected for (0-30 days, zero disables):	N/A	This value cannot be larger than the rogue discovery event expiration (30) configured on the AMP Setup page, unless that value is set to **0**.
Automatically OS scan rogue devices	No	Whether to scan the operating system of rogues. Enabling this feature will cause RAPIDS to perform an OS scan when it gets in IP address for a rogue device. The OS scan will be run when a rogue gets an IP address for the first time or if the IP address changes.
Wired-to-Wireless Time Correlation Window (minutes, zero disables):	360	Specify a time frame for wired and wireless correlation. RAPIDS discovery events detected wirelessly and on LAN will only match if the wireless and LAN discovery events occur during this timeframe.

Classification Options

Table 95: *RAPIDS > Setup > Classification Options Fields and Default Values*

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 acknowledgment happens automatically whenever a rogue device receives a manual classification.

Containment Options

Using RAPIDS, AMP can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Aruba controllers (running ArubaOS 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 96: *RAPIDS > Setup > Containment Options Fields and Default Values*

Field	Default	Description
Manage rogue AP containment	No	Specifies whether RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS. This includes the "Contained" classification. If this setting is enabled, then the **Maximum number of APs to contain a rogue** setting can be configured. Similarly, if this is enabled, then the Contained Rogue option will appear in the classification drop down menu when you add a new classification rule. (See "Viewing and Configuring RAPIDS Rules" on page 203 for more information.)
Manage rogue AP containment in monitor-only mode	No	Specify whether rogue AP containment can be performed in monitor-only mode. Note that containment updates will always be pushed to devices that are running WMS Offload, regardless of this setting.
Maximum number of APs to contain a rogue	N/A	If **Manage rogue AP containment** is enabled, then specify the maximum number of APs that can contain a rogue on Cisco WLC controllers.

Filtering Options

Filtered rogues are dropped from the system before they are processed through the rules engine. This can speed up overall performance but will eliminate all visibility into these types of devices.

Table 97: *RAPIDS > Setup > Filtering Options Fields and Default Values*

Field	Default	Description
Ignore Ad-hoc rogues	No	Filters rogues according to ad-hoc status.
Ignore Rogues by Signal Strength	No	Filters rogues according to signal strength. Since anything below the established threshold will be ignored and possibly dangerous, best practices is to keep this setting disabled. Instead, incorporate signal strength into the classification rules on the **RAPIDS > Rules** page.
Ignore Rogues Discovered by Remote APs	No	Filters rogues according to the remote AP that discovers them. Enabling this option causes AMP to drop all rogue discovery information coming from remote APs.
Ignore IDS Events from Remote APs	No	Filters IDS Events discovered by remote APs.
Ignore Events from VLAN(s)	N/A	Specify a VLAN or list of VLANs to be ignored when a wired rogue discovery event occurs. MAC addresses that appear on these VLANs will not be used for rogue detection or upstream device determination.
Ignore Events from Interface Label(s)	N/A	Specify an interface or list of interfaces to be ignored when a wired rogue discovery event occurs. MAC addresses that appear on these interface labels will not be used for rogue detection or upstream device determination.

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 AMP User Roles" on page 43.
- Use the **AMP Setup** > **General** > **Performance Tuning** page to define the processing priority of RAPIDS in relation to AMP as a whole. (See in "AMP Setup > General" on page 29.)

Defining RAPIDS Rules

The **RAPIDS** > **Rules** page is one of the core components of RAPIDS. This feature allows you to define rules by which any detected device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful.

This section contains the following topics:

Controller Classification with WMS Offload

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 AMP, which AMP then processes. AMP then pushes the WMS classification to all of the ArubaOS controllers that are WMS-offload enabled.

WMS Offload ensures that a particular BSSID has the same classification on all of the controllers. WMS Offload removes some load from master controllers and feeds '`connected-to-lan`' information to the RAPIDS classification engine. RAPIDS classifications and controller classifications are separate and often are not synchronized.

NOTE

RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between AMP and ArubaOS for scenarios involving WMS Offload.

Table 98: *Rogue Device Classification Matrix*

AirWave	ArubaOS (ARM)
Unclassified (default state)	Unknown
Rogue	Rogue
Suspected Neighbor	Interfering
Neighbor	Known Interfering

Table 98: *Rogue Device Classification Matrix (Continued)*

AirWave	ArubaOS (ARM)
Valid	Valid
Contained Rogue	DOS

For additional information about WMS Offload, refer to the *AirWave 7.7 Best Practices Guide* on the **Home > Documentation** page.

Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score. The OUI score of each device is viewable from each rogue's detail page. Table 99 provides list the OUI scores definitions.

Table 99: *Device OUI Scores*

Score	Description
Score of 1	Indicates any device on the network; this is the lowest threat level on the network.
Score of 2	Indicates any device in which the OUI belongs to a manufacturer that produces wireless (802.11) equipment.
Score of 3	Indicates that the OUI matches a block that contains APs from vendors in the Enterprise and small office/ small home market.
Score of 4	Indicates that the OUI matches a block that belonged to a manufacturer that produces small office/ small home access points.

Rogue Device Threat Level

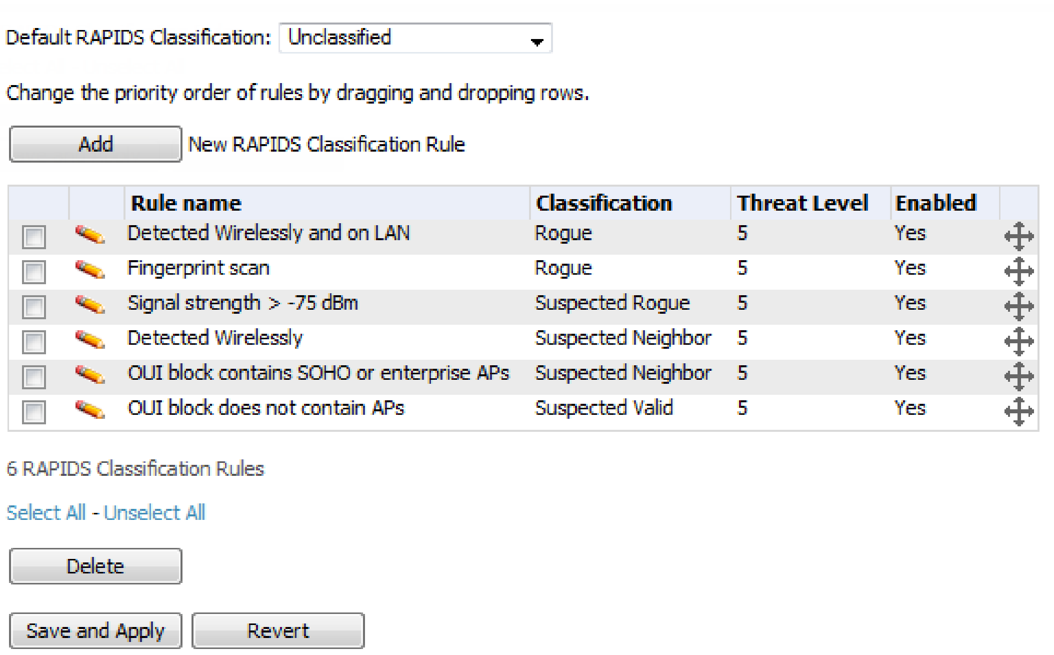
The threat level classification adds granularity for each general RAPIDS classification. Devices of the same classification can have differing threat scores based on the classifying rule, ranging from 1 to 10 with a default value of **5**. This classification process can help identify the greater threat. Alerts can be defined and sorted by threat level.

Threat level and classification are both assigned to a device when a device matches a rule. Once classified, a device's classification and threat level change only if it is classified by a new rule or is manually changed. Threats levels can be manually defined on the **RAPIDS > Detail** page when the RAPIDS classification is manually overridden or you can edit the rule to have a higher threat level.

Viewing and Configuring RAPIDS Rules

To view the RAPIDS rules that are currently configured on AMP, navigate to the **RAPIDS > Rules** page (Figure 118).

Figure 118 *RAPIDS > Rules Page Illustration*



Default RAPIDS Classification: Unclassified

Change the priority order of rules by dragging and dropping rows.

Add New RAPIDS Classification Rule

		Rule name	Classification	Threat Level	Enabled	
□	✎	Detected Wirelessly and on LAN	Rogue	5	Yes	✥
□	✎	Fingerprint scan	Rogue	5	Yes	✥
□	✎	Signal strength > -75 dBm	Suspected Rogue	5	Yes	✥
□	✎	Detected Wirelessly	Suspected Neighbor	5	Yes	✥
□	✎	OUI block contains SOHO or enterprise APs	Suspected Neighbor	5	Yes	✥
□	✎	OUI block does not contain APs	Suspected Valid	5	Yes	✥

6 RAPIDS Classification Rules

Select All - Unselect All

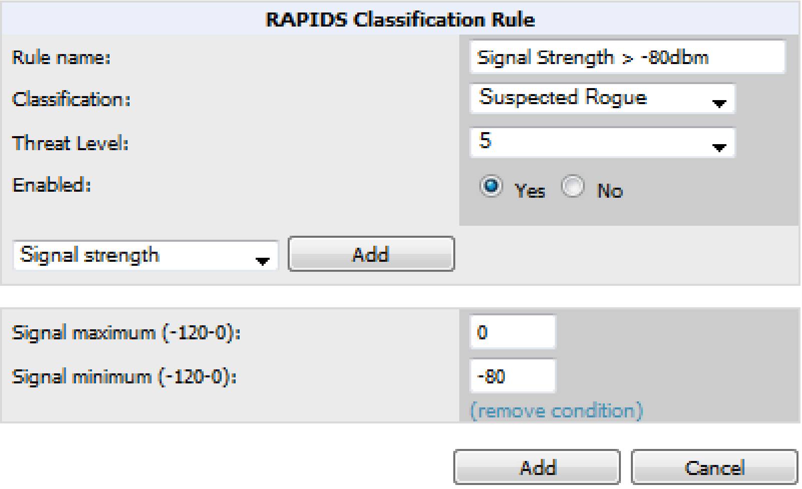
Table 100 defines the fields in the **RAPIDS** > **Rules** page.

Table 100: *RAPIDS > Rules Page*

Field	Description
Default Classification	This drop down specifies the classification that a rogue device receives when it does not match any rules.
Add New RAPIDS Classification Rule	Select 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 203 for additional information.
Enabled	Displays the status of the rule, whether enabled or disabled.
Reorder Drag and Drop Icon ✥	Changes the sequence of rules in relation to each other. Select, then drag and drop, the icon for any rule to move it up or down in relation to other rules. A revised sequence of rules must be saved before rogues are classified in the revised sequence. **NOTE:** The sequence of rules is very important for proper rogue classification. A device gets classified by the first rule to which it complies, even if it conforms to additional rules later in the sequence.

To create a new rule, select the **Add** button next to **New RAPIDS Classification Rule** to launch the **RAPIDS Classification Rule** page (see Figure 119).

Figure 119 *Classification Rule Page*



RAPIDS Classification Rule

Rule name: Signal Strength > -80dbm

Classification: Suspected Rogue

Threat Level: 5

Enabled: ● Yes ○ No

Signal strength

Signal maximum (-120-0): 0

Signal minimum (-120-0): -80

Fill in the settings described in Table 100 then select an option from the drop down menu.

Table 101 defines the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 119). After all rule settings are defined, select **Add**. The new rule automatically appears in the **RAPIDS** > **Rules** page.

Table 101: *Properties Drop Down Menu*

Option	Description
Wireless Properties	
Detected on WLAN	Classifies based on how the rogue is detected on the wireless LAN.
Detecting 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. Note that you can select **no encryption** with a rule that says **Encryption does not match WEP or better.**
Network type	Rogue is running on the selected network type, either **Ad-hoc** or **Infrastructure**.
Signal Strength	Rogue matches signal strength parameters. Specify a minimum and maximum value in dBm.
SSID	Classifies the rogue when it matches or does not match the specified string for the SSID or a specified regular expression. **NOTE:** For SSID matching functions, AMP processes only alpha-numeric characters and the asterisk wildcard character (*). AMP 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).
Detected Client Count	Classifies based on the number of valid clients.
Wireline Properties	

Table 101: *Properties Drop Down Menu (Continued)*

Option	Description
Detected on LAN	Rogue is detected on the wired network. Select **Yes** or **No**.
Fingerprint Scan	Rogue matches fingerprint parameters.
IP Address	Rogue matches a specified IP address or subnet. Enter IP address or subnet information as explained by the fields.
OUI Score	Rogue matches manufacturer OUI criteria. You can specify minimum and maximum OUI score settings from two drop-down lists. Select **remove** to remove one or both criteria, as desired.
Operating System	Rogue matches OS criteria. Specify matching or non-matching OS criteria as prompted by the fields.
Wireless/Wireline Properties	
Manufacturer	Rogue matches the manufacturer information of the rogue device. Specify matching or non-matching manufacturer criteria.
MAC Address	Rogue matches the MAC address. Specify matching or non-matching address criteria, or use a wildcard (*) for partial matches.
Aruba Controller Properties	
Controller Classification	Rogue matches the specified controller classification.
Confidence	Rogue falls within a specified minimum and maximum confidence level, ranging from 1 to 100.

After creating a new rule, click **Add** to return to the **RAPIDS > Rules** page. Click **Save and Apply** to have the new rule take effect.

Deleting or Editing a Rule

To delete a rule from the RAPIDS rules list, go to the **RAPIDS > Rules** page. Select the check box next to the rule you want to delete, and click **Delete**. The rule is automatically deleted from **RAPIDS > Rules**.

To edit any existing rule, select its pencil icon to launch the **RAPIDS Classification Rule** page (see Figure 119). Edit or revise the fields as necessary, then click **Save**.

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

Recommended RAPIDS Rules

- **If Any Device Has Your SSID, then Classify as Rogue**

  The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by AMP. 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, AMP tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

  The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Aruba support.

Using RAPIDS Rules with Additional AMP Functions

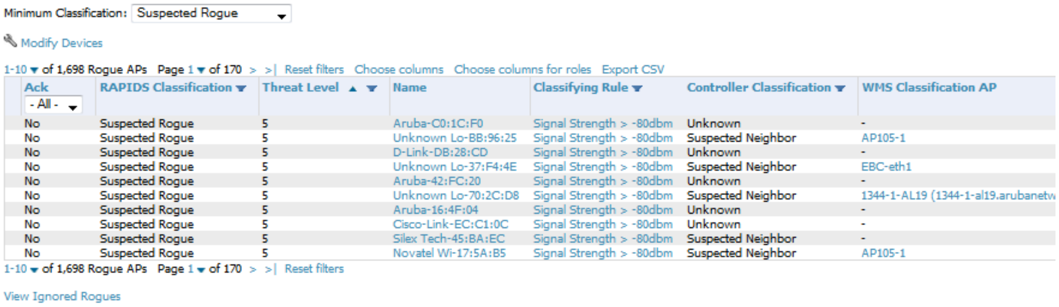
Rules that you configure on the **RAPIDS** > **Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in AMP, with additional information:

- **RAPIDS** > **List**—Lists rogue devices as classified by rules.
- **RAPIDS** > **Rules**—Displays the rules that classify rogue devices.
- **RAPIDS** > **Overview**—Displays general rogue device count and statistical information.
- **System** > **Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports** > **Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

Viewing Rogues on the RAPIDS > List Page

To view a rogue AP, select the **RAPIDS** > **List** tab and select a rogue device type from the **Minimum Classification** drop-down menu (see Figure 120). You can sort the table columns (up/down) by selecting the column head. Most columns can be filtered using the funnel icon (▼). The active links on this page launch additional pages for RAPIDS configuration or device processing.

Figure 120 *RAPIDS > List Page Illustration (partial view)*



Minimum Classification: Suspected Rogue

Modify Devices

1-10 of 1,698 Rogue APs Page 1 of 170 > >| Reset filters Choose columns Choose columns for roles Export CSV

Ack - All -	RAPIDS Classification	Threat Level	Name	Classifying Rule	Controller Classification	WMS Classification AP
No	Suspected Rogue	5	Aruba-C0:1C:F0	Signal Strength > -80dbm	Unknown	-
No	Suspected Rogue	5	Unknown Lo-BB:96:25	Signal Strength > -80dbm	Suspected Neighbor	AP105-1
No	Suspected Rogue	5	D-Link-DB:28:CD	Signal Strength > -80dbm	Unknown	-
No	Suspected Rogue	5	Unknown Lo-37:F4:4E	Signal Strength > -80dbm	Suspected Neighbor	EBC-eth1
No	Suspected Rogue	5	Aruba-42:FC:20	Signal Strength > -80dbm	Unknown	-
No	Suspected Rogue	5	Unknown Lo-70:2C:D8	Signal Strength > -80dbm	Suspected Neighbor	1344-1-AL19 (1344-1-al19.arubanetw
No	Suspected Rogue	5	Aruba-16:4F:04	Signal Strength > -80dbm	Unknown	-
No	Suspected Rogue	5	Cisco-Link-EC:C1:0C	Signal Strength > -80dbm	Unknown	-
No	Suspected Rogue	5	Silex Tech-45:BA:EC	Signal Strength > -80dbm	Suspected Neighbor	-
No	Suspected Rogue	5	Novatel Wi-17:5A:B5	Signal Strength > -80dbm	Suspected Neighbor	AP105-1

1-10 of 1,698 Rogue APs Page 1 of 170 > >| Reset filters

View Ignored Rogues

Table 102 details the column information displayed in Figure 120. For additional information about RAPIDS rules, refer to "Defining RAPIDS Rules" on page 202.

Table 102: *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** link at the top of the **RAPIDS > List** page. Rogues should be acknowledged when the AMP user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 199).
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 203. The threat level is also supported with Triggers (see "Monitoring and Supporting AMP with the System Pages" on page 214).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, AMP assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. Clicking the linked name will redirect you to the **RAPIDS > Detail** page for that rogue device. Refer to "Overview of the RAPIDS > Detail Page" on page 210.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 203).
Controller Classification	Displays the classification of the device based on the controller's hard-coded rules. **NOTE:** This column is hidden unless **Offload WMS Database** is enabled by at least one group on the **Groups > Basic** page.
WMS Classification AP	The AP that provided the information used to classify the device. Click the linked device name to be redirected to the **APs/Devices > Monitor** page for that AP.
WMS Classification Date	The date that WMS set the classification.
Confidence	The confidence level of the suspected rogue. How confidence is calculated varies based on the version of ArubaOS. When an ArubaOS controller sees evidence that a device might be on the wire, it will up the confidence level. If ArubaOS is completely certain that it is on the wire, it gets classified as a rogue.
Wired	Displays whether the rogue device has been discovered on one of your wired networks by polling routers/switches, your SNMP/HTTP scans, or Aruba WIP information. This column displays **Yes** or is blank if wired information was not detected.
Detecting APs	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	If the rogue has been placed in VisualRF, this column will display the name of the floor plan the rogue is on as a link to the VisualRF Floor Plan View page.

Table 102: *RAPIDS > List Column Definitions (Continued)*

Column	Description
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: ● **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, 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. Possible contents of this field include the following encryption types: ● **Open**–No encryption ● **WEP**–Wired Equivalent Privacy ● **WPA**–Wi-Fi Protected Access 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.
Ch	Indicates the most recent RF channel on which the rogue was detected. **NOTE:** It can be detected on more than one channel if it contains more than one radio.
LAN MAC Address	The LAN MAC address of the rogue device.
LAN Vendor	Indicates the LAN vendor of the rogue device, when known.
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Indicates the radio vendor of the rogue device, when known.
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 is 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 AMP. Click the linked device name to be redirected to the **APs/Devices > Monitor** page for that AP.
Switch/Router	Displays the switch or router where the device's LAN MAC address was last seen.

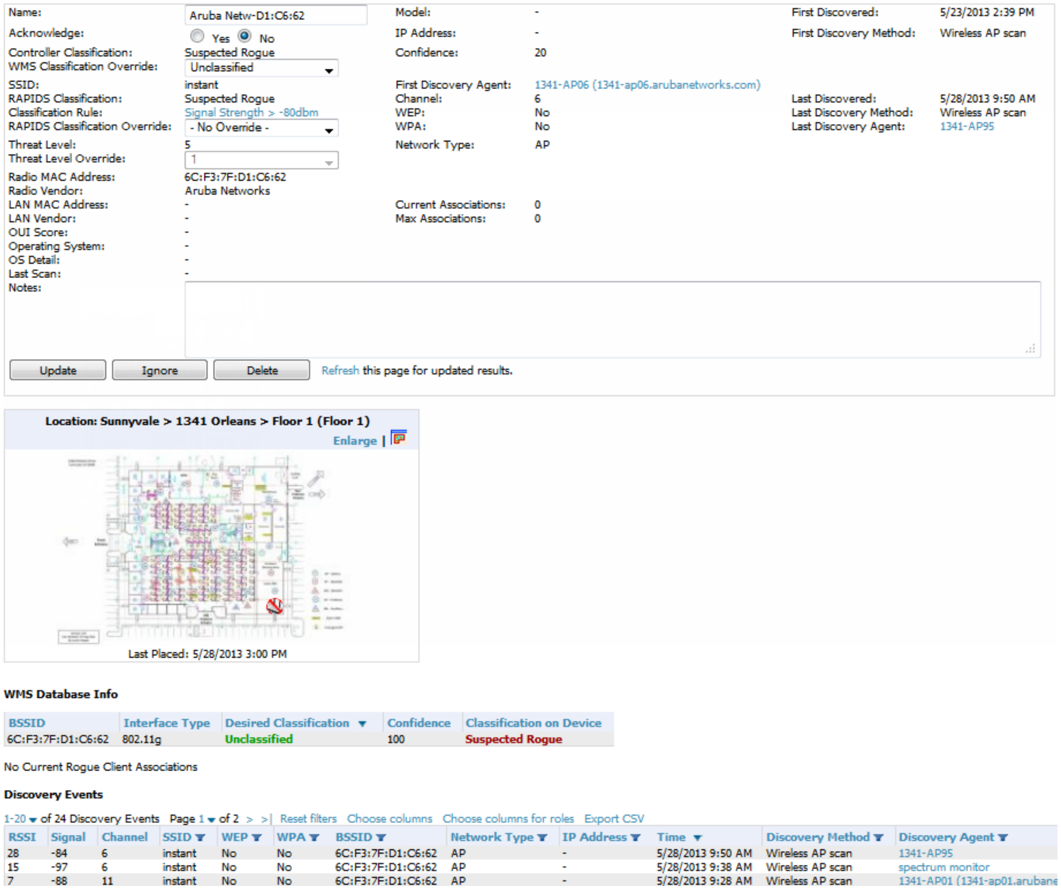
Table 102: *RAPIDS > List Column Definitions (Continued)*

Column	Description
Port	Indicates the physical port of the switch or router where the rogue was last seen.
Notes	Indicates any notes about the rogue device that may have been added.
Last Seen	Indicates the date and time the rogue device was last seen.
Current Associations	The number of current rogue client associations to this device.
Max associations	The highest number of rogue client associations ever detected at one time.

Overview of the RAPIDS > Detail Page

Select a device Name in the **RAPIDS** > **List** page to view the **Detail** page (Figure 121).

Figure 121 *RAPIDS > Detail Page Illustration*



Name:	Aruba Netw-D1:C6:62	Model:	-	First Discovered:	5/23/2013 2:39 PM
Acknowledge:	○ Yes ● No	IP Address:	-	First Discovery Method:	Wireless AP scan
Controller Classification:	Suspected Rogue	Confidence:	20		
WMS Classification Override:	Unclassified				
SSID:	instant	First Discovery Agent:	1341-AP06 (1341-ap06.arubanetworks.com)		
RAPIDS Classification:	Suspected Rogue	Channel:	6	Last Discovered:	5/28/2013 9:50 AM
Classification Rule:	Signal Strength > -80dbm	WEP:	No	Last Discovery Method:	Wireless AP scan
RAPIDS Classification Override:	- No Override -	WPA:	No	Last Discovery Agent:	1341-AP95
Threat Level:	5	Network Type:	AP		
Threat Level Override:	1				
Radio MAC Address:	6C:F3:7F:D1:C6:62				
Radio Vendor:	Aruba Networks				
LAN MAC Address:	-	Current Associations:	0		
LAN Vendor:	-	Max Associations:	0		
OUI Score:	-				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				
Notes:					

Refresh this page for updated results.

Location: Sunnyvale > 1341 Orleans > Floor 1 (Floor 1)

Last Placed: 5/28/2013 3:00 PM

WMS Database Info

BSSID	Interface Type	Desired Classification	Confidence	Classification on Device
6C:F3:7F:D1:C6:62	802.11g	Unclassified	100	Suspected Rogue

No Current Rogue Client Associations

Discovery Events

1-20 of 24 Discovery Events Page 1 of 2 > >| Reset filters Choose columns Choose columns for roles Export CSV

RSSI	Signal	Channel	SSID	WEP	WPA	BSSID	Network Type	IP Address	Time	Discovery Method	Discovery Agent
28	-84	6	instant	No	No	6C:F3:7F:D1:C6:62	AP	-	5/28/2013 9:50 AM	Wireless AP scan	1341-AP95
15	-97	6	instant	No	No	6C:F3:7F:D1:C6:62	AP	-	5/28/2013 9:38 AM	Wireless AP scan	spectrum monitor
7	-88	11	instant	No	No	6C:F3:7F:D1:C6:62	AP	-	5/28/2013 9:28 AM	Wireless AP scan	1341-AP01 (1341-ap01.arubane

Important things to remember regarding the information in the device detail page are:

- Users with the role of **Admin** can see all rogue AP devices.
- Active rogue clients associated with this AP are listed in the **Current Rogue Client Associations** table. Selecting a linked MAC address will take you to the **Clients** > **Client Detail** page, where you can view fingerprinting and device details.

- Users with roles limited by folder can *see* a rogue AP if there is at least one discovering device that they can see.
- The discovery events displayed are from APs that you can see on the network. There may be additional discovery events that remain hidden to certain user roles.
- Each rogue device frequently has multiple discovery methods, all of which are listed.
- As you work through the rogue devices, use the **Name** and **Notes** fields to identify the AP and document its location.
- You can use the global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.
- VisualRF uses the heard signal information to calculate the physical location of the device.
- If the device is seen on the wire, RAPIDS reports the switch and port for easy isolation.
- If you find that the rogue belongs to a neighboring business, for example, you can override the classification to a neighbor and acknowledge the device. Otherwise, it is strongly recommended that you extract the device from your building and delete the rogue device from your system. If you delete a rogue, you will be notified the next time it is discovered.
- Most columns in the **Discovery Events** list table on this page can be filtered using the funnel icon (▼).

To update a rogue device:

1. Select the **Identify OS for Suspected Rogues** option if an IP address is available to obtain operating system information using an nmap scan. Note that if you are running wireline security software on your network, it may identify your AMP as a threat, which you can ignore.
2. Select the **Ignore** button if the rogue device is to be ignored. Ignored devices will not trigger alerts if they are rediscovered or reclassified.
3. Select the **Delete** button if the rogue device is to be removed from AMP 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 AMP. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, select **View Ignored Rogues** at the bottom left of the page.

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. AMP performs a port scan on the device and attempts to determine the operating system. (See "Setting Up RAPIDS" on page 199.)

  You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.
- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To manage the rogue, remove it from the network and acknowledge the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.

NOTE

Not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

Score Override

On the **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 122, Figure 123, and Table 103 illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

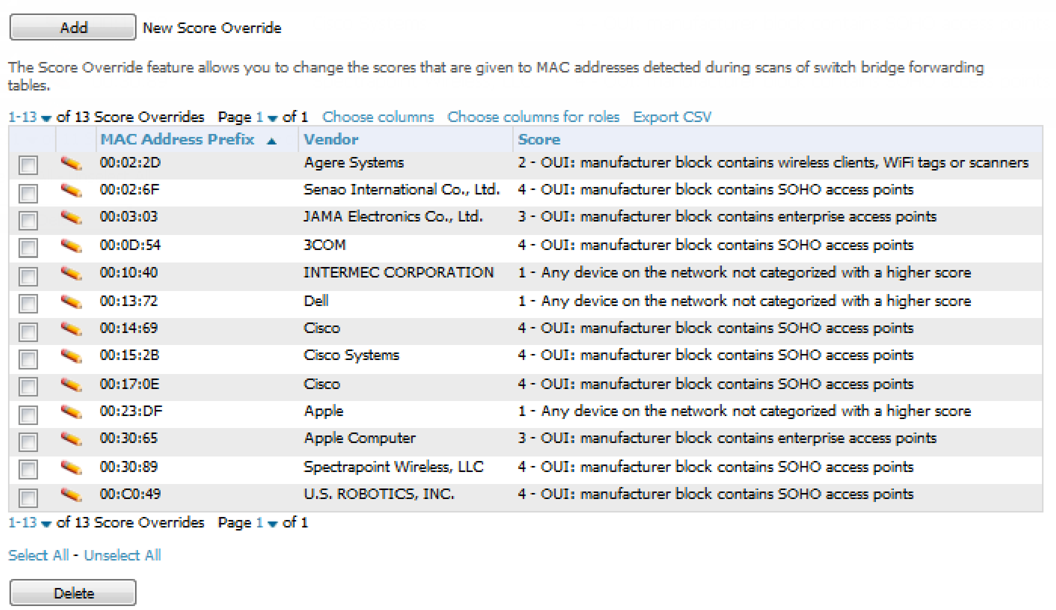
Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.

NOTE

Note that re-scoring 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 122 *RAPIDS > Score Override Page*



Add New Score Override

The Score Override feature allows you to change the scores that are given to MAC addresses detected during scans of switch bridge forwarding tables.

1-13 ▾ of 13 Score Overrides Page 1 ▾ of 1 Choose columns Choose columns for roles Export CSV

		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
□	✎	00:17:0E	Cisco	4 - OUI: manufacturer block contains SOHO access points
□	✎	00:23:DF	Apple	1 - Any device on the network not categorized with a higher score
□	✎	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:C0:49	U.S. ROBOTICS, INC.	4 - OUI: manufacturer block contains SOHO access points

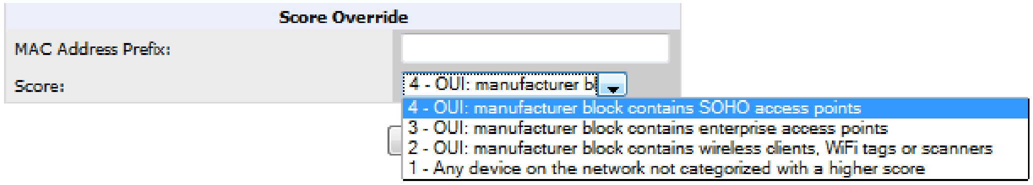
1-13 ▾ of 13 Score Overrides Page 1 ▾ of 1

Select All - Unselect All

Delete

2. Click **Add** to create a new override or select the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears (Figure 123).

Figure 123 *Add/Edit Score Override Page*



Score Override	
MAC Address Prefix:	
Score:	4 - OUI: manufacturer bl ▾

4 - OUI: manufacturer block contains SOHO access points
3 - OUI: manufacturer block contains enterprise access points
2 - OUI: manufacturer block contains wireless clients, WiFi tags or scanners
1 - Any device on the network not categorized with a higher score

Table 103: *RAPIDS > Add/Edit Score Override Page Fields*

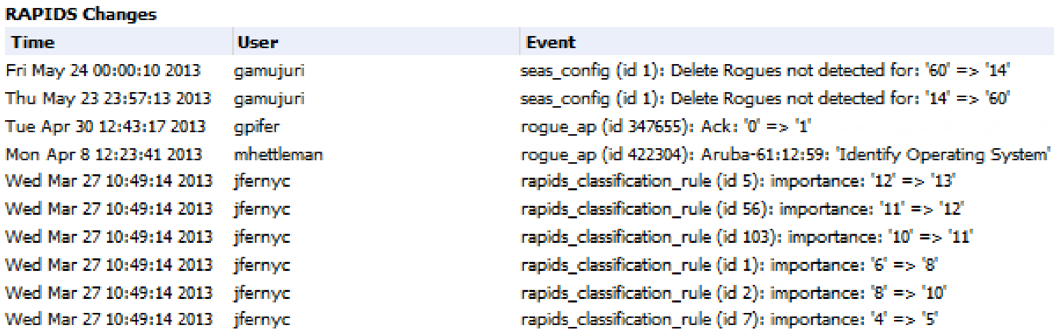
Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

3. Enter in the six-digit MAC prefix for which to define a score, and select the desired score. Once the new score has been saved, all detected devices with that prefix receive the new score.
4. 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 check box, and then click the **Delete** button.

Using the Audit Log

The Audit Log is a record of any changes made to the RAPIDS rules, setup page, and manual changes to specific rogues. This allows you to see how something is changes, when it changed, and who made the alteration. The Audit Log can be found at **RAPIDS > Audit Log**. For more information, see Figure 124.

Figure 124 *Audit Log Page Illustration*



RAPIDS Changes

Time	User	Event
Fri May 24 00:00:10 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '60' => '14'
Thu May 23 23:57:13 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '14' => '60'
Tue Apr 30 12:43:17 2013	gpifer	rogue_ap (id 347655): Ack: '0' => '1'
Mon Apr 8 12:23:41 2013	mhettleman	rogue_ap (id 422304): Aruba-61:12:59: 'Identify Operating System'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 5): importance: '12' => '13'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 56): importance: '11' => '12'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 103): importance: '10' => '11'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 1): importance: '6' => '8'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 2): importance: '8' => '10'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 7): importance: '4' => '5'

Additional Resources

The following AMP tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to "Viewing, Delivering, and Responding to Triggers and Alerts" on page 226.
- **Reports**—The **New Rogue Devices Report** displays summary and detail information about all rogues first discovered in a given time period. For more information, see "Using the New Rogue Devices Report" on page 302.

For additional security-related features and functions, see the following topics in this guide.

- "Configuring Group Security Settings" on page 91
- "Configuring Cisco WLC Security Parameters and Functions" on page 109
- "Configuring Group SSIDs and VLANs" on page 95
- "Monitoring and Supporting AMP with the System Pages" on page 214

Daily WLAN administration often entails network monitoring, supporting WLAN and AMP users, and monitoring AMP system operations.

This chapter contains the following administration procedures:

- "Monitoring and Supporting AMP with the System Pages" on page 214
- "Monitoring and Supporting WLAN Clients" on page 235
- "Evaluating and Diagnosing User Status and Issues" on page 246
- "Managing Mobile Devices with SOTI MobiControl and AirWave " on page 251
- "Monitoring and Supporting AMP with the Home Pages" on page 252
- "Supporting AMP Servers with the Master Console" on page 265
- "Backing Up AirWave" on page 229
- "Using AirWave Failover for Backup" on page 268
- "Logging out of AirWave" on page 270

Monitoring and Supporting AMP with the System Pages

The **System** pages provide a centralized location for system-wide AMP data and settings. Apart from **Triggers**, **Alerts**, and **Backups** pages that are described elsewhere in this chapter, the remaining pages of the **System** section are as follows:

Table 104: *System pages*

System Page	Description	Refer to
Status	Displays status of all AMP services and links to their log pages.	"Using the System > Status Page" on page 215
Syslog & Traps	Displays all syslog messages and SNMP traps that AMP receives.	"Viewing Device Events in System > Syslog & Traps" on page 216
Event Log	This useful debugging tool keeps a list of recent AMP events, including APs coming up and down, services restarting, and most AMP-related errors as well as the user that initiated the action.	"Using the System > Event Log Page" on page 218
Triggers	View and edit triggering conditions that cause AMP to send out alert notifications.	"Viewing, Delivering, and Responding to Triggers and Alerts" on page 226
Alerts	View or acknowledge alerts sent out by the system and use the Triggering Agent links to drill down to the device that triggered the alert.	"Viewing Alerts" on page 227
Backups	View the backup files that are run nightly.	"Backing Up AirWave" on page 229
Configuration Change Jobs	Manages configuration changes in AMP.	"Using the System > Configuration Change Jobs Page" on page 230

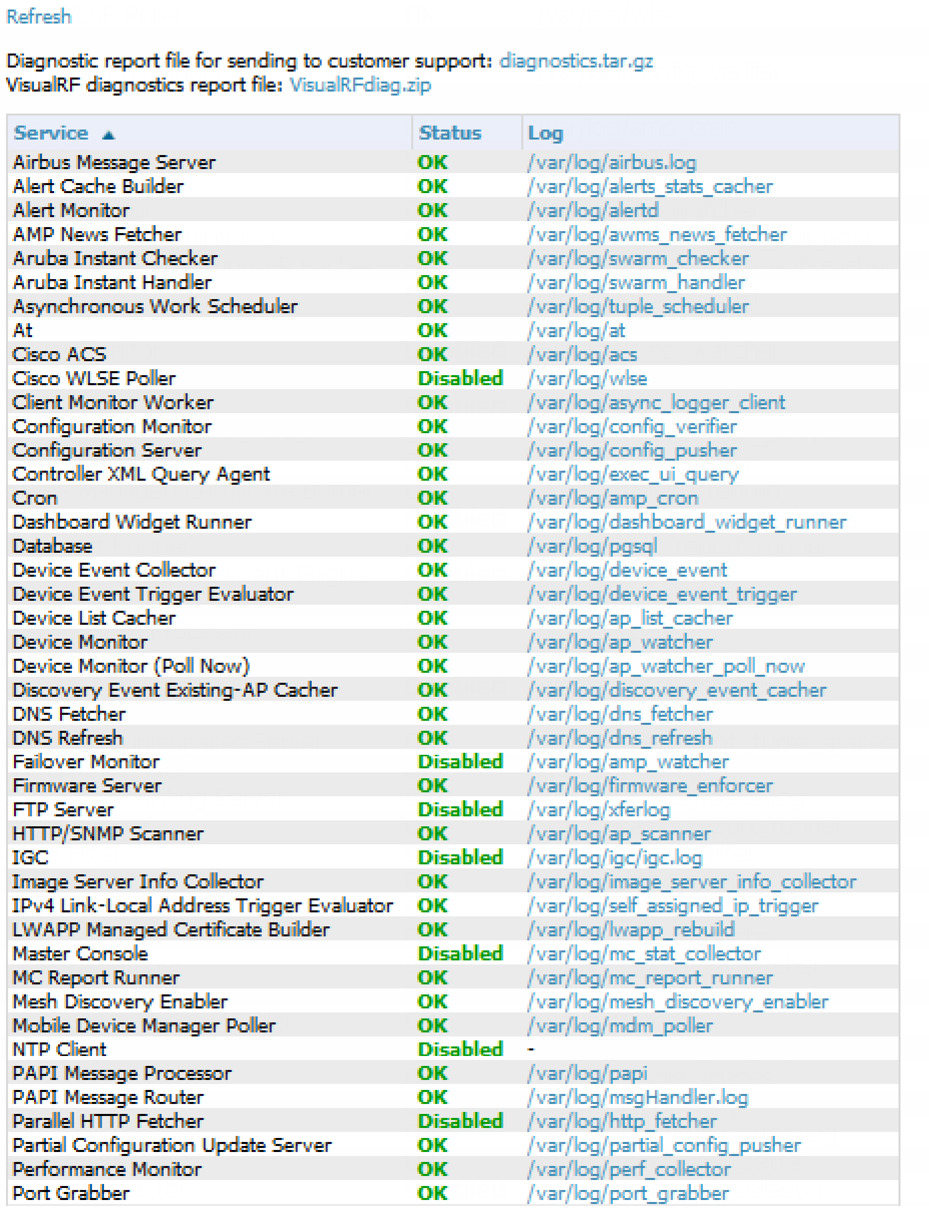
Table 104: *System pages (Continued)*

System Page	Description	Refer to
Firmware Upgrade Jobs	Displays information about current and scheduled firmware upgrades.	"Using the System > Firmware Upgrade Jobs Page" on page 231
Performance	Displays basic AMP hardware information as well as resource usage over time.	"Using the System > Performance Page" on page 232

Using the System > Status Page

The **System** > **Status** page displays the status of all of AMP services. Services will either be **OK**, **Disabled**, or **Down**. If any service is **Down** (displayed in red) please contact Aruba support. The **Reboot System** button provides a graceful way to power cycle your AMP remotely when it is needed. The **Restart AMP** button will restart the AMP services without power cycling the server or reloading the OS. Figure 125 illustrates this page.

Figure 125 *System > Status Page Illustration*



Refresh

Diagnostic report file for sending to customer support: diagnostics.tar.gz
VisualRF diagnostics report file: VisualRFdiag.zip

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
AMP News Fetcher	OK	/var/log/awms_news_fetcher
Aruba Instant Checker	OK	/var/log/swarm_checker
Aruba Instant Handler	OK	/var/log/swarm_handler
Asynchronous Work Scheduler	OK	/var/log/tuple_scheduler
At	OK	/var/log/at
Cisco ACS	OK	/var/log/acs
Cisco WLSE Poller	Disabled	/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
Controller XML Query Agent	OK	/var/log/exec_ui_query
Cron	OK	/var/log/amp_cron
Dashboard Widget Runner	OK	/var/log/dashboard_widget_runner
Database	OK	/var/log/pgsql
Device Event Collector	OK	/var/log/device_event
Device Event Trigger Evaluator	OK	/var/log/device_event_trigger
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
Failover Monitor	Disabled	/var/log/amp_watcher
Firmware Server	OK	/var/log/firmware_enforcer
FTP Server	Disabled	/var/log/xferlog
HTTP/SNMP Scanner	OK	/var/log/ap_scanner
IGC	Disabled	/var/log/igc/igc.log
Image Server Info Collector	OK	/var/log/image_server_info_collector
IPv4 Link-Local Address Trigger Evaluator	OK	/var/log/self_assigned_ip_trigger
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
Mesh Discovery Enabler	OK	/var/log/mesh_discovery_enabler
Mobile Device Manager Poller	OK	/var/log/mdm_poller
NTP Client	Disabled	-
PAPI Message Processor	OK	/var/log/papi
PAPI Message Router	OK	/var/log/msgHandler.log
Parallel HTTP Fetcher	Disabled	/var/log/http_fetcher
Partial Configuration Update Server	OK	/var/log/partial_config_pusher
Performance Monitor	OK	/var/log/perf_collector
Port Grabber	OK	/var/log/port_grabber

The link **diagnostics.tar.gz** contains reports and logs that are helpful to Aruba support in troubleshooting and solving problems. Your Aruba support representative may ask for this file along with other logs that are linked on this page.

Similarly, the **VisualRFdiag.zip** link contains VisualRF diagnostic information that might be requested by Aruba support.

A summary table lists logs that appear on the **System** > **Status** page. These are used to diagnose AMP problems. Additional logs are available via SSH access in the /var/log and /tmp directories; Aruba support engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them. Table 105 describes some of the most important logs:

Table 105: *A Sample of Important Status Logs*

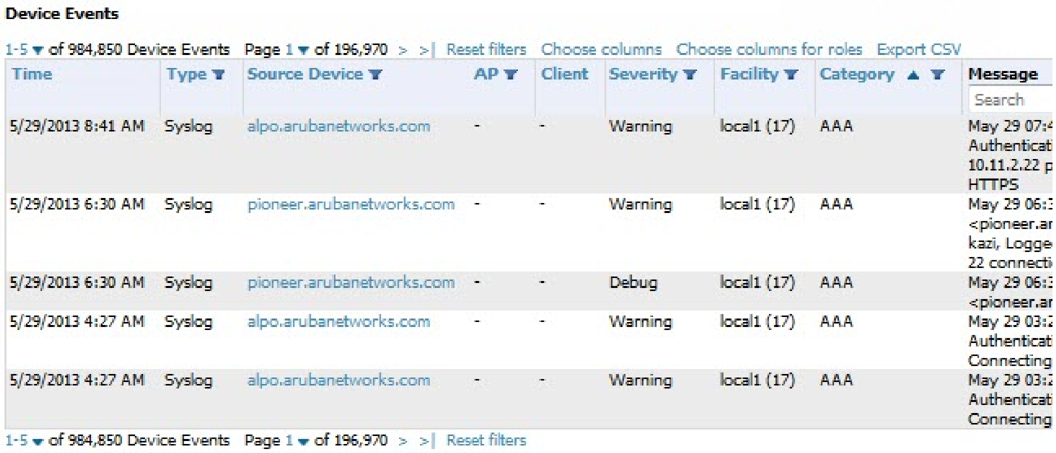
Log	Description
pgsql	Logs database activity.
error_log	Reports problems with the web server. Also linked from the internal server error page that displays on the web page; please send this log to Aruba support whenever reporting an internal server error.
maillog	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
radius	Displays error messages associated with RADIUS accounting.
async_logger	Tracks many device monitoring processes, including user-AP association.
async_logger_client	Logs device configuration checks.
config_pusher	Logs errors in pushing configuration to devices.
visualrf.log	Details errors and messages associated with the VisualRF application.

Viewing Device Events in System > Syslog & Traps

Admins can use the **System** > **Syslog & Traps** page to review all syslog messages and SNMP traps that AMP receives from the trigger type **Device Event**. These device events are listed by time, type, source device, AP, severity, facility, category, and message. Most columns can be filtered using the funnel icon (▼), and messages can be filtered by substring using the **Search** field, as seen in Figure 126.

You can change the historical data retention from the **Device Events (Syslog, Traps)** field in **AMP Setup** > **General**.

Figure 126 *System > Syslog & Traps Page Illustration*



Device Events

1-5 ▾ of 984,850 Device Events   Page 1 ▾ of 196,970 > >| Reset filters   Choose columns   Choose columns for roles   Export CSV

Time	Type	Source Device	AP	Client	Severity	Facility	Category ▲	Message
								Search
5/29/2013 8:41 AM	Syslog	alpo.arubanetworks.com	-	-	Warning	local1 (17)	AAA	May 29 07:4 Authenticati 10.11.2.22 p HTTPS
5/29/2013 6:30 AM	Syslog	pioneer.arubanetworks.com	-	-	Warning	local1 (17)	AAA	May 29 06:3 <pioneer.ar kazi, Logge 22 connecti
5/29/2013 6:30 AM	Syslog	pioneer.arubanetworks.com	-	-	Debug	local1 (17)	AAA	May 29 06:3 <pioneer.ar
5/29/2013 4:27 AM	Syslog	alpo.arubanetworks.com	-	-	Warning	local1 (17)	AAA	May 29 03:2 Authenticati Connecting
5/29/2013 4:27 AM	Syslog	alpo.arubanetworks.com	-	-	Warning	local1 (17)	AAA	May 29 03:2 Authenticati Connecting

1-5 ▾ of 984,850 Device Events   Page 1 ▾ of 196,970 > >| Reset filters

Table 106 describes the columns and the information provided in each:

Table 106: *System > Syslog & Traps Columns and Descriptions*

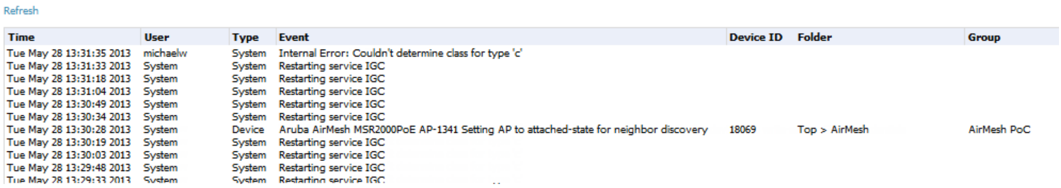
Column	Description
Time	The timestamp of the device event.
Type	Either Syslog or SNMP Trap.
Source Device	The name of the device that sent the message. Will be a link if you have visibility to the device. Can be empty if AMP could not correlate the source IP.
AP	Contains a link to the **APs/Devices > Monitor** page for a device other than the source device that was correlated from some data contained in the message (by LAN MAC, BSSID, or IP Address). Can be blank, and will only be a link if you have visibility to the device.
Client	Displays a user's MAC address if one was found in the message. Can be blank, and will be a link if you have visibility to the user's AP.
Severity	The severity level of the event: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info
Facility	Part of the syslog spec - sort of the logical source of the message. From controllers, will always be one of local0-local7 (you can configure on the controller when sending syslog messages to a particular receiver which facility you want to use in the messages).
Category	If SNMP Trap: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection. For Syslog messages, a category is based on the process name on the controller that sent the syslog message. The categorization for traps and syslog messages only works for events from an Aruba controller.
Message	The raw trap message including the AP MAC Address, time sent, and other information. For syslogs, AMP does not display the numbers at the beginning of the message that indicate the severity and facility. For traps, AMP will attempt to translate them to human-readable format when possible. AMP will not receive processed SNMP traps into the Device Event framework if the AMP doesn't have MIB file to translate the trap. Use the Search field at the top of the column to filter the messages.

Syslog messages also appear in the **APs/Devices** > **Monitor** page for controllers and in **Clients** > **Client Detail** pages under the **Association History** section.

Using the System > Event Log Page

The **System** > **Event Log** page is a very useful debugging tool containing a list of recent AMP events including APs coming up and down, services restarting, and most AMP-related errors as well as the user that initiated the action. Figure 127 illustrates this page, and Table 107 describes the page components.

Figure 127 ***System* > *Event Log*** *Page Illustration*



Refresh

Time	User	Type	Event	Device ID	Folder	Group
Tue May 28 13:31:35 2013	michaelw	System	Internal Error: Couldn't determine class for type 'c'			
Tue May 28 13:31:33 2013	System	System	Restarting service IGC			
Tue May 28 13:31:18 2013	System	System	Restarting service IGC			
Tue May 28 13:31:04 2013	System	System	Restarting service IGC			
Tue May 28 13:30:49 2013	System	System	Restarting service IGC			
Tue May 28 13:30:34 2013	System	System	Restarting service IGC			
Tue May 28 13:30:28 2013	System	Device	Aruba AirMesh MSR2000PoE AP-1341 Setting AP to attached-state for neighbor discovery	18069	Top > AirMesh	AirMesh PoC
Tue May 28 13:30:19 2013	System	System	Restarting service IGC			
Tue May 28 13:30:03 2013	System	System	Restarting service IGC			
Tue May 28 13:29:48 2013	System	System	Restarting service IGC			
Tue May 28 13:29:33 2013	System	System	Restarting service IGC			

Table 107: *Event Log Fields*

Column	Description
Time	Date and time of the event.
User	The AMP user that triggered the event. When AMP itself is responsible, **System** is displayed.
Type	Displays the Type of event recorded, which is one of four types, as follows: ● **Device**–An event localized to one specific device. ● **Group**–A group-wide event. ● **System**–A system-wide event. ● NMS–An event triggered by an NMS server. (See "Integrating AMP with an Existing Network Management Solution (NMS) " on page 70 for more info.) ● **Alert**–If a trigger is configured to report to the log, an **Alert** type event will be logged here.
Event	The event that AMP observed. This information can be useful for debugging, user tracking, and change tracking.
Device ID	If the event is a Device event, then this column shows the device ID.
Folder	If the event is a Device event, this column shows the folder where the device resides.
Group	If the event is a Device event, this column shows the Group in which the device resides.

Triggers and Alerts

AMP monitors key aspects of wireless LAN performance. When certain conditions or parameters arise that are outside of normal bounds, AMP generates (or triggers) alerts that enable you to address problems, often before users have a chance to report them.

All triggers include an option to configure a Severity Level. This level is tied to the Severe Alert Threshold, which is configured on the **Home** > **User Info** page. This threshold value specifies whether triggers categorized as Critical, Major, Minor, Warning, or Normal will result in a Severe Alert. If a trigger is defined to result in a Critical alert, and if the Severe Alert Threshold is defined as Major, then the list of Severe Alerts will include all Major and Critical alerts. Similarly, if this value is set to Normal, which is the lowest threshold, then the list of Severe Alerts will include all alerts.

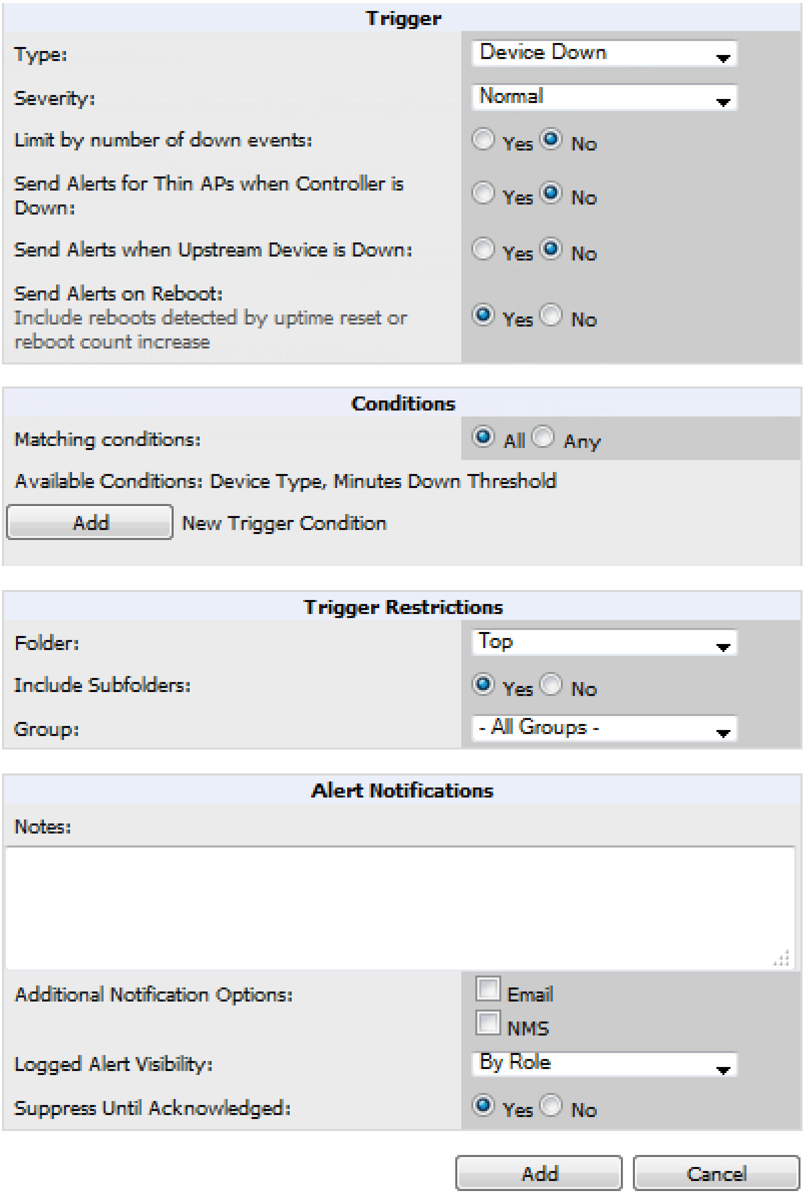
Refer to "Creating New Triggers" on page 219 to configure triggers.

Creating New Triggers

Perform the following steps to create and configure one or more new triggers. These steps define settings that are required for any type of trigger.

1. To create a new trigger, select the **Add New Trigger** button from the **System** > **Triggers** page. The page that appears is illustrated in Figure 128.

Figure 128 *Add New Trigger Page Illustration*



Trigger

Type:	Device Down
Severity:	Normal
Limit by number of down events:	○ Yes ● No
Send Alerts for Thin APs when Controller is Down:	○ Yes ● No
Send Alerts when Upstream Device is Down:	○ Yes ● No
Send Alerts on Reboot: Include reboots detected by uptime reset or reboot count increase	● Yes ○ No

Conditions

Matching conditions:	● All ○ Any

Available Conditions: Device Type, Minutes Down Threshold

Add New Trigger Condition

Trigger Restrictions

Folder:	Top
Include Subfolders:	● Yes ○ No
Group:	- All Groups -

Alert Notifications

Notes:

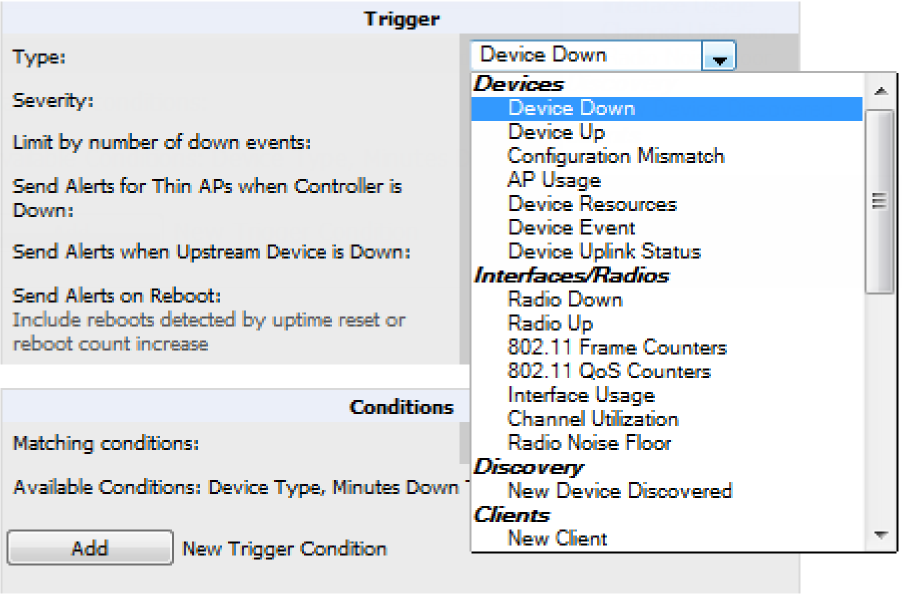
Additional Notification Options:	□ Email □ NMS
Logged Alert Visibility:	By Role
Suppress Until Acknowledged:	● Yes ○ No

2. In the **Trigger** section, choose the desired trigger **Type** and **Severity**. Figure 129 illustrates some of the supported trigger types.

NOTE

The alert summary information at the top of the AMP screen can be configured to separately display severe alerts. Refer to "Configuring Your Own User Information with the Home > User Info Page" on page 263 for more details.

Figure 129 *System > Triggers > Add Trigger Type Drop Down Menu*



The **Add Trigger** page changes depending on the trigger type that you select. In many cases, you must configure at least one **Condition** setting. Conditions, settings and default values vary according to trigger type. Triggers with conditions can be configured to fire if any criteria match as well as if all criteria match.

- Some trigger types share common settings, such as **Duration** (which can be expressed in hours, minutes, seconds, or a combination of these) and **Severity** (from Normal to Critical).
- After you select **Save**, the trigger appears on your next viewing of the **System** > **Triggers** page with all other active triggers.
- You can edit or delete any trigger as desired from the **System** > **Triggers** page.
  - To edit an existing trigger, select the **pencil** icon next to the respective trigger and edit settings in the **Trigger Detail** page described in .
  - To delete a trigger, check the box next to the trigger to remove, and select **Delete**.

3. Configure the **Trigger Restrictions** and **Alert Notifications**. This configuration is consistent regardless of the trigger type to be defined.

   a. The **Trigger Restrictions** settings establishes how widely or how narrowly the trigger applies. Define the folder, subfolder, and Group covered by this trigger. Table 108 describes the options for trigger restrictions.

Table 108: *System > Trigger Restrictions 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. The **Alert Notifications** settings section allows you to enter a note that will be included with the alert. This note will appear with the alert on the **System > Alerts** page. The **Alert Notification** section also allows you to specify whether the alert will be distributed via email, to a network management system (NMS), or to both.

- If you select **Email**, you are prompted to set the sender and recipient email addresses.
- If you select **NMS**, you are prompted to choose one or more of the pre-defined trap destinations, which are configured on the **AMP Setup >NMS** page. Note that this option is only available if an NMS server has been added to AMP.
- 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 acknowledgment to gain visibility. If **No**, a new alert will be created every time the trigger criteria are met. If **Yes**, an alert will only be received the first time the criteria is met. A new alert for the device is not created until the initial one is acknowledged.

Repeat this procedure for as many triggers and conditions as desired.

Complete the creation of your trigger type using one of the following procedures for each trigger:

- "Setting Triggers for Devices" on page 221
- "Setting Triggers for Interfaces and Radios" on page 222
- "Setting Triggers for Discovery" on page 223
- "Setting Triggers for Clients" on page 224
- "Setting Triggers for RADIUS Authentication Issues" on page 225
- "Setting Triggers for IDS Events" on page 225
- "Setting Triggers for AMP Health" on page 226

Setting Triggers for Devices

Perform the following steps to configure device-related triggers.

1. Choose a device type from the **Devices** listed in the **Type** drop-down menu. See Figure 129 in "Creating New Triggers" on page 219. Table 109 itemizes and describes device trigger options and condition settings.

Table 109: *Device Trigger types*

Trigger Option	Description
Device Down	This is the default type whenever configuring a new trigger. This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from AMP. To set the conditions for this trigger type, select **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. Triggers with the **Minutes Down** condition enabled will compare the amount of time an AP has been down to the value (in minutes) set for the condition. When the **Limit by number of down events** is enabled, you can set the number of down events that activate the trigger, as well as the duration of the time window to be measured. AMP will then count the number of times that the device has gone from Up to Down in the specified span of time and display this in the Device Down alert.
Device Up	This trigger type activates when an authorized, previously down AP is now responding to

Table 109: *Device Trigger types (Continued)*

Trigger Option	Description
	SNMP queries. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
Configuration Mismatch	This trigger type activates when the actual configuration on the AP does not match the defined **Group** configuration policy. To set the conditions for this trigger type, select **Add** in the **Conditions** section.
AP Usage	Activates when the total bandwidth through the device has exceeded a predefined threshold for more than a specified period (such as more than 1500 Kbps for more than 120 seconds). You can also select bandwidth direction and page/radio. Selecting this type displays the following new fields in the **Type** section. Define these settings. ● **Alert if AP Usage >= (Kbps)**–This threshold establishes a device-specific bandwidth policy, not a bandwidth policy on the network as a whole. ● **Usage Direction**–Choose **In**, **Out**, or **Combined**. This bandwidth is monitored on the device itself, not on the network as a whole. ● **Severity** - Specify the severity type for the trigger. ● **Duration** - Specify the time frame for the trigger.
Device Resources	This type of trigger indicates that the CPU or memory utilization for a device (including router or switch) has exceeded a defined percentage for a specified period of time.
Device Event	This trigger is used for alerting based on SNMP traps and syslog messages, which are displayed in **System > Syslogs & Traps**, **APs/Devices > Monitor** for affected devices, and in **Clients > Client Detail.** The conditions supported are: ● **Event Contents** (case insensitive substring matches on message content) ● **Event Type** (syslog or trap) ● **Syslog Severity**: Emergency, Alert, Critical, Bug, Error, Warning, Notice, or Info ● Syslog Category ● **SNMP Trap Category**: Hardware, IDS, Client Security, AP Security, AP Status, Software, or Rogue Detection ● **Syslog Category** **NOTE:** During the process of upgrading or installation for non-Master Console/Failover AMPs, AMP creates two default trigger definitions for Device Events: ● SNMP Trap Category of **Hardware** or **Software** ● Event Type is **Syslog** and **Syslog Severity** >= **Critical**
Device Uplink Status	This trigger deploys whenever a RAP's active uplink changes from Ethernet to USB or vice versa. The corresponding events are captured in a RAP's **APs/Devices > Monitor** page.

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Setting Triggers for Interfaces and Radios

To configure radio- and interface-related triggers, choose a trigger type from the **Interfaces/ Radios** category, listed in the **Type** drop-down menu. Table 110 itemizes and describes the radio trigger types and condition settings.

Table 110: *Interfaces/Radio-Related Trigger Types*

Radio Trigger Options	Description
Radio Down	Indicates that a device's radio is down on the network. Once you choose this trigger

Table 110: *Interfaces/Radio-Related Trigger Types (Continued)*

Radio Trigger Options	Description
	type, select **Add New Trigger Condition** to create at least one condition. **This type** requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.
Radio Up	Indicates that a device's radio is up on the network. Once you choose this trigger type, select **Add New Trigger Condition** to create at least one condition. **This type** requires that a radio capability be set as a condition. The **Value** drop-down menu supports several condition options.
802.11 Frame Counters	Enables monitoring of traffic levels. There are multiple rate-related parameters for which you define conditions including ACK Failures, Retry Rate, and Rx Fragment Rate. See the **Option** drop-down menu in the **Conditions** section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
802.11 QoS Counters	Enables monitoring of Quality of Service (QoS) parameters on the network, according to traffic type. The rate of different parameters includes ACK Failures, Duplicated Frames and Transmitted Fragments. See the drop-down field menu in the conditions section of the trigger page for a complete list of parameters. Select **Add New Trigger Condition** to access these settings. Define at least one condition for this trigger type.
Interface Usage	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**.
Channel Utilization	Indicates that channel utilization has crossed particular thresholds. Available conditions are **Interference (%)**, **Radio Type**, **Time Busy (%)**, **Time Receiving (%)**, and **Time Transmitting (%)**.
Radio Noise Floor	Indicates that the Noise Floor dBM has exceeded a certain value for aspecified period of time.

Setting Triggers for Discovery

Perform the following steps to configure triggers related to device discovery.

1. Choose a trigger type from the **Discovery** category, listed in the **Type** drop-down menu. See Figure 129 in "Creating New Triggers" on page 219.

Table 111: *Discovery Trigger Types and Condition Settings*

Discovery Trigger Options	Description
New Device Discovered	This trigger type flags the discovery of a new AP, router, or switch connected to the network (an device that AMP can monitor and configure). Once you choose this trigger type, select **Add New Trigger Condition** to specify a **Device Type** (Access Point, Controller, Remote AP, or Router/Switch)

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Setting Triggers for Clients

Perform the following steps to configure user-related triggers.

1. Choose a trigger type from the **Clients** category, listed in the **Type** drop-down menu. See Figure 129 in "Creating New Triggers" on page 219. Table 112 itemizes and describes the Client-related trigger types, and condition settings for each discovery trigger type.

Table 112: *Client Trigger Types and Condition Settings*

Client Trigger Option	Description
New Client	This trigger type indicates a new user has associated to a device within a defined set of groups or folders. A Filter on connection mode field appears to allow you to filter by **Wired** or **Wireless** clients. Note that the **New Client** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected Clients	This trigger type indicates a device (based on an input list of MAC addresses) has associated to the wireless network. It is required to define one or more MAC addresses with the field that appears.
Client Count	Activates when a device, Radio/Interface, or BSSID reaches a user-count threshold for more than a specified period (such as more than 10 users associated for more than 60 seconds).
Client Usage	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). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
New VPN User	This trigger type indicates a new VPN user has associated to a device within a defined set of groups or folders. Note that the **New VPN User** trigger type does not require the configuration of any condition settings, so the **Condition** section disappears.
Connected VPN Users	This trigger type indicates a VPN device (based on an input list of MAC addresses) has associated to the VPN network. It is required to define one or more VPN usernames with the field that appears.
VPN Session Usage	This trigger type indicates that the sustained rate of bandwidth used in an individual VPN session has exceeded a predefined threshold for more than a specified period, in seconds (such as more than 1500 Kbps for more than 120 seconds). Once you choose this trigger type, select **Add New Trigger Condition** to specify the bandwidth characteristics that triggers an alert. You can apply multiple conditions to this type of trigger. The **Value** field requires that you input a numerical figure for kilobits per second (Kbps).
Inactive Tag	This trigger type flags events in which an RFID tag has not been reported back to AMP by a controller for more than a certain number of hours. This trigger can be used to help identify inventory that might be lost or stolen. Set the time duration for this trigger type if not already completed.
IPv4 Link-Local Addresses	When enabled, this trigger checks whether the total count of self-assigned IP addresses has crossed a set threshold for clients within a selected folder or group. The alert deployed by this trigger includes a link to search for IP addresses containing 169.254.x.x.

Table 112: *Client Trigger Types and Condition Settings (Continued)*

Client Trigger Option	Description
Client Goodput	This trigger type indicates that the goodput for an individual client has exceeded a predefined threshold. Available conditions are Usage Kbps (combined), Usage Kbps (in), and Usage Kbps (out).
Client Speed	This trigger type indicates that the speed for an individual client has exceeded a predefined threshold. The available condition for this trigger is Speed Mbps.

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Setting Triggers for RADIUS Authentication Issues

Perform the following steps to configure RADIUS-related triggers.

1. Choose a trigger type from the **RADIUS Authentication Issues** list in the drop-down **Type** menu. Table 113 itemizes and describes the condition settings for each **RADIUS Authentication** trigger type.

Table 113: *RADIUS Authentication Trigger Types and Condition Settings*

Trigger Options	Description
Client RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. Select **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 user 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.

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Setting Triggers for IDS Events

Perform the following steps to configure Intrusion Detection System (IDS)-related triggers.

1. Choose the **Device IDS Events** trigger type from the drop-down **Type** menu. See Figure 129 in "Creating New Triggers" on page 219. Table 114 describes condition settings for this trigger type.

Table 114: *Device IDS Events Authentication Trigger Types and Condition Settings*

IDS Trigger Options	Description
Device IDS Events	This trigger type is based on the number of IDS events has exceeded the threshold specified as Count in the Condition within the period of time specified in seconds in Duration. Alerts can also be generated for traps based on name, category or severity. Select **Add New Trigger**

Table 114: *Device IDS Events Authentication Trigger Types and Condition Settings (Continued)*

IDS Trigger Options	Description
	Conditionto specify the count characteristics that trigger an IDS alert.
Rogue Device Classified	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 **Yes**. See "Using RAPIDS and Rogue Classification" on page 197 for more information on score definitions and discovery methods. Once you choose this trigger type, select **Add New Trigger Condition** to create one or more conditions. A condition for this trigger enables you to specify the nature of the rogue device in multiple ways.
Client on Rogue AP	This trigger type indicates that a client has associated to a rogue AP. Available conditions include rogue classification, and whether the client is valid.

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Setting Triggers for AMP Health

After completing steps 1-3 in "Creating New Triggers" on page 219, perform the following steps to configure IDS-related triggers.

1. Choose the **Disk Usage** trigger type from the drop-down **Type** menu. See Figure 129 in "Creating New Triggers" on page 219 for trigger types. Table 115 describes the condition settings for this trigger type.

Table 115: *Disk Usage Trigger and Condition Settings*

AMP Health Trigger	Description
Disk Usage	This trigger type is based on the disk usage of AMP. This type of trigger indicates that disk usage for the AMP server has met or surpassed a defined threshold. Select **Add New Trigger Condition** to specify the disk usage characteristics that trigger an alert. Set one of these triggers at **90%** so you receive a warning before AMP suffers performance degradation due to lack of disk space.

2. Repeat this procedure for as many triggers and conditions as desired. Refer to the start of "Creating New Triggers" on page 219 to create a new trigger.

Viewing, Delivering, and Responding to Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

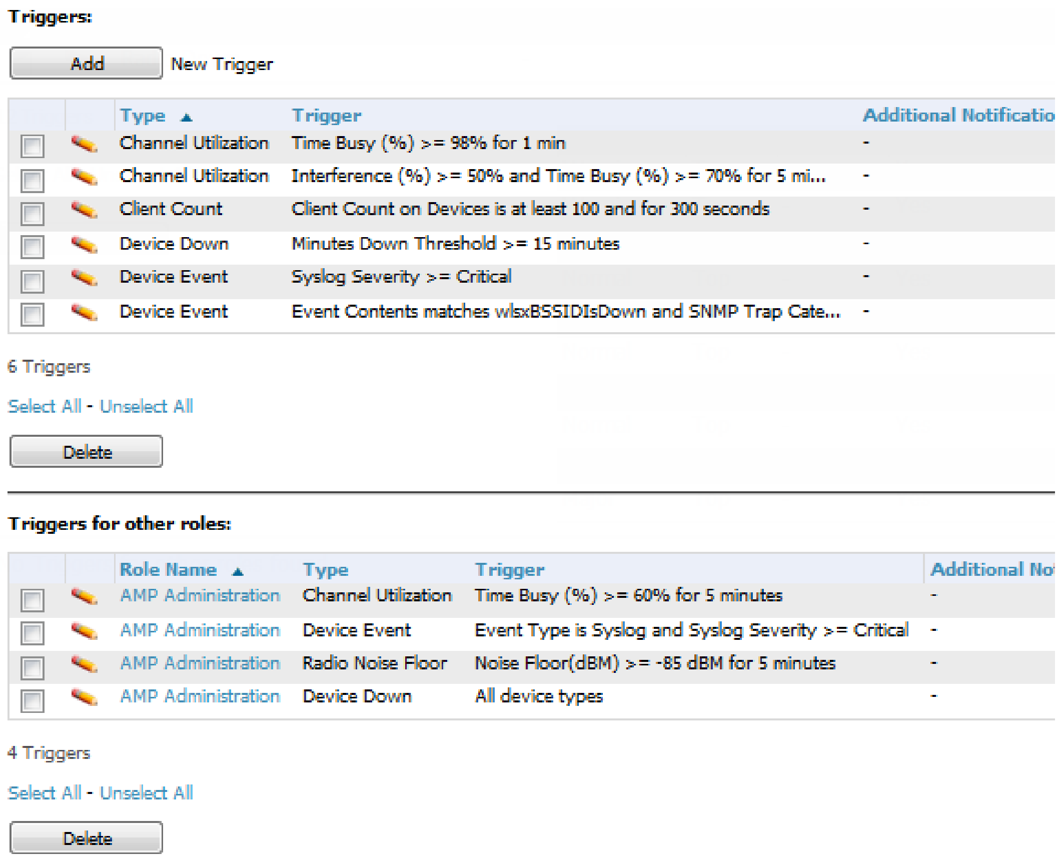
- "Viewing Triggers" on page 227
- "Delivering Triggered Alerts" on page 228
- "Viewing Alerts" on page 227
- "Responding to Alerts" on page 229

AMP monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, AMP generates (or triggers) alerts that enable you to address problems, frequently before users have a chance to report them.

Viewing Triggers

To view defined system triggers, navigate to the **System** > **Triggers** page. Figure 130 illustrates this page.

Figure 130 *System > Triggers Page Illustration (partial view)*



Triggers:

Add New Trigger

		Type ▲	Trigger	Additional Notificatio
□	✎	Channel Utilization	Time Busy (%) >= 98% for 1 min	-
□	✎	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 mi...	-
□	✎	Client Count	Client Count on Devices is at least 100 and for 300 seconds	-
□	✎	Device Down	Minutes Down Threshold >= 15 minutes	-
□	✎	Device Event	Syslog Severity >= Critical	-
□	✎	Device Event	Event Contents matches wlsxBSSIDIsDown and SNMP Trap Cate...	-

6 Triggers

Select All - Unselect All

Delete

Triggers for other roles:

		Role Name ▲	Type	Trigger	Additional No
□	✎	AMP Administration	Channel Utilization	Time Busy (%) >= 60% for 5 minutes	-
□	✎	AMP Administration	Device Event	Event Type is Syslog and Syslog Severity >= Critical	-
□	✎	AMP Administration	Radio Noise Floor	Noise Floor(dBM) >= -85 dBM for 5 minutes	-
□	✎	AMP Administration	Device Down	All device types	-

4 Triggers

Select All - Unselect All

Delete

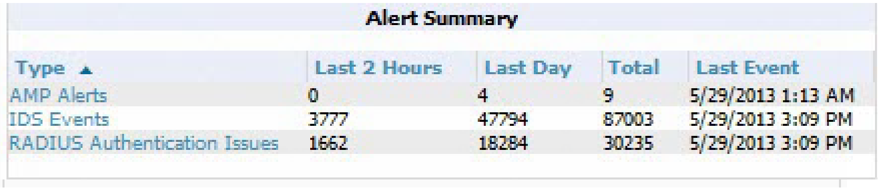
Refer to "Creating New Triggers" on page 219 for additional information.

Viewing Alerts

Apart from visiting **System** > **Alerts**, AMP displays alerts and provides alert details in two additional ways:

1. The **Alert Summary** table, and is illustrated in Figure 131, is available on the following AMP pages:
   - APs/Devices > List
   - Groups > Monitor
   - Home > Overview
   - Clients > Connected or Client Detail

Figure 131 *Alert Summary Table Illustration*



Alert Summary

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	4	9	5/29/2013 1:13 AM
IDS Events	3777	47794	87003	5/29/2013 3:09 PM
RADIUS Authentication Issues	1662	18284	30235	5/29/2013 3:09 PM

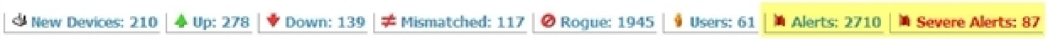
This table displays alerts as follows; select the alert **Type** to display alert details:

- **AMP Alerts**—Displays details for all device alerts.

- **IDS Events**—Displays details of all Intrusion Detection System (IDS) events and attacks under the RAPIDS tab. You must be enabled as a RAPIDS user to see this page.
- **RADIUS Authentication Issues**—Displays RADIUS-related alerts for devices in the top viewable folder available to the AMP user. The detailed list displays the MAC address, username, AP, radio, controller, RADIUS server, and time of each event. Alerts can be sorted by any column.

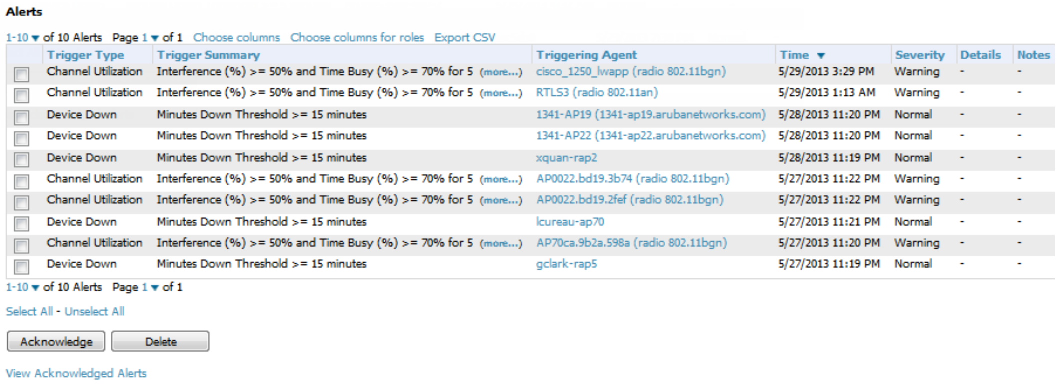
2. The **Alerts** and **Severe Alerts** top header stats in the **Status** bar at the top of all AMP pages, illustrated in Figure 132. The Severe Alert Threshold can be configured on the **Home** > **User Info** page. Refer to "Setting Severe Alert Warning Behavior" on page 27.

Figure 132 *Alerts in the AMP Status Bar (highlighted)*



Select the **Alerts** or the **Severe Alerts** counter or navigate to the **System** > **Alerts** page. "System > Alerts Page Illustration" on page 228 illustrates this page.

Figure 133 *System > Alerts Page Illustration*


Alerts

1-10 ▾ of 10 Alerts Page 1 ▾ of 1 Choose columns Choose columns for roles Export CSV

	Trigger Type	Trigger Summary	Triggering Agent	Time ▾	Severity	Details	Notes
□	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	cisco_1250_lwapp (radio 802.11bgn)	5/29/2013 3:29 PM	Warning	-	-
□	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	RTLS3 (radio 802.11an)	5/29/2013 1:13 AM	Warning	-	-
□	Device Down	Minutes Down Threshold >= 15 minutes	1341-AP19 (1341-ap19.arubanetworks.com)	5/28/2013 11:20 PM	Normal	-	-
□	Device Down	Minutes Down Threshold >= 15 minutes	1341-AP22 (1341-ap22.arubanetworks.com)	5/28/2013 11:20 PM	Normal	-	-
□	Device Down	Minutes Down Threshold >= 15 minutes	xquan-rap2	5/28/2013 11:19 PM	Normal	-	-
□	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	AP0022.bd19.3b74 (radio 802.11bgn)	5/27/2013 11:22 PM	Warning	-	-
□	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	AP0022.bd19.2fef (radio 802.11bgn)	5/27/2013 11:22 PM	Warning	-	-
□	Device Down	Minutes Down Threshold >= 15 minutes	lcureau-ap70	5/27/2013 11:21 PM	Normal	-	-
□	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	AP70ca.9b2a.598a (radio 802.11bgn)	5/27/2013 11:20 PM	Warning	-	-
□	Device Down	Minutes Down Threshold >= 15 minutes	gclark-rap5	5/27/2013 11:19 PM	Normal	-	-

1-10 ▾ of 10 Alerts Page 1 ▾ of 1

For each new alert, the **System** > **Alerts** page displays the items listed in Table 116.

Table 116: *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. Select the name to display its **APs/Devices > Manage** page.
Time	Displays the date and time the trigger was generated.
Severity	Displays the severity code associated with that trigger.
Details	Displays additional details for alerts.

Delivering Triggered Alerts

AMP uses Postfix to deliver alerts and reports via email because it provides a high level of security and queues email locally until delivery. If AMP is located behind a firewall, preventing it from sending email directly to a specified recipient, use the following procedures to forward email to a smarthost.

1. Add the following line to /etc/postfix/main.cf:

   ```
   relayhost = [mail.example.com]
   ```

   where mail.example.com is the IP address or hostname of your smarthost
2. Run **service postfix restart**.
3. Send a test message to an email address:

   ```
   Mail -v user@example.com
   Subject: test mail
   .
   CC:
   ```
4. Press **Enter**.
5. Check the mail log to ensure mail was sent:

   ```
   tail -f /var/log/maillog
   ```

Responding to Alerts

Once you have viewed an alert, you may take one of the following courses of action:

- Leave it in active status if it is unresolved. The alert remains on the **New Alerts** list until you acknowledge or delete it. If an alert already exists, the trigger for that AP or user does not create another alert until the existing alert has been acknowledged or deleted.
- Move the alert to the Alert Log by selecting it and selecting **Acknowledge**. You can see all logged alerts by selecting the **View logged alerts** link at the top of the **System** > **Alerts** page. Select the **Alerts** link to return to the list of new alerts.
- Delete the alert by selecting it from the list and clicking the **Delete** button.

Backing Up AirWave

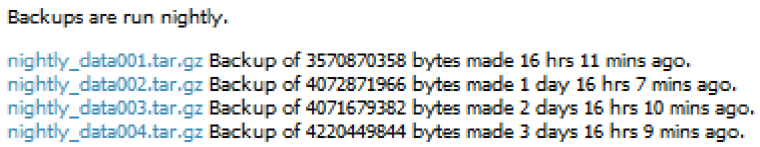
AMP creates nightly archives of all relational data, statistical data, and log files. This occurs by default at 4:15 AM, but is configurable on the **AMP Setup** > **General** page under **Nightly Maintenance Time**.

Although AMP only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. AMP creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other AMP settings.

Viewing and Downloading Backups

To view current AMP backup files, go to the **System** > **Backups** page. Figure 134 illustrates this page.

Figure 134 ***System* > *Backups*** *Page Illustration*



Backups are run nightly.

nightly_data001.tar.gz Backup of 3570870358 bytes made 16 hrs 11 mins ago.
nightly_data002.tar.gz Backup of 4072871966 bytes made 1 day 16 hrs 7 mins ago.
nightly_data003.tar.gz Backup of 4071679382 bytes made 2 days 16 hrs 10 mins ago.
nightly_data004.tar.gz Backup of 4220449844 bytes made 3 days 16 hrs 9 mins ago.

To download a backup file, select the filename URL and the **File Download** popup page appears.

Regularly save the data backup file to another machine or media. This process can be automated easily with a nightly script.

NOTE

Nightly maintenance and amp_backup scripts back up the full AMP data and save the file as nightly_data00[1-4].tar.gz. In previous AMP versions, the scripts created both config backup and data backup files. In order to restore the AMP data, it is only necessary to have most recent data backup file, and AMP no longer uses or supports the config backup file, effective as of AMP 6.3.2.

Running Backup on Demand

To create an immediate backup:

1. Log into the AMP system as **root**.
2. Run the backup script by typing `amp_backup`.

This creates a backup of the system located in `/alternative/databackup.tar.gz`.

Restoring from a Backup

To restore a backup file on a new machine:

1. Use your AMP Installation DVD to build a new machine. The new machine must be running the same version as the AMP that created the backup file.
2. Copy the nightly_data00[1-4].tar.gz file to the `/tmp` directory in the new AMP.

   A file transfer client that supports SFTP/SCP for Windows is WinSCP: http://winscp.sourceforge.net/eng/

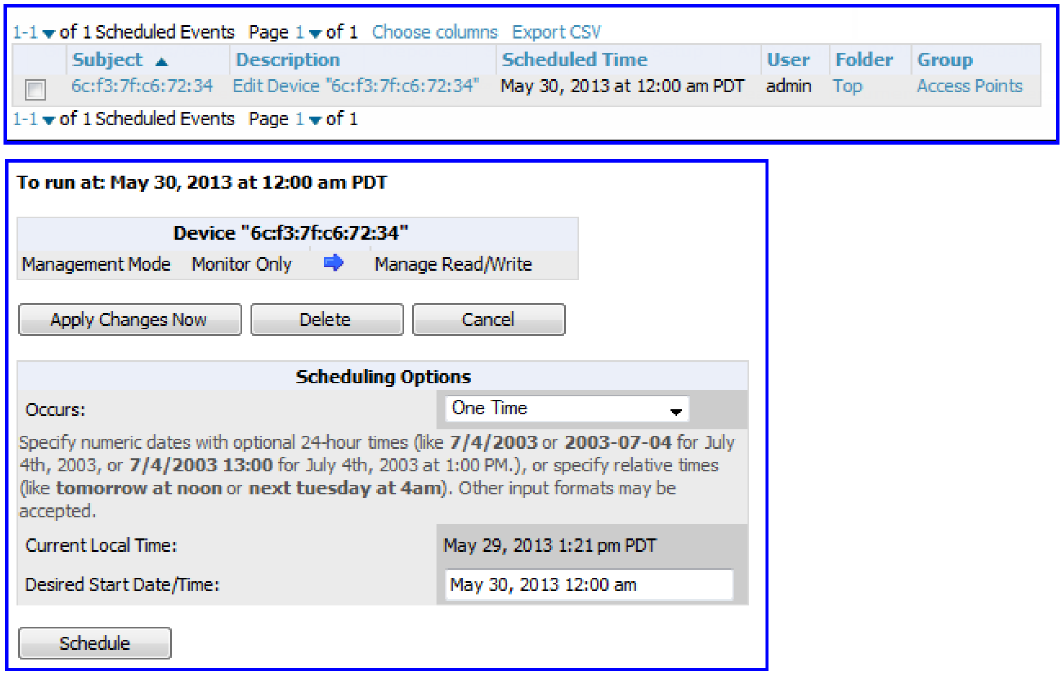
   WinSCP allows you to transfer the nightly00[1-4].tar.gz file from your local PC to the new AMP using the secure copy protocol (SCP).
3. Log onto the new server as **root**.
4. Change to the **scripts** directory by typing `scripts`.
5. Run the restore script by typing `./amp_restore -d /tmp/nightly_data00[1-4].tar.gz`.

Network administrators can now use the nightly backup from a 32-bit AMP on a 64-bit installation, rather than having to create a special backup file or use the special restore script.

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 135.

Figure 135 *System > Configuration Change Jobs Page Illustration*



1-1 ▾ of 1 Scheduled Events Page 1 ▾ of 1 Choose columns Export CSV

	Subject ▲	Description	Scheduled Time	User	Folder	Group
□	6c:f3:7f:c6:72:34	Edit Device "6c:f3:7f:c6:72:34"	May 30, 2013 at 12:00 am PDT	admin	Top	Access Points

1-1 ▾ of 1 Scheduled Events Page 1 ▾ of 1

To run at: May 30, 2013 at 12:00 am PDT

Device "6c:f3:7f:c6:72:34"

Management Mode Monitor Only ➡ Manage Read/Write

Scheduling Options

Occurs: One Time ▾

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

Current Local Time: May 29, 2013 1:21 pm PDT

Desired Start Date/Time: May 30, 2013 12:00 am

1. To edit an existing configuration change job select on the linked description name. On the subsequent edit page you can choose to run the job immediately by selecting **Apply Changes Now**, to reschedule the job by selecting **Schedule**, **Delete** the job, or **Cancel** the job edit.
2. Select the linked AP or group name under the **Subject** column to go to its monitoring page.
3. Select the linked group and folder names under **Folder** or **Group** to go to the AP's folder or group page.
4. Scheduled configuration change jobs will also appear on the **Manage** page for an AP or the **Monitoring** page for a group.

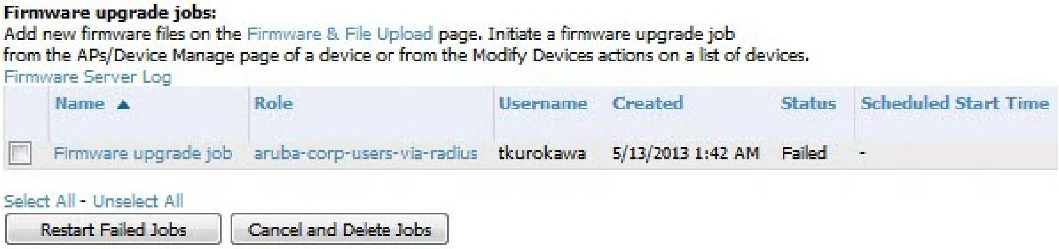
Using the System > Firmware Upgrade Jobs Page

The **System** > **Firmware Upgrade Jobs** page displays a list of recent firmware upgrade jobs that have been initiated in the **APs/Devices** > **Manage** page or **Modify Devices** page for a controller or autonomous AP that supports firmware upgrades in AMP.

Successful upgrade jobs are not archived on this page -- generally you visit this page to review failed or pending firmware upgrade jobs.

Users with the **AP/Device Manager** role and higher can view this page. Audit-only users cannot view this page or tab.

Figure 136 *System > Firmware Upgrade Jobs Page Illustration*



Firmware upgrade jobs:

Add new firmware files on the Firmware & File Upload page. Initiate a firmware upgrade job from the APs/Device Manage page of a device or from the Modify Devices actions on a list of devices.

Firmware Server Log

	Name ▲	Role	Username	Created	Status	Scheduled Start Time
□	Firmware upgrade job	aruba-corp-users-via-radius	tkurokawa	5/13/2013 1:42 AM	Failed	-

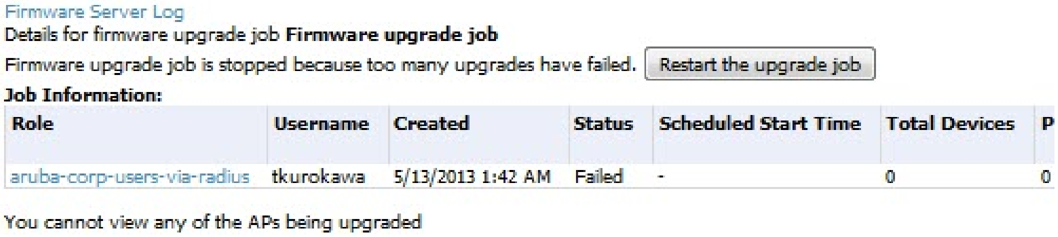
Select All - Unselect All

You can perform the following operations on this page:

- To restart failed firmware upgrade jobs, select the check boxes next to the rows you want to restart and select the **Restart Failed Jobs** button.
- To stop a pending upgrade job and remove it from the list, select the **Cancel and Delete Jobs** button.
- Use additional links on the page as shortcuts to the **Device Setup** > **Upload Firmware & Files** page, or the complete raw text of the Firmware Server Log
- To view additional details about an individual upgrade job including the devices being upgraded, select the name of an upgrade job from the Name column to go to the **System** > **Firmware Upgrade Job Detail** page, illustrated in Figure 137.

  From here you can click the device name to go to its **APs/Devices** > **Monitor** page, or the link under **Firmware File** column to go to the **Device Setup** > **Upload Firmware & Files** page.

Figure 137 *System > Firmware Upgrade Job detail page illustration*



Firmware Server Log

Details for firmware upgrade job **Firmware upgrade job**

Firmware upgrade job is stopped because too many upgrades have failed.

Job Information:

Role	Username	Created	Status	Scheduled Start Time	Total Devices	P
aruba-corp-users-via-radius	tkurokawa	5/13/2013 1:42 AM	Failed	-	0	0

You cannot view any of the APs being upgraded

Refer also to "Loading Device Firmware Onto AMP (optional)" on page 59.

Using the System > Performance Page

The **System** > **Performance** page displays basic AMP hardware information as well as resource usage over time. AMP logs performance statistics such as load average, memory and swap data every minute.

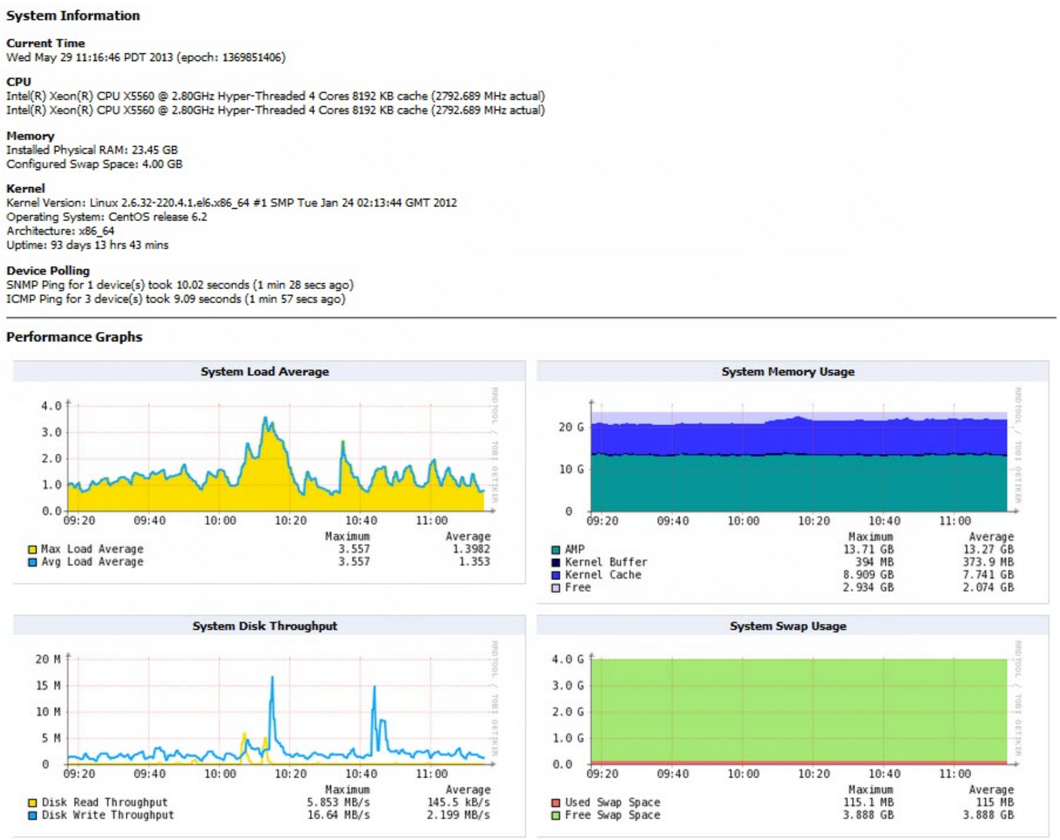
The historical logging is useful to determine the best usable polling period and track the health of AMP over time.

The page is divided into four sections:

- System Information
- Performance Graphs
- Database Statistics
- Disk Usage

Figure 138 illustrates this page, and Table 117 describes fields and information displayed.

Figure 138 *System > Performance Page Illustration (Partial Screen)*



System Information

Current Time
Wed May 29 11:16:46 PDT 2013 (epoch: 1369851406)

CPU
Intel(R) Xeon(R) CPU X5560 @ 2.80GHz Hyper-Threaded 4 Cores 8192 KB cache (2792.689 MHz actual)
Intel(R) Xeon(R) CPU X5560 @ 2.80GHz Hyper-Threaded 4 Cores 8192 KB cache (2792.689 MHz actual)

Memory
Installed Physical RAM: 23.45 GB
Configured Swap Space: 4.00 GB

Kernel
Kernel Version: Linux 2.6.32-220.4.1.el6.x86_64 #1 SMP Tue Jan 24 02:13:44 GMT 2012
Operating System: CentOS release 6.2
Architecture: x86_64
Uptime: 93 days 13 hrs 43 mins

Device Polling
SNMP Ping for 1 device(s) took 10.02 seconds (1 min 28 secs ago)
ICMP Ping for 3 device(s) took 9.09 seconds (1 min 57 secs ago)

Performance Graphs

Table 117: *System > Performance Page Fields and Graphs*

Field	Description
System Information	
Current Time	Displays AMP's current time.
CPU(s)	Basic CPU information as reported by the operating system.
Memory	The amount of physical RAM and Swap space seen by the operating system. Refer

Table 117: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
	to the *AirWave Server Sizing Guide* for hardware requirements.
Kernel	The version of the Linux kernel running on the box.
Device Polling	Displays some AP/Device polling statistics.
Performance Graphs	
System Load Average	The number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical AMP load is around 2-3 times the number of CPU cores you have in your system. A constant load of 4x to 5x is cause for concern. A load above 6x is a serious issue and will probably result in AMP becoming unusable. To lower the load average, try increasing a few polling periods in the **Groups > Basic** page.
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for AMP to have very little free RAM. Linux automatically allocates all free RAM as cache and buffer. If the kernel needs additional RAM for process it will dynamically take it from the cache and buffer.
System Disk Throughput	The rate of reading and writing from and to the disk in bytes per second.
System Swap Usage	The amount of Swap memory used by AMP. Swap is used when the there is no more free physical RAM. A large performance penalty is paid when swap is used. If your AMP consistently uses swap, you should consider installing additional RAM.
System Disk IOPs	The number of disk reads and writes per second.
System Disk Outstanding I/O Requests	The average number of outstanding I/O requests (queue depth). If it's high, it means that I/O requests (disk reads/writes) aren't being serviced as fast as they're being asked for.
System Disk Utilization	The amount of data read from the disk and written to the disk.
System CPU Utilization	The percentage of CPU that has been used by the user and the system as well as the amount that was idle.
Process Counts by Service	This breaks down network usage based on Web server, database, AMP Service, and VisualRF processes.
Average Delay Time by Queue Type	This shows the queue time for Async logger clients and RAPIDS processing.
I/O Throughput by Worker/by Service	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 by Worker/by Service	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).

Table 117: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
System Network Usage	All traffic in and out measured in bits per second of your primary network interface (Eth0 being the most common).
Usage by Protocol	Displays the amount of traffic used by Telnet, HTTPS and SNMP used by your primary network interface (Eth0 being the most common).
AMON	Displays the number of AMON packet traffic used by your network over the last two hours, day, week, month, and year.
SNMP Traps	Displays the number of SNMP Trap packets in your network over the last two hours, day, week, month, and year
Legacy SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the legacy (v1 and v3) SNMP fetcher.
Legacy SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the legacy (v1 and v3) SNMP fetcher.
High Performance SNMP Fetcher Requests	The number of SNMP get and walk requests per second performed by the high performance SNMP (v2c) fetcher.
High Performance SNMP Fetcher Responses	The number of SNMP OIDs received per second performed by the high performance SNMP (v2c) fetcher.
Database Statistics	
Top 5 Tables (by row count)	The five largest tables in AMP. Degraded performance has been noticed for in some cases for tables over 200,000 rows. Decreasing the length of time client data is stored on the AMP page is recommended if a user/client table exceeds 250,000 rows.
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.
Database Transaction Activity	The number of commits and rollbacks performed by the database.
Disk Space	
Disk Space	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 **AMP Setup > General** page or consider additional drive space.

There are several initial steps that you can take to troubleshoot AMP performance problems, including slow page loads and timeout errors. Initial troubleshooting steps would include the following:

- Increasing the polling period settings on the **Groups** > **Basic** page.
- Increasing the polling period time for groups with routers and switches.
- Adding additional memory to the server. Please consult the sizing information in the latest edition of the *AirWave Server Sizing Guide* or contact Aruba support for the latest recommendations.

Monitoring and Supporting WLAN Clients

This section describes the **Clients** pages as follows:

- "Overview of the Clients Pages" on page 235
- "Monitoring Your Network with the Clients > Overview Page" on page 236
- "Monitoring WLAN Users in the Clients > Connected and Clients > All Pages" on page 237
- "Monitoring Rogue Clients With the Clients > Rogue Clients Page" on page 241
- "Supporting Guest WLAN Users With the Clients > Guest Users Page" on page 242
- "Supporting VPN Users with the Clients > VPN Sessions Page" on page 244
- "Supporting RFID Tags With the Clients > Tags Page" on page 245

See also "Evaluating and Diagnosing User Status and Issues" on page 246.

For information about creating AMP users and AMP user roles, refer to:

- "Creating AMP Users" on page 41
- "Creating AMP User Roles" on page 43

If you need to create an AMP user account for frontline personnel who are to support Guest WLAN users, refer to "Supporting Guest WLAN Users With the Clients > Guest Users Page" on page 242.

Overview of the Clients Pages

The **Clients** pages display multiple types of user data for existing WLAN clients and VPN users. The data comes from a number of locations, including data tables on the access points, information from RADIUS accounting servers, and AMP-generated data. AMP supports the following **Clients** pages:

Table 118: *Clients pages*

Clients Page	Description	Refer To
Overview	Provides a graphical summary of all devices on your network, including client and network usage trends; a distribution breakdown by OS, vendor, device type, and SSID; and potential performance issues. If any clients are configured to be Watched Clients, then a Watched Clients table will also appear on this page.	"Monitoring Your Network with the Clients > Overview Page" on page 236
Connected	Displays active users that are currently connected to the WLAN.	"Monitoring WLAN Users in the Clients > Connected and Clients > All Pages" on page 237
All	Displays all users of which AMP is aware, with related information. Non-active users are listed in gray text.	"Monitoring WLAN Users in the Clients > Connected and Clients > All Pages" on page 237
Rogue Clients	Displays connected rogue clients.	"Monitoring Rogue Clients With the Clients > Rogue Clients Page" on page 241
Guest Clients	Displays all guest users in AMP and allows you to create, edit, or delete guest users.	"Supporting Guest WLAN Users With the Clients > Guest Users Page" on page 242
Client Detail	Displays client device information, alerts, signal quality, bandwidth, and association history. This page appears when you select a	"Evaluating User Status with the Clients > Client Detail Page" on

Table 118: *Clients pages (Continued)*

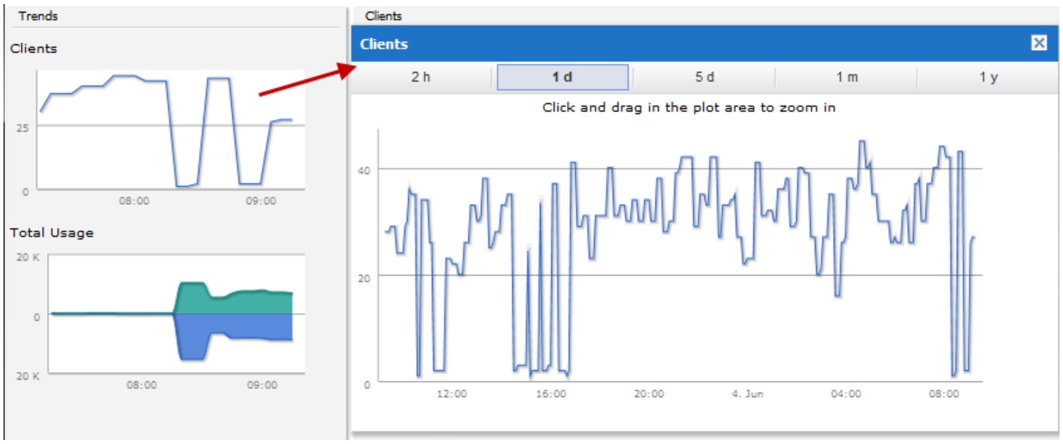
Clients Page	Description	Refer To
	user's MAC address link from these list tables: - **Clients > Connected** - **Clients > All** - **Home > Search** page results that display the user MAC address	page 246
Diagnostics	Displays possible client device issues, diagnostic summary data, user counts, AP information, 802.11 counters summary, and additional information. This page appears when you select a user's MAC address from one of the following pages: - **Clients > Connected** - **Clients > All** - **Home > Search** page results or **Search** field results that display the user MAC address	"Evaluating Client Status with the Clients > Diagnostics Page" on page 250
Tags	Displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that is monitored by AMP.	"Supporting RFID Tags With the Clients > Tags Page" on page 245

Monitoring Your Network with the Clients > Overview Page

The **Clients** > **Overview** page provides a graphical summary of all devices on your network, including client and network usage trends; a distribution breakdown by OS, vendor, device type, and SSID; and potential performance issues. If any clients are configured to be Watched Clients, then a Watched Clients table will also appear on this page.

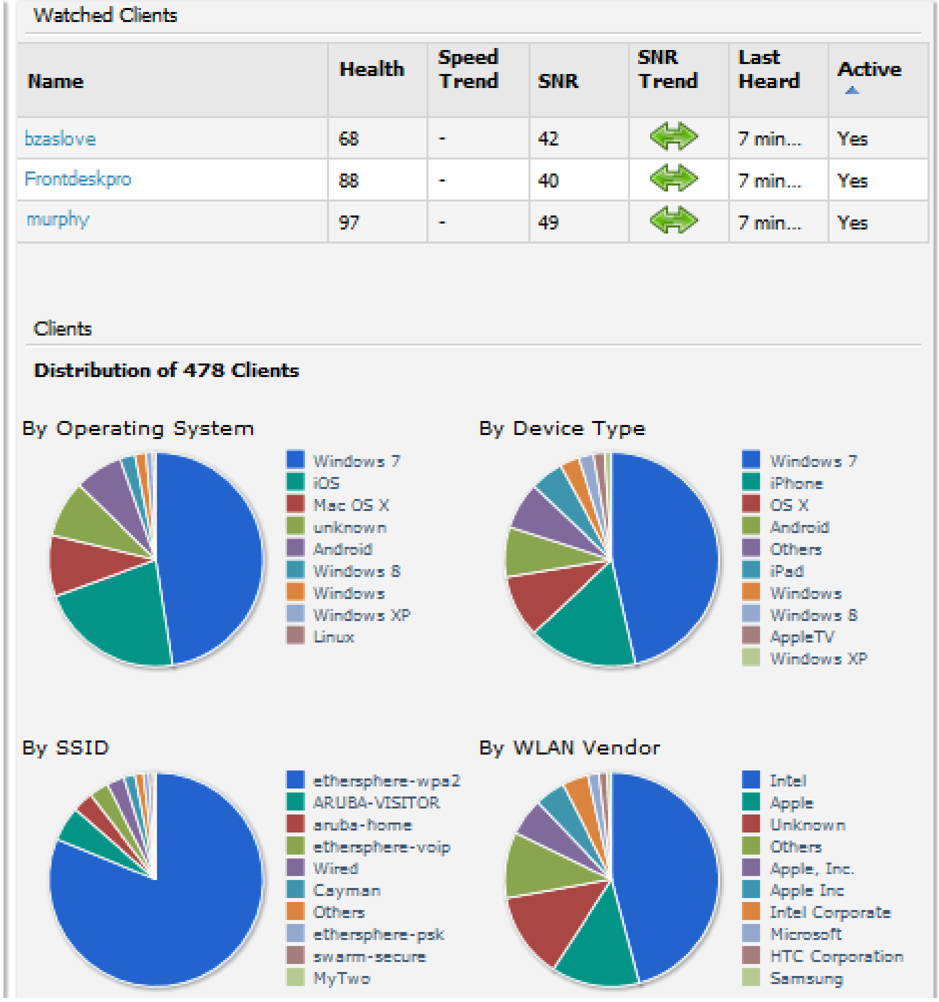
This page is divided into three panes. The left pane is the "Trends" pane. This includes the Clients and Total Usage Highcharts. By default, these charts show data over the last two hours. You can click in either chart to open a popup. From this popup, you can change the time range to 1 day, 5 days, 1 month, or 1 year.

Figure 139 *Trends pane with a Clients popup*



The center pane provides pie charts that provide summarized information about all clients across your network. This information is broken down by operating system, device type, SSID, and WLAN vendor. If any clients on your network are specified as Watched Clients, then a Watched Clients table will appear in this pane, showing the client's health, speed, SNR value, SNR trend, when the client was last heard, and whether the client is active. This table provides a link for each client that take you to the **Clients** > **Diagnostics** page.

Figure 140 *Center pane*



Watched Clients

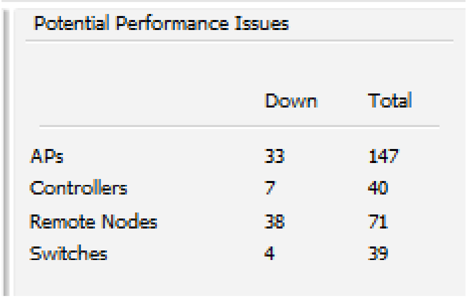
Name	Health	Speed Trend	SNR	SNR Trend	Last Heard	Active
bzaslove	68	-	42	⇔	7 min...	Yes
Frontdeskpro	88	-	40	⇔	7 min...	Yes
murphy	97	-	49	⇔	7 min...	Yes

Clients

Distribution of 478 Clients

The right pane provides information about the total number of APs, Controllers, Remote Nodes, and Switches on your network and the number of those that are currently down. This information can be useful in identifying potential performance issues.

Figure 141 *Right pane*



Potential Performance Issues

	Down	Total
APs	33	147
Controllers	7	40
Remote Nodes	38	71
Switches	4	39

Monitoring WLAN Users in the Clients > Connected and Clients > All Pages

The **Clients** > **All** page shows all users that AMP is aware of, including down clients. The **Clients** > **Connected** page displays all users currently connected in AMP. This page is illustrated in Figure 142 and described in Table 119. It contains the following information at a glance:

- The Folder field shows the current folder of Connected Clients you are viewing. You can view users under a particular folder from the Go to folder dropdown menu.
- Links under the Folder fields showing the **Total Devices**, **Mismatched**, **Clients**, and **Usage** (a static, unlinked statistic) summarize the device information for this folder. Select these links to open detail pages for each:
  - **Total Devices** redirects to the **APs/Devices > List** for that folder,
  - **Mismatched** redirects to the list in **APs/Devices > Mismatched** for that folder.
  - **Clients** refreshes the page but expands to include users in the subfolders.
- Interactive graphs display average and max **Clients** over time, and **Usage** in and out for the selected folder over time.
  - Select a time range option from the upper-right corner of the graphs.
  - Select the WLANs drop down to view up to six clients, or select Total Clients.
  - Click in a graph to view a pop-up of the graph.
- Below the Clients and Usage graphs is the list of connected users.

NOTE

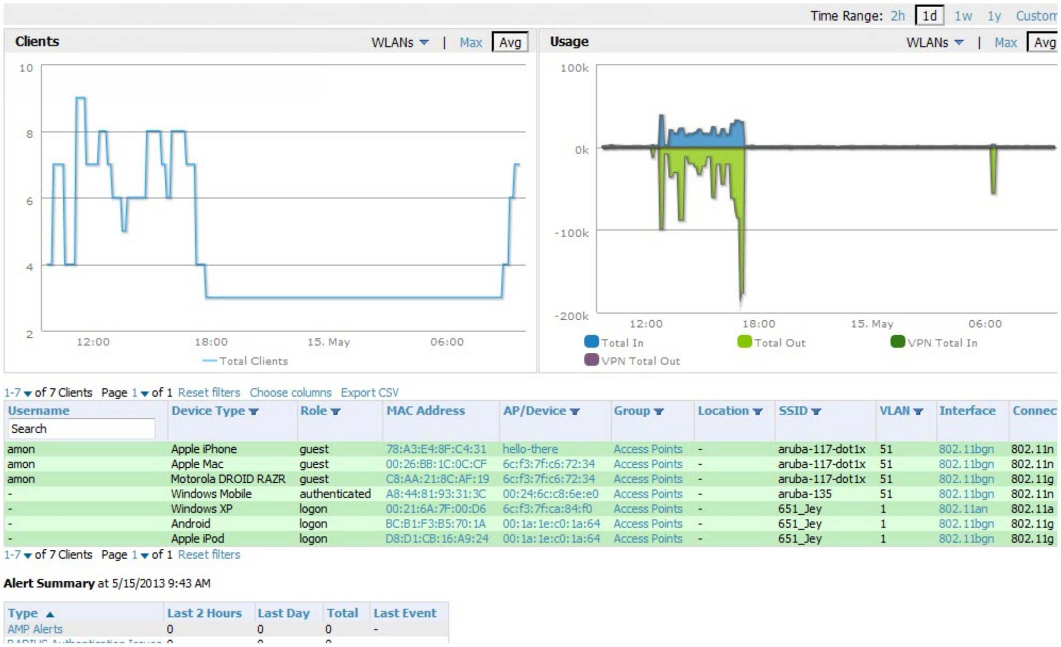
The number of clients in AMP can differ from the number of clients that you see on the controller. This is because AMP and the controller count clients differently. The controller counts connections to the network as clients, while AMP counts devices as clients. For example, in the case where a single device connects to the network multiple times, the controller will count one client for each connection that the device makes to the network. AMP will only recognize the device as a single client, though, regardless of the number of connections.

The information on this page can be adjusted in the following ways:

- The **Alert Summary** section displays custom configured alerts that were defined in the **System > Alerts** page.
- Use the **Filter** icon (▼) next to certain columns (**AP/Device**, **Role**, **VLAN**, **Connection Mode**, and others) to filter the results by one of the values under that column.You can filter the list by substring match under the **Username** column.

The **Clients > Connected** page includes SSID information for users, and can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

Figure 142 *Clients > Connected Page Illustration (Partial View)*



1-7 ▼ of 7 Clients Page 1 ▼ of 1 Reset filters Choose columns Export CSV

Username Search	Device Type ▼	Role ▼	MAC Address	AP/Device ▼	Group ▼	Location ▼	SSID ▼	VLAN ▼	Interface	Connec
amon	Apple iPhone	guest	78:A3:E4:8F:C4:31	hello-there	Access Points	-	aruba-117-dot1x	51	802.11bgn	802.11n
amon	Apple Mac	guest	00:26:BB:1C:0C:CF	6c:f3:7f:c6:72:34	Access Points	-	aruba-117-dot1x	51	802.11bgn	802.11n
amon	Motorola DROID RAZR	guest	C8:AA:21:8C:AF:19	6c:f3:7f:c6:72:34	Access Points	-	aruba-117-dot1x	51	802.11bgn	802.11g
-	Windows Mobile	authenticated	A8:44:81:93:31:3C	00:24:6c:c8:6e:e0	Access Points	-	aruba-135	51	802.11bgn	802.11n
-	Windows XP	logon	00:21:6A:7F:00:D6	6c:f3:7f:ca:84:f0	Access Points	-	651_Jey	1	802.11an	802.11a
-	Android	logon	BC:B1:F3:B5:70:1A	00:1a:1e:c0:1a:64	Access Points	-	651_Jey	1	802.11bgn	802.11g
-	Apple iPod	logon	D8:D1:CB:16:A9:24	00:1a:1e:c0:1a:64	Access Points	-	651_Jey	1	802.11bgn	802.11g

1-7 ▼ of 7 Clients Page 1 ▼ of 1 Reset filters

Alert Summary at 5/15/2013 9:43 AM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
RADIUS Authentication Issues	0	0	0	

Table 119: *Clients > Connected Table Columns and Links(Alphabetical)*

Field	Description
AOS Device Type	The type of client device determined by the Aruba controller-- a fallback in case the rules set in **AMP Setup > Device Type Setup** were unable to determine the device type.
AP/Device	Displays the name of the AP to which the MAC address is associated as a link to this AP's **APs/Devices > Monitor** page.
Association Time	The first time AMP recorded the user for this association.
Auth. Time	The how long ago the user authenticated. **NOTE:** This value displays as a negative number for unauthenticated users.
Auth. Type	The type of authentication employed by the user: ● WPA2 (EAP-PEAP) is the standard setting. ● EAP is reported by Aruba devices via SNMP traps. ● RADIUS accounting servers integrated with AMP will provide the RADIUS Accounting Auth type. ● Web (PAP) - Captive Portal. ● All others are considered to be not authenticated.
Usage	The average bandwidth consumed by the MAC address.
Ch BW	The channel bandwidth that currently supports 802.11n users.
Cipher	Displays WEP with keys. This data is also displayed in the **Client Session** report in the **Session Data By Client** section.
Connection Mode	The Radio mode used by the user to associate to the AP for 802.11n clients.
Device Type	The type of device determined by **AMP Setup > Device Type Setup** rules.
Duration	The length of time the MAC address has been associated.
EAP Supplicant	The party being authenticated in the Extensible Authentication Protocol.
Forward Mode	Forwarding mode for the port: Bridge, Tunnel, or Split Tunnel.
Goodput	The ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes. Note that this information is not available for Instant devices.
Group	The group containing the AP that the user is associated with.
Guest User	Specifies whether the user is a guest.
Interface	The interface on the device to which the user is connected.
LAN Hostname	The LAN hostname of the user MAC.

Table 119: *Clients > Connected Table Columns and Links(Alphabetical) (Continued)*

Field	Description
LAN IP Address	The IP assigned to the user MAC. AMP gathers it from the association table of APs.
Location	If a value appears here, the location of this user's client has been mapped on VisualRF. Select the location to open a new VisualRF Floor Plan Location window.
MAC Address	The radio MAC address of the user associated to APs as a link to the **Users > Detail** page for this user.
Manufacturer	The manufacturer of the user's device.
Model	The model of the user's device.
Name	The product of the user's device.
Network Chipset	The chipset indicates the functions the device was designed to perform.
Network Driver	Driver name or other information.
Notes	Notes about the user.
OS	The device's operating system type.
OS Detail	Additional information on the operating system such as version numbers.
Phone Number	Contact number for the user.
Role	Specifies the role that the Aruba controller assigned to the connected user, such as employee.
Serial Number	Serial number of the device.
Service End	Ending timestamp of the device usage.
Service Start	Beginning timestamp of the device usage.
Sig. Qual.	The average signal quality the user experienced.
SSID	The SSID with which the user is associated.
Speed	The packet and byte counts of data frames successfully transmitted to and received from associated stations. Note that this information is not available for Instant devices.
Tunneled Controller	If a user is connected to an Aruba Mobility Access Switch, this indicates which controller the user is authenticated to.
Username	Displays the name of the user associated to the AP. AMP gathers this data from device traps, SNMP polling, or RADIUS accounting. Usernames appear in italics when a username for that

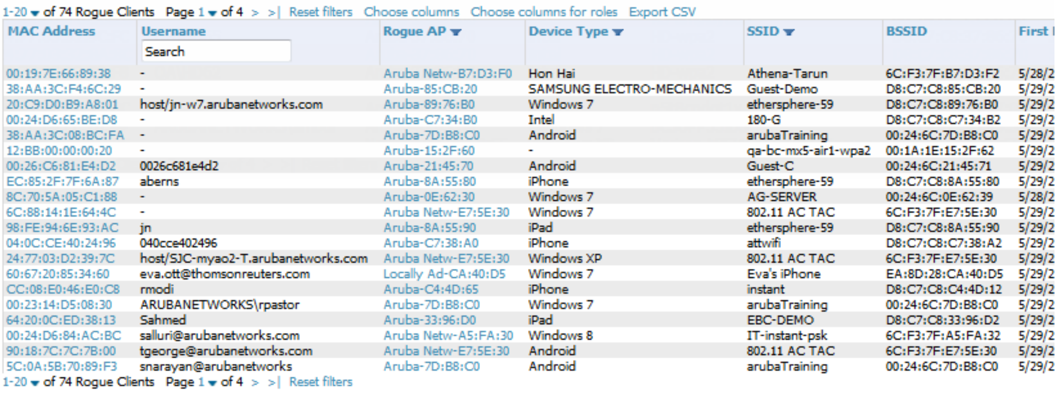
Table 119: *Clients > Connected Table Columns and Links(Alphabetical) (Continued)*

Field	Description
	MAC address has been stored in the database from a previous association, but AMP is not getting a username for the current association. This may indicate that the user has not yet been authenticated for this session or AMP may not be getting a username from an external source.
VLAN	Displays the VLAN assigned to the user, if available.

Monitoring Rogue Clients With the Clients > Rogue Clients Page

You can view connected rogue clients in AMP by selecting the **Clients** > **Rogue Clients** page. In this page, you can click on the MAC address of a rogue to view the Client Details page or on a Rogue AP link to view the **RAPIDS** > **Details** page for the AP. Figure 143 illustrates the **Clients** > **Rogue Clients** page.

Figure 143 *Clients > Rogue Clients Page Illustration*



1-20 ▾ of 74 Rogue Clients Page 1 ▾ of 4 > >| Reset filters Choose columns Choose columns for roles Export CSV

MAC Address	Username Search	Rogue AP ▾	Device Type ▾	SSID ▾	BSSID	First
00:19:7E:66:89:38	-	Aruba Netw-B7:D3:F0	Hon Hai	Athena-Tarun	6C:F3:7F:B7:D3:F2	5/28/2
38:AA:3C:F4:6C:29	-	Aruba-85:CB:20	SAMSUNG ELECTRO-MECHANICS	Guest-Demo	D8:C7:C8:85:CB:20	5/29/2
20:C9:D0:B9:A8:01	host/jn-w7.arubanetworks.com	Aruba-89:76:B0	Windows 7	ethersphere-59	D8:C7:C8:89:76:B0	5/29/2
00:24:D6:65:BE:D8	-	Aruba-C7:34:B0	Intel	180-G	D8:C7:C8:C7:34:B2	5/29/2
38:AA:3C:08:BC:FA	-	Aruba-7D:B8:C0	Android	arubaTraining	00:24:6C:7D:B8:C0	5/29/2
12:BB:00:00:00:20	-	Aruba-15:2F:60	-	qa-bc-mx5-air1-wpa2	00:1A:1E:15:2F:62	5/29/2
00:26:C6:81:E4:D2	0026c681e4d2	Aruba-21:45:70	Android	Guest-C	00:24:6C:21:45:71	5/29/2
EC:85:2F:7F:6A:87	aberns	Aruba-8A:55:80	iPhone	ethersphere-59	D8:C7:C8:8A:55:80	5/29/2
8C:70:5A:05:C1:88	-	Aruba-0E:62:30	Windows 7	AG-SERVER	00:24:6C:0E:62:39	5/28/2
6C:88:14:1E:64:4C	-	Aruba Netw-E7:5E:30	Windows 7	802.11 AC TAC	6C:F3:7F:E7:5E:30	5/29/2
98:FE:94:6E:93:AC	jn	Aruba-8A:55:90	iPad	ethersphere-59	D8:C7:C8:8A:55:90	5/29/2
04:0C:CE:40:24:96	040cce402496	Aruba-C7:38:A0	iPhone	attwifi	D8:C7:C8:C7:38:A2	5/29/2
24:77:03:D2:39:7C	host/SJC-myao2-T.arubanetworks.com	Aruba Netw-E7:5E:30	Windows XP	802.11 AC TAC	6C:F3:7F:E7:5E:30	5/29/2
60:67:20:85:34:60	eva.ott@thomsonreuters.com	Locally Ad-CA:40:D5	Windows 7	Eva's iPhone	EA:8D:28:CA:40:D5	5/29/2
CC:08:E0:46:E0:C8	rmodi	Aruba-C4:4D:65	iPhone	instant	D8:C7:C8:C4:4D:12	5/29/2
00:23:14:D5:08:30	ARUBANETWORKS\rpastor	Aruba-7D:B8:C0	Windows 7	arubaTraining	00:24:6C:7D:B8:C0	5/29/2
64:20:0C:ED:38:13	Sahmed	Aruba-33:96:D0	iPad	EBC-DEMO	D8:C7:C8:33:96:D2	5/29/2
00:24:D6:84:AC:BC	salluri@arubanetworks.com	Aruba Netw-A5:FA:30	Windows 8	IT-instant-psk	6C:F3:7F:A5:FA:32	5/29/2
90:18:7C:7C:7B:00	tgeorge@arubanetworks.com	Aruba Netw-E7:5E:30	Android	802.11 AC TAC	6C:F3:7F:E7:5E:30	5/29/2
5C:0A:5B:70:89:F3	snarayan@arubanetworks	Aruba-7D:B8:C0	Android	arubaTraining	00:24:6C:7D:B8:C0	5/29/2

1-20 ▾ of 74 Rogue Clients Page 1 ▾ of 4 > >| Reset filters

Table 120 describes the fields on this page.

Table 120: *Clients > Rogue Clients Fields*

Field	Description
MAC Address	Displays the MAC address of the rogue client. Click on this to jump to the **Clients > Client Detail** page for this rogue.
Username	The username associated with this client.
Rogue AP	The name of the Rogue AP. Click on this to jump to the **RAPIDS > Detail** page for this AP.
Device Type	The type of device, such as iPhone, Windows 7, etc.
SSID	The SSID of this client.
BSSID	The BSSID of this client.
First Heard	The date and time when this rogue client was first noticed.
Last Heard	The date and time when this rogue client was last noticed.

Table 120: *Clients > Rogue Clients Fields (Continued)*

Field	Description
Location	If a location is available, you can click on this link to open the VisualRF floor plan and location on which this client resides.
Connection Mode	Shows the type of connection, such as 802.11n, 802.11b, etc.
Ch BW	Shows the channel bandwidth for this rogue client.
Signal	Shows the signal value for this rogue client.
SNR	Shows the signal-to-noise ratio.
Channel	Shows the channel on which this rogue client is broadcasting.

Supporting Guest WLAN Users With the Clients > Guest Users Page

AMP supports guest user provisioning for Aruba Networks, Dell Networking W-Series, Alcatel-Lucent, and Cisco WLC devices. This allows frontline staff such as receptionists or help desk technicians to grant wireless access to WLAN visitors or other temporary personnel.

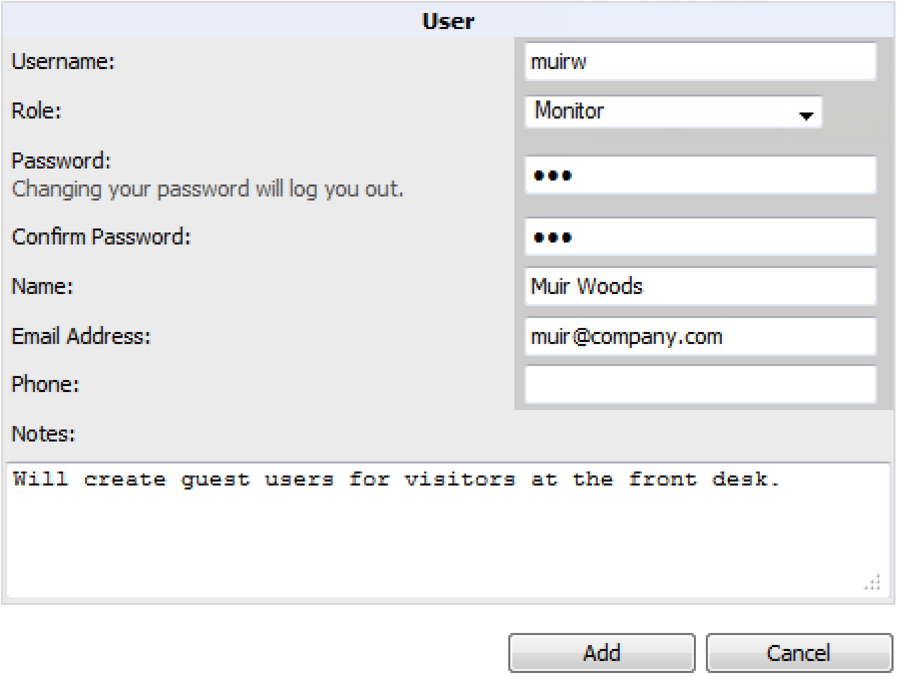
NOTE

The Guest User Preferences section on **AMP Setup > Roles**, as well as the **Clients > Guest Users** subtab, will not appear if **Guest User Configuration** is globally disabled in **AMP Setup > General.**

Perform the following steps in the pages described to configure these settings.

1. Navigate to the **AMP Setup** > **Roles** page and select the **Read-Only Monitoring & Auditing** role type. Under the Guest User Preferences section, enable **Allow creation of Guest Users**.
2. Next, navigate to the **AMP Setup** > **Users** page and create a new user with the role that was just created. Figure 144 illustrates this page.

Figure 144 *AMP Setup > Users Page Illustration*



User

Username:	muirw
Role:	Monitor
Password: Changing your password will log you out.	•••
Confirm Password:	•••
Name:	Muir Woods
Email Address:	muir@company.com
Phone:	

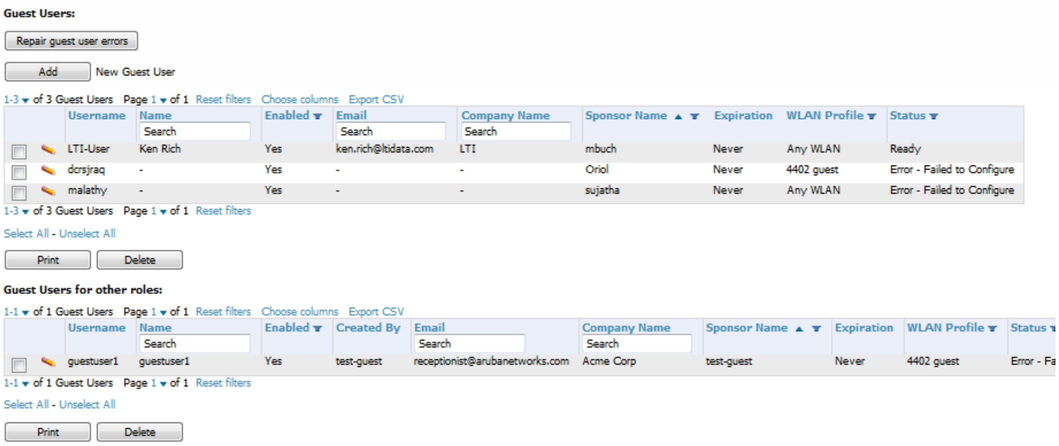
Notes:

```
Will create guest users for visitors at the front desk.
```

3. The newly created login information should be provided to the person or people who will be responsible for creating guest access users.
4. The next step in creating a guest access user is to navigate to the **Users > Guest Clients tab**. From this tab, you can add new guest users, you can edit existing users, and you can repair guest user errors.

   This page displays a list of guest users and data, to include the expiration date, the SSID (for Cisco WLC) and other information. Figure 145 illustrates this page, and Table 121 describes the information.

Figure 145 *Clients > Guest Users Page Illustration*


Guest Users:
Repair guest user errors
Add
New Guest User
1-3 of 3 Guest Users Page 1 of 1 Reset filters Choose columns Export CSV

		Username	Name	Enabled	Email	Company Name	Sponsor Name	Expiration	WLAN Profile	Status
			Search		Search	Search				
□		LTI-User	Ken Rich	Yes	ken.rich@ltidata.com	LTI	mbuch	Never	Any WLAN	Ready
□		dcrsjraq	-	Yes	-	-	Oriol	Never	4402 guest	Error - Failed to Configure
□		malathy	-	Yes	-	-	sujatha	Never	Any WLAN	Error - Failed to Configure

1-3 of 3 Guest Users Page 1 of 1 Reset filters
Select All - Unselect All
Print
Delete
Guest Users for other roles:
1-1 of 1 Guest Users Page 1 of 1 Reset filters Choose columns Export CSV

		Username	Name	Enabled	Created By	Email	Company Name	Sponsor Name	Expiration	WLAN Profile	Status
			Search			Search	Search				
□		guestuser1	guestuser1	Yes	test-guest	receptionist@arubanetworks.com	Acme Corp	test-guest	Never	4402 guest	Error - Fa

1-1 of 1 Guest Users Page 1 of 1 Reset filters
Select All - Unselect All
Print
Delete

Table 121: *Clients > Guest Users Fields*

Field	Description
Repair Guest User Errors	Sets AMP to attempt to push the guest user again in an attempt to repair any errors in the **Status** column.
Add New Guest User	Adds a new guest user to a controller via AMP
Username	Randomly generates a user name for privacy protection. This name appears on the **Guest User** detail page.
Name	Displays the specified guest user name.
Enabled	Enables or disables the user status. Set the status of the guest user as active (enabled) or expired (disabled).
Email	Displays the optional email address of the user.
Company Name	Displays the optional company name for the user.
Sponsor Name	Displays the name of the sponsor for the guest user. This setting is optional.
Expiration	Displays the date the guest user's access is to expire.
WLAN Profile	Select the SSID that the guest user can access. This setting applies to Cisco WLC only.
Status	Reports current status by the controller. If error messages appear in this column, select the user with the checkbox at left, and select the **Repair guest user errors** button.

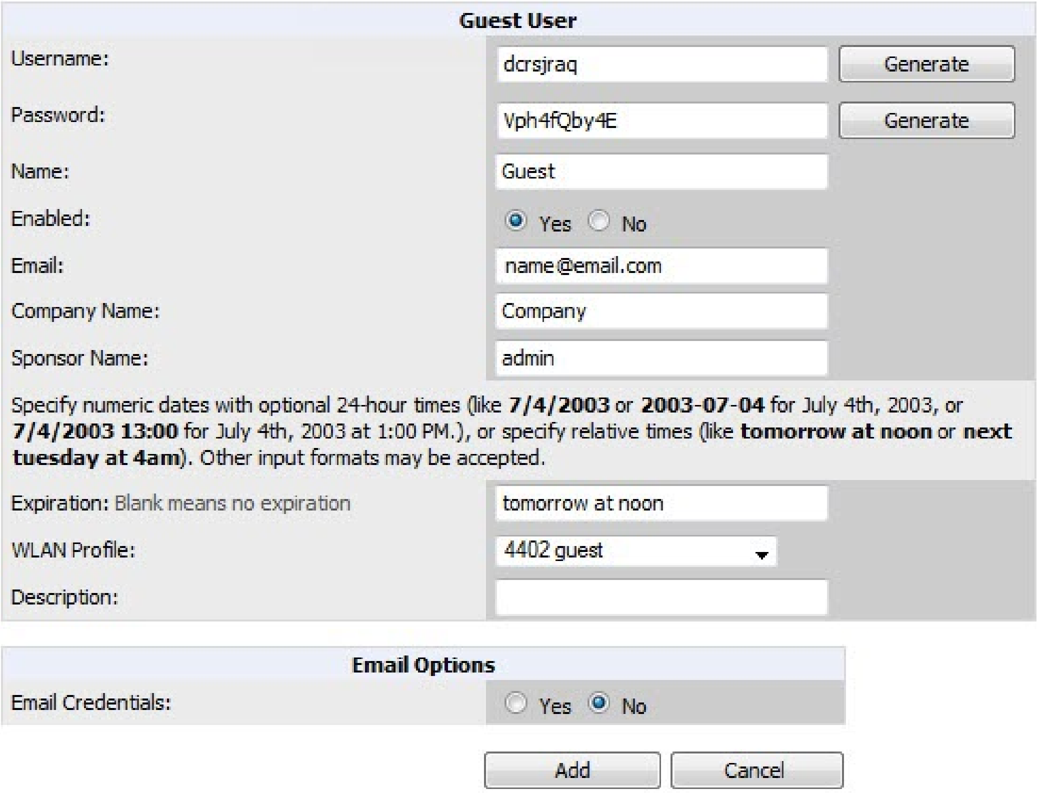
Guest users associated to the wireless network appear on the same list as other wireless users, but are identified as guest users in the **Guest User** column. The **Client Detail** page for a guest user also contains a box with the same guest information that appears for each user on the **Clients > Guest Users** list.

NOTE

The **Enabled, Sponsor Name, WLAN Profile, and Status** columns can be filtered using the funnel icon (▼).

5. To add a new guest user, select **Add**, and complete the fields illustrated in Figure 146. Table 121 above describes most fields. The first three fields are required, and the remaining fields are optional.

Figure 146 *Clients > Guest Users > Add New Guest User Page Illustration*



Guest User

Username:	dcrsjraq	Generate
Password:	Vph4fQby4E	Generate
Name:	Guest	
Enabled:	● Yes ○ No	
Email:	name@email.com	
Company Name:	Company	
Sponsor Name:	admin	

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

Expiration: Blank means no expiration	tomorrow at noon
WLAN Profile:	4402 guest ▾
Description:	

Email Options

Email Credentials:	○ Yes ● No

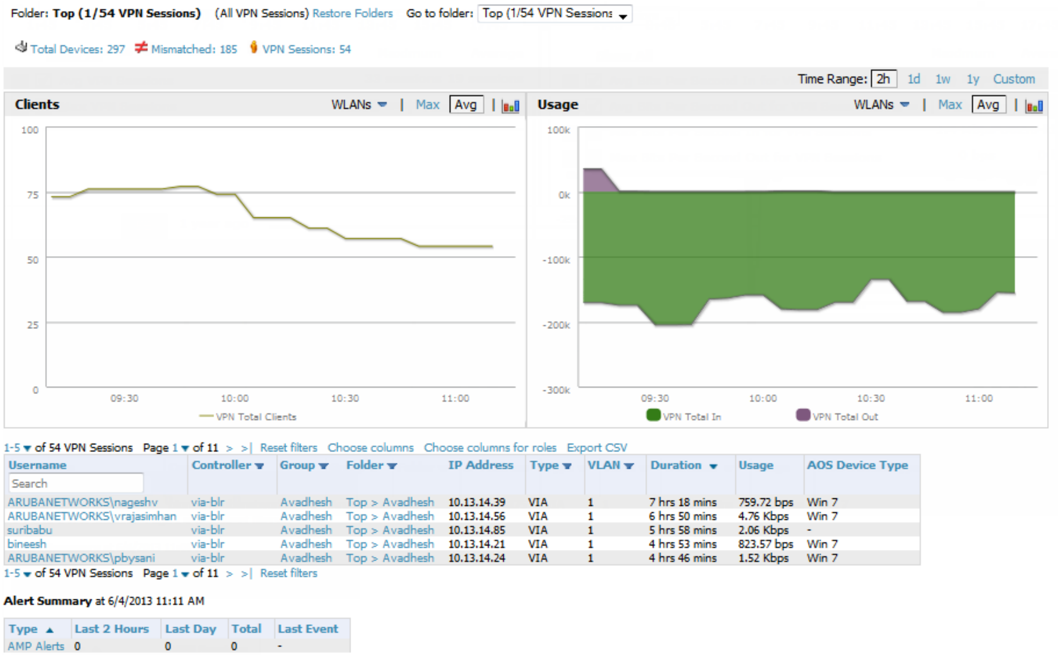
To make the **Username** or **Password** anonymous and to increase security, complete these fields then select **Generate**. The anonymous and secure **Username** and **Password** appear in the respective fields.

6. Select **Add** to complete the new guest user, or select **Cancel** to back out of new user creation. The **Clients > Guest Users** page appears and displays results, as applicable.

Supporting VPN Users with the Clients > VPN Sessions Page

The **Clients > VPN Sessions** page shows active VPN Sessions along with device type and HTTP fingerprinting information.

Figure 147 *Clients > VPN Sessions Page Illustration*



Folder: **Top (1/54 VPN Sessions)** (All VPN Sessions) Restore Folders Go to folder: Top (1/54 VPN Sessions

Total Devices: 297 Mismatched: 185 VPN Sessions: 54

1-5 of 54 VPN Sessions Page 1 of 11 > >| Reset filters Choose columns Choose columns for roles Export CSV

Username	Controller	Group	Folder	IP Address	Type	VLAN	Duration	Usage	AOS Device Type
Search									
ARUBANETWORKS\nageshv	via-blr	Avadhesh	Top > Avadhesh	10.13.14.39	VIA	1	7 hrs 18 mins	759.72 bps	Win 7
ARUBANETWORKS\vrajasimhan	via-blr	Avadhesh	Top > Avadhesh	10.13.14.56	VIA	1	6 hrs 50 mins	4.76 Kbps	Win 7
suribabu	via-blr	Avadhesh	Top > Avadhesh	10.13.14.85	VIA	1	5 hrs 58 mins	2.06 Kbps	-
bineesh	via-blr	Avadhesh	Top > Avadhesh	10.13.14.21	VIA	1	4 hrs 53 mins	823.57 bps	Win 7
ARUBANETWORKS\pbysani	via-blr	Avadhesh	Top > Avadhesh	10.13.14.24	VIA	1	4 hrs 46 mins	1.52 Kbps	Win 7

1-5 of 54 VPN Sessions Page 1 of 11 > >| Reset filters

Alert Summary at 6/4/2013 11:11 AM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-

When a VPN username is selected, a **Clients > VPN User Detail** page displays with current VPN sessions, a user and bandwidth interactive graph, and a historical VPN sessions list table.

Supporting RFID Tags With the Clients > Tags Page

Radio Frequency Identification (RFID) supports identifying and tracking wireless devices with radio waves. RFID uses radio wave tags for these and additional functions. Active tags have a battery and transmit signals autonomously, and passive tags have no battery. RFID tags often support additional and proprietary improvements to network integration, battery life, and other functions.

NOTE

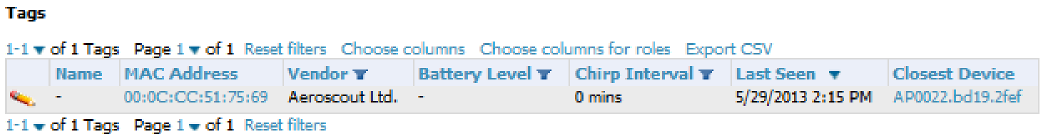
Guest users being pushed to large numbers of controllers may take a very long time to push.

The **Clients** > **Tags** page displays a list of wireless tags, such as Aeroscout, PanGo and Newbury, that are heard by thin APs, and reported back to a controller that AMP monitors. AMP displays the information it receives from the controller in a table on this page. Figure 148 illustrates this page, and Table 122 describes fields and information displayed.

NOTE

The **Vendor**, **Battery Level,** and **Chirp Interval** columns can be filtered using the funnel icon ( ).

Figure 148 *Clients > Tags Page Illustration*



Tags

1-1 of 1 Tags Page 1 of 1 Reset filters Choose columns Choose columns for roles Export CSV

	Name	MAC Address	Vendor	Battery Level	Chirp Interval	Last Seen	Closest Device
	-	00:0C:CC:51:75:69	Aeroscout Ltd.	-	0 mins	5/29/2013 2:15 PM	AP0022.bd19.2fef

1-1 of 1 Tags Page 1 of 1 Reset filters

Table 122: *Clients > 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.
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 AMP.
Closest Device	The device that last reported the tag to the controller (linked to the AP monitoring page in AMP).

- To edit the name of the tag, or to add notes to the tag's record, select the **pencil** icon next to the entry in the list. You can then add or change the name and add notes like Maternity Ward Inventory or Chicago Warehouse, as two examples.
- The **Inactive Tag** trigger can be used to generate an alert if a tag is not reported to AMP after a certain interval. This can help to identify lost or stolen inventory. For more information about enabling this trigger, refer to the section "Monitoring and Supporting AMP with the System Pages" on page 214.

Evaluating and Diagnosing User Status and Issues

If a WLAN user reports difficulty with the wireless network, the administration or Helpdesk personnel can view and process related user information from the **Client Detail** and **Diagnostic** pages. This section describes these two pages.

- "Evaluating User Status with the Clients > Client Detail Page" on page 246
- "Evaluating Client Status with the Clients > Diagnostics Page" on page 250

Evaluating User Status with the Clients > Client Detail Page

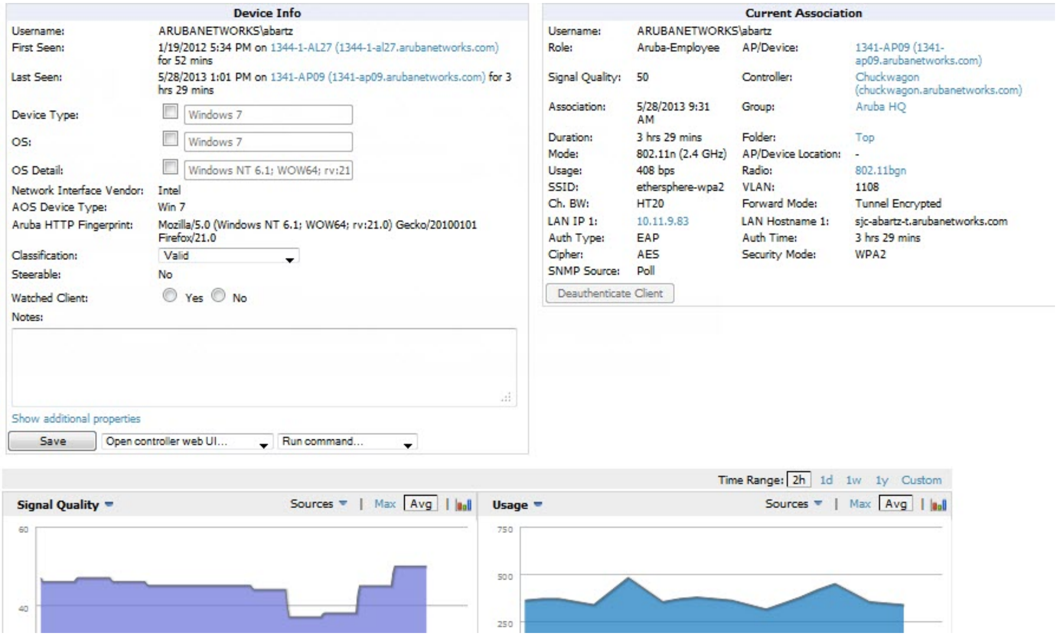
The **Clients** > **Client Detail** page is a focused subtab that becomes visible when you select a specific WLAN user. Access the **Clients** > **Client Detail** page by selecting the **MAC Address** link for a specific user from one of the following pages:

- **Clients** > **Connected**
- **Clients** > **All**
- **Home** > **Search** page results or search field **Client** results that display the user MAC address

This page provides information for the wireless device, signal quality, and bandwidth consumption. It also includes AP association history and current association status. If VisualRF is enabled in **AMP Setup** > **General**, this page provides a graphical map of the user location and facility information. Finally, this page allows you to specify a client as a "Watched" client to be included on a watched list. A watched list is a useful method for tracking performance metrics for selected clients. For example, you might have a regular user who cites repeated connectivity issues when moving from one room to another. Adding this client to a watched list allows you to more easily track this and other watched clients. The **Clients** > **Overview** page provides information on speed and SNR trends for all watched clients.

Figure 149 illustrates the contents of Clients > Client Details page.

Figure 149 *Clients > Client Detail page illustration (partial view)*



Device Info

Username: ARUBANETWORKS\abartz
First Seen: 1/19/2012 5:34 PM on 1344-1-AL27 (1344-1-al27.arubanetworks.com) for 52 mins
Last Seen: 5/28/2013 1:01 PM on 1341-AP09 (1341-ap09.arubanetworks.com) for 3 hrs 29 mins
Device Type: □ Windows 7
OS: □ Windows 7
OS Detail: □ Windows NT 6.1; WOW64; rv:21
Network Interface Vendor: Intel
AOS Device Type: Win 7
Aruba HTTP Fingerprint: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Classification: Valid
Steerable: No
Watched Client: ○ Yes ○ No
Notes:

Show additional properties

Save | Open controller web UI... | Run command...

Current Association

Username: ARUBANETWORKS\abartz
Role: Aruba-Employee | AP/Device: 1341-AP09 (1341-ap09.arubanetworks.com)
Signal Quality: 50 | Controller: Chuckwagon (chuckwagon.arubanetworks.com)
Association: 5/28/2013 9:31 AM | Group: Aruba HQ
Duration: 3 hrs 29 mins | Folder: Top
Mode: 802.11n (2.4 GHz) | AP/Device Location: -
Usage: 408 bps | Radio: 802.11bgn
SSID: ethersphere-wpa2 | VLAN: 1108
Ch. BW: HT20 | Forward Mode: Tunnel Encrypted
LAN IP 1: 10.11.9.83 | LAN Hostname 1: sjc-abartz-t.arubanetworks.com
Auth Type: EAP | Auth Time: 3 hrs 29 mins
Cipher: AES | Security Mode: WPA2
SNMP Source: Poll

Deauthenticate Client

Mobile Device Access Control in Clients > Client Detail and Clients > Connected

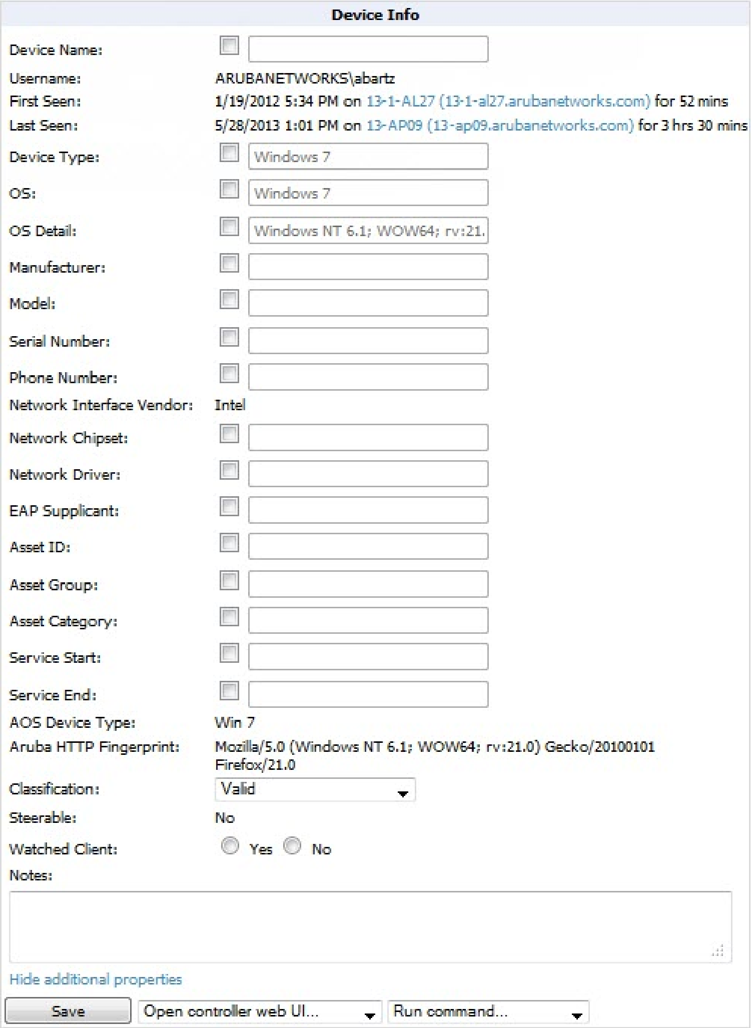
Mobile Device Access Control (MDAC) secures, provisions, and manages network access for Apple® iOS and other employee-owned mobile devices by enabling device fingerprinting, device registration, and increased device visibility. For more information on MDAC, refer to http://www.arubanetworks.com/technology/mobile-device-access-control/.

Use the checkbox next to these fields to enable them in **Clients > Client Detail**:

- Device Type
- OS
- OS Detail
- Manufacturer

To see more options, select the **Show additional properties** link. The results are illustrated in Figure 150:

Figure 150 *Device Info section in Clients > Client Detail after Show additional properties is selected*



Device Info

Device Name:	□
Username:	ARUBANETWORKS\abartz
First Seen:	1/19/2012 5:34 PM on 13-1-AL27 (13-1-al27.arubanetworks.com) for 52 mins
Last Seen:	5/28/2013 1:01 PM on 13-AP09 (13-ap09.arubanetworks.com) for 3 hrs 30 mins
Device Type:	□ Windows 7
OS:	□ Windows 7
OS Detail:	□ Windows NT 6.1; WOW64; rv:21.
Manufacturer:	□
Model:	□
Serial Number:	□
Phone Number:	□
Network Interface Vendor:	Intel
Network Chipset:	□
Network Driver:	□
EAP Supplicant:	□
Asset ID:	□
Asset Group:	□
Asset Category:	□
Service Start:	□
Service End:	□
AOS Device Type:	Win 7
Aruba HTTP Fingerprint:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
Classification:	Valid
Steerable:	No
Watched Client:	○ Yes ○ No
Notes:	

Classifying Aruba Devices in Client Detail

If you have deployed Aruba controllers and have WMS Offload enabled on the network, the **Clients > Client Detail** page allows you to classify the device in the **Device Information** section, and to push this configuration to the controllers that govern the devices. The classifications are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—If the **Protect Valid Stations** option is enabled, this setting designates the device as a legitimate network device. When this **Valid** setting is pushed, this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—When this status is pushed to the device, Aruba will attempt to keep it contained from the network.

You can classify the user regardless of whether WMS Offload is enabled. If WMS Offload is enabled, the classification will get pushed up to the controller.

Quick Links for Clients on Aruba Devices

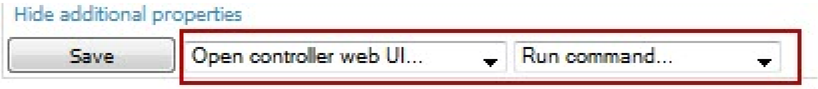
In **Clients > Client Detail**, the following two drop-down menus appear next to the **Save** button in the **Device Info** section:

- **Open controller web UI:** A drop-down menu that allows you to jump to the controller's UI in a new window. Thin APs link to **Controller > Access Points** when not operating in mesh mode, or **Controller > Mesh Nodes** otherwise.

Controllers show several more pages in this menu (**Security Dashboard**, for instance) if the controller is running ArubaOS version 6.1 or greater.

- **Run a command:** A drop-down menu with a list of CLI commands you can run directly from the **APs/Devices > Monitor** page.

Figure 151 *Open controller web UI and Run a command Menus*

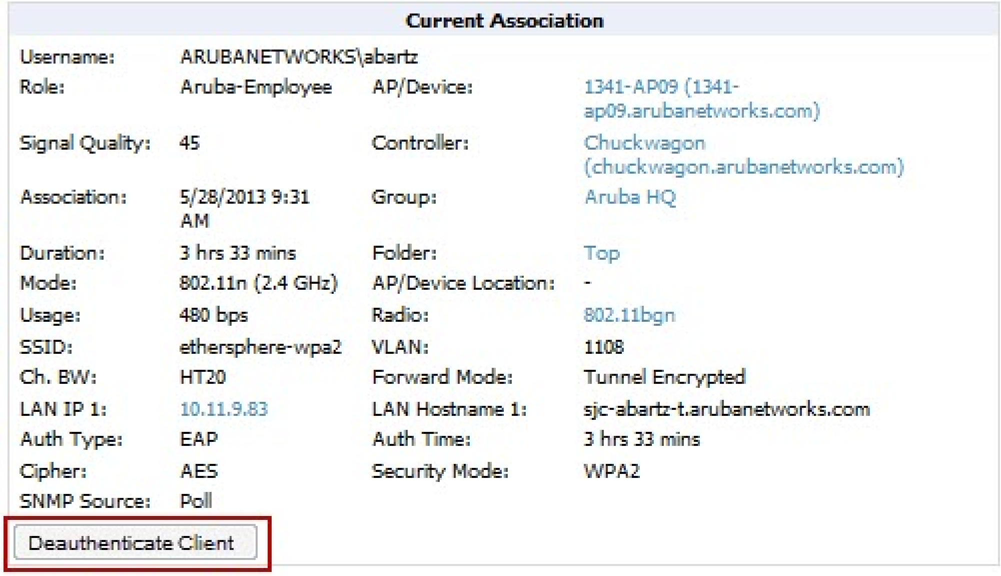


Using the Deauthenticate Client Feature

Some displays of the **Clients > Client Detail** page include the Deauthenticate Client feature in the Current Association section. Specifically, those displays are for devices which support this operation, namely Aruba and Cisco WLC with firmware version v4.0.0.0 or later.

Select Deauthenticate Client to use this feature, as shown in Figure 152:

Figure 152 *Deauthenticate Client button in Current Association section of Clients > Client Detail*



Current Association

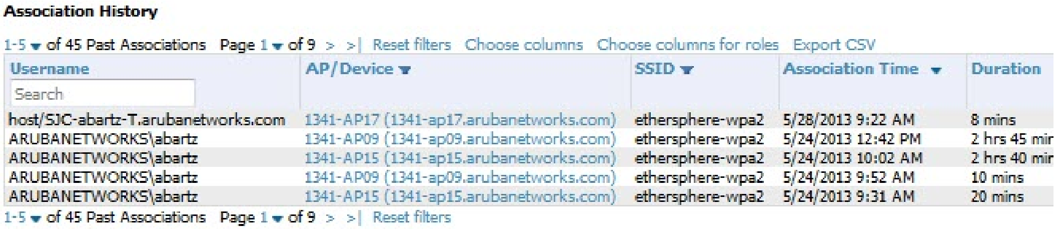
Username:	ARUBANETWORKS\abartz		
Role:	Aruba-Employee	AP/Device:	1341-AP09 (1341-ap09.arubanetworks.com)
Signal Quality:	45	Controller:	Chuckwagon (chuckwagon.arubanetworks.com)
Association:	5/28/2013 9:31 AM	Group:	Aruba HQ
Duration:	3 hrs 33 mins	Folder:	Top
Mode:	802.11n (2.4 GHz)	AP/Device Location:	-
Usage:	480 bps	Radio:	802.11bgn
SSID:	ethersphere-wpa2	VLAN:	1108
Ch. BW:	HT20	Forward Mode:	Tunnel Encrypted
LAN IP 1:	10.11.9.83	LAN Hostname 1:	sjc-abartz-t.arubanetworks.com
Auth Type:	EAP	Auth Time:	3 hrs 33 mins
Cipher:	AES	Security Mode:	WPA2
SNMP Source:	Poll		

Viewing a Client's Association History

Past association details of a client are tracked in the **Association History** table, which is located under the VRF QuickView illustration (if available) and the **Alert Summary** in **Clients > Client Detail**.

The columns in this table, shown in Figure 153, are the same as the fields in the **Current Association** section for this user.

Figure 153 *Association History in Clients > Client Detail (partial view)*



Association History

1-5 of 45 Past Associations Page 1 of 9 > >| Reset filters Choose columns Choose columns for roles Export CSV

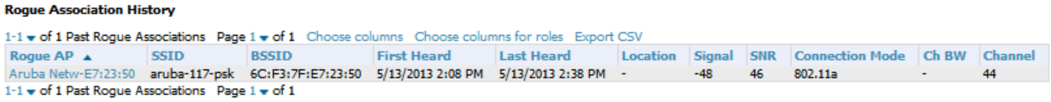
Username	AP/Device	SSID	Association Time	Duration
Search				
host/SJC-abartz-T.arubanetworks.com	1341-AP17 (1341-ap17.arubanetworks.com)	ethersphere-wpa2	5/28/2013 9:22 AM	8 mins
ARUBANETWORKS\abartz	1341-AP09 (1341-ap09.arubanetworks.com)	ethersphere-wpa2	5/24/2013 12:42 PM	2 hrs 45 mir
ARUBANETWORKS\abartz	1341-AP15 (1341-ap15.arubanetworks.com)	ethersphere-wpa2	5/24/2013 10:02 AM	2 hrs 40 mir
ARUBANETWORKS\abartz	1341-AP09 (1341-ap09.arubanetworks.com)	ethersphere-wpa2	5/24/2013 9:52 AM	10 mins
ARUBANETWORKS\abartz	1341-AP15 (1341-ap15.arubanetworks.com)	ethersphere-wpa2	5/24/2013 9:31 AM	20 mins

1-5 of 45 Past Associations Page 1 of 9 > >| Reset filters

Viewing the Rogue Association History for a Client

Past association details of a rogue client are tracked in the **Rogue Association History** table, which is located under the Association History table in **Clients** > **Client Detail**.

Figure 154 *Rogue Association History table in Clients > Client Detail*



Rogue Association History

1-1 ▾ of 1 Past Rogue Associations Page 1 ▾ of 1 Choose columns Choose columns for roles Export CSV

Rogue AP ▲	SSID	BSSID	First Heard	Last Heard	Location	Signal	SNR	Connection Mode	Ch BW	Channel
Aruba Netw-E7:23:50	aruba-117-psk	6C:F3:7F:E7:23:50	5/13/2013 2:08 PM	5/13/2013 2:38 PM	-	-48	46	802.11a	-	44

1-1 ▾ of 1 Past Rogue Associations Page 1 ▾ of 1

Evaluating Client Status with the Clients > Diagnostics Page

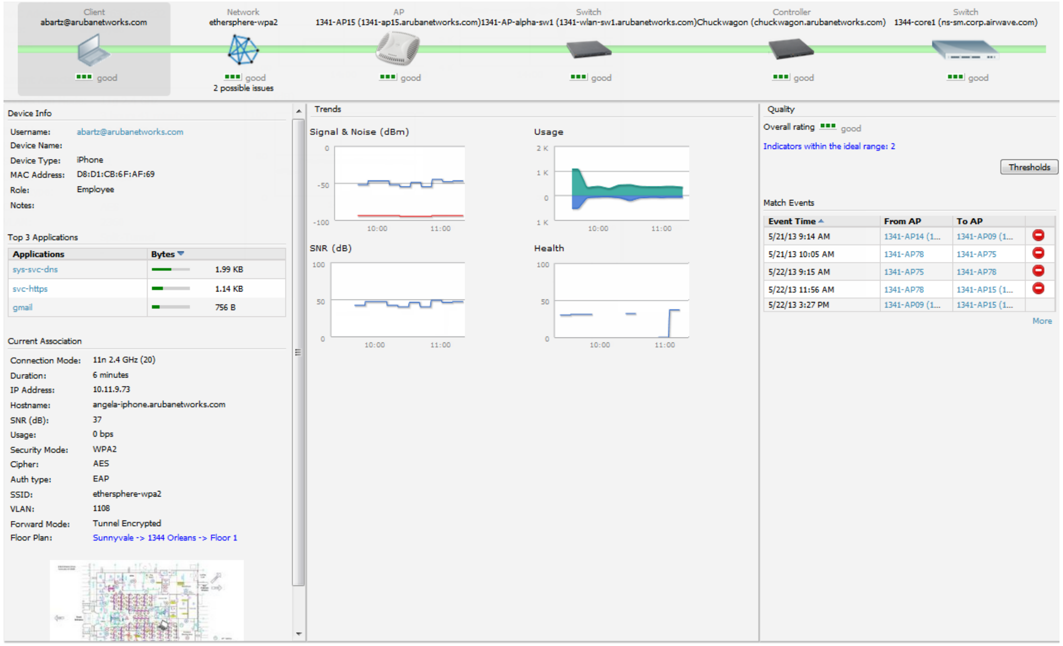
The **Clients** > **Diagnostics** page is accessible from the **Clients** > **Client Detail** page. You can access this page after performing a search for a user and the select the associated MAC address from the search results.

This page provides an overview of a WLAN user's general status and connectivity on the network, as illustrated in Figure 155.

NOTE

This page is only available for connected clients.

Figure 155 *Clients > Diagnostics page illustration*



Client
abartz@arubanetworks.com
■■■ good
Network
ethersphere-wpa2
■■■ good
2 possible issues
AP
1341-AP15 (1341-ap15.arubanetworks.com)
■■■ good
Switch
1341-AP-alpha-sw1 (1341-wlan-sw1.arubanetworks.com)
■■■ good
Controller
Chuckwagon (chuckwagon.arubanetworks.com)
■■■ good
Switch
1344-core1 (ns-sm.corp.airwave.com)
■■■ good

Device Info

Username: abartz@arubanetworks.com
Device Name:
Device Type: iPhone
MAC Address: D8:D1:CB:6F:AF:69
Role: Employee
Notes:

Top 3 Applications

Applications	Bytes ▾
sys-svc-dns	1.99 KB
svc-https	1.14 KB
gmail	756 B

Current Association

Connection Mode: 11n 2.4 GHz (20)
Duration: 6 minutes
IP Address: 10.11.9.73
Hostname: angela-iphone.arubanetworks.com
SNR (dB): 37
Usage: 0 bps
Security Mode: WPA2
Cipher: AES
Auth type: EAP
SSID: ethersphere-wpa2
VLAN: 1108
Forward Mode: Tunnel Encrypted
Floor Plan: Sunnyvale -> 1344 Orleans -> Floor 1

Quality

Overall rating ■■■ good

Indicators within the ideal range: 2

Thresholds

Match Events

Event Time ▲	From AP	To AP
5/21/13 9:14 AM	1341-AP14 (1...	1341-AP09 (1...
5/21/13 10:05 AM	1341-AP78	1341-AP75
5/22/13 9:15 AM	1341-AP75	1341-AP78
5/22/13 11:56 AM	1341-AP78	1341-AP15 (1...
5/22/13 3:27 PM	1341-AP09 (1...	1341-AP15 (1...

More

Each section of the **Clients** > **Diagnostics** page displays information by which to evaluate possible user issues, including the current association, usage, SNR value, health, steer events, and more. You can also click on the **Thresholds** button in the right panel to configure Good and Fair threshold values for APs, Clients, Controllers, Networks, and Switches. Note that values that fall below **Fair** are automatically considered as **Poor**.

Managing Mobile Devices with SOTI MobiControl and AirWave

Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Apple, and Android devices, has been integrated into AMP to provide direct access to the MobiControl Web Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Refer to the following for additional information:

- "Prerequisites for Using MobiControl with AirWave" on page 251
- "Adding a Mobile Device Management Server for MobiControl" on page 251
- "Accessing MobiControl from the Clients > Client Detail Page " on page 252

Prerequisites for Using MobiControl with AirWave

In order to use the MobiControl integration in AirWave, the following is required:

- An AMP running version 7.2.3 or later
- An MDM server with SOTI MobiControl Console 8.0x
- A client device that is:
  - associated with WLAN infrastructure managed by the AMP server running 7.2.3 or later
  - being actively managed by the SOTI MobiControl server

For more information about setting up MobiControl, please see http://www.soti.net/mc/help/.

In order to use SOTI MobiControl from within AMP, you must first add your MDM server and designate it as a MobiControl.

Adding a Mobile Device Management Server for MobiControl

1. To add an MDM server to AMP, navigate to **AMP Setup > MDM Server** and click **Add**. Complete the fields on this page. Table 123 describes the settings and default values:

Table 123: *AMP Setup > MDM Server > Add Fields and Descriptions*

Field	Description
Hostname/IP Address	The address or DNS hostname configured for your MobiControl Web Console.
Protocol	Whether HTTP or HTTPS is to be used when polling the MDM server. The port on which to connect to the MDM server is inferred from the protocol: with HTTP, AMP will connect to port 80 of the SOTI server; with HTTPS, AMP will connect to port 443.
URL Context	The URL context appended to the server URL to build the URL when connecting with the SOTI server. For MobiControl v8.0x the default URL Context is MobiControlWeb. For MobiControl v8.5x the default URL Context is MobiControl.
Enabled	Whether this server can be polled by AMP. Make sure it is set to **Yes**.
Username/Password	The login credentials for accessing the web console of the MobiControl system.
Polling Period	The frequency in which AMP polls the MDM server. The default is 5 minutes.

2. When finished, select **Add.**

The list page for the MDM server also displays:

- **Last Contacted –** The last time AMP was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, AMP will obtain a list of all device IDs and their WLAN MAC addresses. The information about device OS, device OS Detail, Manufacturer, Model, Name are retrieved from MobiControl and populated to the **Clients** > **Client Detail** page for supported mobile devices. A **View device in SOTI MobiControl** link provides direct access to the MobiControl Web Console for additional details about the device. MobiControl information overrides data obtained from ArubaOS controllers running 6.0 or later.

Accessing MobiControl from the Clients > Client Detail Page

In order to access the MobiControl web console for a SOTI-managed mobile device from within AMP, follow these steps:

1. Navigate to a page that lists clients. This can include:
   - **Clients** > **Connected** or **Clients** > **All**
   - Search results that display user MAC addresses
2. Select the MAC address in the **Clients** list table. The **Clients** > **Client Detail** page displays.
3. Under the Classification field, select the **View device in SOTI MobiControl** link. A new window will display the MobiControl Web Console for this device.

Monitoring and Supporting AMP with the Home Pages

The **Home** tab of AMP provides the most frequent starting point for monitoring network status and establishing primary AMP functions after AMP configuration is complete. From the **Home** tab, you can access the following pages.

Table 124: *Home pages*

Home Page	Description	Refer to
Overview	This page condenses a large amount of information about your AMP. You can view the health and usage of your network and use shortcuts to view system information.	"Monitoring AMP with the Home > Overview Page" on page 253.
Firewall	This page allows IT to view mobile app usage and performance on the network.	"Using the Home > Firewall Page" on page 255
RF Performance	This page provides graphs that enable you to identify clients with low SNR rates, speed, and goodput. Users can click on a value in any of the graphs to view detailed client information. When the client information is displayed, an additional drill down to a folder level is available to view a specific client. Note that the Speed and Goodput graphs are only populated with information from Aruba devices that support AMON.	"Viewing the Home > RF Performance Page" on page 256.
RF Capacity	This page provides admin users with a summary of network usage over a one-week period. This information includes the number of clients and the channel utilization percentages. This information is run once per day after nightly maintenance is completed.	"Viewing the Home > RF Capacity Page" on page 257

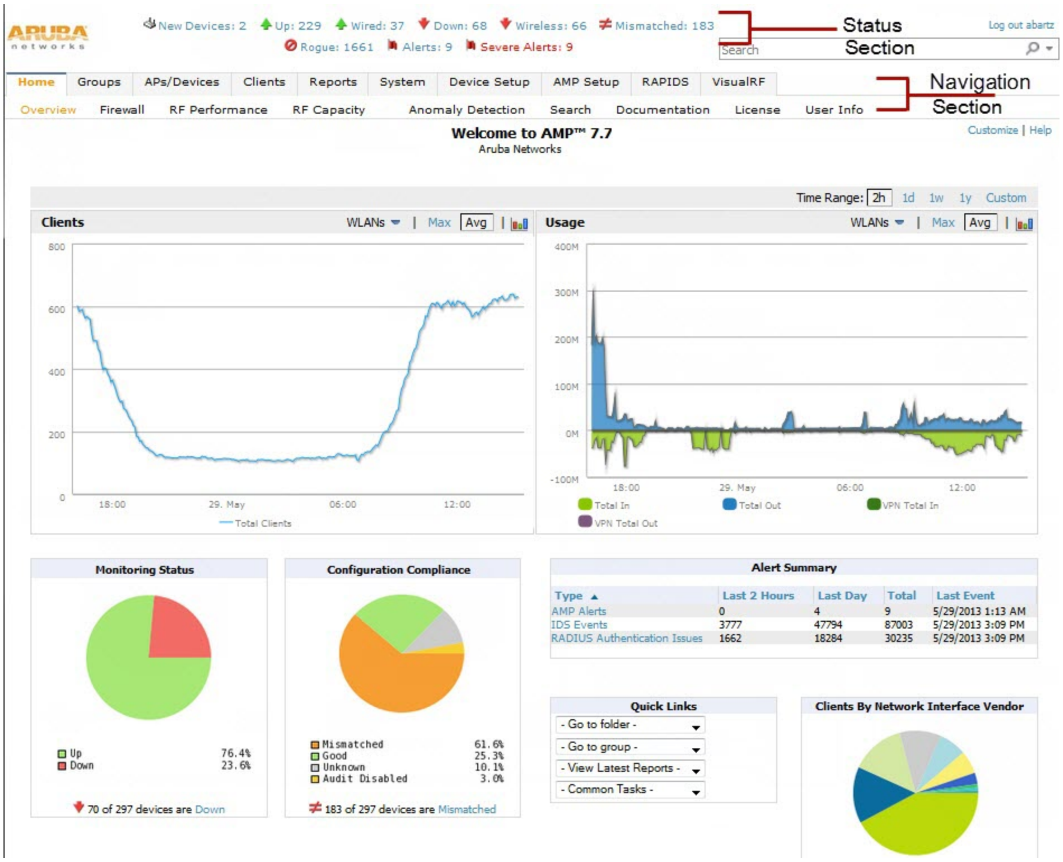
Table 124: *Home pages (Continued)*

Home Page	Description	Refer to
Network Deviations	This page provides graphs that track your network's Client and Usage information and draw attention to unusual network usage patterns	"Viewing the Home > Network Deviations Page" on page 258
Search	This page provides a simple way to find users. managed devices, groups, and rogues.	"The Home > Search Page " on page 260
Documentation	This page contains all relevant AirWave documentation.	"Accessing AirWave Documentation " on page 261
License	This page provides product licensing information	"Viewing and Updating License Information " on page 262
User Info	This page is where logged-in users can configure their name, contact information, rogue count filter level, customized header columns, severe alert threshold, personalized search preferences, record display preferences, and the refresh rate of the console.	"Configuring Your Own User Information with the Home > User Info Page" on page 263

Monitoring AMP with the Home > Overview Page

To view your overall network health, navigate to **Home** > **Overview** page. Figure 156 illustrates this page, and Table 125 describes the contents. The information that displays varies depending on your role.

Figure 156 *Home > Overview Page Illustration*



Alert Summary

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	4	9	5/29/2013 1:13 AM
IDS Events	3777	47794	87003	5/29/2013 3:09 PM
RADIUS Authentication Issues	1662	18284	30235	5/29/2013 3:09 PM

Table 125: *Home > Overview Sections and Charts*

Section	Description
Clients	This chart is a graphical summary of the number of users on the network during a period of time. The time can be adjusted. Select **Show All** to display a list of data series that this graph can display, such as the user count by SSID. Clear the **Max Clients** or **Avg Clients** check box to change the display of the graph. The graph displays the maximum number of users by default. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.
Usage	This adjustable chart displays bandwidth data over time. To remove bandwidth in or out from the graphical display, clear the check box for **Avg Bits Per Second In** or **Out**. To display details for specific devices, select **Show All** and select the devices to be included in the graphical bandwidth summary chart. To view historical graphs in a new window, select the three-bar icon on the upper right of the chart.
Monitoring Status	This pie chart shows the percentage of all devices that are up and down on the network. To review devices that are down, select **Down** in the legend or the chart, and the **APs/Devices > Down** page displays.
Configuration Compliance	The pie chart displays all known device configuration status on the network. Devices are classified as **Good**, **Unknown**, **Mismatched,** or **Audit Disabled**. Select the **Mismatched** link to see the **APs/Devices > Mismatched** page.
Alert Summary	This section displays all known and current alerts configured and enabled in the **System > Alerts** page (refer to "Viewing, Delivering, and Responding to Triggers and Alerts" on page 226). Alerts can be sorted using the column headers (**Type**, **Last 2 Hours**, **Last Day**, **Total**, or **Last Event**). The **Alert Summary** field displays three types of alerts: ● AMP Alerts ● IDS Events ● RADIUS Authentication Issues Select any alert type for more information.
Quick Links	The **Quick Links** section provides drop-down menus that enable you to move to the most common and frequently used pages in AMP as follows: ● **Go to folder**–This menu lists all folders defined in AMP from the **APs/Devices List** page. See "Using Device Folders (Optional)" on page 155. ● **Go to group**–This menu lists all groups defined in AMP, 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" on page 77. ● **View Latest Reports**–AMP supports creating custom reports or viewing the latest daily version of any report. Select any report type to display the daily version. See "Creating, Running, and Emailing Reports" on page 271. ● **Common Tasks**–This menu lists quick links to the most heavily used task-oriented pages in AMP, to include the following: ■ **Configure Alert Thresholds**–This link takes you to the **System > Triggers** page. See "Viewing Triggers" on page 227. ■ **Configure Default Credentials**–This link takes you to the **Device Setup > Communication** page. See "Configuring Communication Settings for Discovered Devices" on page 57. ■ **Discover New Devices on Your Network**–This link takes you to the **Device Setup > Discover** page. See "Discovering, Adding, and Managing Devices " on page 124. ■ **Supported Devices and Features**–This link displays a PDF that summarizes all supported devices and features in chart format for AMP. ■ **Upload Device Firmware**–This link displays the **Device Setup > Upload Firmware & Files & Files**

Table 125: *Home > Overview Sections and Charts (Continued)*

Section	Description
	Upload page. See "Loading Device Firmware Onto AMP (optional)" on page 59. ■ **View Event Log**–This link displays the **System > Event Log** page. See "Using the System > Event Log Page" on page 218.

The **Customize** link on the upper-right side of the page allows you to customize the widgets on the **Home** > **Overview** page. See "Customizing the Dashboard" on page 22 for more information.

Using the Home > Firewall Page

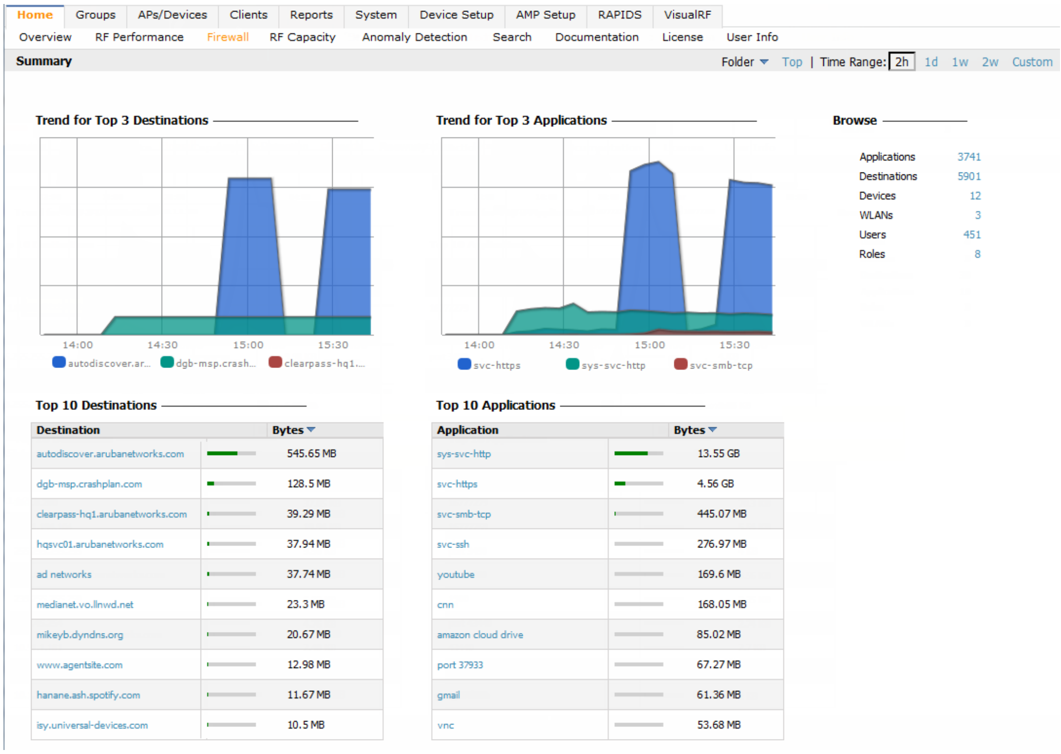
The **Home** > **Firewall** page allows network admins to view mobile app usage and performance on the network. This page is disabled by default. The option to enable this page is on the **AMP Setup** > **General** page under the Additional AMP Services section.

This page mimics the Firewall page on the controller. It provides charts to easily view trending information for the top three destinations and applications for a selected folder. You can drill down to view more specific information based on the application, destination, device, WLAN, user, and role.

AirWave can provide up to two weeks of network data for multiple controllers. This data can be used to troubleshoot application performance in real time, to set WLAN policies, and to plan for future network enhancements.

> NOTE
>
> The **Home > Firewall** pages may show IP addresses rather than resolved names. AirWave receives this message from the controller via AMON and does not automatically resolve the IP addresses. In addition, the query that performs this function requires an authenticated controller user with the appropriate CLI credentials.

Figure 157 *Home > Firewall page*



Applications	3741
Destinations	5901
Devices	12
WLANs	3
Users	451
Roles	8

Top 10 Destinations

Destination	Bytes ▾
autodiscover.arubanetworks.com	545.65 MB
dgb-msp.crashplan.com	128.5 MB
clearpass-hq1.arubanetworks.com	39.29 MB
hqsvc01.arubanetworks.com	37.94 MB
ad networks	37.74 MB
medianet.vo.llnwd.net	23.3 MB
mikeyb.dyndns.org	20.67 MB
www.agentsite.com	12.98 MB
hanane.ash.spotify.com	11.67 MB
isy.universal-devices.com	10.5 MB

Top 10 Applications

Application	Bytes ▾
sys-svc-http	13.55 GB
svc-https	4.56 GB
svc-smb-tcp	445.07 MB
svc-ssh	276.97 MB
youtube	169.6 MB
cnn	168.05 MB
amazon cloud drive	85.02 MB
port 37933	67.27 MB
gmail	61.36 MB
vnc	53.68 MB

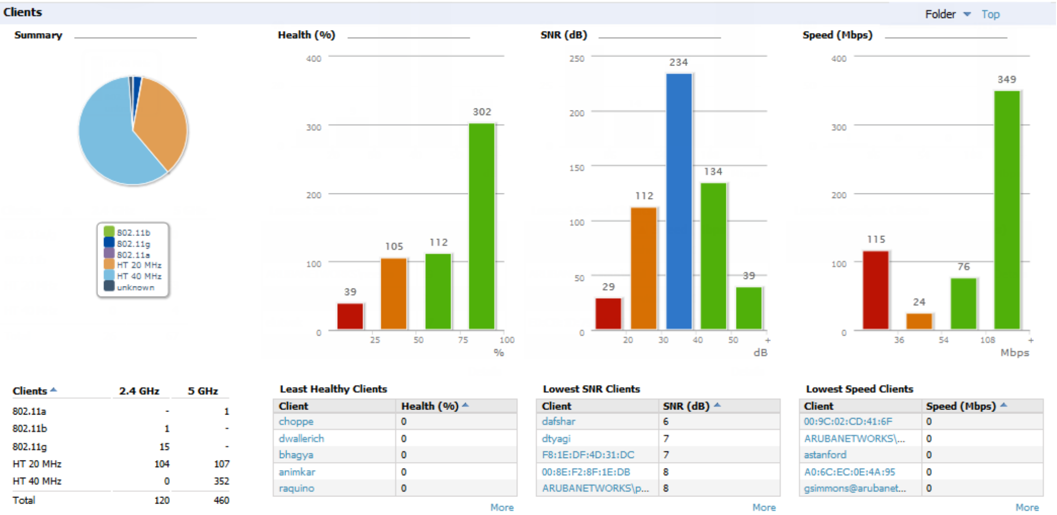
Viewing the Home > RF Performance Page

The **Home** > **RF Performance** page provides graphs that enable you to identify clients with low SNR rates, health, speed, and goodput. In the upper-left corner of this page, you can limit the information that displays by selecting a specific folder from the upper-right corner of the page.

NOTE

The Speed and Goodput graphs are only populated with information from Aruba devices that support AMON. The Health graph and chart are only populated with information from controllers running ArubaOS 6.3 or greater.

Figure 158 *Home > RF Performance*



Clients ▲	2.4 GHz	5 GHz
802.11a	-	1
802.11b	1	-
802.11g	15	-
HT 20 MHz	104	107
HT 40 MHz	0	352
Total	120	460

Least Healthy Clients

Client	Health (%) ▲
choppe	0
dwallerich	0
bhagya	0
animkar	0
raquino	0

More

Lowest SNR Clients

Client	SNR (dB) ▲
dafshar	6
dtyagi	7
F8:1E:DF:4D:31:DC	7
00:8E:F2:8F:1E:DB	8
ARUBANETWORKS\p...	8

More

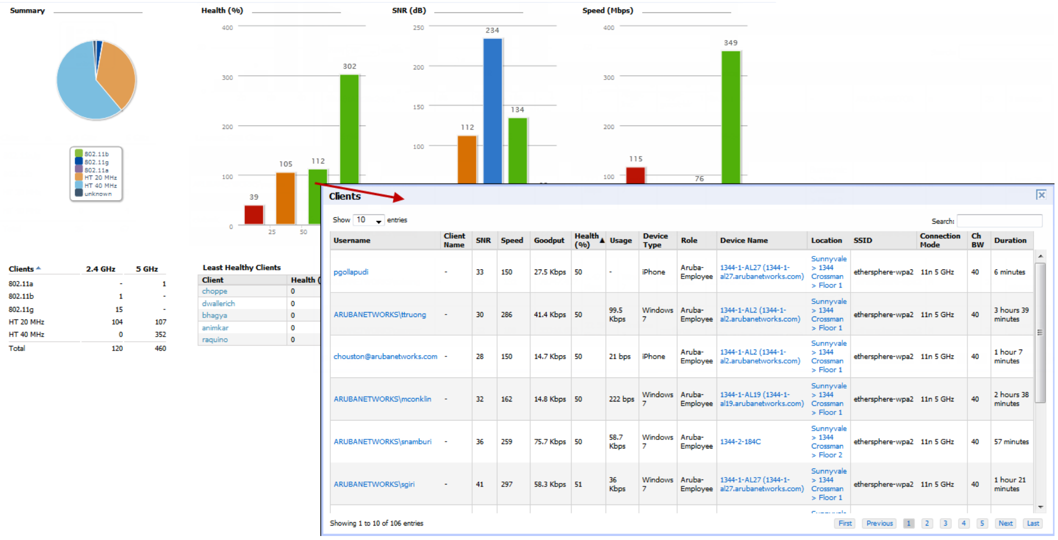
Lowest Speed Clients

Client	Speed (Mbps) ▲
00:9C:02:CD:41:6F	0
ARUBANETWORKS\...	0
astanford	0
A0:6C:EC:0E:4A:95	0
gsimmons@arubanet...	0

More

You can click on a value in any of the graphs to view the associated list of clients.

Figure 159 *Drill down to view all clients*



Username	Client Name	SNR	Speed	Goodput	Health (%) ▲	Usage	Device Type	Role	Device Name	Location	SSID	Connection Mode	Ch BW	Duration
pgollapudi	-	33	150	27.5 Kbps	50	-	iPhone	Aruba-Employee	1344-1-AL27 (1344-1-al27.arubanetworks.com)	Sunnyvale > 1344 Crossman > Floor 1	ethersphere-wpa2	11n 5 GHz	40	6 minutes
ARUBANETWORKS\ttruong	-	30	286	41.4 Kbps	50	99.5 Kbps	Windows 7	Aruba-Employee	1344-1-AL2 (1344-1-al2.arubanetworks.com)	Sunnyvale > 1344 Crossman > Floor 1	ethersphere-wpa2	11n 5 GHz	40	3 hours 39 minutes
chouston@arubanetworks.com	-	28	150	14.7 Kbps	50	21 bps	iPhone	Aruba-Employee	1344-1-AL2 (1344-1-al2.arubanetworks.com)	Sunnyvale > 1344 Crossman > Floor 1	ethersphere-wpa2	11n 5 GHz	40	1 hour 7 minutes
ARUBANETWORKS\mconklin	-	32	162	14.8 Kbps	50	222 bps	Windows 7	Aruba-Employee	1344-1-AL19 (1344-1-al19.arubanetworks.com)	Sunnyvale > 1344 Crossman > Floor 1	ethersphere-wpa2	11n 5 GHz	40	2 hours 38 minutes
ARUBANETWORKS\snamburi	-	36	259	75.7 Kbps	50	58.7 Kbps	Windows 7	Aruba-Employee	1344-2-184C	Sunnyvale > 1344 Crossman > Floor 2	ethersphere-wpa2	11n 5 GHz	40	57 minutes
ARUBANETWORKS\sgiri	-	41	297	58.3 Kbps	51	36 Kbps	Windows 7	Aruba-Employee	1344-1-AL27 (1344-1-al27.arubanetworks.com)	Sunnyvale > 1344 Crossman > Floor 1	ethersphere-wpa2	11n 5 GHz	40	1 hour 21 minutes

Showing 1 to 10 of 106 entries

When the client information is displayed, an additional drill down is available to view information for a specific client, device, or location.

NOTE

When you click on a Username in the Client page, the drill down takes you to the **Clients > Diagnostics** page. Navigate to the **Clients > Client Details** page for additional detailed information about the selected client.

Viewing the Home > RF Capacity Page

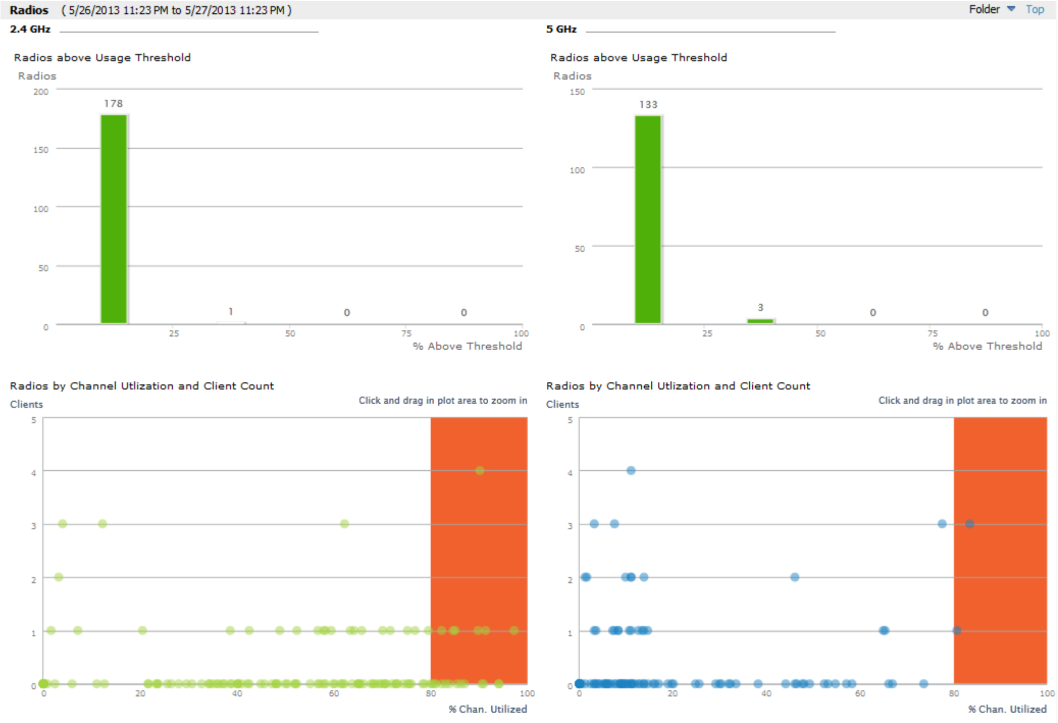
The **Home** > **RF Capacity** page provides summarized client and channel information for traffic that occurred on your network over the last week. This page is updated after nightly maintenance has completed. The process goes over all the radios and determines the maximum client count and maximum channel utilization for each radio.

This page includes two sets of graphs. The top tables show the total number of clients that have connected over the last week (2.4 GHz and 5 GHz) and the percentage of these that were above the usage threshold. The bottom graphs show the number of clients that were connected during low and high channel utilization.

NOTE

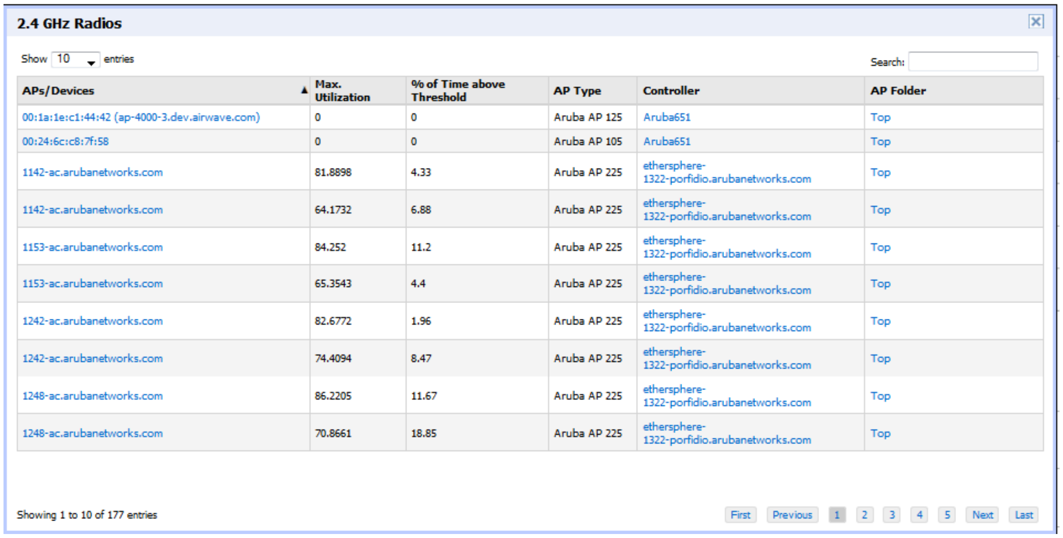
This page is only available to Admin users.

Figure 160 *The Home > RF Capacity page*


Radios (5/26/2013 11:23 PM to 5/27/2013 11:23 PM)
Folder ▼ Top
2.4 GHz
Radios above Usage Threshold
Radios
200
150
100
50
0
178
1
0
0
25
50
75
100
% Above Threshold
5 GHz
Radios above Usage Threshold
Radios
150
100
50
0
133
3
0
0
25
50
75
100
% Above Threshold
Radios by Channel Utlization and Client Count
Clients
Click and drag in plot area to zoom in
5
4
3
2
1
0
20
40
60
80
100
% Chan. Utilized
Radios by Channel Utlization and Client Count
Clients
Click and drag in plot area to zoom in
5
4
3
2
1
0
20
40
60
80
100
% Chan. Utilized

You can click on a bar in the upper graphs to view a popup showing a detailed list of the devices that connected in the week before the RF Capacity page was run. This popup includes additional drill downs to the device, the controller, and the folder. You can also search in this popup.

Figure 161 *Example of 2.4 GHz radio popup*



2.4 GHz Radios

Show 10 entries

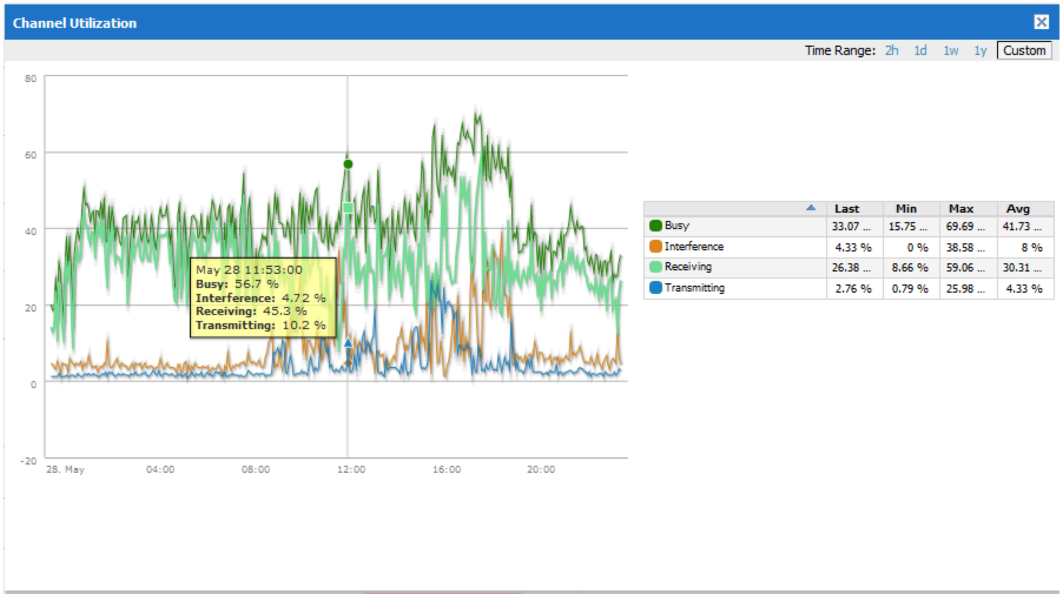
Search:

APs/Devices ▲	Max. Utilization	% of Time above Threshold	AP Type	Controller	AP Folder
00:1a:1e:c1:44:42 (ap-4000-3.dev.airwave.com)	0	0	Aruba AP 125	Aruba651	Top
00:24:6c:c8:7f:58	0	0	Aruba AP 105	Aruba651	Top
1142-ac.arubanetworks.com	81.8898	4.33	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1142-ac.arubanetworks.com	64.1732	6.88	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1153-ac.arubanetworks.com	84.252	11.2	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1153-ac.arubanetworks.com	65.3543	4.4	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1242-ac.arubanetworks.com	82.6772	1.96	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1242-ac.arubanetworks.com	74.4094	8.47	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1248-ac.arubanetworks.com	86.2205	11.67	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top
1248-ac.arubanetworks.com	70.8661	18.85	Aruba AP 225	ethersphere-1322-porfidio.arubanetworks.com	Top

Showing 1 to 10 of 177 entries

The plot points in the lower graph shows the number of clients that were connected during the peak utilization time along with the channel utilization percentage. You can select plot points in the lower graph to view detailed channel utilization information for the selected plot point.

Figure 162 *Example popup showing channel utilization*



Channel Utilization

May 28 11:53:00
Busy: 56.7 %
Interference: 4.72 %
Receiving: 45.3 %
Transmitting: 10.2 %

▲	Last	Min	Max	Avg
🟩 Busy	33.07 ...	15.75 ...	69.69 ...	41.73 ...
🟧 Interference	4.33 %	0 %	38.58 ...	8 %
🟩 Receiving	26.38 ...	8.66 %	59.06 ...	30.31 ...
🟦 Transmitting	2.76 %	0.79 %	25.98 ...	4.33 %

Viewing the Home > Network Deviations Page

The **Home** > **Network Deviations** page provides graphs that track your network's Client and Usage information and draw attention to unusual network usage patterns. These graphs can show you, for example, if heavy network traffic is occurring during off hours, or they can be used to detect the time(s) of day when your network traffic peaks.

By default, the graph lines display, in five-minute intervals, the previous 2 hours of client and usage information for the current day of the week averaged out over the last 40 weeks. The shaded area indicates the standard deviation, which defaults to 1. So, for example, if you launch this page at 9:00 am on a Friday, then a 2-hour graph will show the current and average number of connected clients and usage between 7:00 AM and 9:00 AM on all Fridays over the last 40 weeks, with plot points showing the number of clients for every five minutes. You can also select/drag a set of plot points to zoom in and view a more precise time range. Click the **Reset zoom** button to return to the specified time range.

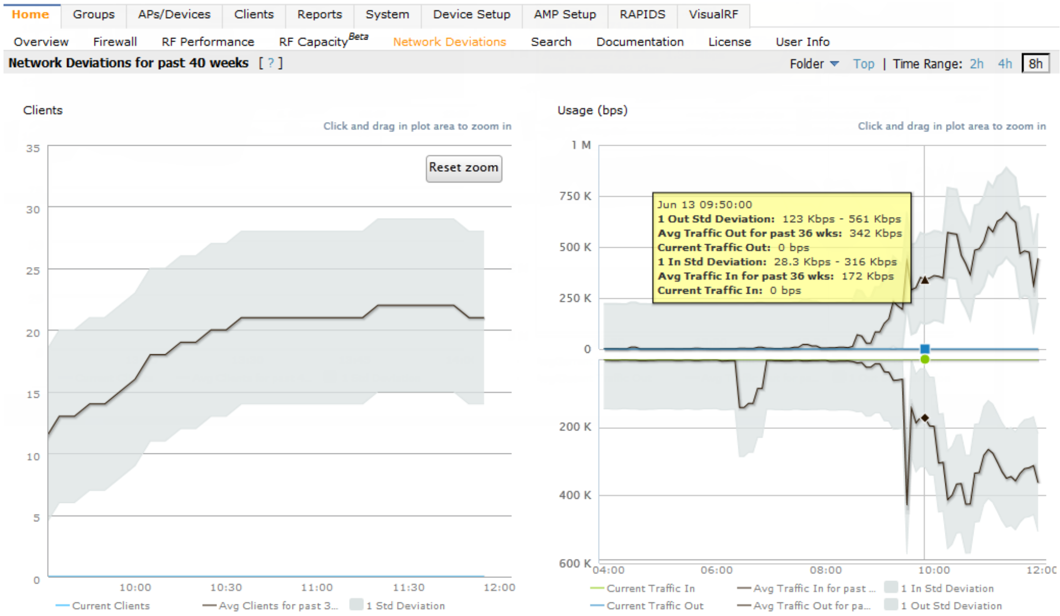
You can change the time range of the graphs to 4 hours, 8 hours, or 1 day using the time-range options in the upper-right corner of this page, and AMP will remember the new setting the next time the page is launched.

The left graph shows client information - specifically the current and average number of clients over the last 40 weeks during the selected time range. The right graphs show usage information - specifically the current and average incoming and outgoing bits-per-second over the last 40 weeks during the selected time range. The shaded/gray color within the graphs indicates the standard deviation. Any blue lines (Avg Clients, Avg Out Usage) or green lines (Avg In Usage) that appear outside of the shaded/gray area can be considered deviation points because the value does not come within the range of the calculated standard deviation.

NOTE

This operation can consume a significant amount of CPU capacity as it parses through large amounts of data. Larger deployments you may have to wait up to a minute before seeing the initial graph plot points. In addition, this page does not automatically refresh, rather it refreshes each time this page is selected and/or each time you click Refresh. As a result, if you click this page, navigate away, and then return to this page, the page will begin to load again. If your network includes a large amount of data, then a best practice is to open this page in a new tab before navigating to another page. In this case, the Network Deviations page will continue to load while you continue to work in AMP.

Figure 163 *Home > Network Deviations page*



Jun 13 09:50:00
1 Out Std Deviation: 123 Kbps - 561 Kbps
Avg Traffic Out for past 36 wks: 342 Kbps
Current Traffic Out: 0 bps
1 In Std Deviation: 28.3 Kbps - 316 Kbps
Avg Traffic In for past 36 wks: 172 Kbps
Current Traffic In: 0 bps

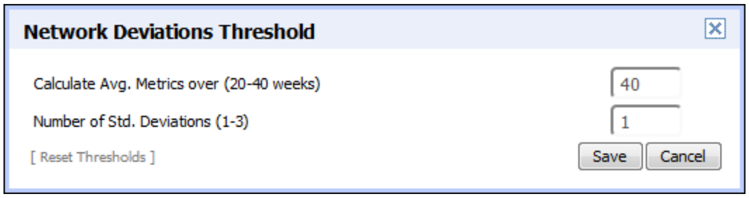
The first time this page is launched, the graphs will display information for all devices in the Top folder. To specify a different folder, simply select one from the folder drop down in the upper-right corner, and then refresh the page. AMP will remember the new setting the next time that the page is launched.

By default, the graphs display average and standard deviation information for the current time over the last 40 weeks. Click the **Thresholds** button in the lower right corner to change these defaults. AMP will remember the new setting the next time that the page is launched.

NOTE

The **Thresholds** button is disabled while the page is loading. The **Folder** drop down is disabled until the first plot points display.

Figure 164 *Network Deviations Threshold*



Network Deviations Threshold

Calculate Avg. Metrics over (20-40 weeks) 40

Number of Std. Deviations (1-3) 1

How Standard Deviation is Calculated

Plot lines may or may not display outside of the shaded, standard deviation range depending on the SD value specified from Thresholds button. Refer to the following example to review the way that standard deviation is calculated.

Standard Deviation Example

Assumptions:

- Mean: 5
- Standard Deviation: 2

```
SD(1):
-------
1*SD +- Mean
1*2 +- 5
2 +- 5
Normal Range: 3 - 7

SD(2):
-------
2*SD +- Mean
2*2 +- 5
4 +- 5
Normal Range: 1 - 9

SD(3):
-------
3*SD +- Mean
3*2 +- 5
6 +- 5
Normal Range: 0 - 11 (-1 is not considered, so 0 is taken)
```

Given the information above, if the Average Client Count over the last 40 weeks is 5, then this is not an anomaly (deviation) for any SD value. On the other hand, if at one point the client count was 8, then this would be an anomaly for SD1, whose normal client range is from 3-7. The plot point would appear outside of the shaded area when the standard deviation is set to 1, but it would be normal from a standard deviation of 2 or 3.

The Home > Search Page

The **Search** field at the top of every AMP page allows you to perform a search across a number of common categories. The **Home** > **Search** page provides the results of the search.

The Search feature can performs partial string searches on a large number of fields including the notes, version, secondary version, radio serial number, device serial number, LAN MAC, radio MAC and apparent IP address of all the APs, as well as the client MAC, VPN user, Client, LAN IP and VPN IP fields. Figure 165 illustrates this page.

To perform a search, enter the keyword or text in the search box. If you are searching for a MAC address, enter that in colon-delimited format. Then perform one of the following search functions:

- Press Enter to perform a default search. This default is based on the user search method preference specified **in Home > User Info**.
- Select a different search method from the list of drop-down options.

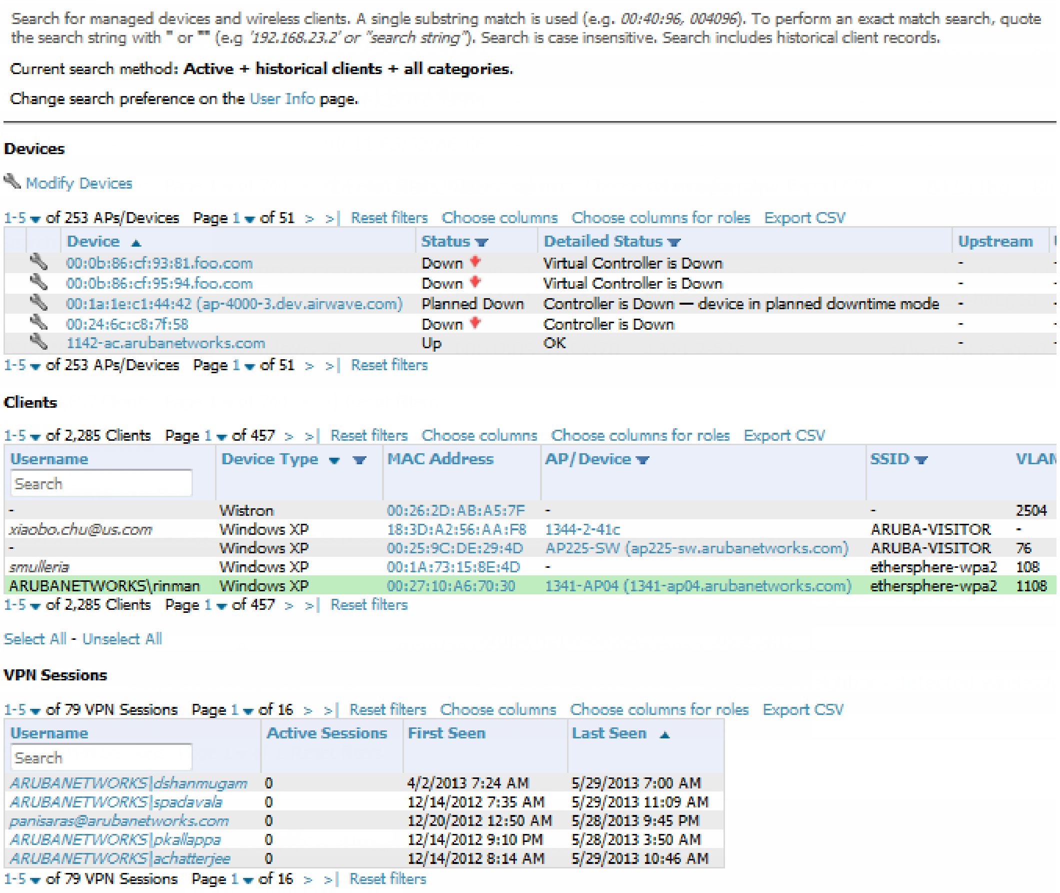
- Select the magnifying lens icon (🔍) to perform a quick search. The search results open in a separate popup and show results for connected clients. (Keep in mind that in some cases, this may already be the default search method.)

The results display after a short moment. Results support several hypertext links to additional pages, and the **Filter** icon over some columns allows 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 are returned for a given search:

- Devices
- Clients
- VPN Sessions
- Rogue Devices and Rogue Clients
- Tags
- Folders and Groups

Figure 165 *Home > Search Page Illustration with Sample Hits on 00: (partial view)*



Search for managed devices and wireless clients. A single substring match is used (e.g. *00:40:96, 004096*). To perform an exact match search, quote the search string with " or "" (e.g *'192.168.23.2' or "search string"*). Search is case insensitive. Search includes historical client records.

Current search method: **Active + historical clients + all categories.**

Change search preference on the User Info page.

Devices

Modify Devices

1-5 ▾ of 253 APs/Devices Page 1 ▾ of 51 > >| Reset filters Choose columns Choose columns for roles Export CSV

Device ▲	Status ▾	Detailed Status ▾	Upstream	
00:0b:86:cf:93:81.foo.com	Down	Virtual Controller is Down	-	-
00:0b:86:cf:95:94.foo.com	Down	Virtual Controller is Down	-	-
00:1a:1e:c1:44:42 (ap-4000-3.dev.airwave.com)	Planned Down	Controller is Down — device in planned downtime mode	-	-
00:24:6c:c8:7f:58	Down	Controller is Down	-	-
1142-ac.arubanetworks.com	Up	OK	-	-

1-5 ▾ of 253 APs/Devices Page 1 ▾ of 51 > >| Reset filters

Clients

1-5 ▾ of 2,285 Clients Page 1 ▾ of 457 > >| Reset filters Choose columns Choose columns for roles Export CSV

Username Search	Device Type ▾ ▾	MAC Address	AP/Device ▾	SSID ▾	VLAN
-	Wistron	00:26:2D:AB:A5:7F	-	-	2504
xiaobo.chu@us.com	Windows XP	18:3D:A2:56:AA:F8	1344-2-41c	ARUBA-VISITOR	-
-	Windows XP	00:25:9C:DE:29:4D	AP225-SW (ap225-sw.arubanetworks.com)	ARUBA-VISITOR	76
smulleria	Windows XP	00:1A:73:15:8E:4D	-	ethersphere-wpa2	108
ARUBANETWORKS\rinman	Windows XP	00:27:10:A6:70:30	1341-AP04 (1341-ap04.arubanetworks.com)	ethersphere-wpa2	1108

1-5 ▾ of 2,285 Clients Page 1 ▾ of 457 > >| Reset filters

Select All - Unselect All

VPN Sessions

1-5 ▾ of 79 VPN Sessions Page 1 ▾ of 16 > >| Reset filters Choose columns Choose columns for roles Export CSV

Username Search	Active Sessions	First Seen	Last Seen ▲
ARUBANETWORKS|dshanmugam	0	4/2/2013 7:24 AM	5/29/2013 7:00 AM
ARUBANETWORKS|spadavala	0	12/14/2012 7:35 AM	5/29/2013 11:09 AM
panisaras@arubanetworks.com	0	12/20/2012 12:50 AM	5/28/2013 9:45 PM
ARUBANETWORKS|pkallappa	0	12/14/2012 9:10 PM	5/28/2013 3:50 AM
ARUBANETWORKS|achatterjee	0	12/14/2012 8:14 AM	5/29/2013 10:46 AM

1-5 ▾ of 79 VPN Sessions Page 1 ▾ of 16 > >| Reset filters

Accessing AirWave Documentation

The **Home** > **Documentation** page provides easy access to all relevant AMP documentation. All of the documents on this page are hosted locally by your AMP server. The PDF files can be viewed by any PDF viewer, and the HTML files can be viewed in any supported browser.

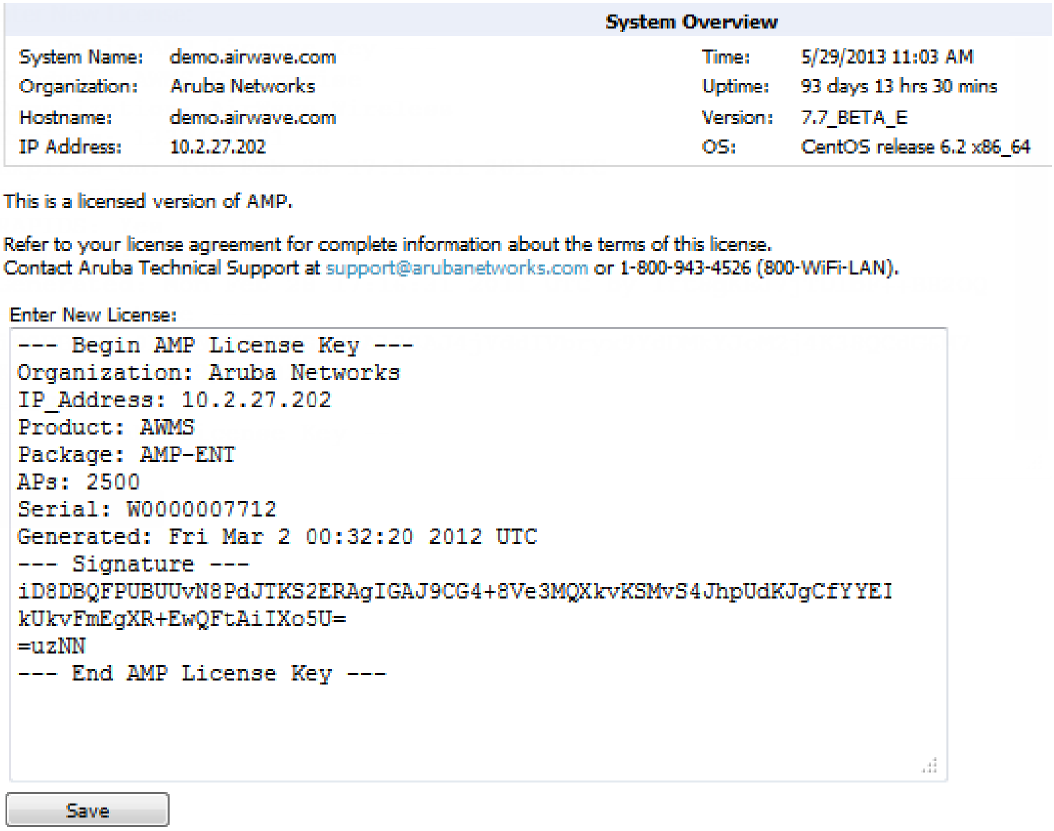
If you have any questions that are not answered by the documentation, please contact Aruba support.

Viewing and Updating License Information

Navigate to the **Home** > **License** page using the standard AMP menu. Figure 166 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 Aruba support.

Figure 166 *Home > License Page Illustration*



System Overview

System Name:	demo.airwave.com	Time:	5/29/2013 11:03 AM
Organization:	Aruba Networks	Uptime:	93 days 13 hrs 30 mins
Hostname:	demo.airwave.com	Version:	7.7_BETA_E
IP Address:	10.2.27.202	OS:	CentOS release 6.2 x86_64

This is a licensed version of AMP.

Refer to your license agreement for complete information about the terms of this license.
Contact Aruba Technical Support at support@arubanetworks.com or 1-800-943-4526 (800-WiFi-LAN).

Enter New License:

```
--- Begin AMP License Key ---
Organization: Aruba Networks
IP_Address: 10.2.27.202
Product: AWMS
Package: AMP-ENT
APs: 2500
Serial: W0000007712
Generated: Fri Mar 2 00:32:20 2012 UTC
--- Signature ---
iD8DBQFPUBUUvN8PdJTKS2ERAgIGAJ9CG4+8Ve3MQXkvKSMvS4JhpUdKJgCfYYEI
kUkvFmEgXR+EwQFtAiIXo5U=
=uzNN
--- End AMP License Key ---
```

Table 126: *Home > License Static Fields and Descriptions*

Field	Description
System Name	Displays a user-definable name for AMP. 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 AMP.
IP Address	Displays the static IP address assigned to AMP. The IP Address can be configured from the **AMP Setup > Network** page.
Time	Displays the current date and time set on AMP.
Uptime	Displays the amount of time since the operating system was last booted.

Table 126: *Home > License Static Fields and Descriptions (Continued)*

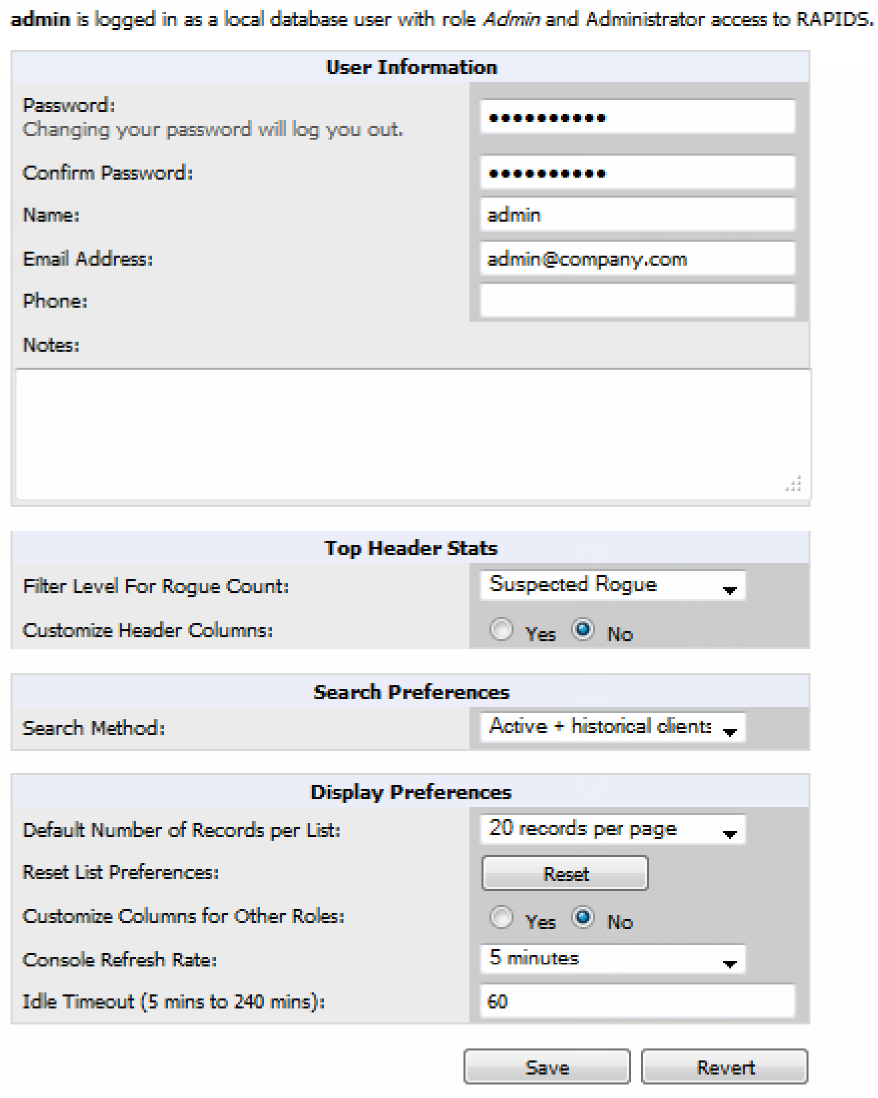
Field	Description
Version	Displays the version number of AMP code currently running.
OS	Displays the version of Linux installed on the server.

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 AMP. This page includes the authentication type (local user, RADIUS, or TACACS+) and access level. This page enables customization some of the information displayed in AMP, and is the place to change your password.

The logged-in users can customize the information displayed in the AMP header. Figure 167 illustrates the **Home** > **User Info** page, and Table 127 lists the fields.

Figure 167 *Home > User Info Page Illustration*



admin is logged in as a local database user with role *Admin* and Administrator access to RAPIDS.

User Information

Password: Changing your password will log you out.	••••••••••
Confirm Password:	••••••••••
Name:	admin
Email Address:	admin@company.com
Phone:	
Notes:	

Top Header Stats

Filter Level For Rogue Count:	Suspected Rogue
Customize Header Columns:	○ Yes ● No

Search Preferences

Search Method:	Active + historical clients

Display Preferences

Default Number of Records per List:	20 records per page
Reset List Preferences:	Reset
Customize Columns for Other Roles:	○ Yes ● No
Console Refresh Rate:	5 minutes
Idle Timeout (5 mins to 240 mins):	60

Table 127: *Home > User Info Fields and Descriptions*

Field	Description
Top Header Stats	
Filter Level For Rogue Count	Specifies the minimum classification that will cause a device to be included in the rogue count header information. More about the classifications can be found in "Controller Classification with WMS Offload" on page 202.
Customize Header Columns	Enables/disables the ability to control which statistics hyperlinks (also known as Top Header Stats) are displayed at the top of every AMP screen.
Stats	Select the specific data you would like to see in the Top Header Stats. Refer to the "Status Section" topic in the *AirWave 7.7 Installation Guide*. **Note**: This field only appears if you selected **Yes** in the previous field.
Severe Alert Threshold	Configures the minimum severity of an alert to be included in the Severe Alerts count. See "Setting Severe Alert Warning Behavior" on page 27 for details. **Note:** The severe alerts count header info will only be displayed if 'Severe Alerts' is selected in the **Stats** section above and if a severe alert exists. **Note**: This field only appears if you selected **Yes** in the **Customize Header Columns** field.
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. **Note:** This field only appears if you selected **Yes** in **Customize Header Columns**.
Search Preferences	
Search Method	Specify one of the following search methods: ● Use System Defaults: The Search Method will be based on the system-wide configuration setting. This method is configured on the **AMP Setup > General** page.Active clients + all devices: This looks at all active clients (not historical) and all devices. This search is not case-sensitive. ● Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a popup window rather than on the **Home > Search** page. This popup window includes top-level navigation that allows you to filter the results based on Clients, APs, Controllers, and Switches. ● Active clients + all categories: This looks at all active clients (not historical) and all categories. This search is not case-sensitive. ● Active clients + all categories (exact match): This looks at all active clients (not historical) and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields. ● Active + historical clients + all categories: This looks at all active and historical clients and all categories. This search is not case-sensitive. ● Active + historical clients + all categories (exact match): This looks at all active and historical clients and all categories. This search returns only matches that are exactly as typed (IP, username, device name, etc). This search is case-sensitive for all searched fields.
Display Preferences	

Table 127: *Home > User Info Fields and Descriptions (Continued)*

Field	Description
Default Number of Records per List	Defines the number of rows to appear in any list by default. If a row count is manually set, it will override the default setting.
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 select **Choose Columns for roles** above the list. Make the desired column changes; select the roles to update and **Save**.
Console Refresh Rate	The frequency in which lists and charts automatically refresh on a page.
Idle Timeout (5 mins to 240 mins)	Number of minutes of idle time until AMP automatically ends the user session. This setting only the logged-in user of this AMP. The default is 60 minutes. To set the max idle timeout for all users of this AMP, see "Setting Up Login Configuration Options" on page 49.

To configure your own user account with the **Home** > **User Info** page, enter the following information in the **User Information** section:

- **Name**—Enter the ID by which you log into and operate in AMP.
- **Email Address**—Enter the email address to be used for alerts, triggers, and additional AMP functions that support an email address.
- **Phone**—Enter the area code and phone number, if desired.
- **Notes**—Enter any additional text-based information that helps other AMP users or administrators to understand the functions, roles, or other rights of the user being created.

Supporting AMP Servers with the Master Console

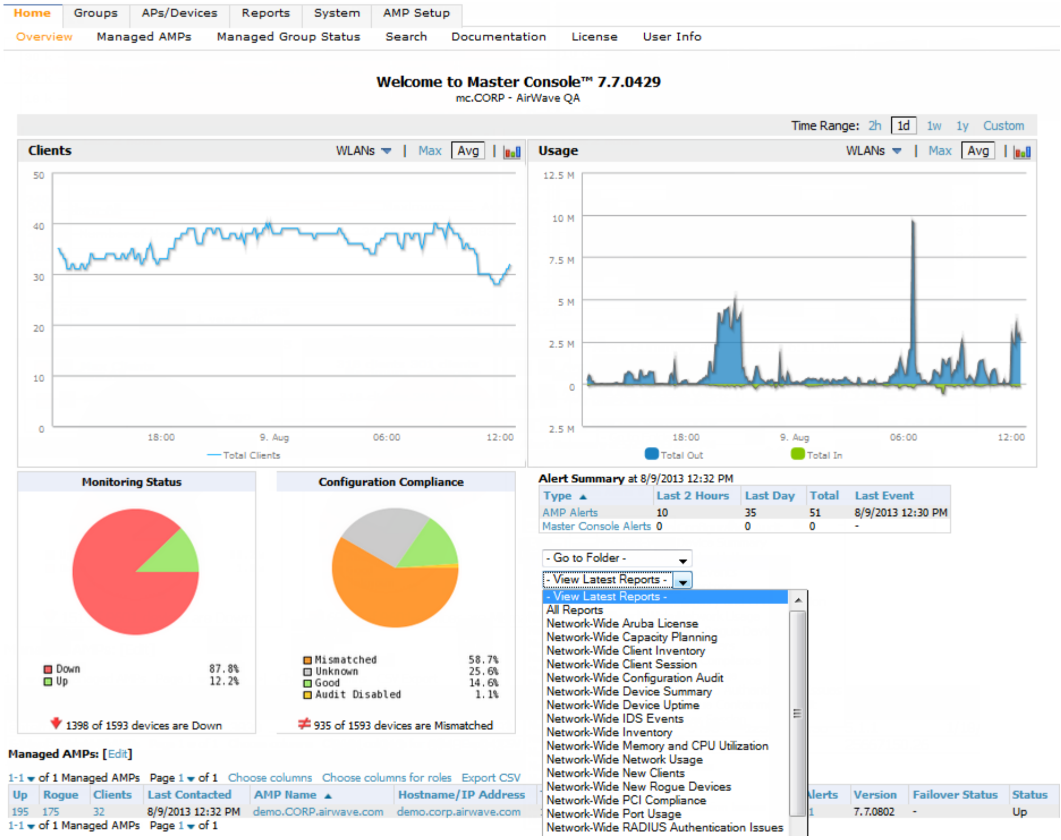
The **Master Console** (MC) is used to monitor multiple AMP stations from one central location. The **Master Console** is designed for customers running multiple AMP servers. Once an AMP station has been added to the MC, it will be polled for basic AMP information.

NOTE

The license key determines if the server will behave as a Master Console or as a standard AMP server.

Much like the normal **Home** > **Overview** page, the **Master Console Home** > **Overview** page provides summary statistics for the entire network at a glance. Figure 168 illustrates the Overview page:

Figure 168 *Master Console Home > Overview Page Illustration*



Welcome to Master Console™ 7.7.0429
mc.CORP - AirWave QA

Monitoring Status

🟥 Down	87.8%
🟩 Up	12.2%

1398 of 1593 devices are Down

Configuration Compliance

🟧 Mismatched	58.7%
⬜ Unknown	25.6%
🟩 Good	14.6%
🟨 Audit Disabled	1.1%

≠ 935 of 1593 devices are Mismatched

Alert Summary at 8/9/2013 12:32 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	10	35	51	8/9/2013 12:30 PM
Master Console Alerts	0	0	0	-

- View Latest Reports -
All Reports
Network-Wide Aruba License
Network-Wide Capacity Planning
Network-Wide Client Inventory
Network-Wide Client Session
Network-Wide Configuration Audit
Network-Wide Device Summary
Network-Wide Device Uptime
Network-Wide IDS Events
Network-Wide Inventory
Network-Wide Memory and CPU Utilization
Network-Wide Network Usage
Network-Wide New Clients
Network-Wide New Rogue Devices
Network-Wide PCI Compliance
Network-Wide Port Usage
Network-Wide RADIUS Authentication Issues

Managed AMPs: [Edit]

1-1 of 1 Managed AMPs Page 1 of 1 Choose columns Choose columns for roles Export CSV

Up	Rogue	Clients	Last Contacted	AMP Name ▲	Hostname/IP Address	lerts	Version	Failover Status	Status
195	175	32	8/9/2013 12:32 PM	demo.CORP.airwave.com	demo.corp.airwave.com	1	7.7.0802	-	Up

1-1 of 1 Managed AMPs Page 1 of 1

- Reports can be run from the **Master Console** to display information from multiple AMP stations; because such reports can be extremely large, reports can also be run as summary only so that they generate more quickly and finish as a manageable file size.
- The **Master Console** can also be used to populate group-level configuration on managed AMP installations using the **Global Groups** feature.
- The **Master Console** offers a display of devices that are in a **Down** or **Error** state anywhere on the network. This information is supported on **Master Console** pages that display device lists such as **Home > Overview** and **APs Devices > List**.
- The **Master Console** and **Failover** servers can be configured with a **Managed AMP Down** trigger that generates an alert if communication is lost to a managed or watched AMP station. The **Master Console** or **Failover** server can also send email or NMS notifications about the event.

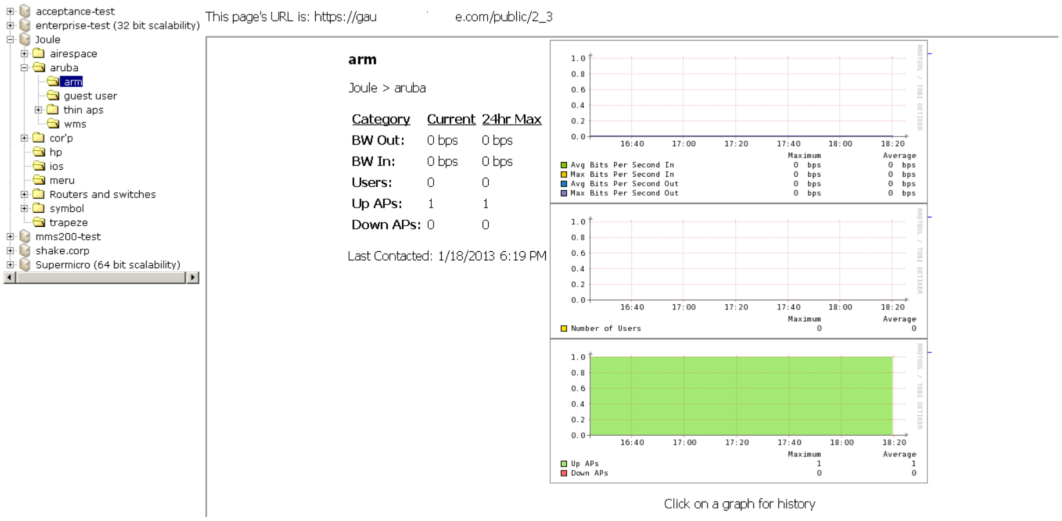
NOTE

XML APIs are not supported on the Master Console.

Using the Public Portal on Master Console

The **Master Console** also contains an optional Public Portal that allows any user to view basic group-level data for each managed AMP. This feature is disabled by default for security reasons; no AMP or Master Console login is required to view the public portal. The Public Portal can be enabled in **AMP Setup > General** in the **Master Console** section. Once enabled, a new **Portal** tab will appear to the right of the **Groups** tab (refer to the navigation section in Figure 168 in "Supporting AMP Servers with the Master Console" on page 265). The URL of the public portal will be https://your.AMP.name/public. When you upgrade to the latest version of AMP, the public portal is disabled by default, regardless of the type of license.

Figure 169 *Public Portal Page Illustration*



This page's URL is: https://gau e.com/public/2_3

arm

Joule > aruba

Category	Current	24hr Max
BW Out:	0 bps	0 bps
BW In:	0 bps	0 bps
Users:	0	0
Up APs:	1	1
Down APs:	0	0

Last Contacted: 1/18/2013 6:19 PM

Click on a graph for history

The Public Portal supports configuration of the iPhone interface. This can be configured using the Master Console AMP page. See "Defining General AMP Server Settings" on page 28.

Adding a Managed AMP with the Master Console

Perform the following steps to add a managed AMP console.

1. Navigate to the **Home** > **Managed AMPs** page.
2. Select the **pencil** icon to edit or reconfigure an existing AMP console, or select **Add New Managed AMP** to create a new AMP console. The **Managed AMP** page appears. Complete the settings on this page as described in Table 128.

Table 128: *Managed AMP fields and default values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the AMP server to be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed AMP server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed AMP server.
Username	N/A	The username used by the Master Console to login to the managed AMP server. The user needs to be an AP/Device Manager or AMP Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console to login to the managed AMP server.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed AMP server.
Manage Group Configuration	No	Defines whether the Master Console can manage device groups on the managed AMP server.

3. When finished, select **Add** to return to the **Managed AMPs** list page.

Using Global Groups with Master Console

To push configurations to managed groups using the AMP Global Groups feature, follow these steps:

1. Navigate to the Master Console's **Groups > List** page.
2. Select **Add** to add a new group, or select the name of the group to edit settings for an existing group.
3. Select the **Duplicate** icon to create a new group with identical configuration to an existing group. Groups created on the Master Console will act as Global Groups, or groups with master configurations that can be pushed out to subscriber groups on managed AMPs. Global groups are visible to all users, so they cannot contain APs (which can be restricted based on user role).
4. Selecting the name of an existing group on the **Master Console** loads the subtabs for **Basic, Security, SSIDs, AAA Servers, Templates, Radio, Cisco WLC Config, Proxim Mesh,** and **MAC ACL** pages, if such pages and configurations are active for the devices in that group.

   These subtabs contain the same fields as the group subtabs on a monitored AMP, but each field also has a check box. The Master Console can also configure global templates that can be used in subscriber groups. The process is the same as described in the "Creating and Using Templates" on page 178, 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 check box selected; for fields with check boxes selected, the value or setting can be changed on the corresponding tab for each managed group. For list pages, override options are available only on the **Add** page for each list. It will take several minutes for changes to Global Groups on the **Master Console** to be pushed to the managed AMPs; make sure that the **Manage Group Configuration** option is enabled for each managed AMP.

Once Global Groups have been configured on the **Master Console**, groups must be created or configured on the managed AMPs to subscribe to a particular Global Group. To configure subscriber groups, enable **Use Global Groups** on the **Group > Basic** page of a group on a managed AMP. Select the name of the Global Group from the drop-down menu, and then select **Save and Apply**. Note that the MC doesn’t push anything when you create new subscriber groups; the copy of the Global Group already on the managed AMP provides the information.

Once the configuration is pushed, the non-overridden fields from the Global Group will appear on the subscriber group as static values and settings. Only fields that had the override check box selected in the Global Group will appear as fields that can be set at the level of the subscriber group. Any changes to a static field must be made on the Global Group.

The Global Groups feature can also be used without the Master Console. For more information about how this feature works, refer to "Configuring and Using Device Groups" on page 77.

Using AirWave Failover for Backup

The failover version of AMP provides a many-to-one hot backup server. The Failover AMP polls the watched AMPs to verify that each is up and running. If the watched AMP is unreachable for the specified number of polls, the Failover AMP automatically restores the most recent saved backup from the watched AMP and begins polling its APs.

Navigation Section of AMP Failover

The **Navigation** section displays tabs to all main GUI pages within AMP Failover. The top bar is a static navigation bar containing tabs for the main components of AMP, while the lower bar is context-sensitive and displays the subtabs for the highlighted tab. Table 129 describes the contents of this page.

Table 129: *Contents of the Navigation Section of Failover*

Main Tab	Description	Subtabs
Home	The **Home** page provides basic AMP Failover information including system name, hostname, IP address, current time, running time, software version, and watched AMP information.	Overview User Info Watched AMPs License
System	The **System** page provides information related to AMP operation and administration including overall system status, performance monitoring, and backups.	Status Triggers Alerts Event Log Backups Performance
AMP Setup	The **Setup** page provides all information relating to the configuration of AMP itself and its connection to your network.	General Network Users TACACS+

Adding Watched AMP Stations

Navigate to the **Home** > **Watched AMPs** page to begin backing up and monitoring AMP stations. Once an AMP installation has been added to the Watched AMPs list, the Failover AMP will download the most recent backup and begin polling. The Failover AMP and the Watched AMP must be on the same version or else the watched AMP will be unable to restore properly. If any of the watched AMPs are not on the same version, you will need to upgrade. The Failover AMP will need HTTPS access (port 443) to the watched AMP to verify that the web page is active and to fetch downloads.

Once the Failover AMP determines that the Watched AMP s not up (based on the user-defined missed poll threshold), it will restore the data backup of the Watched AMP and begin monitoring the watched AMP APs and devices. There are many variables that affect how long this will take including how long client historical data is being retained, but for an AMP with 1,000 APs it might take up to 10 minutes. For an AMP with 2,500 APs, it might take as long as 20 minutes. The Failover AMP will retain its original IP address.

In summary, the Failover AMP could take over for the Watched AMP in as little as five minutes; it might take up to an additional 10-20 minutes to unpack the watched AMP data and begin monitoring APs. The most important factors are the missed poll threshold, which is defined by the user, and the size of the watched AMP backup, which is affected by the total number of APs and by the amount of data being saved, especially client historical data.

To restore the Watched AMP, run the backup script from the command line and copy the current data file and the old Watched AMP configuration file to the Watched AMP. Then run the restore script. More information about backups and restores can be found in "Backing Up AirWave" on page 229.

Table 130: *Home > Watched AMPs page fields and default values*

Setting	Default	Description
IP/Hostname	None	The IP address or Hostname of the watched AMP. The Failover AMP needs HTTPS access to the watched AMPs.
Username	None	A username with management rights on the watched AMP
Password	None	The password for the username with management rights specified above.
HTTP Timeout (5-1000 Sec)	60	The amount of time before AMP considers a polling attempt failed.

Table 130: *Home > Watched AMPs page fields and default values (Continued)*

Setting	Default	Description
Polling Enabled	Yes	Enables or disables polling of the Watched AMP. **NOTE:** You do not need to disable polling of the watched AMP system if it is set to be down during nightly maintenance or is being upgraded.
Polling Period	5 minutes	The amount of time between polls of the Watched AMP.
Missed Poll Threshold	None	The number of polls that can be missed before the failover AMP will begin actively monitoring the Watched AMP APs.

NOTE

When selecting a backup file, be sure to select the one that is most relevant, whether that is failover-as-amp or failover-as-failover. An AMP acting as a failover keeps its nightly backups in **/var/airwave-backup**, and the backups of watched AMPs are stored in **/var/airwave-backup/watched_amps**. In the event of a failover, a new backup-as-failover is made and placed in **/var/airwave-backup/watcher**. However, the existing backups-as-failover in **/var/airwave-backup** remains there until they are aged out by standard rotation.

Logging out of AirWave

To log out of AirWave, select the **Logout** link on the upper right hand corner of every AMP page.

You will be logged off automatically based on the number of minutes set in the **Idle Timeout** setting of **Home** > **User Info**. Refer to "Setting Up Login Configuration Options" on page 49.

This section describes AMP reports, including access, creation, scheduling, and distribution. It includes the following sections:

- "Overview of AMP Reports" on page 271
- "Using Daily Reports" on page 281
- "Defining Reports" on page 274
- "Emailing and Exporting Reports" on page 312

AMP ships with several reports enabled by default. Default reports may run nightly or weekly, depending on the AMP release. Review the list of defined and scheduled reports with the **Reports > Generated** and **Reports > Definition** pages to determine if default reports are desired. If not, you can delete, disable, or reschedule any of them.

AMP supports additional specialized reports as follows:

- **System > Status** page supports the diagnostic report file for sending to customer support: diagnostics.tar.gz.
- **System > Status** page supports the VisualRF diagnostics report file: VisualRFdiag.tar.gz.
- **VisualRF > Network View** supports the Bill of Materials (BOM) report. Refer to "Using VisualRF" on page 315.

Overview of AMP Reports

Reports are powerful tools in network analysis, user configuration, device optimization, and network monitoring on multiple levels. Among their benefits, reports provide an interface for multiple configurations.

AirWave reports have the following general parameters:

- AMP runs daily versions of all reports during predefined windows of time. All reports can be scheduled to run in the background.
- The daily version of any report is available instantly in the **Reports > Generated** page.
- The **Inventory** and the **Configuration Audit** reports are the only reports that don’t span a period of time. Instead, these two reports provide a snapshot of the current state of the network.
- Users can create all other reports over a custom time period on the **Reports > Definitions** page. All reports can be printed, emailed, or exported to CSV, PDF, or XML format.

Reports > Definitions Page Overview

The **Reports > Definitions** page allows you to define new reports and see the reports already defined.

The **Definitions** page includes these sections:

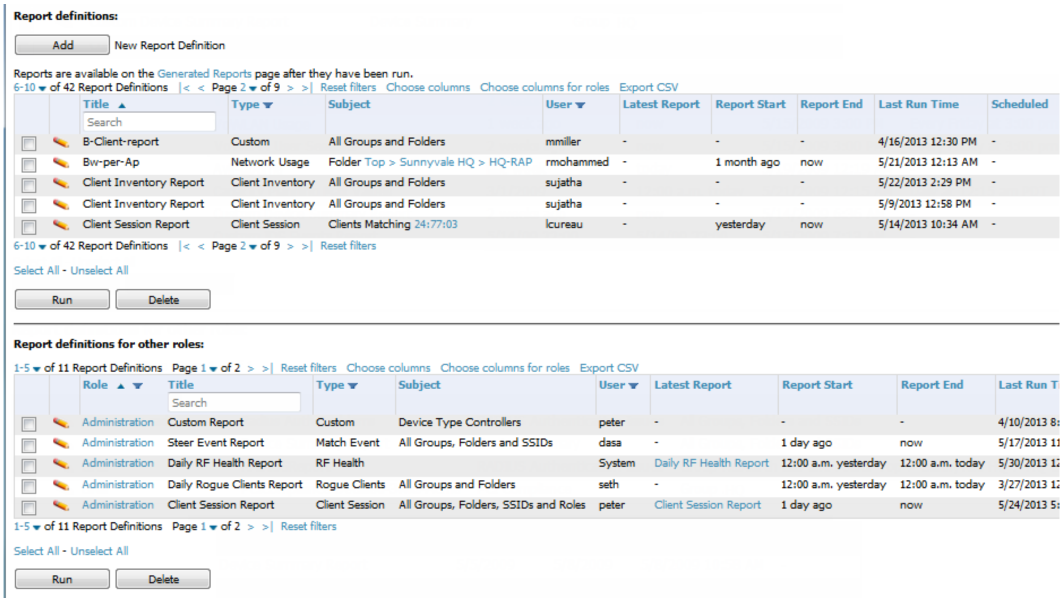
- **Report Definitions** section—The **Add** button allows you to define a custom report using the **Custom Options** drag and drop interface, or from any of the report types in the drop down menu. The **Report Definitions** table has a complete list of all saved report definitions with an option to return to each definition’s table to further customize your report. When you create a report, the following additional buttons are available:
  - **Add and Run** allows you to create a report definition and run that report immediately.
  - **Run Now** (visible from the expanded **Report Definitions** menu) allows immediate running of a custom report as soon as you set the parameters. You must save its definition separately, if you want to remember the parameters.
- **Report definitions for other roles** section—This section, supported for **admin** users, displays additional reports that have been scheduled for other roles. This section of the page adds the **Role** column, and other columns are the same.

Each pane includes a **Latest Report** column with the most recently run reports for each definition and role created. **Run** and **Delete** buttons allow you to select a report from the definitions table to run or delete. Once you define a report from the **Definition** page, it appears on the **Generated** page. The **Reports** > **Definition** page is shown in Figure 170, and Table 131 describes the fields available when you select a specific report definition.

Table 131: *Reports > Definition Page Fields and Descriptions*

Field	Description
Report Definition	Displays a field for entering report title and drop down menu, shown in Figure 171, 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 **Yes**. Options include report frequency, start time, and current system time.
Report Visibility	Allows you to determine a report's visibility according to user role or by subject.
Email Options	Reveals email address preferences for sending reports by selecting **Yes**. Be sure to always enter a valid e-mail address.
Add and Run	Available when adding a new Report Definition. Allows you to create a report definition and run that report right then.
Run Now	Available when adding a new Report Definition. 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.
Save and Run	Available when viewing an existing Report Definition. Allows you to edit a report definition and run that report right then.

Figure 170 *Reports > Definitions Page Illustration*



Report definitions:

Add
New Report Definition

Reports are available on the Generated Reports page after they have been run.

6-10 ▾ of 42 Report Definitions |< < Page 2 ▾ of 9 > >| Reset filters Choose columns Choose columns for roles Export CSV

		Title ▲	Type ▾	Subject	User ▾	Latest Report	Report Start	Report End	Last Run Time	Scheduled
		Search								
□	✎	B-Client-report	Custom	All Groups and Folders	mmiller	-	-	-	4/16/2013 12:30 PM	-
□	✎	Bw-per-Ap	Network Usage	Folder Top > Sunnyvale HQ > HQ-RAP	rmohammed	-	1 month ago	now	5/21/2013 12:13 AM	-
□	✎	Client Inventory Report	Client Inventory	All Groups and Folders	sujatha	-	-	-	5/22/2013 2:29 PM	-
□	✎	Client Inventory Report	Client Inventory	All Groups and Folders	sujatha	-	-	-	5/9/2013 12:58 PM	-
□	✎	Client Session Report	Client Session	Clients Matching 24:77:03	lcureau	-	yesterday	now	5/14/2013 10:34 AM	-

6-10 ▾ of 42 Report Definitions |< < Page 2 ▾ of 9 > >| Reset filters
Select All - Unselect All
Run
Delete

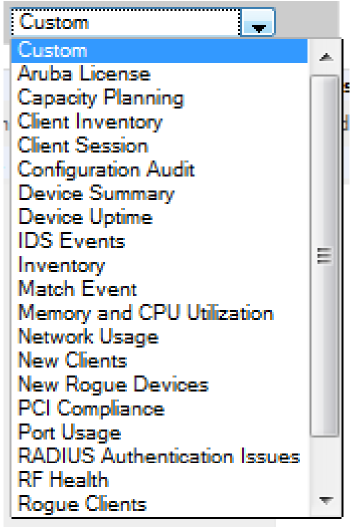
Report definitions for other roles:

1-5 ▾ of 11 Report Definitions Page 1 ▾ of 2 > >| Reset filters Choose columns Choose columns for roles Export CSV

		Role ▲ ▾	Title	Type ▾	Subject	User ▾	Latest Report	Report Start	Report End	Last Run T
			Search							
□	✎	Administration	Custom Report	Custom	Device Type Controllers	peter	-	-	-	4/10/2013 8:
□	✎	Administration	Steer Event Report	Match Event	All Groups, Folders and SSIDs	dasa	-	1 day ago	now	5/17/2013 11
□	✎	Administration	Daily RF Health Report	RF Health		System	Daily RF Health Report	12:00 a.m. yesterday	12:00 a.m. today	5/30/2013 12
□	✎	Administration	Daily Rogue Clients Report	Rogue Clients	All Groups and Folders	seth	-	12:00 a.m. yesterday	12:00 a.m. today	3/27/2013 12
□	✎	Administration	Client Session Report	Client Session	All Groups, Folders, SSIDs and Roles	peter	Client Session Report	1 day ago	now	5/24/2013 5:

1-5 ▾ of 11 Report Definitions Page 1 ▾ of 2 > >| Reset filters
Select All - Unselect All
Run
Delete

Figure 171 *Report Type Drop down Menu in Reports > Definitions Illustration*



Only **admin** users have complete access to all report information. The AMP reports and online displays of information can vary with configuration, User Roles, and Folders.

Reports > Generated Page Overview

The **Reports** > **Generated** page displays reports that have been run, as well as the most recent daily version of any report. An **Admin** user can see and edit all report definitions in AMP. Users with **Monitor Only** roles can see reports and definitions only if they have access to all devices in the reports.

The **Reports** > **Generated** page contains three primary sections, as follows:

- Generated reports configured for the current role and for additional roles
- Generated reports for other roles
- The latest daily reports for immediate online viewing

You can select a check box beside any report and click **Rerun** to view an updated report. When you run or rerun a report, the Generation Time column changes to pending until the report is completed.

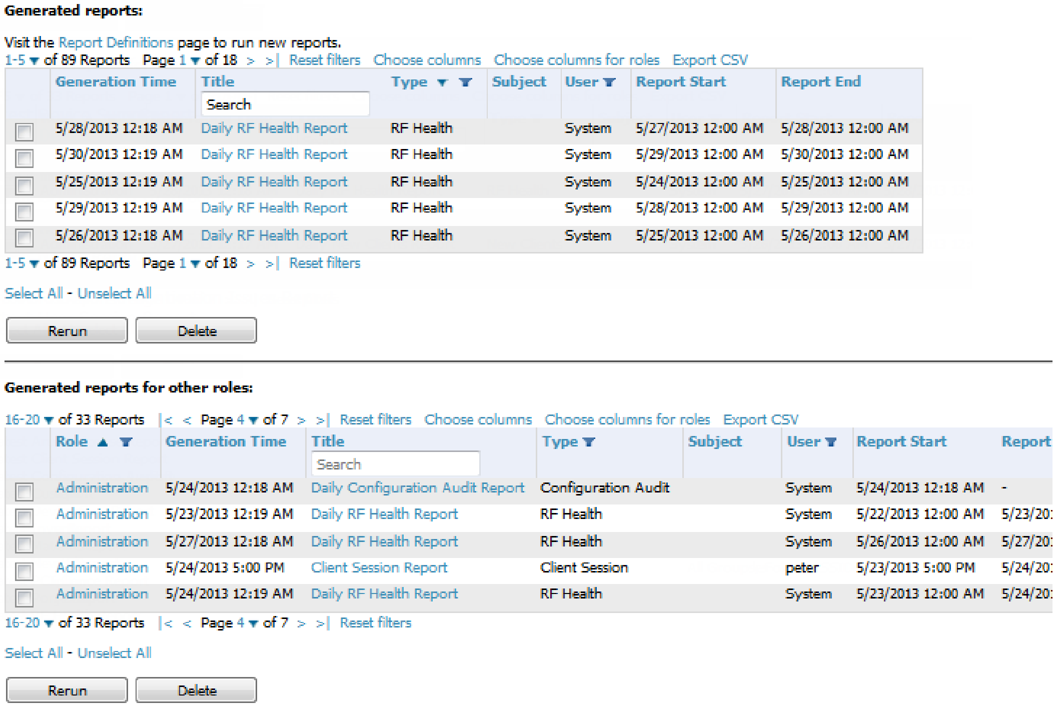
You can kill a report that is pending by running the following from the AMP CLI:

```
#echo 'delete from report where state=1'
```

Note that the report status in the database is as follows:

state=0: Failed
state=1: Pending
state=2: In progress

Figure 172 *Reports > Generated Page Example*



Generated reports:

Visit the Report Definitions page to run new reports.

1-5 ▼ of 89 Reports Page 1 ▼ of 18 > >| Reset filters Choose columns Choose columns for roles Export CSV

	Generation Time	Title	Type	Subject	User	Report Start	Report End
		Search					
□	5/28/2013 12:18 AM	Daily RF Health Report	RF Health		System	5/27/2013 12:00 AM	5/28/2013 12:00 AM
□	5/30/2013 12:19 AM	Daily RF Health Report	RF Health		System	5/29/2013 12:00 AM	5/30/2013 12:00 AM
□	5/25/2013 12:19 AM	Daily RF Health Report	RF Health		System	5/24/2013 12:00 AM	5/25/2013 12:00 AM
□	5/29/2013 12:19 AM	Daily RF Health Report	RF Health		System	5/28/2013 12:00 AM	5/29/2013 12:00 AM
□	5/26/2013 12:18 AM	Daily RF Health Report	RF Health		System	5/25/2013 12:00 AM	5/26/2013 12:00 AM

1-5 ▼ of 89 Reports Page 1 ▼ of 18 > >| Reset filters

Select All - Unselect All

Generated reports for other roles:

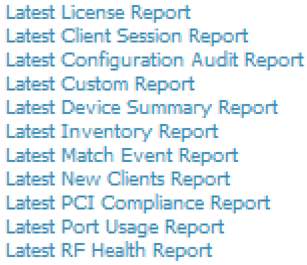
16-20 ▼ of 33 Reports |< < Page 4 ▼ of 7 > >| Reset filters Choose columns Choose columns for roles Export CSV

	Role ▲	Generation Time	Title	Type	Subject	User	Report Start	Report
			Search					
□	Administration	5/24/2013 12:18 AM	Daily Configuration Audit Report	Configuration Audit		System	5/24/2013 12:18 AM	-
□	Administration	5/23/2013 12:19 AM	Daily RF Health Report	RF Health		System	5/22/2013 12:00 AM	5/23/20
□	Administration	5/27/2013 12:18 AM	Daily RF Health Report	RF Health		System	5/26/2013 12:00 AM	5/27/20
□	Administration	5/24/2013 5:00 PM	Client Session Report	Client Session		peter	5/23/2013 5:00 PM	5/24/20
□	Administration	5/24/2013 12:19 AM	Daily RF Health Report	RF Health		System	5/23/2013 12:00 AM	5/24/20

16-20 ▼ of 33 Reports |< < Page 4 ▼ of 7 > >| Reset filters

Select All - Unselect All

Figure 173 *Reports > Generated Page with Single-click Report Viewing Options*



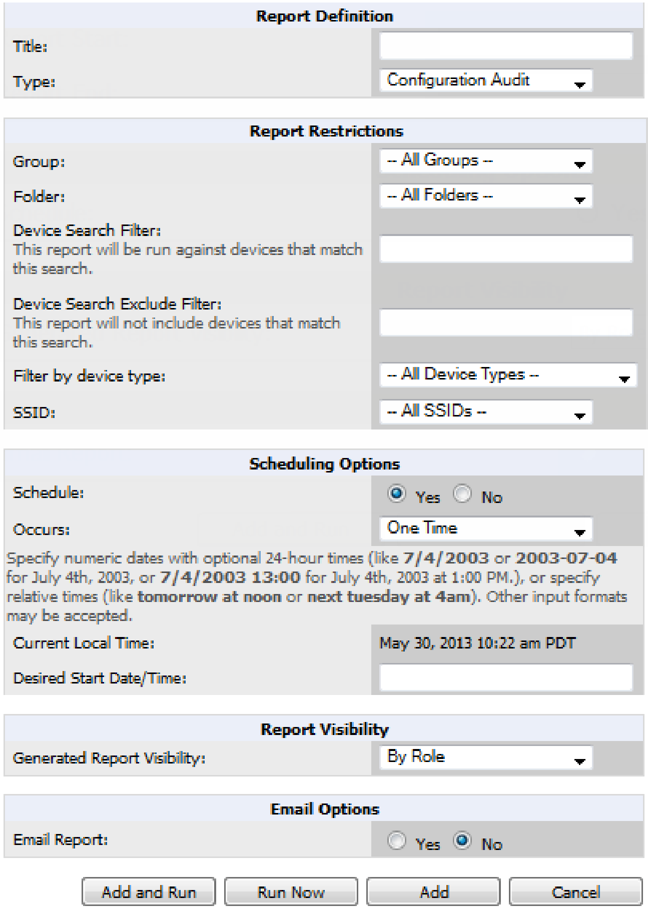
Latest License Report
Latest Client Session Report
Latest Configuration Audit Report
Latest Custom Report
Latest Device Summary Report
Latest Inventory Report
Latest Match Event Report
Latest New Clients Report
Latest PCI Compliance Report
Latest Port Usage Report
Latest RF Health Report

Defining Reports

You can create reports in AMP for any time period you want, to be run when you want, and distributed to recipients that you define. Reports that you create will display on the **Reports > Definition** page and on the **Reports > Generated** page.

1. To create or edit a report, browse to the **Reports > Definition** page and click the **Add** button, or select the **pencil** icon to edit an existing report definition. Figure 174 illustrates one view of the **Reports > Definition** page.

Figure 174 *Defining a Report*



Report Definition

Title:	
Type:	Configuration Audit

Report Restrictions

Group:	-- All Groups --
Folder:	-- All Folders --
Device Search Filter: This report will be run against devices that match this search.	
Device Search Exclude Filter: This report will not include devices that match this search.	
Filter by device type:	-- All Device Types --
SSID:	-- All SSIDs --

Scheduling Options

Schedule:	● Yes ○ No
Occurs:	One Time

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

Current Local Time:	May 30, 2013 10:22 am PDT
Desired Start Date/Time:	

Report Visibility

Generated Report Visibility:	By Role

Email Options

Email Report:	○ Yes ● No

2. Complete the fields described in Table 132 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 281.

Table 132: *Reports > Definitions > Add page fields and default values*

Field	Default	Description
Report Definition		
Title	Empty	Enter a **Report Title**. Use 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	Custom	Choose the type of report you wish to create in the Report Type drop-down menu.
Report Restrictions - (These vary based on report type)		
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 check boxes appears, allowing you to choose the groups to include in the report.
Folder	All Folders	

Table 132: *Reports > Definitions > Add page fields and default values (Continued)*

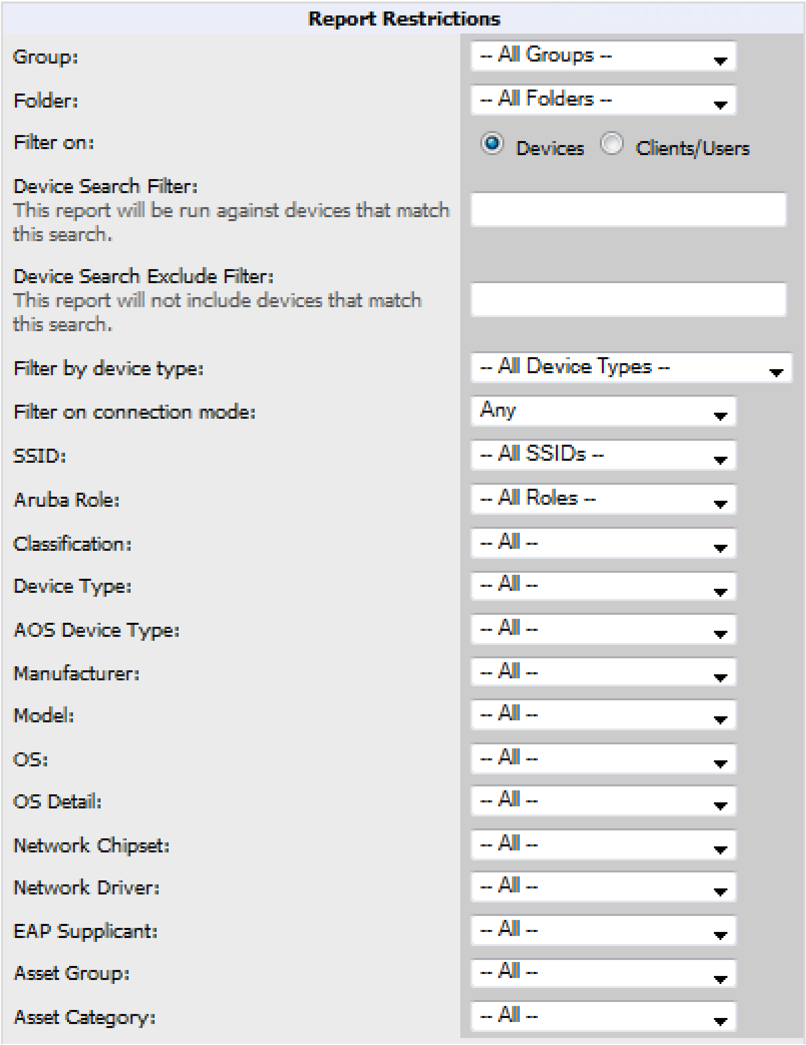
Field	Default	Description
Device Search Filter	Blank	Add a specific alpha numeric string for finding devices that match that which you entered. Note that once you enter a search string, new or deleted devices that match the search string will automatically be included or excluded in all future reports generated until you delete or change the search string. For certain reports, such as **New Clients** and **Client Session**, will allow you to search devices associated with a specific client/user or device. **NOTE:** If the Report Type is Custom, this field will not display until a custom option is selected.
Device Search Exclude Filter	Blank	Add a specific alpha numeric string for excluding 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. Certain reports, such as **New Clients** and **Client Session**, allow you to search devices associated with a specific client/user or device. **NOTE:** If the Report Type is Custom, this field will not display until a custom option is selected.
Filter by device type	All Device Types	Filter this report by device type. By selecting the second option - **Use selected device types** - you can select the check boxes next to the specific device types you want to filter on: Access Points (such as campus APs remote APs, and different types of Mesh APs), Controllers (Master, Local, Standby, and Virtual), Switches & Routers (Aruba and non-Aruba), and Universal & Custom Devices.
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 AMP at the present time.
Scheduling Options		
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: ● **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. ● **Current Local Time**–Displays for reference the time of the AMP 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.

Table 132: *Reports > Definitions > Add page fields and default values (Continued)*

Field	Default	Description
Report Visibility		
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) or by Subject (displaying reports by Subject on the **Reports > Generated** page). ● **By Role**: When you create a report definition, the reports are visible to everybody who has the same role as you (ie AMP Administrator), and to nobody else. ● **By Subject**: When the report is run, AMP users have access to the report if they are allowed to view all the devices in the report.
Email Options		
Email Report	No	Select **Yes** to display sender and recipient fields. Enter a valid Sender Address where marked to indicate the address that appears in the **From** field of the emailed report. Enter a valid recipient email addresses, separated by commas when using multiple email addresses. **NOTE:** AMP will not attempt to email a report with an excessively large number of rows in the detail section.

In the report restrictions section you can customize any detailed information contained in a chosen report. Figure 175 shows a sample **Report Restrictions** page for the New Clients report.

Figure 175 *Report Restrictions Illustration*



Report Restrictions

Group:	-- All Groups --
Folder:	-- All Folders --
Filter on:	● Devices ○ Clients/Users
Device Search Filter: This report will be run against devices that match this search.	
Device Search Exclude Filter: This report will not include devices that match this search.	
Filter by device type:	-- All Device Types --
Filter on connection mode:	Any
SSID:	-- All SSIDs --
Aruba Role:	-- All Roles --
Classification:	-- All --
Device Type:	-- All --
AOS Device Type:	-- All --
Manufacturer:	-- All --
Model:	-- All --
OS:	-- All --
OS Detail:	-- All --
Network Chipset:	-- All --
Network Driver:	-- All --
EAP Supplicant:	-- All --
Asset Group:	-- All --
Asset Category:	-- All --

By default all data will be included. Deselect the check box to hide specific information. The list can also be reordered by dragging and dropping the separate lines. The order displayed here will match the column order in the report.

3. Do one of the following:
   - Select **Add and Run** to generate the report immediately, in addition to saving report settings.
   - Select **Run Now** to generate the report immediately without creating a new report definition or saving the report settings.
   - Select **Add** (only) to complete the report creation, to be run at the time scheduled.
   - Select **Cancel** to exit from the **Add** page.

Table 133 describes the configurable settings for the custom report to be created. Select any of the report names to view additional information on that report type.

Table 133: *Report Types and Scheduling Options Supported for Custom Reports*

Report Type	Can by Run by Time Period	Can be Run by Group/Folder	Description
"Using Custom Reports" on page 282	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 Aruba License Report" on page 283	No	Yes	Tracks licenses on Aruba devices in your network. This report includes information on the type, quantity, percent used, installation date, expiration date, and the license keys.
"Using the Capacity Planning Report" on page 283	Yes	Yes	Tracks bandwidth capacity and consumption according to thresholds for data throughput. This is a device-oriented report.
"Using the Client Inventory Report" on page 285	No	Yes	Provides information about clients that have connected to you network
"Using the Client Session Report" on page 288	Yes	Yes	Summarizes user data by radio mode, SSID and VLAN, as well as lists all sessions.
"Using the Configuration Audit Report" on page 290	No	Yes	Provides a snapshot of the configuration of all specified access points in AMP, at report run time.
"Using the Device Summary Report" on page 291	Yes	Yes	Summarizes user and bandwidth statistics and lists devices in AMP.
"Using the Device Uptime Report" on page 292	Yes	Yes	Summarizes device uptime within defined groups or folders.
"Using the IDS Events Report" on page 294	Yes	Yes	Summarizes IDS events; can be limited to a summary of a certain number of events.
"Using the Inventory Report" on page 295	No	Yes	Provides an audit of vendors, models and firmware versions of devices in AMP.
"Using the Match Event Report" on page 297	No	Yes	Summarizes matching events per folder, AP, and client. This can be useful in determining the APs that have the highest number of matching/steering traffic.
"Using the Memory	Yes	Yes	Summarizes usage for controllers for defined top

Table 133: *Report Types and Scheduling Options Supported for Custom Reports (Continued)*

Report Type	Can by Run by Time Period	Can be Run by Group/Folder	Description
and CPU Utilization Report" on page 298			number of devices; can be run with or without per-CPU details and details about device memory usage.
"Using the Network Usage Report" on page 299	Yes	Yes	Summarizes bandwidth data and number of users.
"Using the New Clients Report" on page 301	Yes	No	Provides a summary list of new clients, including username, role, MAC address, vendor, discovering AP, association time, duration, folder, and group.
"Using the New Rogue Devices Report" on page 302	Yes	No	Shows new rogue devices by score, discovering AP, and MAC address vendor.
"Using the PCI Compliance Report" on page 304	Yes	Yes	Provides a summary of network compliance with PCI requirements, according to the PCI requirements enabled in AMP using the **AMP Setup > PCI Compliance** page.
"Using the Port Usage Report" on page 305	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" on page 307	Yes	Yes	Summarizes RADIUS authentication issues by controller and by user, as well as a list of all issues.
"Using the RF Health Report" on page 308	Yes	Yes	Tracks problematic radios, changes, errors, and interfering devices.
"Using the Rogue Clients Report" on page 309	Yes	Yes	Summarizes the number of valid users that connected to rogues. This report can be filtered by rogue classification. Ad-hoc devices can be included, and specific details that should be included about the clients can be selected.
"Using the Rogue Containment Audit Report" on page 311	No	Yes	Identifies discrepancies between access point containment status specified in AMP compared to containment status identified by the controller at report run time.

Table 133: *Report Types and Scheduling Options Supported for Custom Reports (Continued)*

Report Type	Can by Run by Time Period	Can be Run by Group/Folder	Description
"Using the VPN Session Report" on page 312	Yes	Yes	Summarizes connected VPN sessions over a specified period of time. This report can be based on clients/users or devices and can be filtered by folder and device type. It can also include detailed information for sessions and users.

Using Daily Reports

This section describes the default and custom-scheduled reports supported in AMP. These reports can be accessed from the **Reports** > **Generated** page.

Viewing Generated Reports

The **Reports** > **Generated** page supports the following general viewing options:

- By default, the reports on the **Reports** > **Generated** page are sorted by Generation Time. You can sort reports by any other column header in sequential or reverse sequential order. You can also choose columns, export the Generated Reports list in CSV, and modify the pagination of this list.
- The **Reports** > **Detail** page launches when you select any report title from this page.

The **Generated Reports** page contains fewer columns and information than the **Definitions** page. Table 134 describes each column for the **Reports** > **Generated** page.

Table 134: *Reports > Generated 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. Selecting the link in this field displays the latest version of a given report. When the latest version of a given report is not available, this field is blank. In this case, a report can be run by selecting the report title and selecting **Run**.
Title	Displays title of the report. This is a user-configured field when creating the report.
Type	Displays the type of the report.
Subject	Displays the scope of the report, to include groups, folders, SSIDs, or any combination of these that are included in the report.
User	This displays the user who created the customized 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	In the **Reports definitions for other roles** section, this column indicates the roles for which additional reports are defined.

Using Custom Reports

Custom reports allow users to specify the data that should be included in a report.

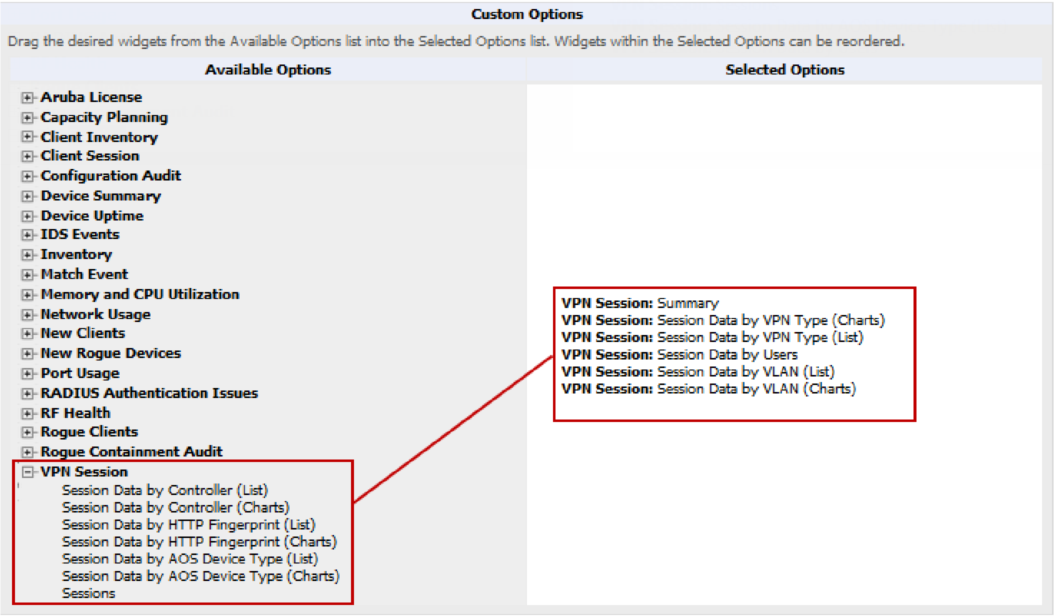
NOTE

Take care when creating and viewing custom reports, as some reports require you to define a time range and others default to show all data. You may notice, for example, that in some cases, a custom report will show client information with a device count that differs from its session data. This can occur because the Client Session data is restricted to a specific time range (for example, "1 month ago until now"). The Client Inventory information, on the other hand, by default shows all data. Users have to explicitly select the **Limit to Active Devices** drop down and then select **Active during report timeframe** option to configure the time range.

Perform these steps to create a **Custom Report**.

1. Navigate to the **Reports** > **Definitions** page.
2. Select **Add**.
3. Enter a Title for the new report.
4. Select the **Custom** option from the Type drop-down menu. The **Custom Options** section appears as shown in Figure 176. In this figure, a custom VPN Session report is being created for viewing VPN data for VLANs and Users.

Figure 176 *Custom Options Page Illustration*



Custom Options

Drag the desired widgets from the Available Options list into the Selected Options list. Widgets within the Selected Options can be reordered.

Available Options

- ⊞ **Aruba License**
- ⊞ **Capacity Planning**
- ⊞ **Client Inventory**
- ⊞ **Client Session**
- ⊞ **Configuration Audit**
- ⊞ **Device Summary**
- ⊞ **Device Uptime**
- ⊞ **IDS Events**
- ⊞ **Inventory**
- ⊞ **Match Event**
- ⊞ **Memory and CPU Utilization**
- ⊞ **Network Usage**
- ⊞ **New Clients**
- ⊞ **New Rogue Devices**
- ⊞ **Port Usage**
- ⊞ **RADIUS Authentication Issues**
- ⊞ **RF Health**
- ⊞ **Rogue Clients**
- ⊞ **Rogue Containment Audit**
- ⊟ **VPN Session**
  - Session Data by Controller (List)
  - Session Data by Controller (Charts)
  - Session Data by HTTP Fingerprint (List)
  - Session Data by HTTP Fingerprint (Charts)
  - Session Data by AOS Device Type (List)
  - Session Data by AOS Device Type (Charts)
  - Sessions

Selected Options

VPN Session: Summary
VPN Session: Session Data by VPN Type (Charts)
VPN Session: Session Data by VPN Type (List)
VPN Session: Session Data by Users
VPN Session: Session Data by VLAN (List)
VPN Session: Session Data by VLAN (Charts)

The left pane of the **Custom Options** section lists all available data that can be included in the report. 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.

5. Below the **Custom Options** panes is a **Report Restrictions** section. All reports allow you to restrict based a specified Group, Folder, and Device Type. When you select Custom Options to include in a report, additional restrictions will be available based on the options that you include. For example, if you select Device Summary: Most Utilized by Usage, then you can restrict the report to include and/or exclude specific devices. Some detailed reporting options, such as New Rogue Devices: Discovery Events, allow you to specify the columns to include in the report.
6. Below the **Report Restrictions** section are **Scheduling Options**, **Report Visibility**, and **Email Options** sections. Choose the parameters as needed for your report, especially a **Report Start** and **Report End**.
7. When finished, select **Add and Run** to add the report to your list and run it immediately, **Run Now** to run without being added to the list, **Add** to add but not run the report, or **Cancel** to exit this page.

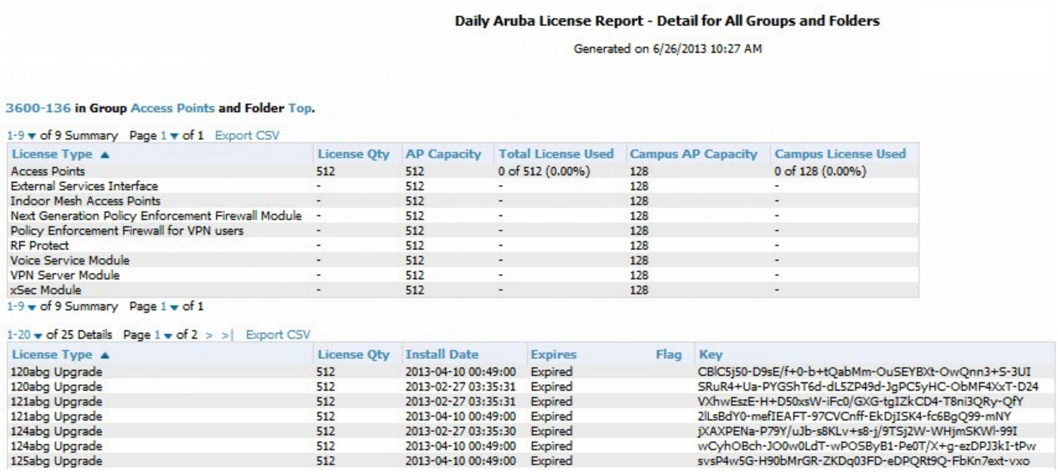
Using the Aruba License Report

The Aruba License Report tracks licenses on Aruba devices in your network. This report includes information on the type, quantity, percent used, installation date, expiration date, and the license keys.

NOTE

This report includes the built-in license count only when the installed license count is less than the license limits.

Figure 177 *Aruba Detail Page*



Daily Aruba License Report - Detail for All Groups and Folders

Generated on 6/26/2013 10:27 AM

3600-136 in Group Access Points and Folder Top.

1-9 ▾ of 9 Summary   Page 1 ▾ of 1   Export CSV

License Type ▲	License Qty	AP Capacity	Total License Used	Campus AP Capacity	Campus License Used
Access Points	512	512	0 of 512 (0.00%)	128	0 of 128 (0.00%)
External Services Interface	-	512	-	128	-
Indoor Mesh Access Points	-	512	-	128	-
Next Generation Policy Enforcement Firewall Module	-	512	-	128	-
Policy Enforcement Firewall for VPN users	-	512	-	128	-
RF Protect	-	512	-	128	-
Voice Service Module	-	512	-	128	-
VPN Server Module	-	512	-	128	-
xSec Module	-	512	-	128	-

1-9 ▾ of 9 Summary   Page 1 ▾ of 1

1-20 ▾ of 25 Details   Page 1 ▾ of 2 > >| Export CSV

License Type ▲	License Qty	Install Date	Expires	Flag	Key
120abg Upgrade	512	2013-04-10 00:49:00	Expired		CBlC5j50-D9sE/f+0-b+tQabMm-OuSEYBXt-OwQnn3+S-3UI
120abg Upgrade	512	2013-02-27 03:35:31	Expired		SRuR4+Ua-PYGShT6d-dL5ZP49d-JgPC5yHC-ObMF4XxT-D24
121abg Upgrade	512	2013-02-27 03:35:31	Expired		VXhwEszE-H+D50xsW-iFc0/GXG-tgIZkCD4-T8ni3QRy-QfY
121abg Upgrade	512	2013-04-10 00:49:00	Expired		2lLsBdY0-mefIEAFT-97CVCnff-EkDjISK4-fc6BgQ99-mNY
124abg Upgrade	512	2013-02-27 03:35:30	Expired		jXAXPENa-P79Y/uJb-s8KLv+s8-j/9TSj2W-WHjmSKWl-99I
124abg Upgrade	512	2013-04-10 00:49:00	Expired		wCyhOBch-JO0w0LdT-wPOSByB1-Pe0T/X+g-ezDPJ3kI-tPw
125abg Upgrade	512	2013-04-10 00:49:00	Expired		svsP4w5G-H90bMrGR-ZKDq03FD-eDPQRt9Q-FbKn7ext-vxo

Using the Capacity Planning Report

The Capacity Planning Report tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. This report is based on interface-level activity and can be used to assist in analyzing device capacity and performance on the network. This analysis can help to achieve network efficiency and an improved user experience.

Refer also to the "Using the Network Usage Report" on page 299 for additional bandwidth information.

Example

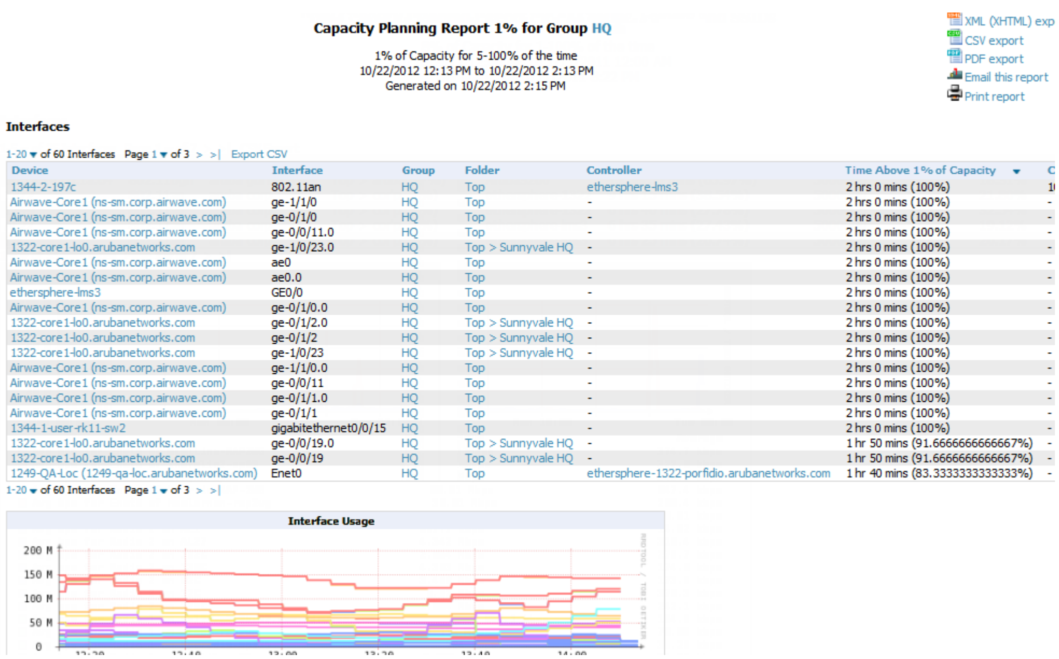
The following example creates a sample Capacity Planning report. This report looks for devices that are under-utilized. This report will search for devices over a 2-hour period that were at 1% of capacity for 5-100% of the time. This report focuses only on devices in a group named "HQ," Perform similar steps to create your own Capacity Planning report. Note that any field omitted from this example is assumed to remain the default value.

1. Click on the **Add New Report Definition** button on the **Reports > Definitions** page.
2. Enter the title for the report. In this example, the report is called "Capacity Planning Report 1% for Group HQ."
3. Select Capacity Planning from the Type drop-down menu.
4. In this example, AMP includes a group named "HQ." Select HQ from the Groups drop down menu.
5. Set the Capacity Threshold value to 1.
6. Set the Min Time Above Threshold value to 5.
7. Set the Max Time Above Threshold value to 100.
8. Enter a date and time range for the period of time that you want to review. In the case below, the report gathers data for the time range from 12:13 PM to 2:13 PM on October 22, 2012.
9. Click the **Save and Run** button.

Output

The following figure illustrates the output of the Capacity Planning Report. The fields on this page are described in Table 135.

Figure 178 *Capacity Planning Report Detail Page (partial view)*



Capacity Planning Report 1% for Group HQ

1% of Capacity for 5-100% of the time
10/22/2012 12:13 PM to 10/22/2012 2:13 PM
Generated on 10/22/2012 2:15 PM

XML (XHTML) exp
CSV export
PDF export
Email this report
Print report

Interfaces

1-20 ▾ of 60 Interfaces Page 1 ▾ of 3 > >| Export CSV

Device	Interface	Group	Folder	Controller	Time Above 1% of Capacity ▾	C
1344-2-197c	802.11an	HQ	Top	ethersphere-lms3	2 hrs 0 mins (100%)	1
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-1/1/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/0/11.0	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-1/0/23.0	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ae0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ae0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
ethersphere-lms3	GE0/0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/1/2.0	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/1/2	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-1/0/23	HQ	Top > Sunnyvale HQ	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-1/1/0.0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/0/11	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/1.0	HQ	Top	-	2 hrs 0 mins (100%)	-
Airwave-Core1 (ns-sm.corp.airwave.com)	ge-0/1/1	HQ	Top	-	2 hrs 0 mins (100%)	-
1344-1-user-rk11-sw2	gigabitethernet0/0/15	HQ	Top	-	2 hrs 0 mins (100%)	-
1322-core1-lo0.arubanetworks.com	ge-0/0/19.0	HQ	Top > Sunnyvale HQ	-	1 hr 50 mins (91.6666666666667%)	-
1322-core1-lo0.arubanetworks.com	ge-0/0/19	HQ	Top > Sunnyvale HQ	-	1 hr 50 mins (91.6666666666667%)	-
1249-QA-Loc (1249-qa-loc.arubanetworks.com)	Enet0	HQ	Top	ethersphere-1322-porfidio.arubanetworks.com	1 hr 40 mins (83.3333333333333%)	-

1-20 ▾ of 60 Interfaces Page 1 ▾ of 3 > >|

Interface Usage

Table 135: *Capacity Planning Report output details*

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.

Table 135: *Capacity Planning Report output details (Continued)*

Field	Description
Overall Usage (In)	Displays overall device usage for incoming data.
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 Client Inventory Report

The Client Inventory Report can be used for viewing information about clients that have connected to you network. Similar to the Inventory Report, you can filter this report to search for specific devices (such as, "Aruba"). You can also filter this report based on the connection mode (wired or wireless).

This report also gives you the option to filter instead on specific devices and/or users. Whether viewing information for devices or clients, the report can configured to display additional options. For many of these options, you can choose to view all information or a specific set of information (Matching option). If Matching is selected, a text entry field displays. When you put your cursor in the text entry field, an additional side menu displays providing you with a list of available options that you can select.

- AOS Device Type - All or Matching
- Device Manufacturer - All or Matching
- Device Model - All or Matching
- Device Type - All or Matching
- OS Summary - All or Matching
- Steerable Clients
- Asset Category - All or Matching
- Asset Group - All or Matching
- Device Manufacturer and Model
- Device OS Detail - All or Matching
- EAP Supplicant - All or Matching
- Last Aruba Role
- Last Authentication Type
- Last Connection Mode
- Last SSID
- Network Chipset - All or Matching
- Network Driver - All or Matching
- Network Vendor

This report allows you to include details about every client, for example, the User Name, MAC Address, Role, AP Radio information, and more. Finally, you can limit this report to include devices that active or inactive at the time when this report is run.

Example

The following example configures a Client Inventory Report that summarizes information for iPhone, iPod, and iPad devices on your network and how those devices are connecting. This report turns off the Device Manufacturer and OS summaries because these are only Apple (manufacturer) and iOS (OS) devices. The report omits the Device Model Summary option because, in this case, the information will be redundant with Device Type.

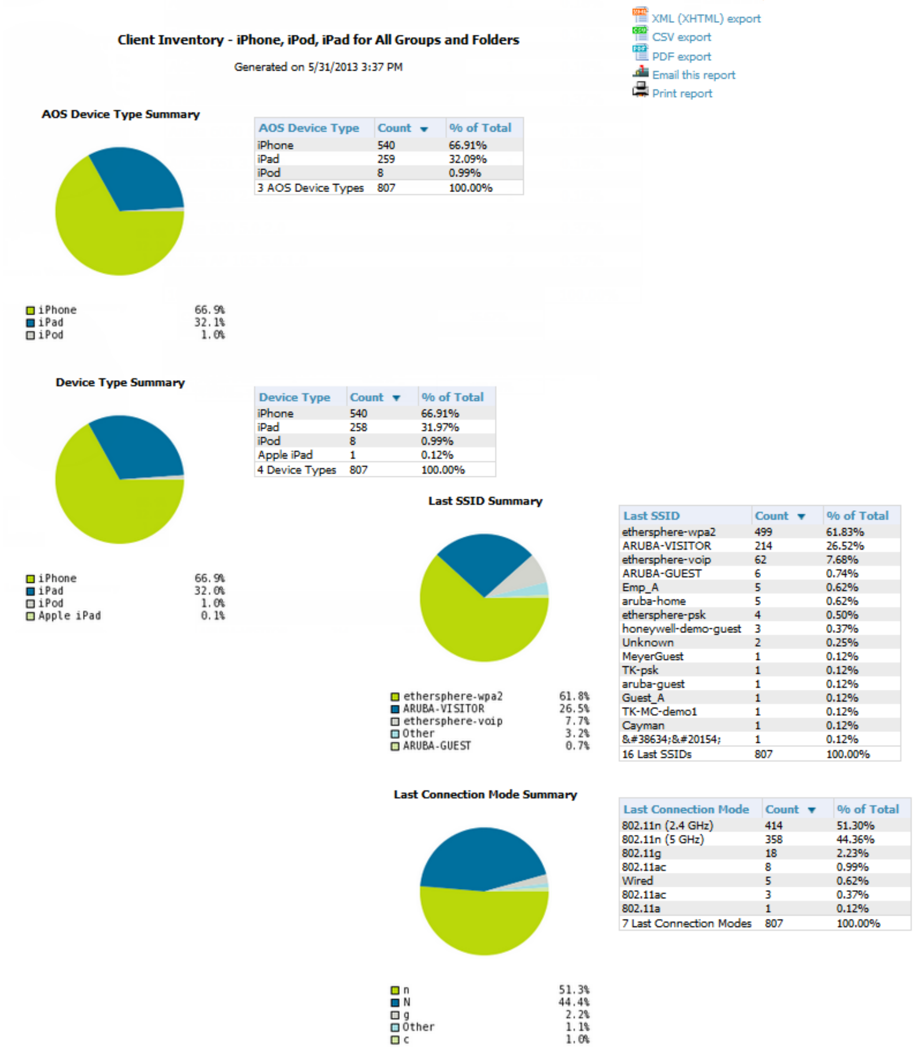
The report output shows a summary of the last connection mode and the last SSID for all devices. This can help determine where and how the clients are connecting.

1. Click on the **Add New Report Definition** button on the **Reports > Definitions** page.
2. Enter the title for the report. In this example, the report is called "Client Inventory - iPhone, iPod, iPad"
3. Select Client Inventory from the Type drop-down menu.
4. Select the following options in the Summarize Report By section:
   - AOS Device Type Summary
   - Device Type Summary
   - Last Connection Mode Summary
   - Last SSID Summary
5. Specify "Matching" in the Model section, and select the following options:
   - iPad
   - iPhone
   - iPod
6. Click the **Save and Run** button.

Output

Figure 179 illustrates the output of this Client Inventory Report. The fields on this page are described in Table 136.

Figure 179 *Reports > Generated > Client Inventory (split view)*



Client Inventory - iPhone, iPod, iPad for All Groups and Folders

Generated on 5/31/2013 3:37 PM

AOS Device Type Summary

AOS Device Type	Count ▼	% of Total
iPhone	540	66.91%
iPad	259	32.09%
iPod	8	0.99%
3 AOS Device Types	807	100.00%

Device Type Summary

Device Type	Count ▼	% of Total
iPhone	540	66.91%
iPad	258	31.97%
iPod	8	0.99%
Apple iPad	1	0.12%
4 Device Types	807	100.00%

Last SSID Summary

Last SSID	Count ▼	% of Total
ethersphere-wpa2	499	61.83%
ARUBA-VISITOR	214	26.52%
ethersphere-voip	62	7.68%
ARUBA-GUEST	6	0.74%
Emp_A	5	0.62%
aruba-home	5	0.62%
ethersphere-psk	4	0.50%
honeywell-demo-guest	3	0.37%
Unknown	2	0.25%
MeyerGuest	1	0.12%
TK-psk	1	0.12%
aruba-guest	1	0.12%
Guest_A	1	0.12%
TK-MC-demo1	1	0.12%
Cayman	1	0.12%
&#38634;&#20154;	1	0.12%
16 Last SSIDs	807	100.00%

Last Connection Mode Summary

Last Connection Mode	Count ▼	% of Total
802.11n (2.4 GHz)	414	51.30%
802.11n (5 GHz)	358	44.36%
802.11g	18	2.23%
802.11ac	8	0.99%
Wired	5	0.62%
802.11ac	3	0.37%
802.11a	1	0.12%
7 Last Connection Modes	807	100.00%

Table 136: *Client Inventory Report output details*

Field	Description
AOS Device Type	Displays the device type or name.
Count	Shows the total number of each device current included in the client inventory.
% of Total	Shows the percentage of each of those devices that are included in the client inventory.
Last SSID Summary	The SSID that each device most recently connected to. This includes the total number of clients and the percentage of each of those devices that connected to the SSID.
Last Connection Mode	The connection mode that each device most recently connected using.This includes the total number of clients and the percentage of each of those devices that connected for each connection mode.

Using the Client Session Report

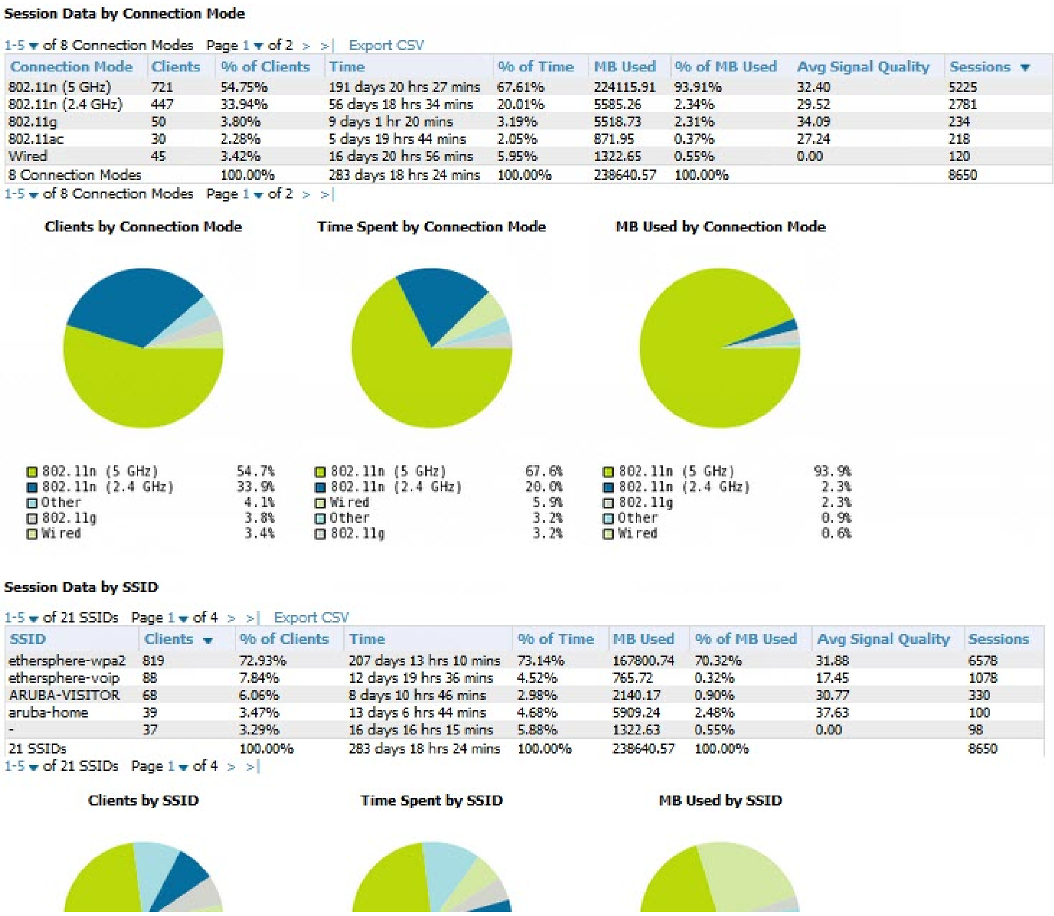
The Client Session Report extensively itemizes user-level activity by session, meaning any instance in which a user connects to the network. In list and chart form, this report tracks and display session information that can include any or all of the following:

- Session Data by Cipher (List or Chart)
- Session Data by Connection Mode (List or Chart)
- Session Data by Role (List or Chart)
- Session Data by SSID (List or Chart)
- Session Data by VLAN (List or Chart)
- Top Clients by Total MB Used
- Session Data by AOS Device Type (List or Chart)
- Session Data by Asset Category (List or Chart)
- Session Data by Asset Group (List or Chart)
- Session Data by Device Type (List or Chart)
- Session Data by EAP Supplicant (List or Chart)
- Session Data by Manufacturer (List or Chart)
- Session Data by Model (List or Chart)
- Session Data by Network Chipset (List or Chart)
- Session Data by Network Driver (List or Chart)
- Session Data by Network Interface Vendor (List or Chart)
- Session Data by OS (List or Chart)
- Session Data by OS Detail (List or Chart)
- Top Clients by Total MB Used by Folder

In addition, each report can be filtered based SSID, Device Type, Manufacturer, Model, and more.

Finally, you can specify the details that you want to include in the Sessions information, such as the MAC Address, Username, Role, SSID, and more.

Figure 180 *Client Session Detail Partial View*



Session Data by Connection Mode

1-5 ▾ of 8 Connection Modes Page 1 ▾ of 2 > >| Export CSV

Connection Mode	Clients	% of Clients	Time	% of Time	MB Used	% of MB Used	Avg Signal Quality	Sessions ▾
802.11n (5 GHz)	721	54.75%	191 days 20 hrs 27 mins	67.61%	224115.91	93.91%	32.40	5225
802.11n (2.4 GHz)	447	33.94%	56 days 18 hrs 34 mins	20.01%	5585.26	2.34%	29.52	2781
802.11g	50	3.80%	9 days 1 hr 20 mins	3.19%	5518.73	2.31%	34.09	234
802.11ac	30	2.28%	5 days 19 hrs 44 mins	2.05%	871.95	0.37%	27.24	218
Wired	45	3.42%	16 days 20 hrs 56 mins	5.95%	1322.65	0.55%	0.00	120
8 Connection Modes		100.00%	283 days 18 hrs 24 mins	100.00%	238640.57	100.00%		8650

1-5 ▾ of 8 Connection Modes Page 1 ▾ of 2 > >|

Session Data by SSID

1-5 ▾ of 21 SSIDs Page 1 ▾ of 4 > >| Export CSV

SSID	Clients ▾	% of Clients	Time	% of Time	MB Used	% of MB Used	Avg Signal Quality	Sessions
ethersphere-wpa2	819	72.93%	207 days 13 hrs 10 mins	73.14%	167800.74	70.32%	31.88	6578
ethersphere-voip	88	7.84%	12 days 19 hrs 36 mins	4.52%	765.72	0.32%	17.45	1078
ARUBA-VISITOR	68	6.06%	8 days 10 hrs 46 mins	2.98%	2140.17	0.90%	30.77	330
aruba-home	39	3.47%	13 days 6 hrs 44 mins	4.68%	5909.24	2.48%	37.63	100
-	37	3.29%	16 days 16 hrs 15 mins	5.88%	1322.63	0.55%	0.00	98
21 SSIDs		100.00%	283 days 18 hrs 24 mins	100.00%	238640.57	100.00%		8650

1-5 ▾ of 21 SSIDs Page 1 ▾ of 4 > >|

Each Client Session Report includes a Client Session Summary section. Table 137 describes the fields that display in this summary.

Table 137: *Client Session Summary Fields and Descriptions*

Field	Description
Sessions	The number of client sessions that occurred during the time range specified in this report.
Unique Clients	The number of unique clients that connected.
Guest Users	The number of guest users that connected.
Unique APs	The number of unique APs that were available.
Average session duration	The average amount of time that a client was connected during this time range. This is determined by {[disconnect time] - [connect time]}.
Total traffic (MB)	The total amount of traffic that passed through the network during this time range.
Avg traffic per session (MB)	The average amount of traffic generated by each session.

Table 137: *Client Session Summary Fields and Descriptions (Continued)*

Field	Description
Avg traffic per client (MB)	The average amount of traffic generated by each client.
Avg bandwidth per client (Kbps)	The average client bandwidth.
Avg signal quality	The average signal quality for each session.

Using the Configuration Audit Report

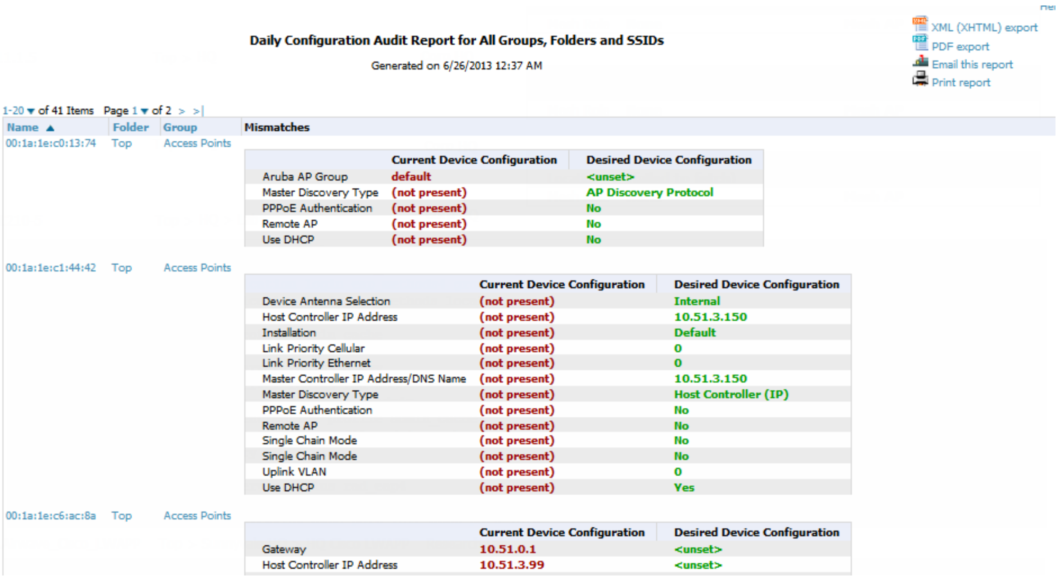
The Configuration Audit Report provides an inventory of device configurations on the network, enabling you to display information one device at a time, one folder at a time, or one device group at a time. This report links to additional configuration pages.

Perform these steps to view the most recent version of the report, then to configure a given device using this report.

1. Navigate to the **Reports** > **Generated** page.
2. Scroll to the bottom, and select **Latest Configuration Audit Report** to display **Detail** device configuration information for all devices. The ensuing **Detail** report can be very large in size, and provides multiple links to additional device configuration or information display pages.
3. You can display device-specific configuration to reduce report size and to focus on a specific device. When viewing configured devices on the **Detail** page, select a device in the **Name** column. The device-specific configuration appears.
4. You can create or assign a template for a given device from the **Detail** page. Select **Add a Template** when viewing device-specific configuration information.
5. You can audit the current device configuration from the **Detail** page. Select **Audit** when viewing device-specific information.
6. You can display archived configuration about a given device from the **Detail** page. Select **Show Archived Device Configuration**.

Figure 181 and Table 138 illustrate and describe the general Configuration Audit report and related contents.

Figure 181 *Daily Configuration Audit Report Page, partial view*



Daily Configuration Audit Report for All Groups, Folders and SSIDs

Generated on 6/26/2013 12:37 AM

1-20 ▾ of 41 Items Page 1 ▾ of 2 > >|

Name ▲	Folder	Group	Mismatches
00:1a:1e:c0:13:74	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Aruba AP Group	default	<unset>
Master Discovery Type	(not present)	AP Discovery Protocol
PPPoE Authentication	(not present)	No
Remote AP	(not present)	No
Use DHCP	(not present)	No

Name ▲	Folder	Group	Mismatches
00:1a:1e:c1:44:42	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Device Antenna Selection	(not present)	Internal
Host Controller IP Address	(not present)	10.51.3.150
Installation	(not present)	Default
Link Priority Cellular	(not present)	0
Link Priority Ethernet	(not present)	0
Master Controller IP Address/DNS Name	(not present)	10.51.3.150
Master Discovery Type	(not present)	Host Controller (IP)
PPPoE Authentication	(not present)	No
Remote AP	(not present)	No
Single Chain Mode	(not present)	No
Single Chain Mode	(not present)	No
Uplink VLAN	(not present)	0
Use DHCP	(not present)	Yes

Name ▲	Folder	Group	Mismatches
00:1a:1e:c6:ac:8a	Top	Access Points	

	Current Device Configuration	Desired Device Configuration
Gateway	10.51.0.1	<unset>
Host Controller IP Address	10.51.3.99	<unset>

Table 138: *Daily Configuration Audit Report*

Field	Description
Name	Displays the device name for every device on the network. Selecting a given device name in this column allows you to display device-specific configuration.
Folder	Displays the folder in which the device is configured in AMP. Selecting 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. Selecting 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 Simultaneous Users**—By default, this list displays the 10 devices that support the highest numbers of users. This list provides links to additional information or configuration pages for each device to make adjustments, as desired.
- **Most Utilized by Bandwidth**—By default, this list displays the 10 devices that consistently have the highest bandwidth consumption during the time period defined for the report. This list provides links to additional information or configuration pages for each device.
- **Least Utilized by Maximum Number of Simultaneous Users**—By default, this list displays the 10 devices that are the least used, according to the number of users.
- **Least Utilized by Bandwidth**—By default, this list displays the 10 devices that are the least used, according to the bandwidth throughput.
- **Devices**—This list displays all devices in AMP. By default it is sorted alphabetically by device name.

NOTE

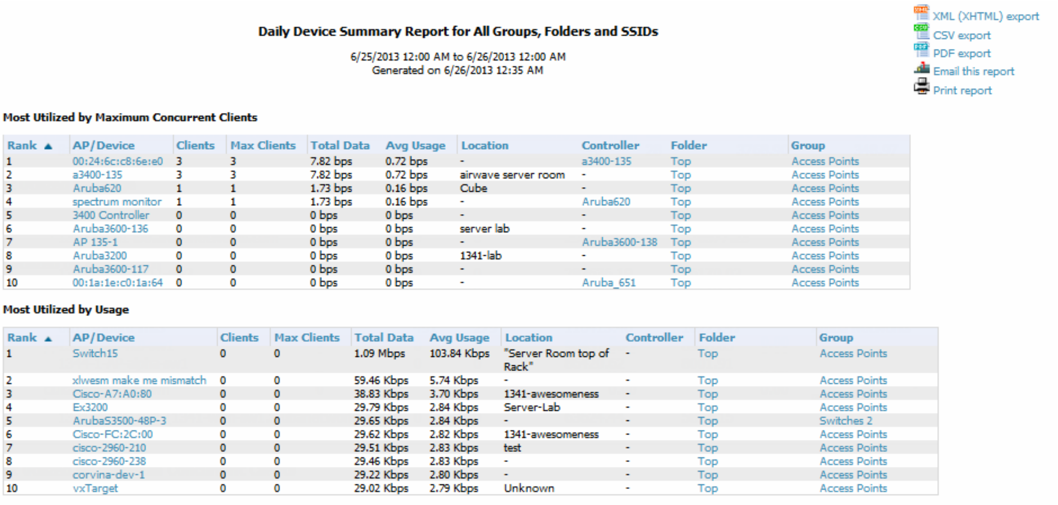
You can specify the number of devices that appear in each of the first four categories in the **Reports > Definitions > Add** page.

Any section of this report can be sorted by any of the columns. 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.

Figure 182 and Table 139 illustrate and describe the Device Summary Report.

Figure 182 *Daily Device Summary Report Illustration (partial view)*



XML (XHTML) export
CSV export
PDF export
Email this report
Print report

Daily Device Summary Report for All Groups, Folders and SSIDs

6/25/2013 12:00 AM to 6/26/2013 12:00 AM
Generated on 6/26/2013 12:35 AM

Most Utilized by Maximum Concurrent Clients

Rank ▲	AP/Device	Clients	Max Clients	Total Data	Avg Usage	Location	Controller	Folder	Group
1	00:24:6c:c8:6e:e0	3	3	7.82 bps	0.72 bps	-	a3400-135	Top	Access Points
2	a3400-135	3	3	7.82 bps	0.72 bps	airwave server room	-	Top	Access Points
3	Aruba620	1	1	1.73 bps	0.16 bps	Cube	-	Top	Access Points
4	spectrum monitor	1	1	1.73 bps	0.16 bps	-	Aruba620	Top	Access Points
5	3400 Controller	0	0	0 bps	0 bps	-	-	Top	Access Points
6	Aruba3600-136	0	0	0 bps	0 bps	server lab	-	Top	Access Points
7	AP 135-1	0	0	0 bps	0 bps	-	Aruba3600-138	Top	Access Points
8	Aruba3200	0	0	0 bps	0 bps	1341-lab	-	Top	Access Points
9	Aruba3600-117	0	0	0 bps	0 bps	-	-	Top	Access Points
10	00:1a:1e:c0:1a:64	0	0	0 bps	0 bps	-	Aruba_651	Top	Access Points

Most Utilized by Usage

Rank ▲	AP/Device	Clients	Max Clients	Total Data	Avg Usage	Location	Controller	Folder	Group
1	Switch15	0	0	1.09 Mbps	103.84 Kbps	"Server Room top of Rack"	-	Top	Access Points
2	xlwesm make me mismatch	0	0	59.46 Kbps	5.74 Kbps	-	-	Top	Access Points
3	Cisco-A7:A0:80	0	0	38.83 Kbps	3.70 Kbps	1341-awesomeness	-	Top	Access Points
4	Ex3200	0	0	29.79 Kbps	2.84 Kbps	Server-Lab	-	Top	Access Points
5	ArubaS3500-48P-3	0	0	29.65 Kbps	2.84 Kbps	-	-	Top	Switches 2
6	Cisco-FC:2C:00	0	0	29.62 Kbps	2.82 Kbps	1341-awesomeness	-	Top	Access Points
7	cisco-2960-210	0	0	29.51 Kbps	2.83 Kbps	test	-	Top	Access Points
8	cisco-2960-238	0	0	29.46 Kbps	2.83 Kbps	-	-	Top	Access Points
9	corvina-dev-1	0	0	29.22 Kbps	2.80 Kbps	-	-	Top	Access Points
10	vxTarget	0	0	29.02 Kbps	2.79 Kbps	Unknown	-	Top	Access Points

Table 139: *Daily Device Summary Report Unique Fields and Descriptions*

Field	Description
Rank	Ranks the device from 1 to 10.
AP/Device	The AP name or device MAC address.
Clients	The number of clients that were last connected to the device.
Max Clients	The highest number of clients that were connected to the device during the time/date range of the report. If a range is not specified, then this value will match the value for Clients.
Total Data	Displays the total rate of data in that traveled through device during the period of time covered by the report.
Average Usage	Displays the average rate of data in that traveled through device during the period of time covered by the report.
Location	Displays the location information if available.
Controller	The controller that the device is associated to.
Folder/Group	Displays the folder and group information for the device.

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:

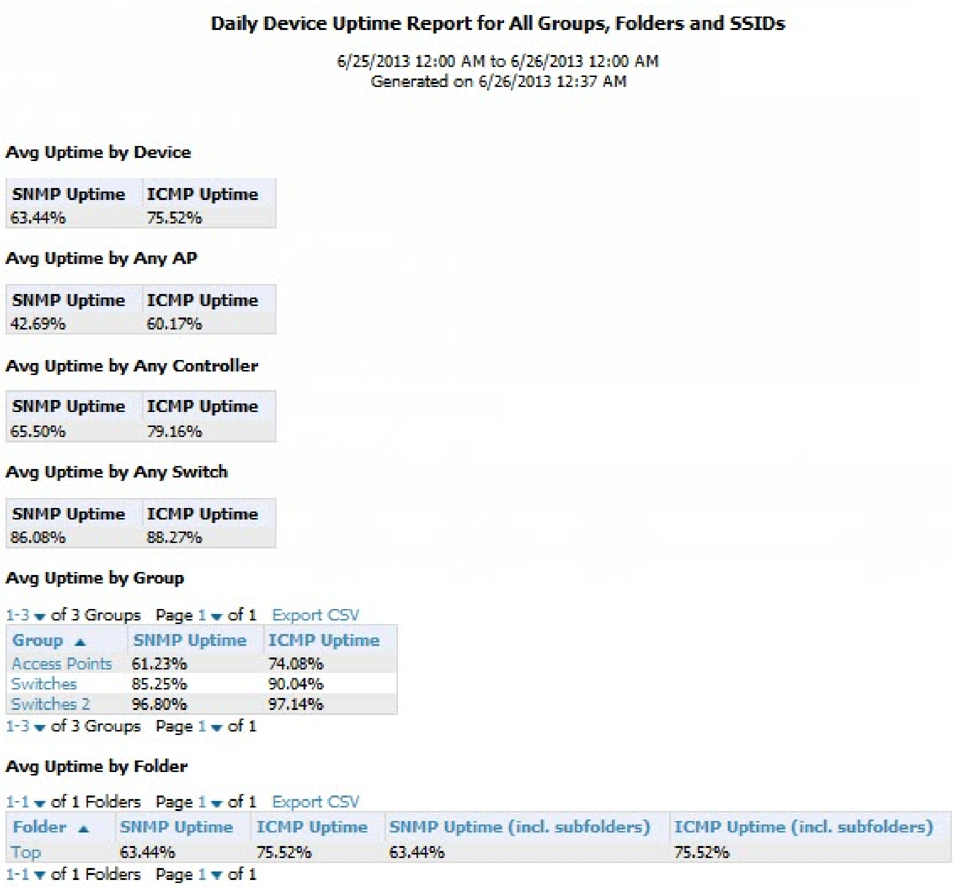
- Total average uptime by SNMP and ICMP
- Average uptime by device group
- Average uptime by device folder

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. It can demonstrate service parameters, can establish locations that have superior or problematic uptime availability, and can help with additional analysis in multiple ways. Locations, device groups, or other groupings within a network can be identified as needing attention or can be proven to have superior performance when using this report.

The Device Uptime Report contains columns that track bootstrap count (number of times the device has gone down for a firmware change), reboot count, downtime duration, and downtime duration percent. As mentioned above, you can optionally ignore device downtime during planned maintenance periods in this report, and you can restrict the report to business days only.

The Device Uptime Report is described in the image and table that follow.

Figure 183 *Device Uptime Report Illustration*



Daily Device Uptime Report for All Groups, Folders and SSIDs

6/25/2013 12:00 AM to 6/26/2013 12:00 AM
Generated on 6/26/2013 12:37 AM

Avg Uptime by Device

SNMP Uptime	ICMP Uptime
63.44%	75.52%

Avg Uptime by Any AP

SNMP Uptime	ICMP Uptime
42.69%	60.17%

Avg Uptime by Any Controller

SNMP Uptime	ICMP Uptime
65.50%	79.16%

Avg Uptime by Any Switch

SNMP Uptime	ICMP Uptime
86.08%	88.27%

Avg Uptime by Group

1-3 ▾ of 3 Groups Page 1 ▾ of 1 Export CSV

Group ▲	SNMP Uptime	ICMP Uptime
Access Points	61.23%	74.08%
Switches	85.25%	90.04%
Switches 2	96.80%	97.14%

1-3 ▾ of 3 Groups Page 1 ▾ of 1

Avg Uptime by Folder

1-1 ▾ of 1 Folders Page 1 ▾ of 1 Export CSV

Folder ▲	SNMP Uptime	ICMP Uptime	SNMP Uptime (incl. subfolders)	ICMP Uptime (incl. subfolders)
Top	63.44%	75.52%	63.44%	75.52%

1-1 ▾ of 1 Folders Page 1 ▾ of 1

Table 140: *Device Uptime Report Unique Fields and Descriptions*

Field	Description
SNMP Uptime	Displays the percentage of time the device was reachable via ICMP. AMP 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. AMP 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

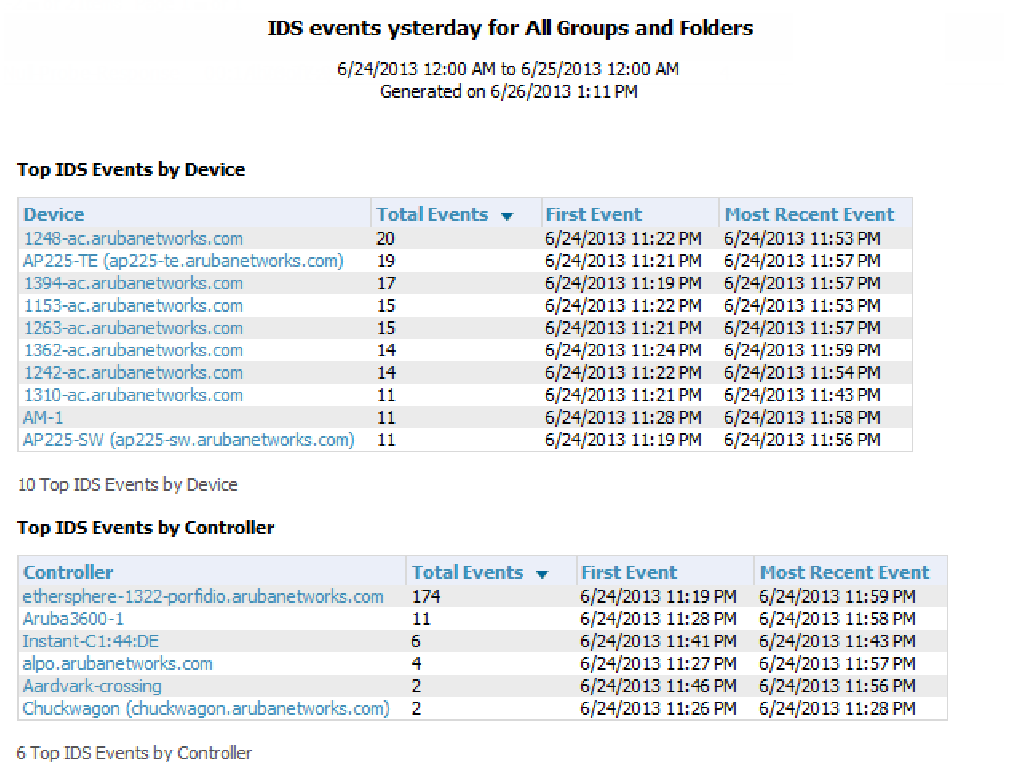
The IDS Events Report lists and tracks IDS events on the network involving APs or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response. You can filter this report to show IDS events for specific devices (Controllers, APs, etc.) By default, this report will show up to 10 IDS for each specified device type. You can change this value to anything other than 0.

> NOTE
>
> Your role must be enabled to view RAPIDS in order to see this report. In addition, this report requires that you enter a start and stop time range.

The **Home** > **Overview** page also cites IDS events. Triggers can be configured for IDS events. Refer to "Creating New Triggers" on page 219 for additional information.

Figure 184 and Table 141 illustrate and describe the IDS Events Detail report. Selecting the AP device or controller name takes you to the **APs/Devices** > **List** page.

Figure 184 *IDS Events Report Illustration*



IDS events ysterday for All Groups and Folders

6/24/2013 12:00 AM to 6/25/2013 12:00 AM
Generated on 6/26/2013 1:11 PM

Top IDS Events by Device

Device	Total Events ▼	First Event	Most Recent Event
1248-ac.arubanetworks.com	20	6/24/2013 11:22 PM	6/24/2013 11:53 PM
AP225-TE (ap225-te.arubanetworks.com)	19	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1394-ac.arubanetworks.com	17	6/24/2013 11:19 PM	6/24/2013 11:57 PM
1153-ac.arubanetworks.com	15	6/24/2013 11:22 PM	6/24/2013 11:53 PM
1263-ac.arubanetworks.com	15	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1362-ac.arubanetworks.com	14	6/24/2013 11:24 PM	6/24/2013 11:59 PM
1242-ac.arubanetworks.com	14	6/24/2013 11:22 PM	6/24/2013 11:54 PM
1310-ac.arubanetworks.com	11	6/24/2013 11:21 PM	6/24/2013 11:43 PM
AM-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
AP225-SW (ap225-sw.arubanetworks.com)	11	6/24/2013 11:19 PM	6/24/2013 11:56 PM

10 Top IDS Events by Device

Top IDS Events by Controller

Controller	Total Events ▼	First Event	Most Recent Event
ethersphere-1322-porfidio.arubanetworks.com	174	6/24/2013 11:19 PM	6/24/2013 11:59 PM
Aruba3600-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
Instant-C1:44:DE	6	6/24/2013 11:41 PM	6/24/2013 11:43 PM
alpo.arubanetworks.com	4	6/24/2013 11:27 PM	6/24/2013 11:57 PM
Aardvark-crossing	2	6/24/2013 11:46 PM	6/24/2013 11:56 PM
Chuckwagon (chuckwagon.arubanetworks.com)	2	6/24/2013 11:26 PM	6/24/2013 11:28 PM

6 Top IDS Events by Controller

Table 141: *IDS Events Detail Unique Fields and Descriptions*

Field	Description
Device/Controller	These columns list the controllers and other devices for which IDS events have occurred in the specified time range, and provides a link to the **APs/Devices > Monitor** page for each.
Total Events	Shows the number of events for each AP and/or Controller.
First Event	Shows the date and time of the first event.

Table 141: *IDS Events Detail Unique Fields and Descriptions (Continued)*

Field	Description
Most Recent Event	Shows the date and time of the last/most recent event.
Attack	Displays the name or label for the IDS event.
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 on the network. The output breaks down this information by vendor, model (including firmware and bootloader), and device type.

Example

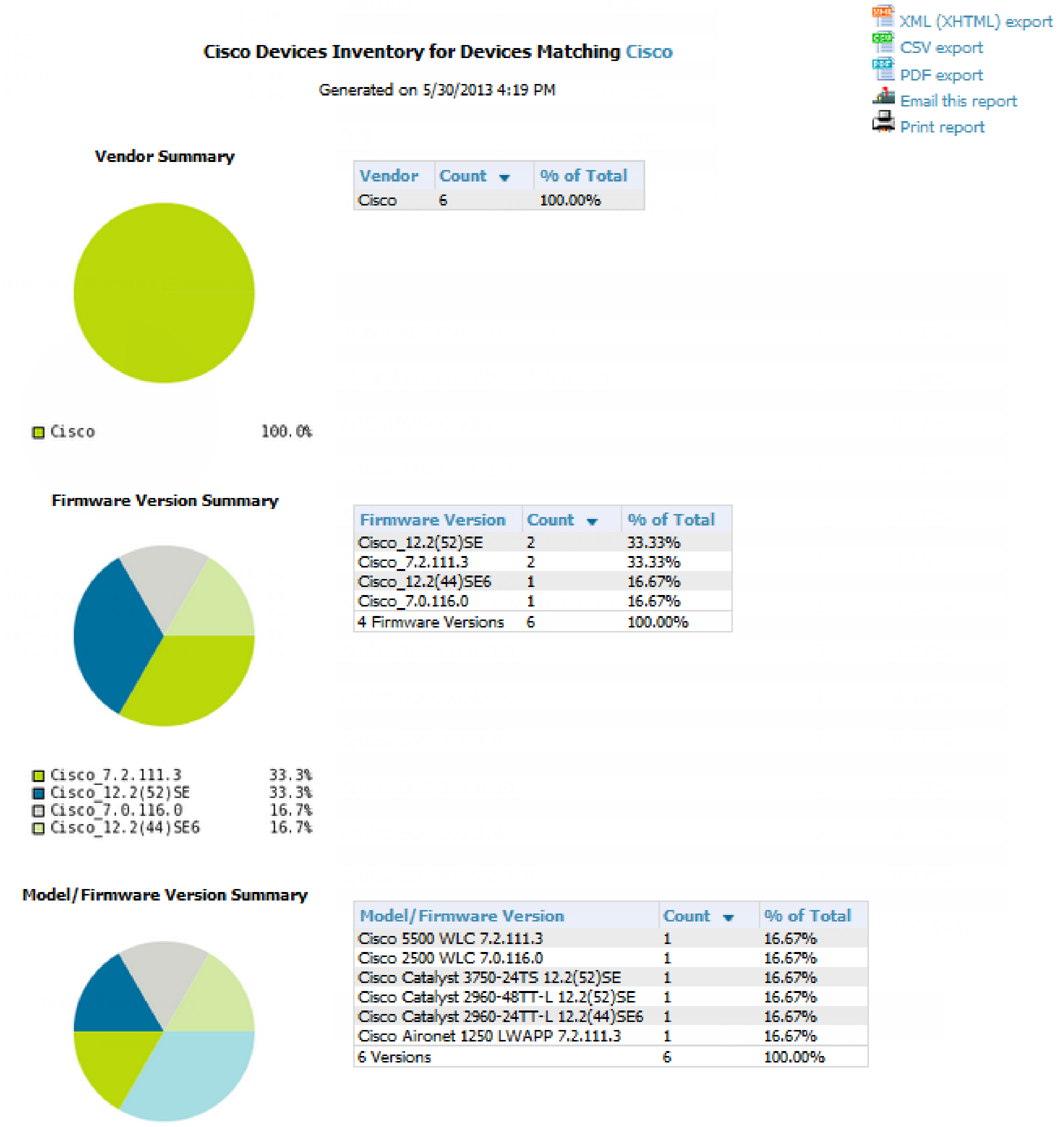
The following example creates a sample Inventory report. This report looks for all Cisco devices currently on your network. Perform similar steps to create this report. Note that any field omitted from this example is assumed to remain the default value.

1. Click on the **Add New Report Definition** button on the **Reports** > **Definitions** page.
2. Enter the title for the report. In this example, the report is called "Cisco Devices Inventory."
3. Select Inventory from the Type drop-down menu.
4. Type Cisco in the Device Search Filter field.
5. In the Summarize report by section, select the Type Summary check box. This is the only summary option not selected by default. For the purposes of this report, the Type Summary will break down the list of Cisco devices on your network based on the device type.
6. Click the **Save and Run** button.

Output

Figure 185 illustrates the output of the Inventory report.

Figure 185 *Inventory Report Illustration (partial view)*



Cisco Devices Inventory for Devices Matching Cisco

Generated on 5/30/2013 4:19 PM

Vendor	Count	% of Total
Cisco	6	100.00%

Firmware Version	Count	% of Total
Cisco_12.2(52)SE	2	33.33%
Cisco_7.2.111.3	2	33.33%
Cisco_12.2(44)SE6	1	16.67%
Cisco_7.0.116.0	1	16.67%
4 Firmware Versions	6	100.00%

Model/Firmware Version	Count	% of Total
Cisco 5500 WLC 7.2.111.3	1	16.67%
Cisco 2500 WLC 7.0.116.0	1	16.67%
Cisco Catalyst 3750-24TS 12.2(52)SE	1	16.67%
Cisco Catalyst 2960-48TT-L 12.2(52)SE	1	16.67%
Cisco Catalyst 2960-24TT-L 12.2(44)SE6	1	16.67%
Cisco Aironet 1250 LWAPP 7.2.111.3	1	16.67%
6 Versions	6	100.00%

Table 142: *Inventory Report output details*

Field	Description
Vendor	Displays the device type or name. In the example above, the only vendor specified in the report definition was Cisco.
Count	Shows the total number of each device current included in the client inventory.
% of Total	Shows the percentage of each of those devices that are included in the client inventory.
Firmware Version	The firmware version on each device. This includes the total number of devices and the percentage of each of those devices compared to other devices. In the example above, 33% (or 2 total) of the Cisco devices are on firmware Cisco_ 7.2.111.3.

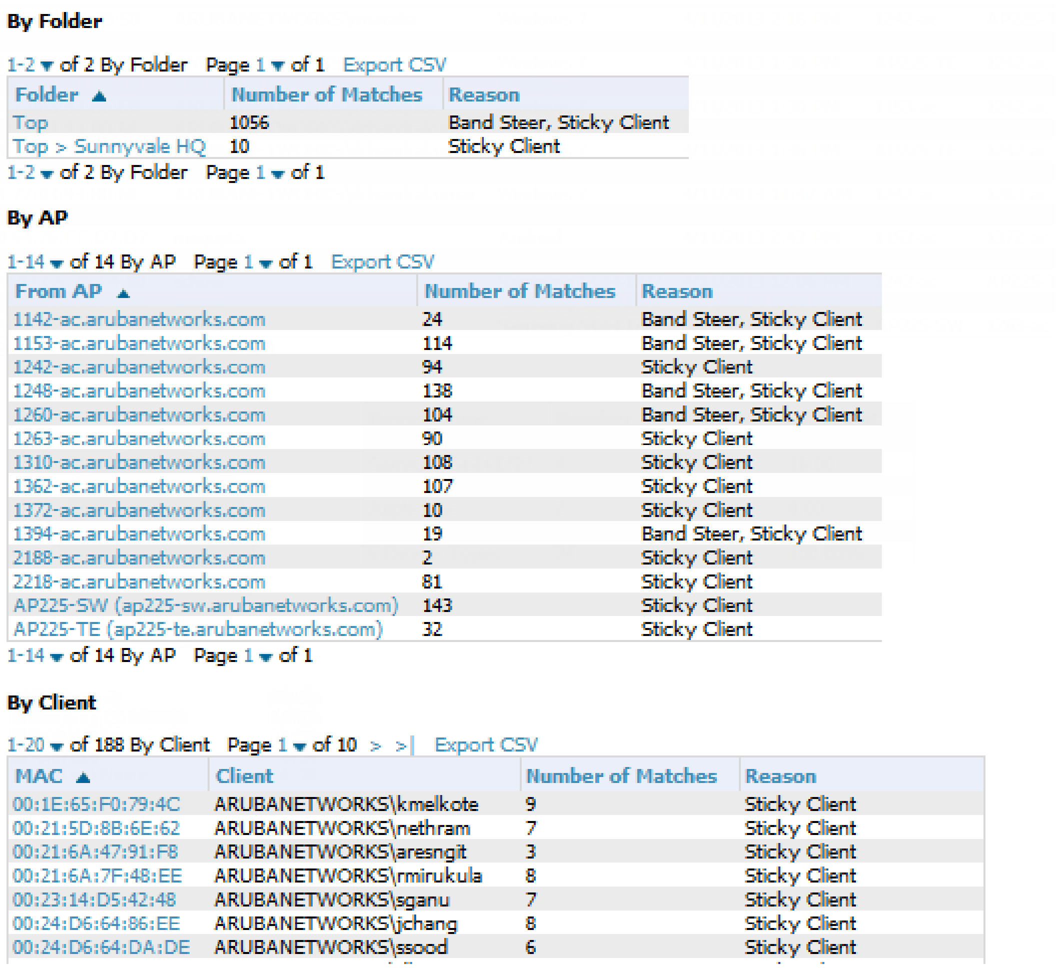
Table 142: *Inventory Report output details (Continued)*

Field	Description
Model/Firmware Version	This field further breaks down the firmware version into specific device models and specific versions. This includes the total number of devices and the percentage of each of those devices compared to other devices. As indicated previously, the example above shows that 2 of the Cisco devices are on firmware Cisco_7.2.111.3. Each is a separate model, though.

Using the Match Event Report

Use the Match Events report to track matching events that occurred on devices. This information can be broken down based on a specific folder, AP, and/or client. You can also include graphical information that summarizes events by connection mode, device type, and reason. Similarly, you can choose to show detailed information in the report, including MAC addresses, clients, device types, event time, the from and to AP, the reason for the match, whether the match was a success, and the connection mode.

Figure 186 *Sample output for Match Event Report (partial view)*



By Folder

1-2 ▾ of 2 By Folder Page 1 ▾ of 1 Export CSV

Folder ▲	Number of Matches	Reason
Top	1056	Band Steer, Sticky Client
Top > Sunnyvale HQ	10	Sticky Client

1-2 ▾ of 2 By Folder Page 1 ▾ of 1

By AP

1-14 ▾ of 14 By AP Page 1 ▾ of 1 Export CSV

From AP ▲	Number of Matches	Reason
1142-ac.arubanetworks.com	24	Band Steer, Sticky Client
1153-ac.arubanetworks.com	114	Band Steer, Sticky Client
1242-ac.arubanetworks.com	94	Sticky Client
1248-ac.arubanetworks.com	138	Band Steer, Sticky Client
1260-ac.arubanetworks.com	104	Band Steer, Sticky Client
1263-ac.arubanetworks.com	90	Sticky Client
1310-ac.arubanetworks.com	108	Sticky Client
1362-ac.arubanetworks.com	107	Sticky Client
1372-ac.arubanetworks.com	10	Sticky Client
1394-ac.arubanetworks.com	19	Band Steer, Sticky Client
2188-ac.arubanetworks.com	2	Sticky Client
2218-ac.arubanetworks.com	81	Sticky Client
AP225-SW (ap225-sw.arubanetworks.com)	143	Sticky Client
AP225-TE (ap225-te.arubanetworks.com)	32	Sticky Client

1-14 ▾ of 14 By AP Page 1 ▾ of 1

By Client

1-20 ▾ of 188 By Client Page 1 ▾ of 10 > >| Export CSV

MAC ▲	Client	Number of Matches	Reason
00:1E:65:F0:79:4C	ARUBANETWORKS\kmelkote	9	Sticky Client
00:21:5D:8B:6E:62	ARUBANETWORKS\nethram	7	Sticky Client
00:21:6A:47:91:F8	ARUBANETWORKS\aresngit	3	Sticky Client
00:21:6A:7F:48:EE	ARUBANETWORKS\rmirukula	8	Sticky Client
00:23:14:D5:42:48	ARUBANETWORKS\sganu	7	Sticky Client
00:24:D6:64:86:EE	ARUBANETWORKS\jchang	8	Sticky Client
00:24:D6:64:DA:DE	ARUBANETWORKS\ssood	6	Sticky Client

Table 143: *Match Event Report output details*

Field	Description
Folder/AP/Client	The total number of matches that occurred in each folder, each AP, and each Client. The tables also include a reason for the match event. This information is obtained directly from the controller. Data will only display for a Folder, AP, and Client if each has experienced at least one match event.
Device Type Summary	This shows the total number and percentage of match events that occurred on all device types (for example, iPhone, Kindle, etc.). The graph shows the top 5 devices.
Reasons for Match Summary	This graph and table break down the number and percentage of matches based on the match reason.
Connection Mode Summary	This graph and table show the number and percentage of matches based on the device's connection mode.

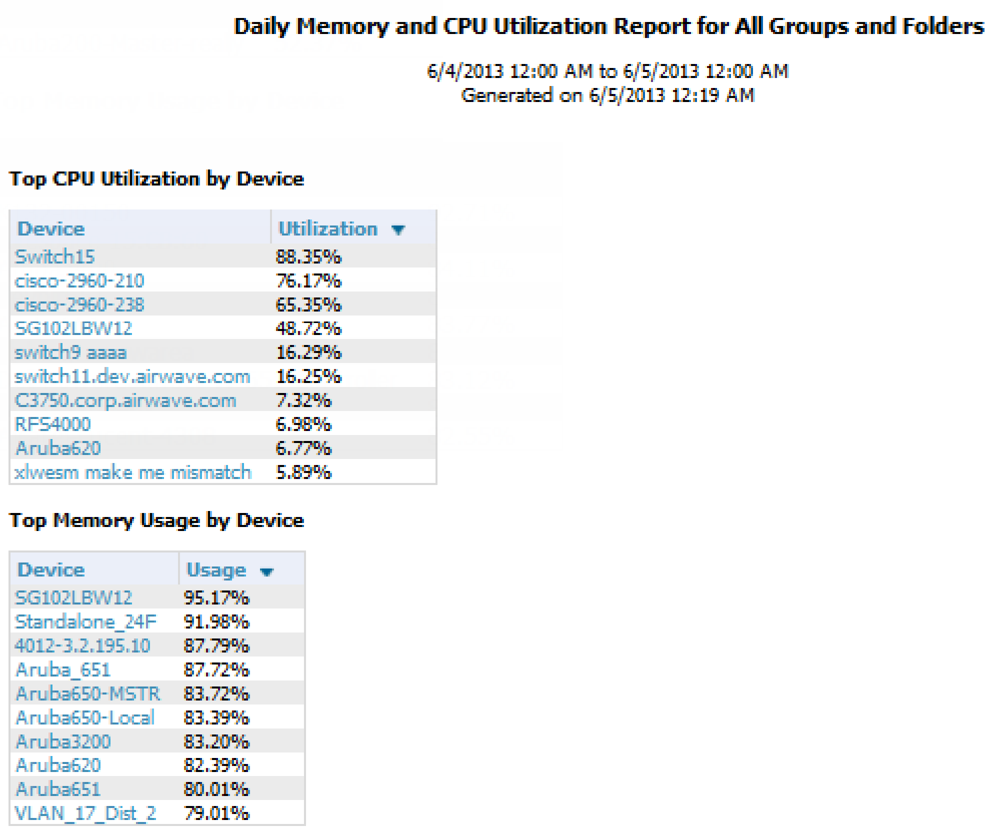
Using the Memory and CPU Utilization Report

The Memory and CPU Utilization Report displays the top percentage of memory utilization and usage for devices and CPUs. You can filter this report to show memory and utilization information for specific devices (Controllers, APs, etc.) By default, this report will show up to 10 IDS for each specified device type. You can change this value to anything other than 0.

To create a scheduled and generated report of this type, refer to "Using Daily Reports" on page 281.

Figure 187 illustrates the this report.

Figure 187 *Daily Memory and CPU Usage Report Illustration*



Daily Memory and CPU Utilization Report for All Groups and Folders

6/4/2013 12:00 AM to 6/5/2013 12:00 AM
Generated on 6/5/2013 12:19 AM

Top CPU Utilization by Device

Device	Utilization ▼
Switch15	88.35%
cisco-2960-210	76.17%
cisco-2960-238	65.35%
SG102LBW12	48.72%
switch9 aaaa	16.29%
switch11.dev.airwave.com	16.25%
C3750.corp.airwave.com	7.32%
RFS4000	6.98%
Aruba620	6.77%
xlwesm make me mismatch	5.89%

Top Memory Usage by Device

Device	Usage ▼
SG102LBW12	95.17%
Standalone_24F	91.98%
4012-3.2.195.10	87.79%
Aruba_651	87.72%
Aruba650-MSTR	83.72%
Aruba650-Local	83.39%
Aruba3200	83.20%
Aruba620	82.39%
Aruba651	80.01%
VLAN_17_Dist_2	79.01%

Using the Network Usage Report

The Network Usage Report contains network-wide information in two categories:

- **Usage**—maximum and average bandwidth
- **Clients**—average bandwidth in and out

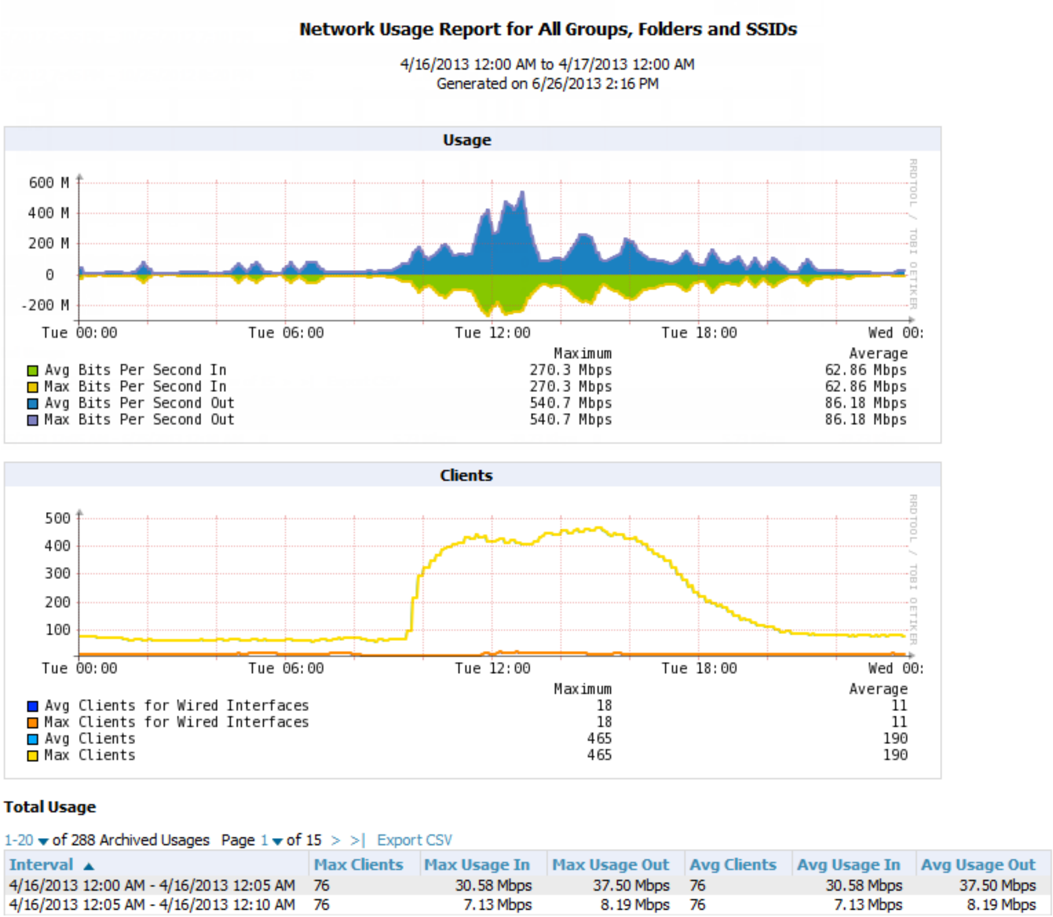
This information can be broken down by Groups and Folders. It can also be summarized by Usage, Client Count, and by both for folders.

When you create this report, you can specify to view information for all or specific device types and all or specific SSIDs. You can summarize the report based on Client Count, Usage, and/or Usage and Client Count by Folder.

This report by default includes graphical information. You can specify to include tabular information below each graph. If you select this option, then you can also specify the columns that display in the tables.

Figure 188 illustrates the Network Usage Report. The fields that display on this output are described in Table 144.

Figure 188 *Network Usage Report Illustration*



Network Usage Report for All Groups, Folders and SSIDs

4/16/2013 12:00 AM to 4/17/2013 12:00 AM
Generated on 6/26/2013 2:16 PM

	Maximum	Average
🟩 Avg Bits Per Second In	270.3 Mbps	62.86 Mbps
🟨 Max Bits Per Second In	270.3 Mbps	62.86 Mbps
🟦 Avg Bits Per Second Out	540.7 Mbps	86.18 Mbps
🟪 Max Bits Per Second Out	540.7 Mbps	86.18 Mbps

	Maximum	Average
🟦 Avg Clients for Wired Interfaces	18	11
🟧 Max Clients for Wired Interfaces	18	11
🟦 Avg Clients	465	190
🟨 Max Clients	465	190

Total Usage

1-20 ▾ of 288 Archived Usages Page 1 ▾ of 15 > >| Export CSV

Interval ▲	Max Clients	Max Usage In	Max Usage Out	Avg Clients	Avg Usage In	Avg Usage Out
4/16/2013 12:00 AM - 4/16/2013 12:05 AM	76	30.58 Mbps	37.50 Mbps	76	30.58 Mbps	37.50 Mbps
4/16/2013 12:05 AM - 4/16/2013 12:10 AM	76	7.13 Mbps	8.19 Mbps	76	7.13 Mbps	8.19 Mbps

Table 144: *Total Usage table output details*

Field	Description
Interval	This table is broken down in five-minute intervals. The Interval column describes the network usage information during these specific five minutes.
Max Clients	The maximum number of clients that were connected during this interval.
Max Usage In	Shows the maximum amount of incoming traffic on the network during this interval. This value is shown in Mbps.
Max Usage Out	Shows the maximum amount of outgoing traffic on the network during this interval. This value is shown in Mbps.
Avg Clients	The average number of clients that were connected during this interval.
Avg Usage In	Shows the average amount of incoming traffic on the network during this interval. This value is shown in Mbps.
Avg Usage Out	Shows the average amount of outgoing traffic on the network during this interval. This value is shown in Mbps.

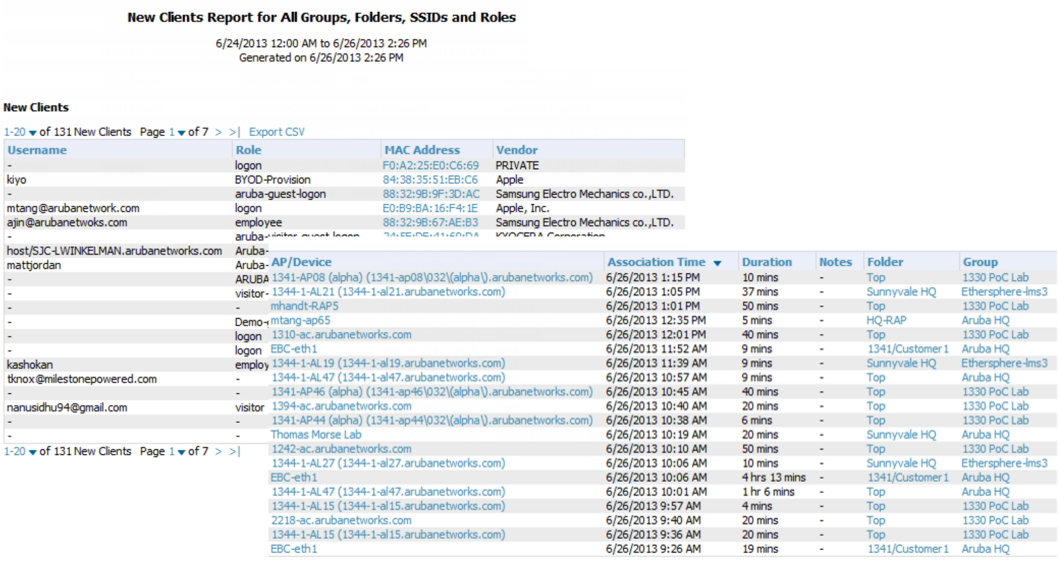
Using the New Clients Report

The New Clients 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. This report gives you the option to filter instead on specific devices and/or users. Whether viewing information for devices or clients, the report can configured to display additional options. For many of these options, you can choose to view all information or a specific set of information (Matching option). If Matching is selected, a text entry field displays. When you put your cursor in the text entry field, an additional side menu displays providing you with a list of available options that you can select.

- SSID - All or Selected
- Aruba Role - All or Selected
- Classification (for possible Rogue devices) - All or Selected
- Device Type - All or Matching
- AOS Device Type - All or Matching
- Manufacturer - All or Matching
- Model - All or Matching
- OS - All or Matching
- OS Detail - All or Matching
- Network Chipset - All or Matching
- Network Driver - All or Matching
- EAP Supplicant - All or Matching
- Asset Group - All or Matching
- Asset Category - All or Matching

Figure 189 illustrates the fields and information in the New Clients Report. The fields that display on this output are described in Table 145.

Figure 189 *New Clients Report Illustration (split view)*



New Clients Report for All Groups, Folders, SSIDs and Roles

6/24/2013 12:00 AM to 6/26/2013 2:26 PM
Generated on 6/26/2013 2:26 PM

New Clients

1-20 ▾ of 131 New Clients Page 1 ▾ of 7 > >| Export CSV

Username	Role	MAC Address	Vendor
-	logon	F0:A2:25:E0:C6:69	PRIVATE
kiyo	BYOD-Provision	84:38:35:51:EB:C6	Apple
-	aruba-guest-logon	88:32:9B:9F:3D:AC	Samsung Electro Mechanics co.,LTD.
mtang@arubanetwork.com	logon	E0:B9:BA:16:F4:1E	Apple, Inc.
ajin@arubanetwoks.com	employee	88:32:9B:67:AE:B3	Samsung Electro Mechanics co.,LTD.
-	aruba-visitor-guest-logon	24:FE:DE:41:60:DA	KYOCERA Corporation
host/SJC-LWINKELMAN.arubanetworks.com	Aruba-		
mattjordan	Aruba-		
-	ARUBA		
-	visitor-		
-	-		
-	Demo-		
-	logon		
-	logon		
kashokan	employ		
tknox@milestonepowered.com	-		
-	-		
nanusidhu94@gmail.com	visitor		
-	-		
-	-		

1-20 ▾ of 131 New Clients Page 1 ▾ of 7 > >|

AP/Device	Association Time ▾	Duration	Notes	Folder	Group
1341-AP08 (alpha) (1341-ap08\032\(alpha\).arubanetworks.com)	6/26/2013 1:15 PM	10 mins	-	Top	1330 PoC Lab
1344-1-AL21 (1344-1-al21.arubanetworks.com)	6/26/2013 1:05 PM	37 mins	-	Sunnyvale HQ	Ethersphere-lms3
mhandt-RAP5	6/26/2013 1:01 PM	50 mins	-	Top	1330 PoC Lab
mtang-ap65	6/26/2013 12:35 PM	5 mins	-	HQ-RAP	Aruba HQ
1310-ac.arubanetworks.com	6/26/2013 12:01 PM	40 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 11:52 AM	9 mins	-	1341/Customer1	Aruba HQ
1344-1-AL19 (1344-1-al19.arubanetworks.com)	6/26/2013 11:39 AM	9 mins	-	Sunnyvale HQ	Ethersphere-lms3
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:57 AM	9 mins	-	Top	Aruba HQ
1341-AP46 (alpha) (1341-ap46\032\(alpha\).arubanetworks.com)	6/26/2013 10:45 AM	40 mins	-	Top	1330 PoC Lab
1394-ac.arubanetworks.com	6/26/2013 10:40 AM	20 mins	-	Top	1330 PoC Lab
1341-AP44 (alpha) (1341-ap44\032\(alpha\).arubanetworks.com)	6/26/2013 10:38 AM	6 mins	-	Top	1330 PoC Lab
Thomas Morse Lab	6/26/2013 10:19 AM	20 mins	-	Sunnyvale HQ	Aruba HQ
1242-ac.arubanetworks.com	6/26/2013 10:10 AM	50 mins	-	Top	1330 PoC Lab
1344-1-AL27 (1344-1-al27.arubanetworks.com)	6/26/2013 10:06 AM	10 mins	-	Sunnyvale HQ	Ethersphere-lms3
EBC-eth1	6/26/2013 10:06 AM	4 hrs 13 mins	-	1341/Customer1	Aruba HQ
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:01 AM	1 hr 6 mins	-	Top	Aruba HQ
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:57 AM	4 mins	-	Top	1330 PoC Lab
2218-ac.arubanetworks.com	6/26/2013 9:40 AM	20 mins	-	Top	1330 PoC Lab
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:36 AM	20 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 9:26 AM	19 mins	-	1341/Customer1	Aruba HQ

Table 145: *New Clients Report output details*

Field	Description
Username	The client name, if available.
Role	The client's role, if available
MAC Address	The new client's MAC address
Vendor	The vendor for the client device.
AP/Device	The AP/Device that the client is currently connected to.
Association Time	The time when the client last associated with the device.
Duration	How long the client has been connected to the device.
Folder/Group	Shows the folder and group of the device that the client is currently connected to.

Using the New Rogue Devices Report

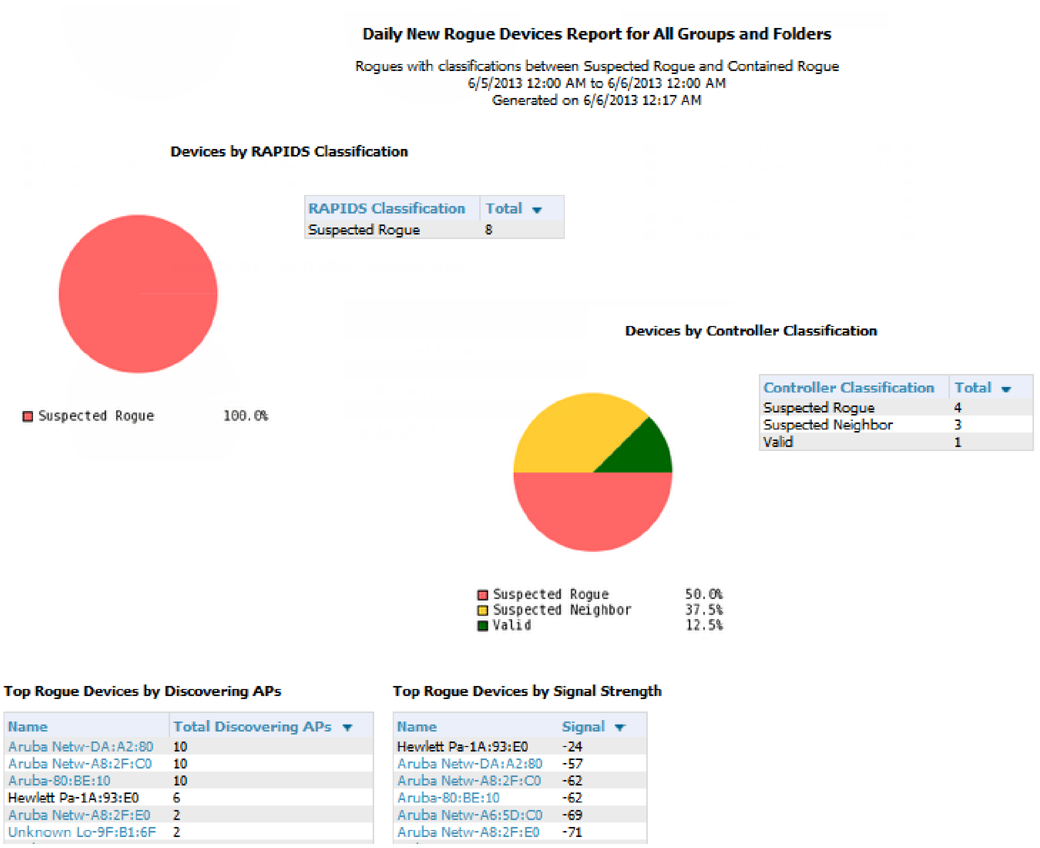
The New Rogue Devices Report summarizes rogue device information including the following categories of information:

- Rogue devices by RAPIDS classification—described in "Using RAPIDS and Rogue Classification" on page 197
- Top rogue devices by number of discovering APs
- Top rogue devices by signal strength
- Graphical summary of rogue devices by LAN MAC address vendor
- Graphical summary of rogue devices by radio MAC address vendor
- Text-based table summary of rogue device counts
- Detailed and text-based table of rogue devices discovered only wirelessly with extensive device parameters and hyperlink interoperability to additional AMP pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional AMP pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional AMP pages

This report is not run by default, but is available after you define it.

Refer to Figure 190 for a sample illustration of this report.

Figure 190 *New Rogue Devices Report Illustration (partial view)*



Daily New Rogue Devices Report for All Groups and Folders

Rogues with classifications between Suspected Rogue and Contained Rogue
6/5/2013 12:00 AM to 6/6/2013 12:00 AM
Generated on 6/6/2013 12:17 AM

Devices by RAPIDS Classification

RAPIDS Classification	Total ▼
Suspected Rogue	8

Devices by Controller Classification

Controller Classification	Total ▼
Suspected Rogue	4
Suspected Neighbor	3
Valid	1

Top Rogue Devices by Discovering APs

Name	Total Discovering APs ▼
Aruba Netw-DA:A2:80	10
Aruba Netw-A8:2F:C0	10
Aruba-80:BE:10	10
Hewlett Pa-1A:93:E0	6
Aruba Netw-A8:2F:E0	2
Unknown Lo-9F:B1:6F	2

Top Rogue Devices by Signal Strength

Name	Signal ▼
Hewlett Pa-1A:93:E0	-24
Aruba Netw-DA:A2:80	-57
Aruba Netw-A8:2F:C0	-62
Aruba-80:BE:10	-62
Aruba Netw-A6:5D:C0	-69
Aruba Netw-A8:2F:E0	-71

The rogue device inventories that comprise this report contain many fields, described in Table 146.

Table 146: *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 197 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 197 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 146: *New Rogue Devices Report Fields (Continued)*

Field	Description
Model	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 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.

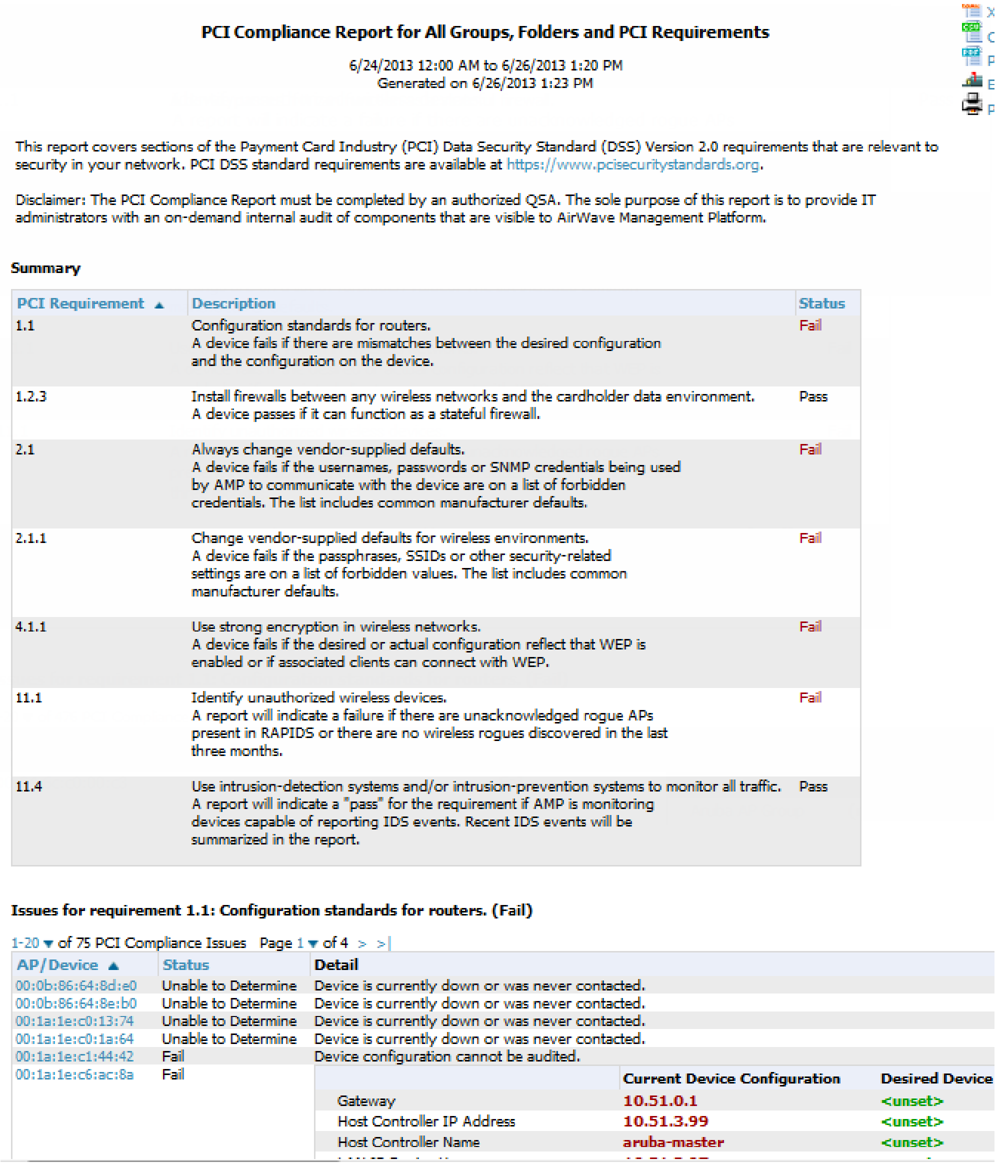
Using the PCI Compliance Report

AMP supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI Compliance Report displays current PCI configurations and status as enabled on the network. Verify that AMP is enabled to monitor compliance with PCI requirements, as described in the "Enabling or Disabling PCI Auditing" on page 73.

In addition to citing simple pass or fail status with regard to each PCI requirement, AMP introduces very detailed diagnostic information to recommend the specific action or actions required to achieve Pass status, when sufficient information is available. Refer to the "Auditing PCI Compliance on the Network" on page 71 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.

"PCI Compliance Report Illustration Example" on page 305 illustrates the fields and information in a PCI Compliance Report.

Figure 191 *PCI Compliance Report Illustration Example*



PCI Compliance Report for All Groups, Folders and PCI Requirements

6/24/2013 12:00 AM to 6/26/2013 1:20 PM
Generated on 6/26/2013 1:23 PM

This report covers sections of the Payment Card Industry (PCI) Data Security Standard (DSS) Version 2.0 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 that are visible to AirWave Management Platform.

Summary

PCI Requirement ▲	Description	Status
1.1	Configuration standards for routers. A device fails if there are mismatches between the desired configuration and the configuration on the device.	Fail
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 AMP to communicate with the device are on a list of forbidden credentials. The list includes common manufacturer defaults.	Fail
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.	Fail
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 clients can connect with WEP.	Fail
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.	Fail
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 AMP is monitoring devices capable of reporting IDS events. Recent IDS events will be summarized in the report.	Pass

Issues for requirement 1.1: Configuration standards for routers. (Fail)

1-20 ▾ of 75 PCI Compliance Issues Page 1 ▾ of 4 > >|

AP/Device ▲	Status	Detail
00:0b:86:64:8d:e0	Unable to Determine	Device is currently down or was never contacted.
00:0b:86:64:8e:b0	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:13:74	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c0:1a:64	Unable to Determine	Device is currently down or was never contacted.
00:1a:1e:c1:44:42	Fail	Device configuration cannot be audited.
00:1a:1e:c6:ac:8a	Fail	

	Current Device Configuration	Desired Device
Gateway	10.51.0.1	<unset>
Host Controller IP Address	10.51.3.99	<unset>
Host Controller Name	aruba-master	<unset>

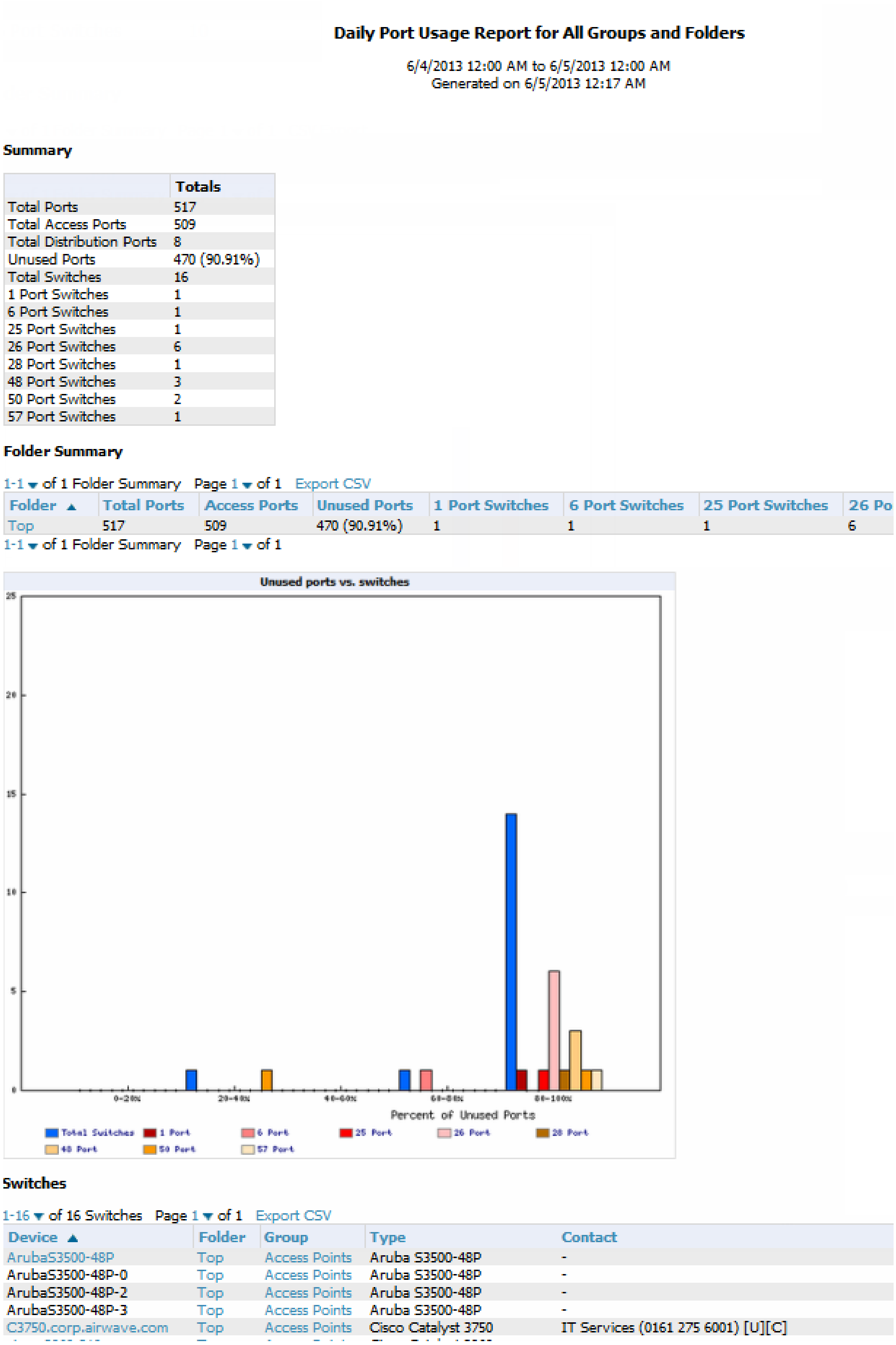
Using the Port Usage Report

You can generate a wide array of port usage statistics from the Port Usage Report including each of the following:

- List of all the switches and ports in your network by folder
- List of unused ports
- List of access and distribution ports
- Histogram displaying unused ports vs. unused switches by type (access or distribution)
- List of most used switches
- List of most used ports

A sample of the types of information used to generate in a Port Usage Report appears in Figure 192. The fields that display for the switching summary information are described in Table 147.

Figure 192 *Port Usage Report Detail Page (partial view)*



Daily Port Usage Report for All Groups and Folders

6/4/2013 12:00 AM to 6/5/2013 12:00 AM
Generated on 6/5/2013 12:17 AM

Summary

	Totals
Total Ports	517
Total Access Ports	509
Total Distribution Ports	8
Unused Ports	470 (90.91%)
Total Switches	16
1 Port Switches	1
6 Port Switches	1
25 Port Switches	1
26 Port Switches	6
28 Port Switches	1
48 Port Switches	3
50 Port Switches	2
57 Port Switches	1

Folder Summary

1-1 ▾ of 1 Folder Summary Page 1 ▾ of 1 Export CSV

Folder ▲	Total Ports	Access Ports	Unused Ports	1 Port Switches	6 Port Switches	25 Port Switches	26 Po
Top	517	509	470 (90.91%)	1	1	1	6

1-1 ▾ of 1 Folder Summary Page 1 ▾ of 1

Switches

1-16 ▾ of 16 Switches Page 1 ▾ of 1 Export CSV

Device ▲	Folder	Group	Type	Contact
ArubaS3500-48P	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-0	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-2	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-3	Top	Access Points	Aruba S3500-48P	-
C3750.corp.airwave.com	Top	Access Points	Cisco Catalyst 3750	IT Services (0161 275 6001) [U][C]

Table 147: *Switches table fields*

Field	Description
Device	The name of the device
Folder/Group	The folder and group that this devices belongs to

Table 147: *Switches table fields (Continued)*

Field	Description
Type	The switch type
Contact	Displays the contact info for the switch, if available
Location	Displays the location information for the switch, if available
Total Ports	The total number of ports available on the device
Access Ports	The total number of Access Ports available on the device
Unused Ports (%)	The percentage of the ports on the device that are unused
Traffic In	The amount of incoming traffic on the device
Traffic Out	The amount of outbound traffic on the device

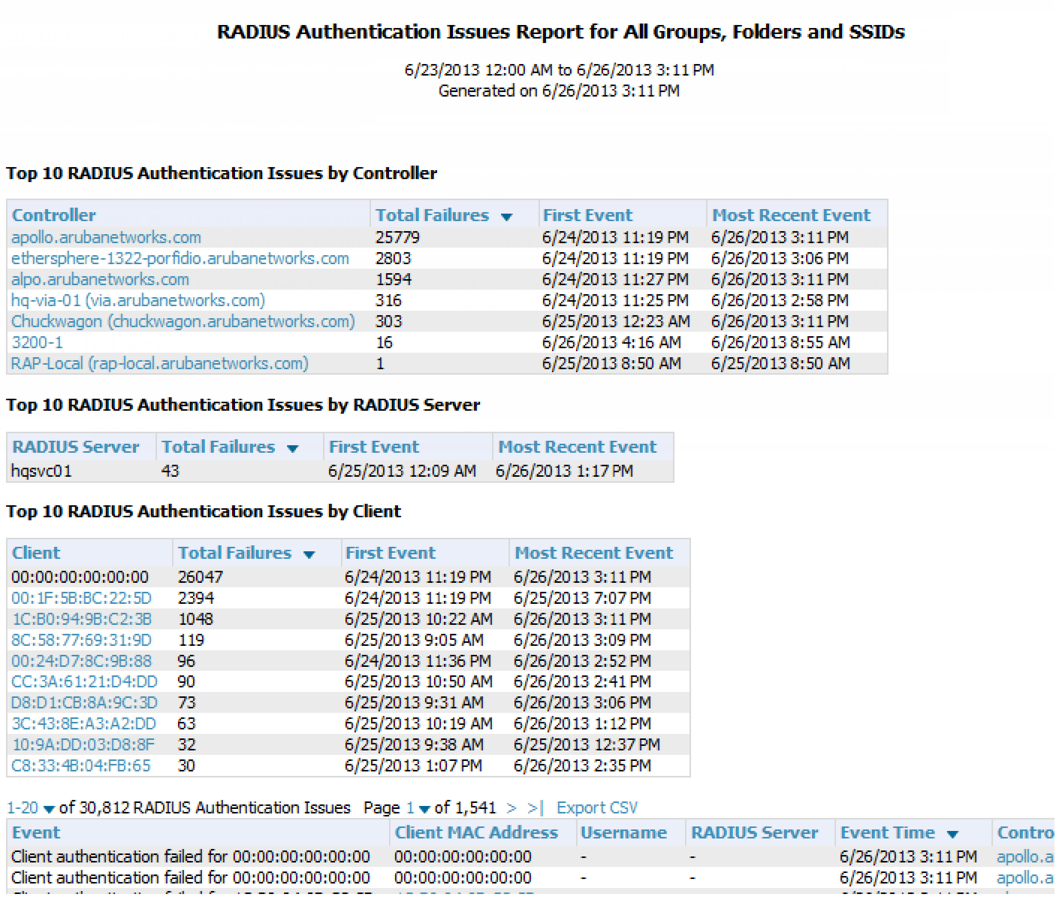
Using the RADIUS Authentication Issues Report

The RADIUS Authentication Issues Report contains issues that may appear with controllers, RADIUS servers, and users. For each of these, the report includes the number of total failures and the first and most recent event times. By default, this report will show up to 10 RADIUS authentication items in each table. You can change this value to anything other than 0.

You can filter this report based on BSSID. You can also specify to view detailed information about RADIUS failures. If this is selected, then an additional table display summarizing authentication issues for each authentication event.

Figure 193 illustrates the fields and information in the RADIUS Authentication Issues Report.

Figure 193 *RADIUS Authentication Issues detail page illustration (partial view(*



RADIUS Authentication Issues Report for All Groups, Folders and SSIDs

6/23/2013 12:00 AM to 6/26/2013 3:11 PM
Generated on 6/26/2013 3:11 PM

Top 10 RADIUS Authentication Issues by Controller

Controller	Total Failures ▼	First Event	Most Recent Event
apollo.arubanetworks.com	25779	6/24/2013 11:19 PM	6/26/2013 3:11 PM
ethersphere-1322-porfidio.arubanetworks.com	2803	6/24/2013 11:19 PM	6/26/2013 3:06 PM
alpo.arubanetworks.com	1594	6/24/2013 11:27 PM	6/26/2013 3:11 PM
hq-via-01 (via.arubanetworks.com)	316	6/24/2013 11:25 PM	6/26/2013 2:58 PM
Chuckwagon (chuckwagon.arubanetworks.com)	303	6/25/2013 12:23 AM	6/26/2013 3:11 PM
3200-1	16	6/26/2013 4:16 AM	6/26/2013 8:55 AM
RAP-Local (rap-local.arubanetworks.com)	1	6/25/2013 8:50 AM	6/25/2013 8:50 AM

Top 10 RADIUS Authentication Issues by RADIUS Server

RADIUS Server	Total Failures ▼	First Event	Most Recent Event
hqsvc01	43	6/25/2013 12:09 AM	6/26/2013 1:17 PM

Top 10 RADIUS Authentication Issues by Client

Client	Total Failures ▼	First Event	Most Recent Event
00:00:00:00:00:00	26047	6/24/2013 11:19 PM	6/26/2013 3:11 PM
00:1F:5B:BC:22:5D	2394	6/24/2013 11:19 PM	6/25/2013 7:07 PM
1C:B0:94:9B:C2:3B	1048	6/25/2013 10:22 AM	6/26/2013 3:11 PM
8C:58:77:69:31:9D	119	6/25/2013 9:05 AM	6/26/2013 3:09 PM
00:24:D7:8C:9B:88	96	6/24/2013 11:36 PM	6/26/2013 2:52 PM
CC:3A:61:21:D4:DD	90	6/25/2013 10:50 AM	6/26/2013 2:41 PM
D8:D1:CB:8A:9C:3D	73	6/25/2013 9:31 AM	6/26/2013 3:06 PM
3C:43:8E:A3:A2:DD	63	6/25/2013 10:19 AM	6/26/2013 1:12 PM
10:9A:DD:03:D8:8F	32	6/25/2013 9:38 AM	6/25/2013 12:37 PM
C8:33:4B:04:FB:65	30	6/25/2013 1:07 PM	6/26/2013 2:35 PM

1-20 ▼ of 30,812 RADIUS Authentication Issues Page 1 ▼ of 1,541 > >| Export CSV

Event	Client MAC Address	Username	RADIUS Server	Event Time ▼	Contro
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a

Using the RF Health Report

The RF Health Report tracks the top AP radio issues by noise, MAC/Phy errors, channel changes, transmit power changes, mode changes, and interfering devices (the last two apply only if there are ARM events). This report assists in pinpointing the most problematic devices on your network, and lists the top devices by problem type.

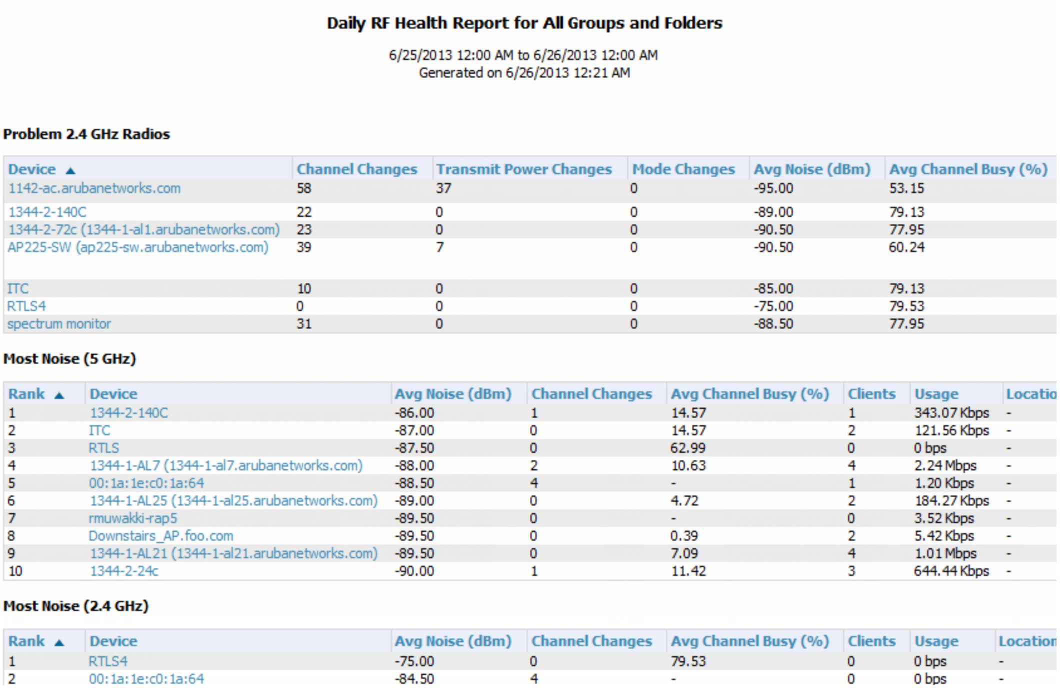
Problematic APs are displayed in two separate lists Problem Radios lists, grouped by radio frequency. A device will make it into the list if it violates two or more thresholds. (For more on the thresholds that indicate problems, refer to "Evaluating Radio Statistics for an AP" on page 145.)

Other lists grouped by radio frequency include Most Noise, Most Interfering, Most/Least Utilized by Channel Usage, Most MAC/Phy Errors, Most Channel Changes, Most Transmit Power Changes, Clients with Least Goodput, Clients with Least Speed, and Radios with Least Goodput.

If an RF Health Report has not been generated before, you can create it by following the instructions on the "Defining Reports" on page 274 section of this chapter.

Figure 194 illustrates a sample RF Health Report.

Figure 194 *Daily RF Health Report Page Illustration (partial view)*



Daily RF Health Report for All Groups and Folders

6/25/2013 12:00 AM to 6/26/2013 12:00 AM
Generated on 6/26/2013 12:21 AM

Problem 2.4 GHz Radios

Device ▲	Channel Changes	Transmit Power Changes	Mode Changes	Avg Noise (dBm)	Avg Channel Busy (%)
1142-ac.arubanetworks.com	58	37	0	-95.00	53.15
1344-2-140C	22	0	0	-89.00	79.13
1344-2-72c (1344-1-al1.arubanetworks.com)	23	0	0	-90.50	77.95
AP225-SW (ap225-sw.arubanetworks.com)	39	7	0	-90.50	60.24
ITC	10	0	0	-85.00	79.13
RTLS4	0	0	0	-75.00	79.53
spectrum monitor	31	0	0	-88.50	77.95

Most Noise (5 GHz)

Rank ▲	Device	Avg Noise (dBm)	Channel Changes	Avg Channel Busy (%)	Clients	Usage	Locatio
1	1344-2-140C	-86.00	1	14.57	1	343.07 Kbps	-
2	ITC	-87.00	0	14.57	2	121.56 Kbps	-
3	RTLS	-87.50	0	62.99	0	0 bps	-
4	1344-1-AL7 (1344-1-al7.arubanetworks.com)	-88.00	2	10.63	4	2.24 Mbps	-
5	00:1a:1e:c0:1a:64	-88.50	4	-	1	1.20 Kbps	-
6	1344-1-AL25 (1344-1-al25.arubanetworks.com)	-89.00	0	4.72	2	184.27 Kbps	-
7	rmuwakki-rap5	-89.50	0	-	0	3.52 Kbps	-
8	Downstairs_AP.foo.com	-89.50	0	0.39	2	5.42 Kbps	-
9	1344-1-AL21 (1344-1-al21.arubanetworks.com)	-89.50	0	7.09	4	1.01 Mbps	-
10	1344-2-24c	-90.00	1	11.42	3	644.44 Kbps	-

Most Noise (2.4 GHz)

Rank ▲	Device	Avg Noise (dBm)	Channel Changes	Avg Channel Busy (%)	Clients	Usage	Location
1	RTLS4	-75.00	0	79.53	0	0 bps	-
2	00:1a:1e:c0:1a:64	-84.50	4	-	0	0 bps	-

All tables in RF Health indicate the rank, device type, number of users, bandwidth, location, controller, folder, and group, and all are sorted according to rank. Selecting a value under the **Device** column in any table will take you to the **APs/Devices > Monitor > Radio Statistics** page for the band indicated in the table title (5 GHz or 2.4 GHz).

- Every list contains Rank, Device (name, not type), Channel Changes, Average Noise, Average Channel Utilization, Clients, Usage, Location, Controller name, Speed, Goodput, Folder, and Group.
- The third column in the list (after Device) will be the column the list is sorted by.
- If that column would otherwise be in the list (Channel Changes), it does not show up in the list where it would otherwise.
- Note that sometimes the sorted column is not one of those common ones, such as the Interfering Devices section.

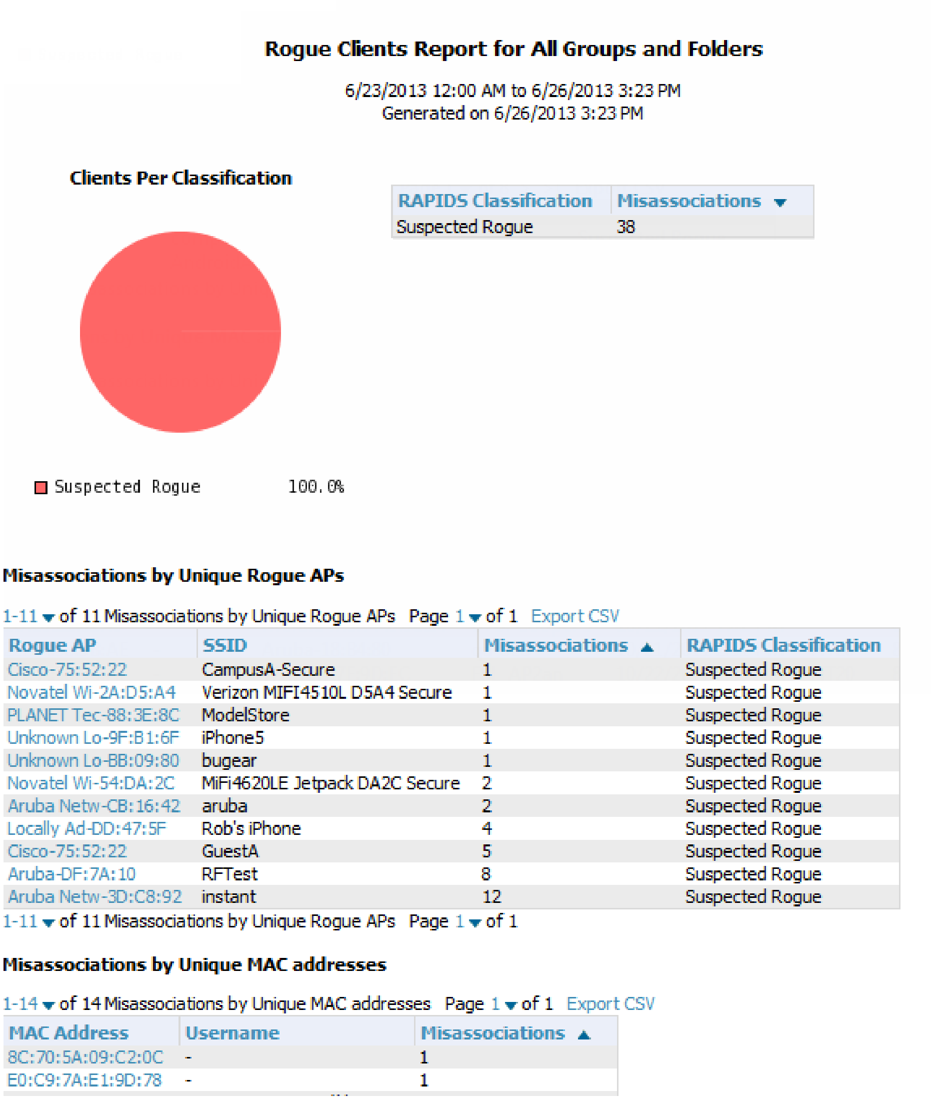
AMP limits data storage to 183 days (approximately six months) per radio. If you create an RF Health Report with a date range longer than 183 days, it will only include Channel Changes, Transmit Power Changes, Average Utilization, Mac/Phy Errors and Average Noise based on whatever part of the report intersects the last 183 days. This differs from most reports because other data (like bandwidth and users) will max out at 425 days, and AMP validates reports so you can only run them over a 366-day duration.

Using the Rogue Clients Report

The Rogue Clients report tracks the number of valid users that connected to rogues in the specified time frame, and can be filtered by rogue classification. You can specify to include ad-hoc devices can be included and detailed information about the clients.

By default, the minimum RAPIDS classification is Suspected Rogue, and the maximum is Contained Rogue.

Figure 195 *Rogue Clients Report Page Illustration*



Rogue Clients Report for All Groups and Folders

6/23/2013 12:00 AM to 6/26/2013 3:23 PM
Generated on 6/26/2013 3:23 PM

Clients Per Classification

RAPIDS Classification	Misassociations ▼
Suspected Rogue	38

🟥 Suspected Rogue 100.0%

Misassociations by Unique Rogue APs

1-11 ▼ of 11 Misassociations by Unique Rogue APs Page 1 ▼ of 1 Export CSV

Rogue AP	SSID	Misassociations ▲	RAPIDS Classification
Cisco-75:52:22	CampusA-Secure	1	Suspected Rogue
Novatel Wi-2A:D5:A4	Verizon MIFI4510L D5A4 Secure	1	Suspected Rogue
PLANET Tec-88:3E:8C	ModelStore	1	Suspected Rogue
Unknown Lo-9F:B1:6F	iPhone5	1	Suspected Rogue
Unknown Lo-BB:09:80	bugear	1	Suspected Rogue
Novatel Wi-54:DA:2C	MiFi4620LE Jetpack DA2C Secure	2	Suspected Rogue
Aruba Netw-CB:16:42	aruba	2	Suspected Rogue
Locally Ad-DD:47:5F	Rob's iPhone	4	Suspected Rogue
Cisco-75:52:22	GuestA	5	Suspected Rogue
Aruba-DF:7A:10	RFTest	8	Suspected Rogue
Aruba Netw-3D:C8:92	instant	12	Suspected Rogue

1-11 ▼ of 11 Misassociations by Unique Rogue APs Page 1 ▼ of 1

Misassociations by Unique MAC addresses

1-14 ▼ of 14 Misassociations by Unique MAC addresses Page 1 ▼ of 1 Export CSV

MAC Address	Username	Misassociations ▲
8C:70:5A:09:C2:0C	-	1
E0:C9:7A:E1:9D:78	-	1

Table 148: *Rogue Clients fields and descriptions*

Field	Description
Misassociations by Unique Rogue APs	For each Rogue AP, this table includes the SSID of the device, the number of misassociations, and the RAPIDS Classification.
Misassociations by Unique MAC addresses	This table shows details about MAC address that are being registered as rogue clients, including the username (if available) and the number of misassociations.
Rogue Clients	
MAC Address	The MAC address of the rogue client.
Username	The username of the rogue client, if available
SSID	The SSID of the rogue client

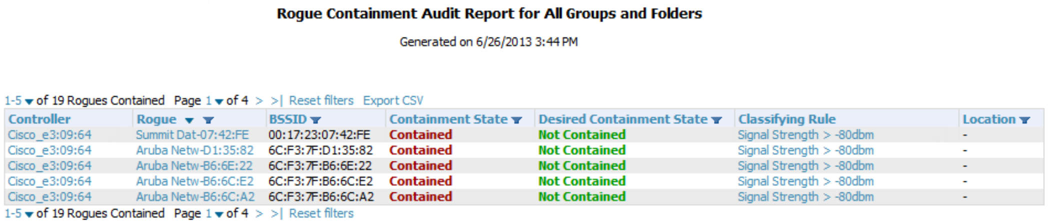
Table 148: *Rogue Clients fields and descriptions (Continued)*

Field	Description
First Heard	The date/time when the rogue client was first detected on the network.
Ch BW	The channel bandwidth of the client, if avaialble
Radio Mode	The radio mode that the rogue client is using.
SNR	The signal-to-noise ratio, if available.
Channel	The channel of the rogue device, if available.
Loation	The location of the rogue client, if available
RAPIDS Classification	The current classification of the rogue client.

Using the Rogue Containment Audit Report

The Rogue Containment Audit report that lets you know if any containment is failing. Figure 196 illustrates the output of this report, and Table 149 describes the fields available in the report.

Figure 196 *Rogue Containment Audit Report Page Illustration*



Rogue Containment Audit Report for All Groups and Folders

Generated on 6/26/2013 3:44 PM

1-5 ▾ of 19 Rogues Contained Page 1 ▾ of 4 > >| Reset filters Export CSV

Controller	Rogue ▾ ▼	BSSID ▼	Containment State ▼	Desired Containment State ▼	Classifying Rule	Location ▼
Cisco_e3:09:64	Summit Dat-07:42:FE	00:17:23:07:42:FE	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-D1:35:82	6C:F3:7F:D1:35:82	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6E:22	6C:F3:7F:B6:6E:22	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:E2	6C:F3:7F:B6:6C:E2	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:A2	6C:F3:7F:B6:6C:A2	Contained	Not Contained	Signal Strength > -80dbm	-

1-5 ▾ of 19 Rogues Contained Page 1 ▾ of 4 > >| Reset filters

Table 149: *Rogue Containment Report fields and descriptions*

Field	Description
Controller	The controller attempted to contain the Rogue
Rogue	The name of the rogue device
BSSID	The BSSID of the rogue device
Containment State	Shows the current containment state
Desired Containment State	Shows the desired containment state
Classifying Rule	Shows the rule that the controller followed when determining the status of the rogue
Location	The location of the rogue device, if available

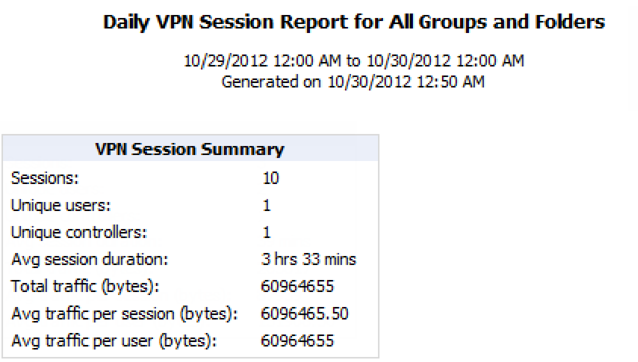
Using the VPN Session Report

The **VPN Session Report** extensively itemizes VPN activity by session. This report can be filtered to show devices or clients/users, including those that match a certain search criteria. You can also specify device types to include in the report. Finally, you can specify to include summary or detailed information about VPN sessions and users.

The output can display in chart and table form.

In list and chart form, this report tracks and display session information that can include any or all of the following:

Figure 197 *VPN Session Report Summary View*



Daily VPN Session Report for All Groups and Folders

10/29/2012 12:00 AM to 10/30/2012 12:00 AM
Generated on 10/30/2012 12:50 AM

VPN Session Summary	
Sessions:	10
Unique users:	1
Unique controllers:	1
Avg session duration:	3 hrs 33 mins
Total traffic (bytes):	60964655
Avg traffic per session (bytes):	6096465.50
Avg traffic per user (bytes):	60964655

Table 150 describes the fields that display when "Summarize Report By" list information is selected for the following tables:

- VPN Session Data by VPN Type
- VPN Session Data by Controller
- VPN Session Data by AOS Device Type
- VPN Session Data by HTTP Fingerprint
- VPN Session Data by VLAN

Table 150: *VPN Session Data tables for each session type*

Field	Description
Name	The VPN Type, Controller, AOS Device Type, HTTP Fingerprint, or VLAN
Users	The number of users that logged a VPN session over the specified time range for each VPN Type, Controller, AOS Device Type, HTTP Fingerprint, and VLAN
Total Duration	The amount of time that each type was connected during the specified time range.
Total Data	The amount of data in MB each type was collected during the specified time range.

Emailing and Exporting Reports

This section describes three ways that you can distribute reports in AMP:

- "Emailing Reports in General Email Applications" on page 313
- "Emailing Reports to Smarthost" on page 313
- "Exporting Reports to XML, CSV, or PDF" on page 313

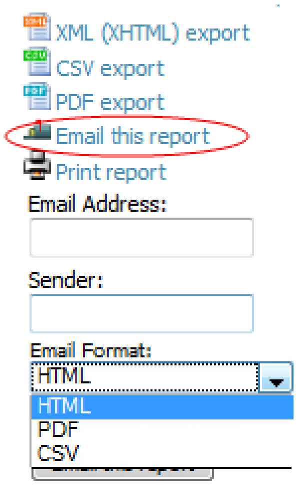
Emailing Reports in General Email Applications

Perform these steps to set up email distribution of reports in AMP

All reports contain a link to export the report to an XML, CSV, or PDF file. Reports can also be e-mailed in either HTML, PDF, or CSV format.

Select **Email This Report** to email the report, and then specify the email addresses, separated by commas, to which reports are sent along with the sender address. Finally, specify whether the report should be sent in HTML or PDF format.

Figure 198 *Email this report*



Email Address:

Sender:

Email Format: HTML

Additional information about email-based report generation is described in "Defining Reports" on page 274 and in "Emailing Reports to Smarthost" on page 313.

Emailing Reports to Smarthost

AMP uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If AMP sits behind a firewall, which prevents it from sending email directly to the specified recipient, use the following procedure to forward email to a smarthost.

1. Add the following line to `/etc/postfix/main.cf`:

   ```
   relayhost = [mail.example.com]
   ```

   Where: `mail.example.com` is the IP address or hostname of your smarthost.
2. Run **`service postfix restart`**
3. Send a test message to an email address.

   ```
   Mail -v xxx@xxx.com
   Subject: test mail
   .
   CC:
   ```
4. Press **Enter**.
5. Check the mail log to ensure mail was sent by running this command:

   ```
   tail -f /var/log/maillog
   ```

Exporting Reports to XML, CSV, or PDF

AMP allows you to export individual reports in XML (xhtml), CSV, or PDF. 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 can be read by an HTML browser or opened in Excel. The CSV files can be opened in any text editor. The PDF files can be viewed using any reader.

NOTE

Support for graphics and links is included when exporting. This method of exporting also prevents **Missing File C:\filename.css** error messages.

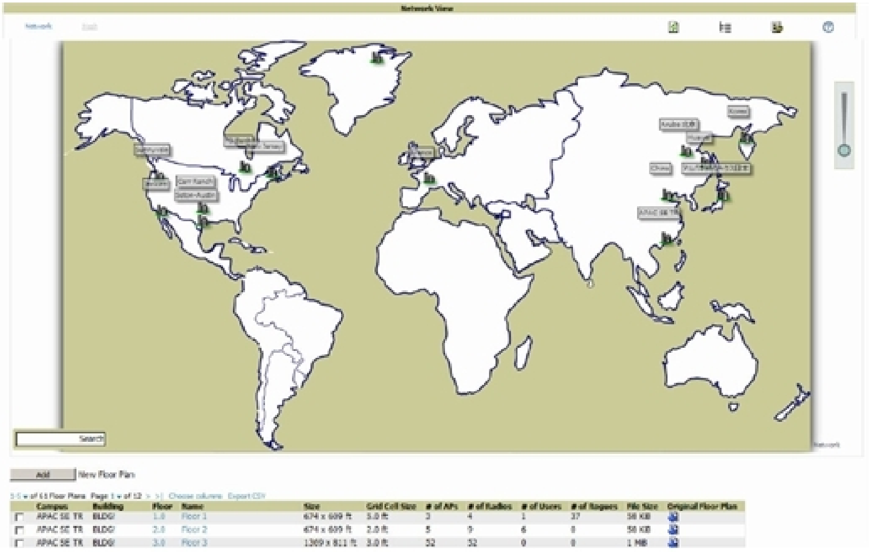
Chapter 9
Using VisualRF

This chapter contains information about VisualRF and includes the following topics:

The VisualRF module provides a real-time picture of the actual radio environment of your wireless network and the ability to plan the wireless coverage of new sites. To understand what is happening on your wireless network, you need to know where your users and devices are located, and you need to monitor the RF environment in those areas. VisualRF puts this information at your fingertips through integrated mapping and location data.

VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. Moreover, VisualRF does not require dedicated RF sensors or a costly additional location appliance - all the necessary information is gathered from your existing wireless access points and controllers.

Figure 199 *Example VisualRF Page Showing all networks*



1-5 ▾ of 61 Floor Plans Page 1 ▾ of 12 > >| Choose columns Export CSV

	Campus	Building	Floor	Name	Size	Grid Cell Size	# of APs	# of Radios	# of Users	# of Rogues	File Size	Original Floor Plan
□	APAC SE TR	BLDG!	1.0	Floor 1	674 x 609 ft	5.0 ft	3	4	1	37	58 KB	
□	APAC SE TR	BLDG!	2.0	Floor 2	674 x 609 ft	2.0 ft	5	9	6	0	58 KB	
□	APAC SE TR	BLDG!	3.0	Floor 3	1309 x 811 ft	3.0 ft	52	52	0	0	1 MB	

Features

- Mesh monitoring page specially for viewing Aruba AirMesh devices. VisualRF automatically renders Mesh APs based on GPS coordinates.
- Floor plan upload wizard enables direct importation of JPG/JPEG, GIF, PNG, PDF (single page only) and CAD files for floor plans. **NOTE**: PDF floor plans must be generated from a source file. Other PDFs, such as those scanned from a printer, will not import properly. Similarly, CAD files must be generated by AutoCAD.
- Batch upload wizard enables batch uploads of multiple CAD files with corresponding walls, and access points.
- Accurate calculation of the location of all client devices (laptops, RFID Tags, PDAs, Phones) using RF data from your existing APs and controllers. Increased accuracy of device placement can be achieved with periodic site surveys.
- Graphical navigation allows your Help Desk to view floor plans simply by clicking on the appropriate campus, building, or floor.
- Tree view allows you to navigate to a specific campus, building, or floor via a tree navigation.
- Heatmaps depict the strength of RF coverage in each location.
- Speed (data rate) view which depicts the highest possible speed at every location on a floor plan.
- Built into AMP or onscreen display of alerts and error conditions. For instance, an AP icon will display in red when a critical alert is active or when usage conditions exceed pre-defined thresholds.
- Location playback viewer which allows visual tracking of up to 24 hours of location history.
- Dynamically recalculates path loss and device locations based on real-time data from your wireless LAN, for increased location accuracy.
- Calibrates RF data from multiple vendors' APs (and across different product lines from the same vendor) for accurate display even in multi-vendor and multi-architecture environments. Refer to the *Supported Infrastructure Devices* document for a list of vendors and supported devices.
- Full planning capabilities based on speed or signal requirements.

Useful Terms

- **AP-to-AP Signal (Neighbor)** - Some APs/Controllers have the ability to report the signal strength of APs that they hear. AMP uses these signal strength readings to dynamically attenuate floor plans to increase the accuracy of client locations and heat maps.
- **Client Surveys** - Client surveys within VisualRF use access points to understand which clients they hear and at what signal strength.
- **dB (Decibels)** - difference/ratio between two signal levels.
- **dBm** - dB as compared to 1 mW. It is a logarithmic measurement (integer) which is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so it is easy to evaluate performance between various vendors.
- **mW** - 1/1000 of a Watt. It is a linear measurement (always positive) generally used to represent transmission.
- **QuickView** - Flash front end for VisualRF, which displays information generated by the back-end service.
- **Rogue Surveys** - Rogue surveys are facilitated by AMC, VisualRF and the client's radio to understand which access points they hear and what signal strength.
- **RSSI (Received Signal Strength Indicator)** - IEEE defines RSSI is a mechanism by which RF energy is to be measured by the circuitry on a wireless NIC (0-255). RSSI is not standard across vendors. Each vendor determines their own RSSI scale/values.
- **Unassociated Client Information** - Some APs/Controllers have the ability to report the signal strength of visible clients that are associated to a radio on a neighboring AP. AMP also uses these signal strength readings to more accurately place these unassociated clients.

- **VisualRF** - The AMP service that calculates location, calculates path loss, and provides floor plan editing capabilities.
- **VisualRF Plan** - Makes the planning portions of VisualRF available in an offline software package that does not require a server. For more information about VisualRF Plan, see "About VisualRF Plan" on page 361.

Starting VisualRF

In order to launch VisualRF, **AMP Setup > General** must specify to display the VisualRF tab, and the VisualRF engine must be switched on in **VisualRF > Setup**. Both of these pages are visible to logged-in administrators only. By default:

- **Display VisualRF** is enabled in **AMP Setup > General**.
- **Enable VisualRF Engine** is disabled in **VisualRF > Setup**.

To enable VisualRF, follow these instructions while logged in as an administrator:

1. Navigate to **VisualRF > Setup**.
2. In the **Server Settings** section, select **Yes** in the **Enable VisualRF Engine** field, and then select **Save**.

Basic QuickView Navigation

The top-level menus of VisualRF are split into two major categories: Network and Mesh, as shown in Figure 200 and Figure 201. Selecting these menus will cause relevant submenus and sections to display below:

Figure 200 *Default VisualRF Top Level Menu - Network View*

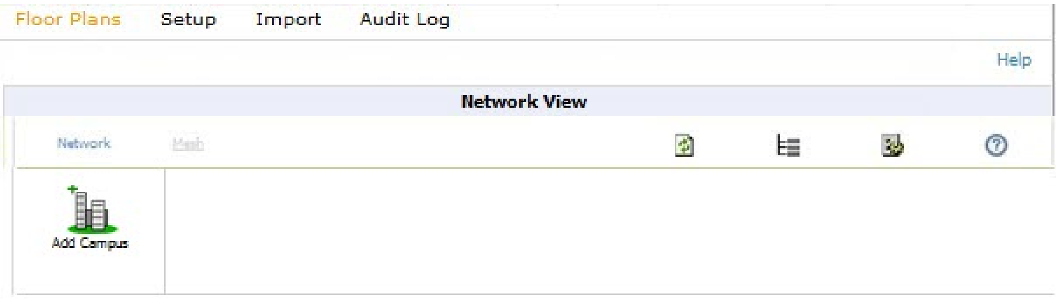


Figure 201 *Default VisualRF Top Level Menu - Mesh View*

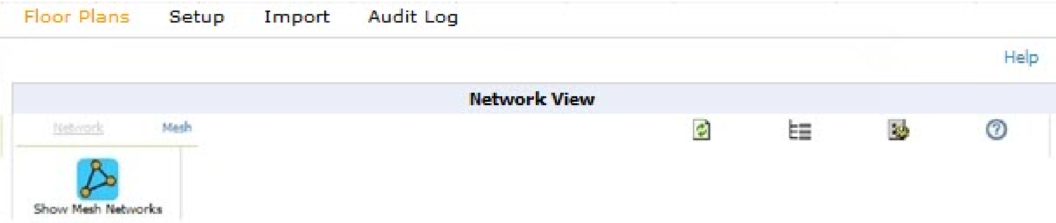


Table 151 describes the top level icons and their functions on VisualRF.

Table 151: *Top Level Icons and Descriptions*

Operation	Icon	Description
Refresh	⟳	Refresh the floor plan to see changes.

Table 151: *Top Level Icons and Descriptions (Continued)*

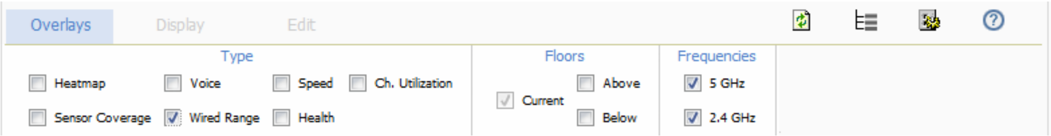
Operation	Icon	Description
Open Site Tree	☰	Display the Network Tree View Window on top of the floor plan.
Preferences	⚙	Configure personal viewing preferences. The Preferences menu allows you to configure user preferences (APs, Clients, overlay types, grid lines, alerts, icon sizes, etc.). See "Configuring QuickView Personal Preferences" on page 328 for more details.
Help	?	Launch the online help. **NOTE:** This User Guide currently contains the most up-to-date help information for the VisualRF interface.

Network View Navigation

When viewing a floor plan in Network View, the top-level menu changes to **Overlays**, **Display**, and **Edit** toggles.

Overlays

Figure 202 *Overlays Menu*



☐ Heatmap ☐ Voice ☐ Speed ☐ Ch. Utilization
☐ Sensor Coverage ☑ Wired Range ☐ Health
☑ Current ☐ Above ☐ Below
☑ 5 GHz ☑ 2.4 GHz

The **Overlays** menu contains three common sections: **Type**, **Floors**, and **Frequencies**. Selecting options in the **Type** section will display additional menu sections that affect the data overlays on the floor plan you are viewing. These additional options appear between the **Type** and **Floors** sections.

Type section

Select one of the following types:

- **Heatmap** - Evaluate coverage based on signal levels by providing the highest dBm (energy level) for all areas of a floor plan. When this option is selected, the **Signal Cutoff** drop-down menu displays. From this drop-down, you can select a common cutoff value or you can specify a custom value.
- **Sensor Coverage** - Provides the farthest area which a sensor can hear. When this option is selected, the **Client Transmit Power** drop-down menu displays. Use this drop-down to select a transmit power value for the overlay.
- **Voice** - Provides color-coded overlay based on number of radios covering each grid cell based on the selected signal cutoff. When this option is selected, the **Signal Cutoff** drop-down menu displays. From this drop-down, you can select a common cutoff value or you can specify a custom value.
- **Wired Range** - Displays the distance an Ethernet cable can be pulled from an IDF. The max range is equal to 300 feet minus 5 percent minus 1.1x the floor height.
- **Speed** - Evaluate coverage based on transmit power of client by providing the highest data rate a user will receive for all areas of a floor plan. When this option is selected, the **Client Transmit Power** drop-down menu displays. Use this drop-down to select a transmit power value for the overlay. Additionally, a **Rates** section appears enabling you to select either 54Mbps, 300Mbps, and 450Mbps.
- **Health** - Determine client health using this overlay. This option is available for controllers running ArubaOS 6.3 or greater.

- **Ch. Utilization** - View how much airtime is used in the environment. Airtime usage is a good measure of how busy an area is. When you select this option, a new **Data Set** menu appears where you can select the Current or Maximum Total, Receive, Transmit, or Interference information to display on the floor plan.

Floors section

The Floors section shows the overlay information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Select all options to see all floors, or one or more of the following options:

- Above - show the data from APs located on the floor above
- Current (default)
- Below - show the data from APs located on the floor below

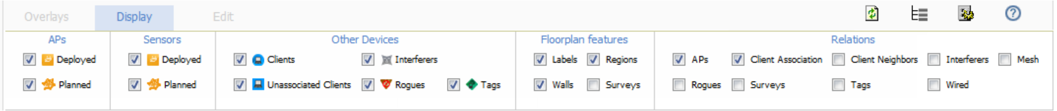
Frequencies section

Select the desired frequency from the following options:

- 5 GHz (lines are always green)
- 2.4 GHz (lines are always blue)

Display Menu

Figure 203 *Display Menu*



APs: ☑ Deployed ☑ Planned

Sensors: ☑ Deployed ☑ Planned

Other Devices: ☑ Clients ☑ Interferers ☑ Unassociated Clients ☑ Rogues ☑ Tags

Floorplan features: ☑ Labels ☑ Regions ☑ Walls ☐ Surveys

Relations: ☑ APs ☑ Client Association ☐ Client Neighbors ☐ Interferers ☐ Mesh ☐ Rogues ☐ Surveys ☐ Tags ☐ Wired

APs Section

- **Deployed** - Toggle deployed APs on or off. Deployed APs on the floor plan are indicated by the icon.
- **Planned** - Toggled planned APs on or off. Planned APs on the floor plan are indicated by the icon.

Sensors Section

- **Deployed** - Toggle deployed sensors on or off. Deployed sensors on the floor plan are indicated by the icon.
- **Planned** - Toggled planned sensors on or off. Planned sensors on the floor plan are indicated by the icon.

Other Devices Section

- **Clients** - Turns the display of wireless users on or off. Clients on the floor plan are indicated by the icon.
- **Unassociated Clients** - Toggle display of unassociated clients. Unassociated clients on the floor plan are indicated by the icon.
- **Interferers** - Toggle interferers on or off. Interferers on the floor plan are indicated by the icon.
- **Rogues** - Toggle rogue devices on or off. Rogues on the floor plan are indicated by the icon.
- **Tags** - Toggle WiFi Tags on or off. Tags on the floor plan are indicated by the icon.

NOTE

Interferer indicators works for AOS customers running 6.1 or newer that have run the mgmt-server type AMP command, and have APs performing Spectrum analysis through hybrid scanning or dedicated spectrum monitors.

Floorplan Features section

- **Walls** - Toggle walls on or off.
- **Labels** - Toggle labels on or off.
- **Regions** - Toggle regions on or off.

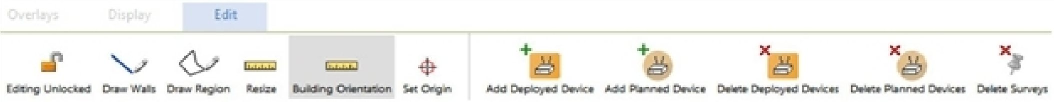
- **Surveys** - Toggle surveys on or off.

Relations section

- **Client Association** - Toggle line between the wireless client and AP of association.
- **Rogues** - Toggle lines between rogue APs and radios which hear the AP.
- **Client Neighbors** - Toggle lines between client and radios that hear the client excluding the radio of association.
- **APs** - Toggle lines between APs which heard each other.
- **Tags** - Toggle lines between WiFi Tags and radios which hear the Tags. For Tags there is no radio of association.
- **Wired** - Toggle lines between APs/sensors and their IDF.
- **Mesh** - Toggle lines between Mesh portals and nodes.
- **Surveys** - Toggle lines between client (x,y) to APs by client during survey.
- **Interferers** - Toggle lines between interferers and the radios that have discovered them. For interferers, there is no radio of association.

Edit Menu

Figure 204 *Edit Menu Options*



Options in the **Edit** menu allow you to add information to the floor plan. Table 152 explains the options in the **Edit** menu:

Table 152: *Edit Icons and Descriptions*

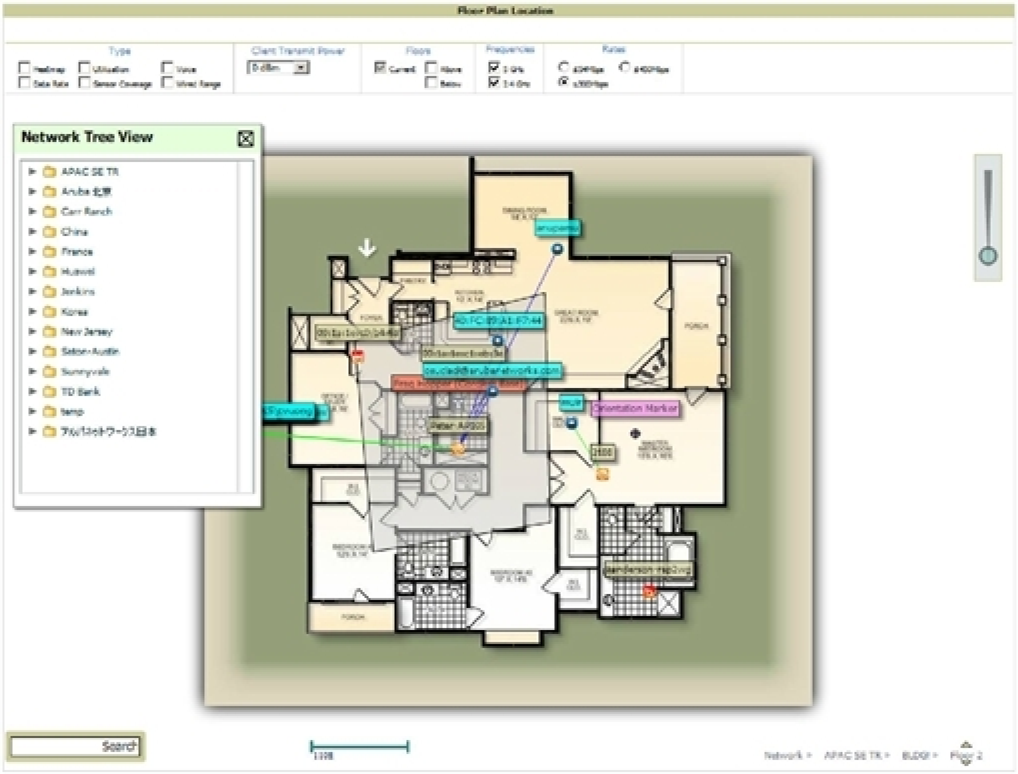
Operation	Description
Edit Locked/Unlocked	Specifies whether to lock or unlock a floor plan for editing.
Draw Walls	Add walls onto a floor plan. Refer to "Adding Exterior Walls" on page 333.
Draw Region	Add a region onto a floor plan. Click once to begin drawing a region, and double click (or Ctrl+click) when you are finished drawing. Specify a Region Type for the new region. Region types include Location Testing, Planning, Wiring Closet, and Location Probability. Refer to "Adding Regions" on page 337 for more information on adding regions.
Resize	Update the scale of the floor plan to properly reflect the accurate dimensions of the floor plan.
Building Orientation	For customers who leverage external APIs, this option enables you to retrieve device location using longitude and latitude coordinates for two GPS points rather than (x,y) coordinates relative to the floor plan image. **NOTE:** This option can be ignored for customers who do not leverage the external APIs.
Set Origin	Set a single origination point per floor. The origination point is used for multi-floor buildings so that VisualRF knows how to vertically align multiple floor plans. This is especially useful in multi-floor buildings for ensuring that multi-floor heatmaps display properly.

Table 152: *Edit Icons and Descriptions (Continued)*

Operation	Description
	A best practice is to select a common location that is identifiable on all floors, such as the corner of the building, a stairwell, elevator shaft, etc., and then place the orientation icon in the same location on all floor plans in the building. Then, for example, if you crop out more white space on the first floor (for a lobby, for example), VisualRF will have enough information to adjust and ensure that the floors are not misaligned.
Add Deployed Device	Provision APs onto a floor plan (APs monitored by AMP).
Add Planned Device	Manually plan APs onto a floor plan (APs not monitored by AMP).
Delete Planned Devices/Delete Deployed Device	Remove all specified devices on a floor plan.
Delete Surveys	Remove all surveys (rogue and client) on floor plan.

Figure 205 shows additional navigation controls when viewing floor plans. In the bottom left corner of the window is the **Search** box. In the top right corner is the zoom control. You can also zoom by using **Ctrl** + your mouse wheel as well as the + and - keys. In the bottom right corner are navigation tools related to network, campus, and building.

Figure 205 *On-Screen Navigation Options*

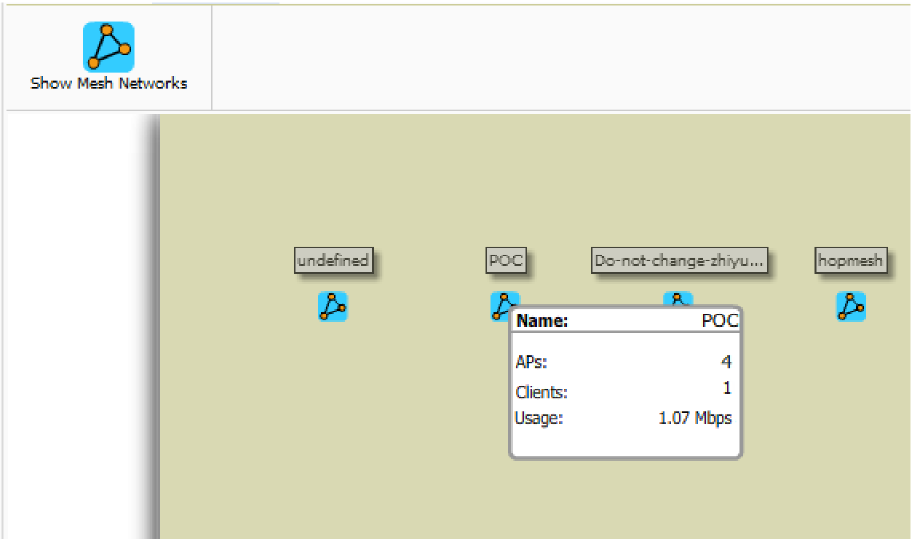


Mesh View Navigation

Mesh view provides a visual Mesh monitoring page specially for viewing Aruba AirMesh devices. It automatically renders Mesh APs based on GPS coordinates.

Figure 206 displays an example of a Mesh Network view with a mouseover above a network icon:

Figure 206 *Viewing Mesh Networks in VisualRF*

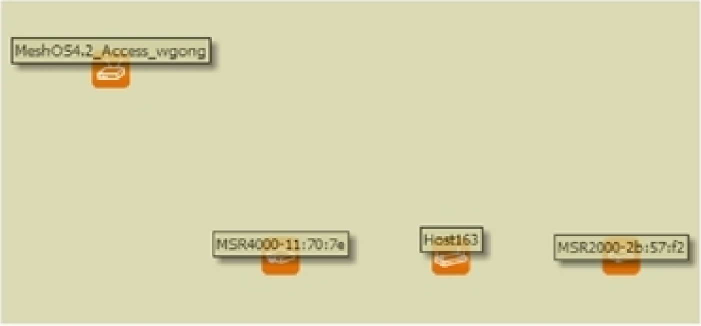


Name:	POC
APs:	4
Clients:	1
Usage:	1.07 Mbps

You can mouse over each mesh network icon to view the number of APs, Clients, and the Usage.

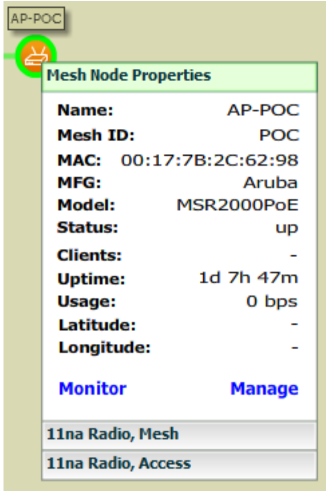
Clicking on an AirMesh network will display the APs with labels:

Figure 207 *APs in a mesh network*



Select an AirMesh AP icon to bring up the popup menu showing the Mesh Node Properties by default. This window shows the node’s name, MeshID, MAC, Manufacturer, and other information. Clicking the blue **Monitor** link inside this window opens the **APs/Devices** > **Monitor** page in a new tab. Clicking the blue **Manage** link inside this window opens the **APs/Devices** > **Manage** page for this AP in a new tab.

Figure 208 *Properties for a Mesh Gateway Illustration*



AP-POC

Mesh Node Properties

Name:	AP-POC
Mesh ID:	POC
MAC:	00:17:7B:2C:62:98
MFG:	Aruba
Model:	MSR2000PoE
Status:	up
Clients:	-
Uptime:	1d 7h 47m
Usage:	0 bps
Latitude:	-
Longitude:	-

For radio-level status information on an AirMesh device in your network, select the menus in the AP's popup window for each radio (**11na Radio**, **Access**; **11na Radio, Mesh**; and so forth).

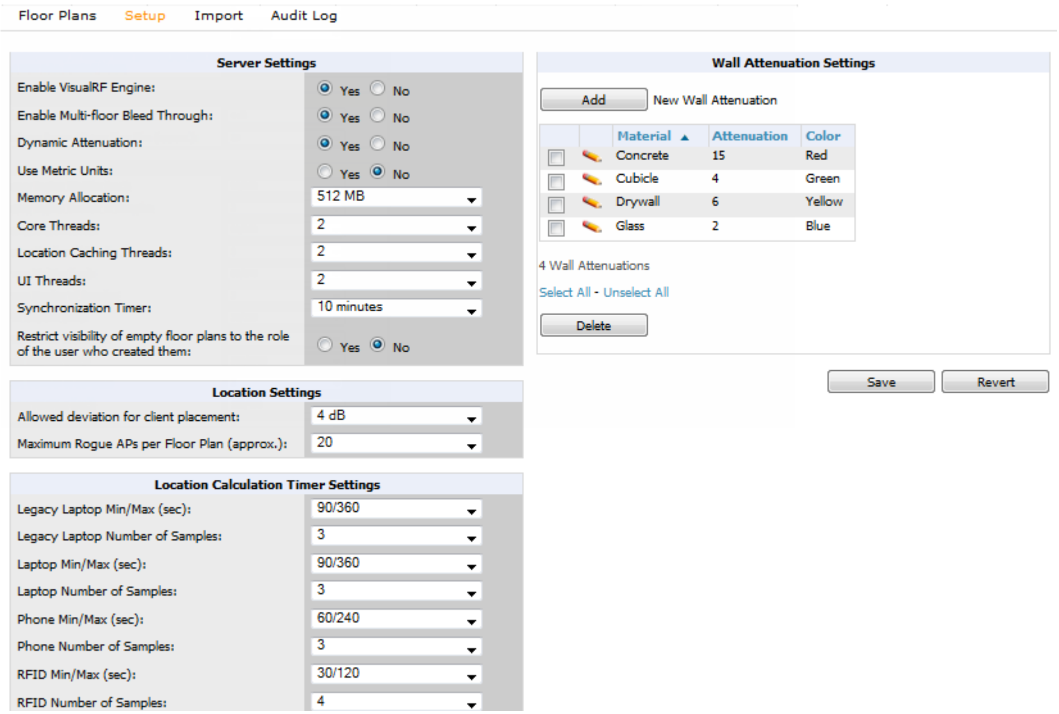
Using the Settings in the VisualRF > Setup Page

The **VisualRF** > **Setup** page, illustrated in Figure 209, configures advanced settings for VisualRF. Please reconfigure these settings very carefully because these settings can impact your server's performance as well as your location accuracy.

NOTE

Selecting **Save** will cause VisualRF to restart, disrupting or delaying the usability. This delay can last anywhere from a minute to upwards of 30 minutes, depending on the size of the VisualRF database.

Figure 209 *The VisualRF > Setup Page (partial view)*



Server Settings

Enable VisualRF Engine:	● Yes ○ No
Enable Multi-floor Bleed Through:	● Yes ○ No
Dynamic Attenuation:	● Yes ○ No
Use Metric Units:	○ Yes ● No
Memory Allocation:	512 MB
Core Threads:	2
Location Caching Threads:	2
UI Threads:	2
Synchronization Timer:	10 minutes
Restrict visibility of empty floor plans to the role of the user who created them:	○ Yes ● No

Location Settings

Allowed deviation for client placement:	4 dB
Maximum Rogue APs per Floor Plan (approx.):	20

Location Calculation Timer Settings

Legacy Laptop Min/Max (sec):	90/360
Legacy Laptop Number of Samples:	3
Laptop Min/Max (sec):	90/360
Laptop Number of Samples:	3
Phone Min/Max (sec):	60/240
Phone Number of Samples:	3
RFID Min/Max (sec):	30/120
RFID Number of Samples:	4

Wall Attenuation Settings

	Material ▲	Attenuation	Color
□	Concrete	15	Red
□	Cubicle	4	Green
□	Drywall	6	Yellow
□	Glass	2	Blue

4 Wall Attenuations

Server Settings

To enable VisualRF and tune memory and performance, navigate to the **Server Settings** section on this page. The settings in this section are detailed in Table 153.

Table 153: *Server Settings Section of the VisualRF > Setup Page*

Setting	Default	Description
Enable VisualRF Engine	No	Enables or disables the VisualRF engine. This setting must be enabled to use VisualRF. If you do not have a license for VisualRF, this page will not appear.
Enable Multi-floor Bleed-Through	Yes	Enables or disables calculating the impact APs on floors above and below the currently viewed floor in the Quick View.
Dynamic Attenuation	Yes	Incorporate AP to AP readings as well as site survey information and dynamically recalculate the path loss of each radio to every grid cell on the floor plan, increasing coverage and location accuracy.
Use Metric Units	No	Instructs the VisualRF engine to display all units of measurements in metric
Memory Allocation	512 MB	The amount of memory dedicate to VisualRF. It is not dynamically allocated and all the memory is consumed upon starting the service. Be sure to check the memory and swap utilization in the **Systems > Performance** page before making any changes. The exact amount of memory used per floor plan will vary heavily based on the size, number of devices and number of grid cells on the floor plan. ● 25 floors or less 512 MB ● 25 to 50 floors 768 MB ● 50 to 75 floors 1 GB ● 75 to 100 floors 1.5 GB ● 100 to 200 floors 3 GB ● 200 to 300 floors 5 GB (64-bit only) ● Above 300 8 GB (64-bit only) **NOTE:** If you see Out of Memory errors in the httpd/error_log on the **System > Status** page, you should increase memory allocation.
Core Threads	1x number of cores	Number of threads that calculate path loss for each floor. These threads also regenerate a floor's RF properties when new APs, walls, or regions are added to a floor plan.
Location Caching Threads	1x number of cores	Number of threads that calculate the location of all clients associated with access points on this floor plan.
UI Threads	1x number of cores	Number of threads that service the users accessing QuickView, as well as AMP-to-VisualRF communication. **NOTE**: If users experience timeout errors while using QuickView, allocate additional UI Threads.
Synchronization Timer	15 minutes	This timer indicates how often VisualRF will synchronize with the APs within AMP. This synchronization includes checking the Up/Down status and parsing the XML.
Restrict visibility of empty floor plans to the role of the user who created them	No	When enabled, only the creator can view an empty floor plan.

Location Settings

To tune location accuracy, go to the **Location Settings** section on this page as described in Table 154:

Table 154: *Location Settings Section in VisualRF > Setup*

Setting	Default	Description
Allowed deviation for client placement	4 dB	When VisualRF locates a client or rogue it utilizes signal metrics from all the APs that hear the client or rogue device. VisualRF builds a fingerprint location for all clients with similar transmit-power capability. All subsequent clients that fall within the deviation is placed on the same location fingerprint or *x, y* coordinates. **Example:** AP1 hears Client1 at -72, and AP2 hears Client 1 at -64. VisualRF calculates the client's location to be at coordinates 100, 200. Client2 is heard by AP1 at -71 and AP2 at -65. VisualRF will use the average of the difference in signals (AP1 -72 and -71) to see if the client matches a pre-calculated location fingerprint. 1 + 1 (differences in signals) / 2 (# of APs) = 1 which falls within the deviation of 2, hence the client would be located at 100,200.
Maximum Rogue APs per Floor Plan	20	Sets the maximum number of rogues AMP will place on a Floor. Use this filter in combination with the **RAPIDS Export Threshold** configured on the **RAPIDS > Setup** page to intelligently control the number of rogue devices displayed per floor. **NOTE:** Increasing this value can increase the load on the server and the clutter on the screen.

Location Calculation Timer Settings

To tune the frequency for calculating device locations within the VisualRF UI, navigate to the **Location Calculation Timer Settings** section. The available settings are described in Table 155:

Table 155: *Location Calculation Timer Settings Section of VisualRF > Setup*

Setting	Default	Description
Legacy Laptop Min/Max (sec)	90/360	This timer determines how often to calculate the location for legacy laptop devices. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 90 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 360 seconds) and then recalculate.
Legacy Laptop Number of Samples	3	See definition above.
Laptop Min/Max (sec)	90/360	This timer determines how often to calculate the location for laptop (non-legacy) devices. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 90 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the

Table 155: *Location Calculation Timer Settings Section of VisualRF > Setup (Continued)*

Setting	Default	Description
		number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 360 seconds) and then recalculate.
Laptop Number of Samples	3	See definition above.
Phone Min/Max (sec)	60/240	This timer determines how often to calculate the location of phones. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 60 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 240 seconds) and then recalculate.
Phone Number of Samples	3	See definition above.
RFID Min/Max (sec)	30/120	This timer determines how often to calculate the location of RFIDs (such as devices with tag readers for tracking). Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 30 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 4 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 120 seconds) and then recalculate.
RFID Number of Samples	4	See definition above.
Scale Min/Max (sec)	500/2000	
Scale Number of Samples	3	
Printer Min/Max (sec)	120/480	This timer determines how often to calculate the location of printers. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 120 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 480 seconds) and then recalculate.

Table 155: *Location Calculation Timer Settings Section of VisualRF > Setup (Continued)*

Setting	Default	Description
Printer Number of Samples	3	See definition above.
Rogue Min/Max (sec)	500/2000	This timer determines how often to calculate the location of rogues. Taken with the data samples the calculation acts as follows: ● After the minimum timer (default is 500 seconds), check to see if the number of data samples received from all APs that hear this client are greater than or equal to the number of samples setting for legacy laptop devices (default of 3 data samples). ● If so (**Yes** to question above), then recalculate the client device's location based on the samples received. ● If not (**No** to the question above), then wait until the number of sample setting is met before recalculating. If the number of samples is never met, wait until the maximum timer (default is 2000 seconds) and then recalculate.
Rogue Number of Samples	3	See definition above.
Default Min/Max (sec)	90/360	
Default Number of Samples	3	

Attenuation Settings

Attenuation settings describe type and dB settings for walls within a floor plan.

To edit the wall settings and select a color for wall types within the VisualRF UI, navigate to the **Wall Attenuation Settings** section on the **VisualRF** > **Setup** page, and select the pencil icon next to the setting that you want to edit. The VisualRF default attenuation values and dB values are described in Table 156.

NOTE

All of these values are global variables that cannot be overridden for individual floor plans. VisualRF uses these values to calculate path loss and client locations. Walls within VisualRF are interpreted as pure dB loss without adjusting for wall thickness.

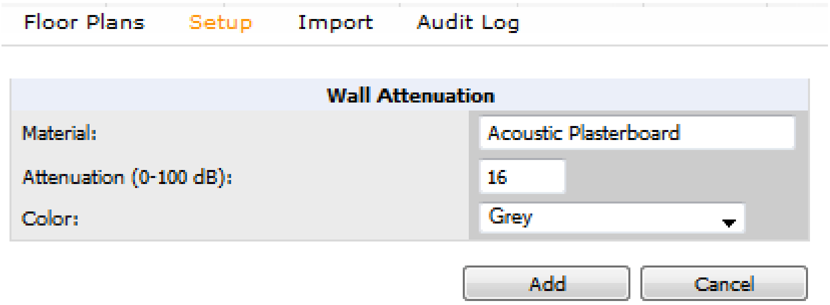
Table 156: *Wall Attenuation Settings in VisualRF > Setup*

Setting	Default dB	Description
Concrete Attenuation (dB)	15	Specifies the attenuation for any concrete walls drawn in VisualRF.
Cubicle Attenuation (dB)	4	Specifies the attenuation for any cubicle walls drawn in VisualRF.
Drywall Attenuation (dB)	6	Specifies the attenuation for any drywall walls drawn in VisualRF.
Glass Attenuation (dB)	6	Specifies the attenuation for any glass walls that are drawn in VisualRF.

Adding a New Attenuation

In some cases, it may be necessary to create a special attenuation setting. Click on the **Add** button to specify a new wall attenuation.

Figure 210 *Add a New Wall Attenuation*



Wall Attenuation

Material: Acoustic Plasterboard

Attenuation (0-100 dB): 16

Color: Grey

Update the fields as described in Table 157. Click the **Add** button on the form when you are finished.

Table 157: *New Wall Attenuation*

Setting	Description
Material	Specify the type of material for the new wall.
Attenuation (0-100 dB)	Specify the attenuation decibel value.
Color	Select a color for the new wall.

VisualRF Resource Utilization

When tuning the VisualRF server, use the default settings as recommended. If you do change any of these settings, change one at a time and see how the system performs. Each time you restart VisualRF, you will notice a delay before returning to normal processing. This delay can last anywhere from a minute to upwards of 30 minutes, depending on the size of the VisualRF database.

If you use the ‘top’ command to check on VisualRF resource utilization, ensure you use the ‘1’ and ‘H’ flags to show cores and threads. Remember ‘top’ also takes 1-2 minutes to normalize and provide accurate data.

NOTE

It is normal for VisualRF to consume 20% of each core with a combination of threads. It will utilize excess CPU cycles on all cores when required.

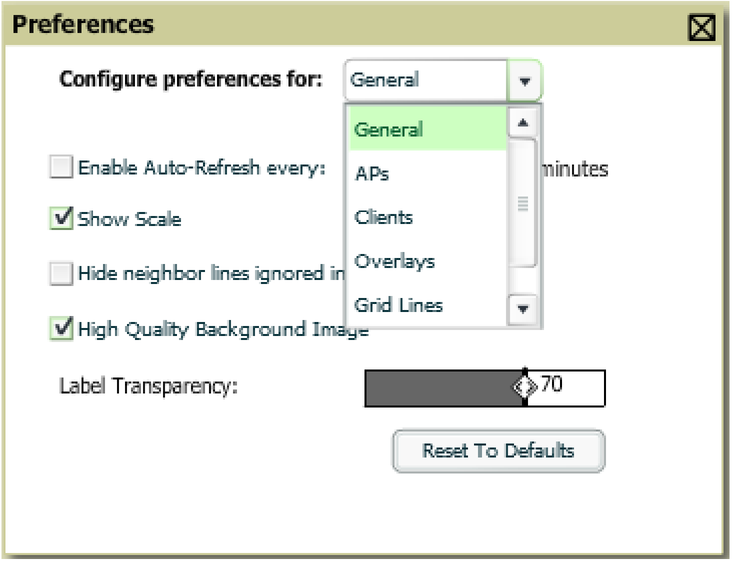
Configuring QuickView Personal Preferences

To configure your personal preferences in QuickView, select the **Preferences** icon on the **VisualRF** > **Floor Plans** page and choose from the options that follow. These preferences are stored in the database, so they are retained across browsers and machines.

General

Select from the **Configure Preferences for** drop-down menu, as shown in Figure 211.

Figure 211 *QuickView Preferences Page Illustration (General preferences selected)*



Preferences

Configure preferences for: General

□ Enable Auto-Refresh every: minutes

☑ Show Scale

□ Hide neighbor lines ignored in

☑ High Quality Background Image

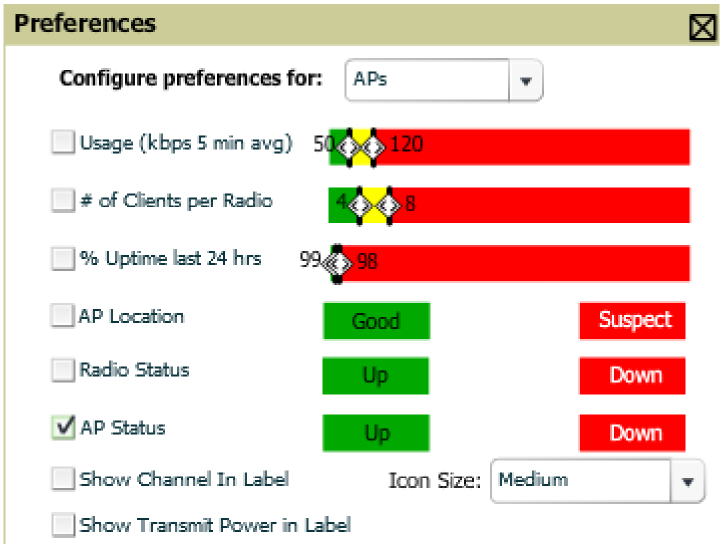
Label Transparency: 70

- Enable auto-refresh toggle. If enabled, specify the Refresh Interval in
- Show Scale
- Hide neighbor lines ignored in location calculation
- High Quality Background Image - you can disable to increase rendering speed
- Label Transparency - specify the transparency level for labels in the floor plan
- Reset to Defaults - launches a dialog box asking you to verify whether to reset all preferences to the default values. Select **Yes** to reset all preferences or **Cancel** to leave preferences as configured.

APs

Select from the **Configure Preferences for** drop-down menu:

Figure 212 *QuickView Preferences Page Illustration (APs preferences selected)*



Preferences

Configure preferences for: APs

□ Usage (kbps 5 min avg) 50 120

□ # of Clients per Radio 4 8

□ % Uptime last 24 hrs 99 98

□ AP Location Good Suspect

□ Radio Status Up Down

☑ AP Status Up Down

□ Show Channel In Label Icon Size: Medium

□ Show Transmit Power in Label

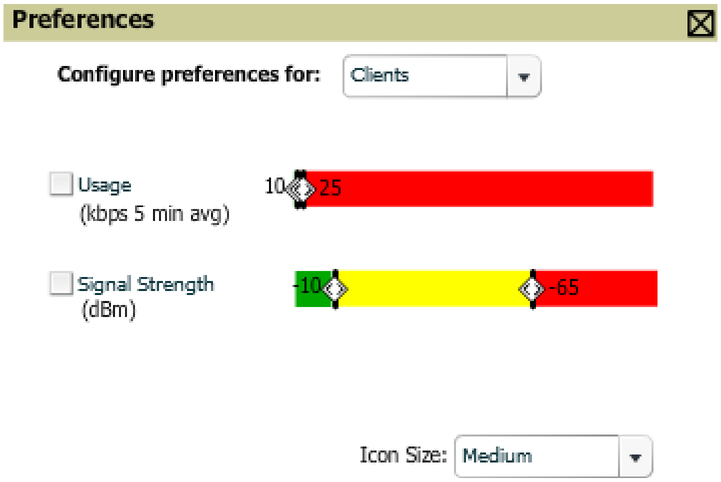
- Usage - select the kbps threshold for normal (green), high (yellow), and excessive (red)

- # of Clients per Radio - select the number of number of clients per radio for normal (green), high (yellow), and excessive (red)
- % of Uptime for the last 24 hours for normal (green) and excessive (red)
- AP Location - specify whether to display green for a good location or red for a suspect location within a floor plan
- Radio Status - specify whether to display red or green depending on the status of the radios within the AP
- AP Status - specify whether to display red or green in relation to up/down status of AP
- Icon Size - select the size of the AP icon display on the floor plan
- Show Channel in Label - view the channel info within the AP label
- Show Transmit Power in Label - view transmit power within the AP label

Clients

Select from the **Configure Preferences for** drop-down menu.

Figure 213 *QuickView Preferences Page Illustration (Clients preferences selected)*



Preferences

Configure preferences for: Clients

□ Usage (kbps 5 min avg) 10 25

□ Signal Strength (dBm) -10 -65

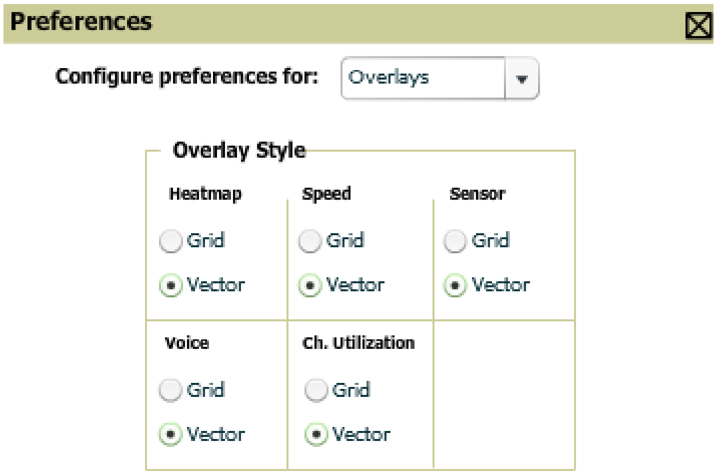
Icon Size: Medium

- Usage - select the kbps threshold for normal (green), high (yellow), and excessive (red).
- Signal Strength - select the dBm client threshold between excellent and poor
- Icon Size - select the size of the client device icon display on the floor plan

Overlays

Select from the **Configuration Preferences for** drop down to change the display type for Heatmap, Speed, Sensor, Voice, and Channel Utilization.

Figure 214 *QuickView Preferences Page Illustration (Overlays preferences selected)*



Preferences ☒

Configure preferences for: Overlays

Overlay Style

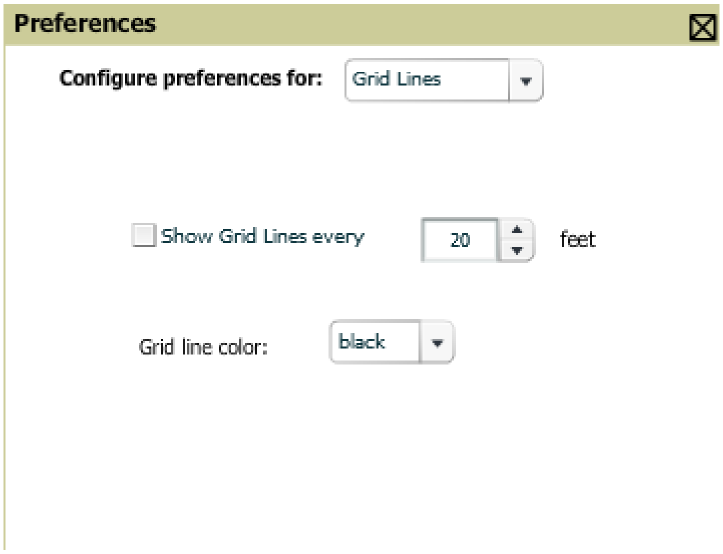
Heatmap	Speed	Sensor
○ Grid ● Vector	○ Grid ● Vector	○ Grid ● Vector
Voice	**Ch. Utilization**	
○ Grid ● Vector	○ Grid ● Vector	

- Grid - non vector overlay
- Vector - provides a smoother overlay with mouse-over capabilities

Grid Lines

Select from the **Configuration Preferences for** drop down to toggle grid lines on or off.

Figure 215 *QuickView Preferences Page Illustration (Grid Lines preferences selected)*



Preferences ☒

Configure preferences for: Grid Lines

□ Show Grid Lines every 20 feet

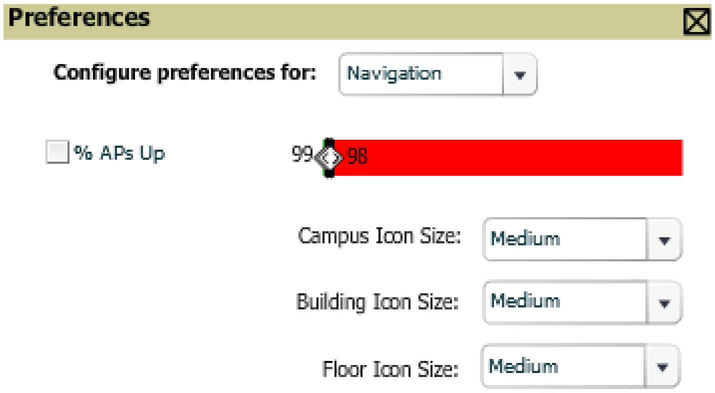
Grid line color: black

- Show Grid Lines - if enabled, specify the number of feet between grid lines
- Color of grid lines - select a color for grid lines

Navigation

Select from the **Configure Preferences for** drop-down menu (campus and buildings).

Figure 216 *QuickView Preferences Page Illustration (Navigation preferences selected)*



Preferences

Configure preferences for: Navigation

□ % APs Up 99 98

Campus Icon Size: Medium

Building Icon Size: Medium

Floor Icon Size: Medium

- % of APs Up for the last 24 hours for normal (green) and excessive (red)
- Icon Size for campus, building, and floor. Specify Tiny, Small, Medium, Large, or Huge icons.

NOTE

The remaining sections in this chapter apply to networks, campuses, buildings, and floor plans that have already been set up in VisualRF. If you do not yet have any of this information in VisualRF for your network, refer to "Planning and Provisioning" on page 346.

Increasing Location Accuracy

The Location Service will use all RF information available to increase location accuracy of clients, tags, and rogue devices. Understanding your infrastructure's inherent capabilities helps you learn the extra effort required to ensure location accuracy.

There are three key elements read from controllers or access points that increase location accuracy:

- Signal strength of a client as heard by the AP of association
- Signal strength of a client as heard by APs other than the AP of association
- Signal strength at which an AP hears other APs.

These factors are detailed further in Table 158:

Table 158: *Elements Read From Controllers to Increase Location Accuracy*

MFG/Model	Client Signal Associated AP	AP-to-AP Signals (Dynamic Attenuation)	Unassociated Client Signal	Rogue AP Signal
Aruba	Yes	Yes	Yes	Yes
Cisco LWAPP	Yes	Yes	Yes	Yes
Cisco IOS	Yes	No	No	With WLSE
Cisco VxWorks	Yes	No	No	No

Table 158: *Elements Read From Controllers to Increase Location Accuracy (Continued)*

MFG/Model	Client Signal Associated AP	AP-to-AP Signals (Dynamic Attenuation)	Unassociated Client Signal	Rogue AP Signal
Trapeze	Yes	No	No	Yes
Meru	No	No	No	Yes
Proxim	Yes	Yes	Yes	Yes
Symbol Auton. AP	Yes	No	No	Yes
Symbol Thin AP	Yes	No	Yes	Yes
Proxim AP-2000	Yes	No	Yes	Yes
Proxim AP-4000	Yes	Yes	Yes	Yes
ProCurve WeSM	Yes	Yes	No	Yes
ProCurve 530	Yes	Yes	Yes	Yes
ProCurve 420	Yes	Yes	No	Yes

AMP provides four main methods to increase accuracy once your access points are deployed:

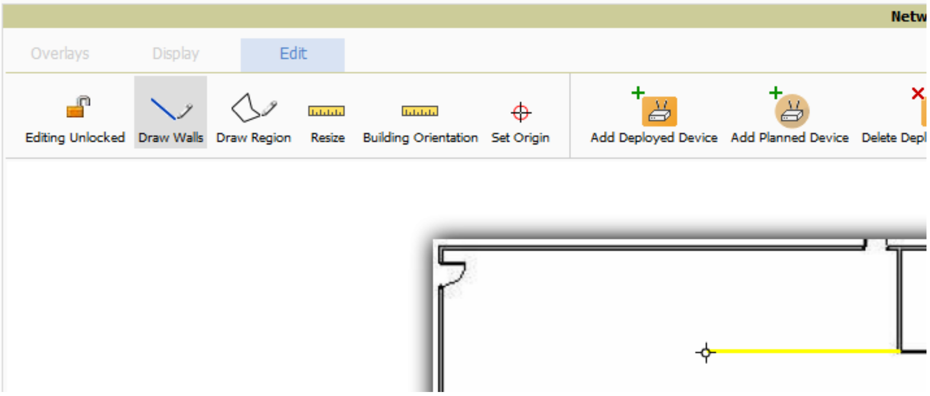
- Adding Exterior Walls - increases location accuracy by reducing the statistical probability of placements outside the office confines. See "Adding Exterior Walls" on page 333.
- Client Training for Stationary Devices - ensures non-mobile clients like desktops or scales will always remain in a defined static location. Statically assigning non-mobile devices reduces the CPU load on your server because VisualRF does not evaluate any signal metrics for this MAC address when associated with an AP on the floor plan. See "Location Training for Stationary Devices" on page 334.
- Remote Client Surveys - provides additional attenuation inputs for corners and low-coverage areas without the burden of actually carrying a laptop to the physical location. See "Adding Client Surveys" on page 335.
- Location Probability Regions - Probability regions will increase or decrease the chances of a device being located within the region. See "Adding Location Probability Regions" on page 337.

Adding Exterior Walls

Because VisualRF utilizes much existing RF information, generally only external walls are required for accurate client locations. VisualRF's Dynamic Attenuation feature uses AP-to-AP information to calculate attenuation for interior areas, negating the need to enter interior walls. If your devices support AP-to-AP information in the table above, you should only draw exterior walls.

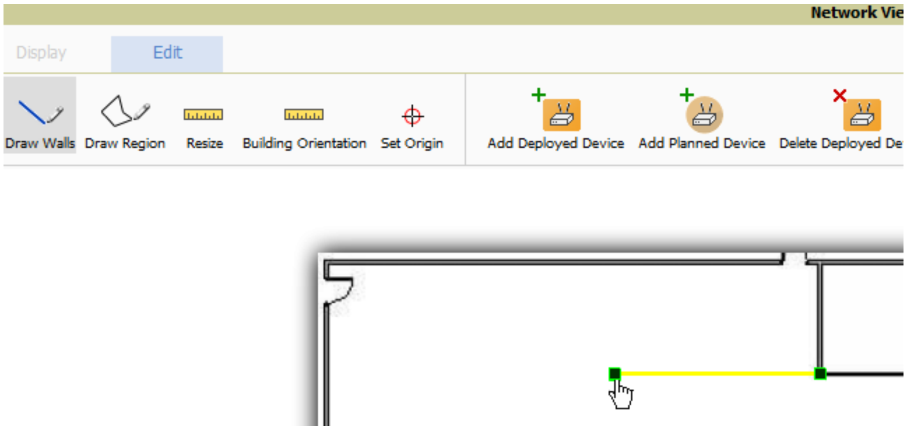
1. Select **Draw Walls** button in the Edit menu.
2. The cursor changes to a crosshair. Use this to draw the wall directly over the floor plan, as shown in Figure 217:

Figure 217 *Drawing a wall*



3. To move or resize the wall, select the **Draw Walls** button in the Edit menu again. The cursor changes to a hand, and the ends of the wall is highlighted. Click and drag the end point handles to change the wall, as shown in Figure 218:

Figure 218 *Moving and resizing an existing wall*



- To change the attenuation of a wall, right-click the wall and select the appropriate building material.
- To delete a wall, select the wall and press the **Delete** key. You can also right-click on a wall and select **Delete This Wall** from the popup menu.

4. Once all walls are provisioned on the floor plan, select **Save** (floppy disk icon above the zoom bar).

NOTE

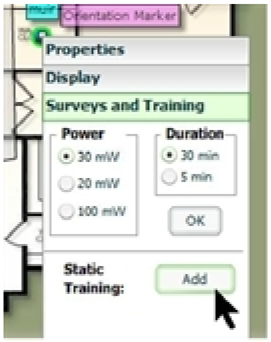
Drawing only outside walls is recommended. If you are seeing inaccurate client locations or heat maps after entering exterior walls, proceed to Client Surveys. If you still experience problems, then you can proceed to adding interior walls.

Location Training for Stationary Devices

QuickView provides the ability to statically assign a permanent *x,y* coordinate to stationary devices like PCs, Scales, and Point-of-Sale terminals. This will reduce the calculation requirements on the VisualRF location service and increase the accuracy of the RF characteristics of individual floor plans.

1. Drag the client device to the proper location.
2. Select the device and a popup menu appears. From that menu, select **Surveys and Training.**
3. Click the **Add** button for Static Training, as shown in Figure 219:

Figure 219 *Surveys and Training menu for a client device*



To remove a statically trained device, select client, and select the Surveys and Training option. Select **Delete** button (which will have replaced the **Add** button) for Static Training.

NOTE

The static locations are automatically saved, so the **Save** icon (floppy disk) will not appear.

Adding Client Surveys

Client surveys provide a method for increasing the accuracy of the attenuation grid by taking real signal samplings from client devices associated with the WLAN.

Key differentiators of AMPs client surveys are:

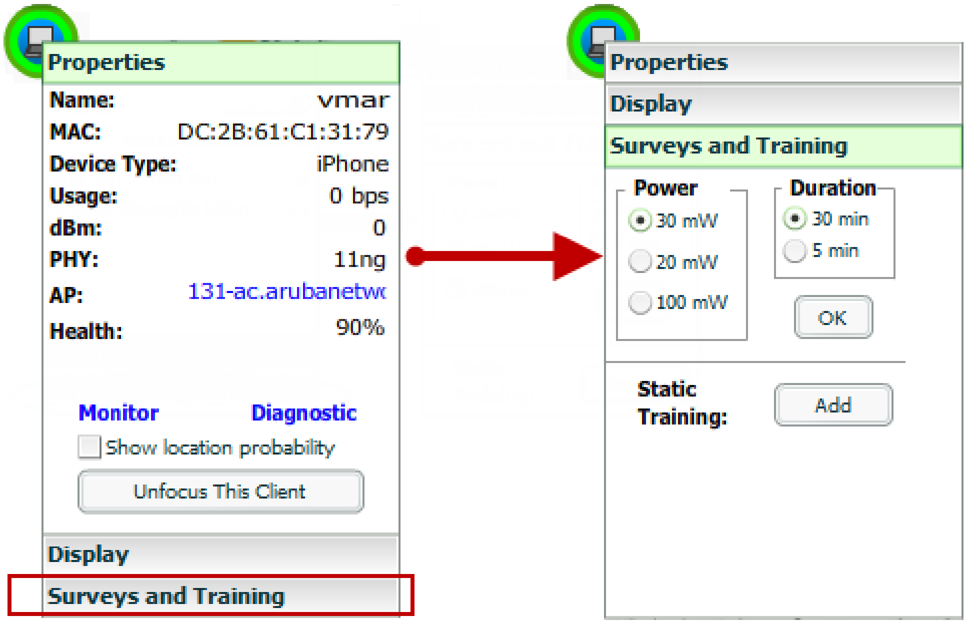
1. They take readings from the access points and not the client.
2. They take numerous samples.

This produces a more accurate representation because signals obtained from the client's card (the signal level at which a client hears the AP) can vary from vendor to vendor. The signal levels at which APs can hear a client are already normalized. Using multiple samples alleviates spikes or troughs that come from using a single sample.

To start a client survey, follow these steps:

1. Drag the client to the proper location.
2. Select the client to see the **Properties** pop-up menu, as shown in Figure 220:

Figure 220 *Client Surveys*



Properties

Name: vmar
MAC: DC:2B:61:C1:31:79
Device Type: iPhone
Usage: 0 bps
dBm: 0
PHY: 11ng
AP: 131-ac.arubanetw
Health: 90%

□ Show location probability

Power
● 30 mW
○ 20 mW
○ 100 mW

Duration
● 30 min
○ 5 min

3. Select the **Surveys and Training** option.
4. Select the appropriate transmit power for the wireless client. Leave the default to **30mW** if you are unsure.
5. Select the **Duration** or the time that you want to sample the client's signal measurements. Longer durations will increase Path Loss accuracy and location accuracy.
6. Select **OK** to begin the survey.

To display survey locations, select the **Display** menu and select **Surveys.** Note the following information about this procedure:

- Ensure the client will remain in the same location for at least the duration of the survey.
- You should delete and resurvey an area or a floor plan after a remodel or significant interior movement.
- Surveys should be conducted during normal business hours to reflect normal RF activity on the floor.
- 11a clients automatically inherit the proper transmit power from the 11g configuration. Example: 30mW Pre-2006 laptops equate to 20mW for 11a clients.
- AMP dynamically assigns a transmit power to every client based on OUI as shown in Table 159. This step increases the accuracy for surveys by allowing an override.

Table 159: *Auto-assigned Client Type and Transmit Power*

Client Type	Transmit Power 11g
Pre-2006 Laptops	30 mW
Post -2006 Laptops	100 mW
SOHO WLAN Cards (D-Link, Net Gear, LINKSYS)	30 mW
RFID Tags	10 mW
PDA	20 mW

Table 159: *Auto-assigned Client Type and Transmit Power (Continued)*

Client Type	Transmit Power 11g
iPhone	20 mW
Desktop	100 mW
Cisco Cards	100 mW

Adding Regions

You can specify regions for areas designated as Wiring Closets and for Location Testing, Location Probability, and Planning.

Adding Location Probability Regions

Location probability regions are optional regions that can be used to increase the accuracy of device location in VisualRF.

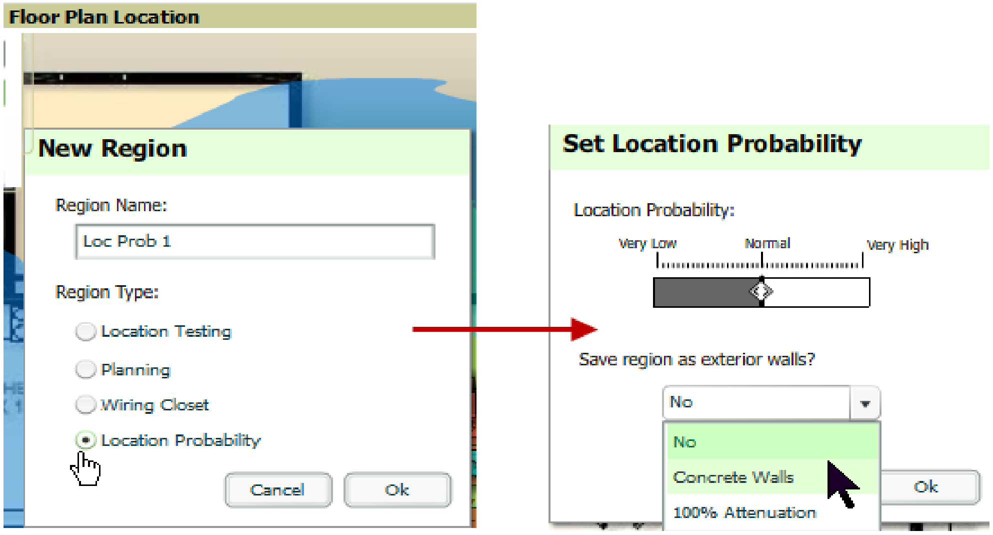
VisualRF calculates device locations based on probability. VisualRF determines the probability of a device being located in every grid cell and places the device where the probability is the highest.

Probability regions will add or remove up to 20% chance from the device location probability. They can be used to push users into regions where they are more likely to be located, like conference rooms and cubical farms, or they can be used to pull users out of regions where they are less likely to be like parking lots and courtyards.

To add a probability region to a floor plan, follow these steps:

1. Select the **Edit** menu and click the **Draw Region** option.
2. Outline the desired probability region. Double click or Ctrl+click to end the outline process.
3. Name the region, select a Region Type of **Location Probability** and select OK.
4. Move the location probability slider to the desired level, as shown on Figure 221. **Very Low** will decrease the probability of a device being placed in that region by 20%. **Very High** will increase the probability of a device being placed in that region by 20%.

Figure 221 *Adding a New Location Probability Region*



Region Name: Loc Prob 1

Region Type: ● Location Probability

Save region as exterior walls? No

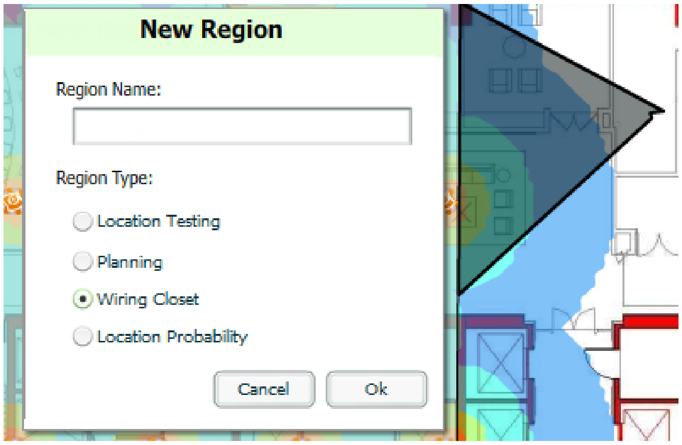
5. Optionally, you can save the location region as the exterior walls. 100% attenuation can be selected to force VisualRF to only place devices inside of the selected region. No device will ever be placed outside of the probability region when 100% attenuation is selected. 100% attenuation is only recommended for tall buildings where it is extremely unlikely that any user is located outside of the building. No heat map or attenuation grid is calculated for devices outside of the 100% attenuation region.

Adding a Wiring Closet

To add a Wiring Closet to VisualRF, follow these steps:

1. In the **Edit** menu, select the **Draw Region** option.
2. Outline the desired region. Double click or press **Ctrl+click** to end the outline process.
3. Name the region, select a Region Type of **Wiring Closet**, and click the **OK** button, as shown in Figure 222.

Figure 222 *Adding a new Wiring Closet Region*



New Region

Region Name:

Region Type:

○ Location Testing

○ Planning

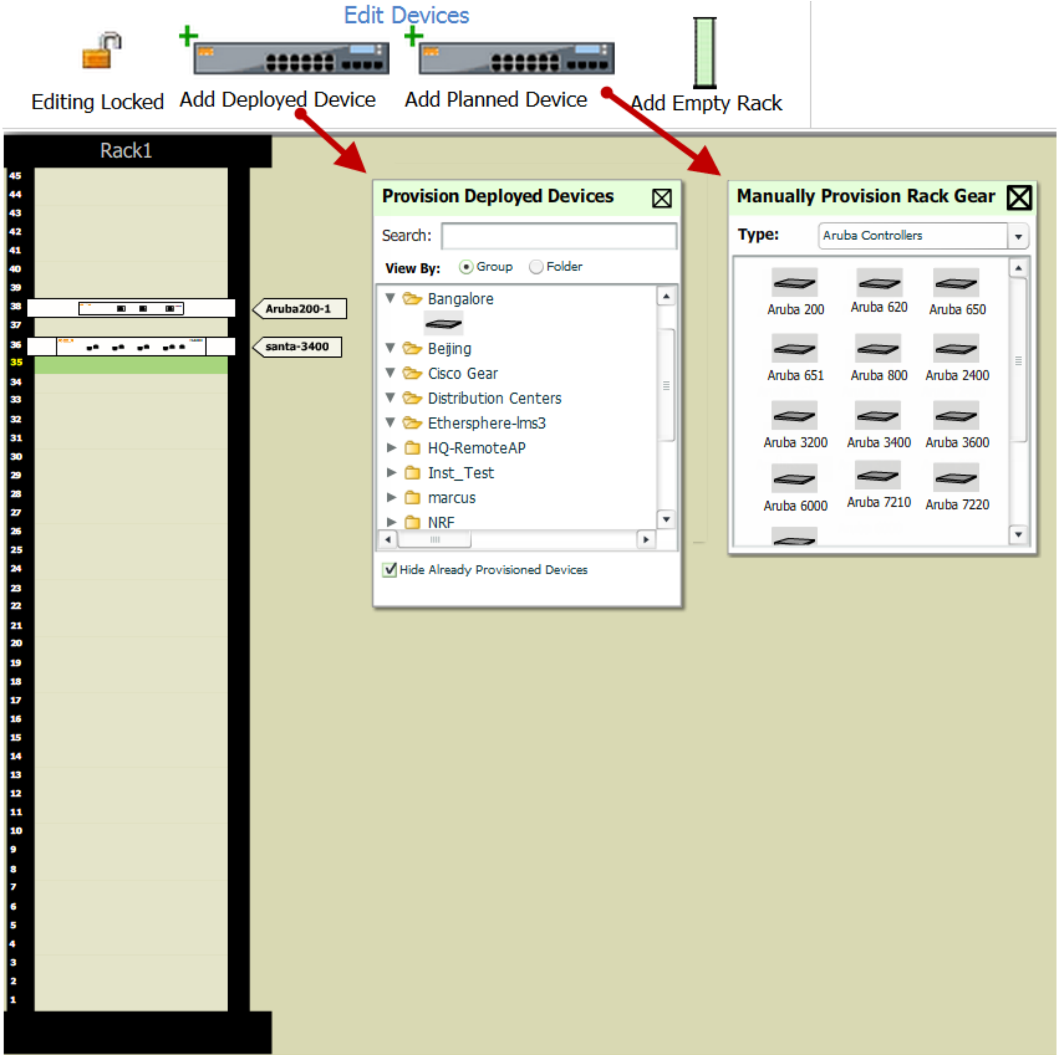
● Wiring Closet

○ Location Probability

Now that the Wiring Closet is defined you will see a green Wiring Closet icon on your floor plan. Double click that icon.

1. Add a rack to the wired closet by selecting the **Add Empty Rack** icon and dragging it to the background.
2. To add a planned device, select the **Add Planned Device** icon to view the **Manually Provision Rack Gear** menu. Select the device type in the **Type** menu, and then find the device you want to add. Drag it into the rack at the appropriate location.
3. To add a wired device that is currently being monitored by AMP, select **Add Deployed Device**.
   a. Locate the device to be added.
   b. Drag the device to the appropriate location in the rack.

Figure 223 *Provisioning Devices*

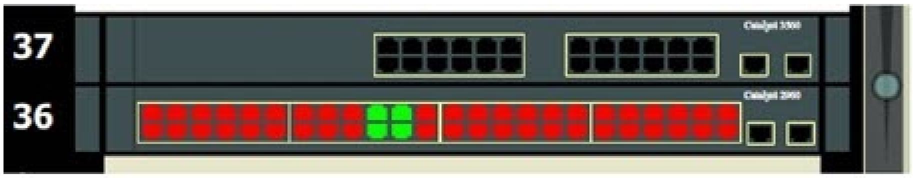


Wired devices that are added to a wired closet are included in any BOM report covering that floor.

Viewing Port Status on Deployed Switches

Deployed switches on a rack will display the port status as red (down) and green (up) interface icons, which corresponds with the operationally up devices on the **APs/Devices** > **Interfaces** list. Planned switches do not display these status indicators in VisualRF.

Figure 224 *Deployed switch showing red and green port status icons*



Fine-Tuning Location Service in VisualRF > Setup

There are several options on the **VisualRF** > **Setup** page which increase client location accuracy. All of these items will increase the processing requirements for the location service and could negatively impact the overall performance of

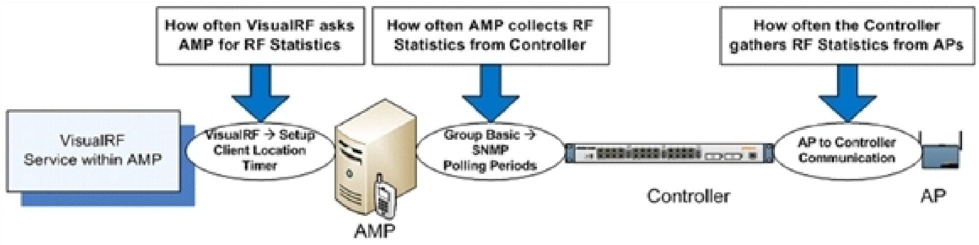
AMP.

- **Grid Size** - decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy. You can right-click on a floor plan within a building view and change this setting.
- **Dynamic Attenuation** - enabling dynamic attenuation (which is on by default) instructs the location service to sample the current RF environment and to dynamically adjust Path Loss.

Configuring Infrastructure

Ensure that the hardware is configured to retrieve the RF information and that it provides this information on a timely basis. There are three unique timing mechanisms which impact location accuracy: how often the infrastructure collects and correlates RF statistics in their MIB, how often the AMP queries those MIB entries, and how often VisualRF service queries AMP for this RF information.

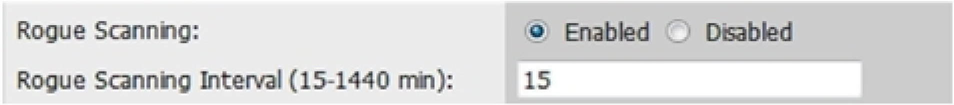
Figure 225 *Timing Factors Impacting Location Accuracy*


How often VisualRF asks AMP for RF Statistics
How often AMP collects RF Statistics from Controller
How often the Controller gathers RF Statistics from APs
VisualRF Service within AMP
VisualRF → Setup Client Location Timer
Group Basic → SNMP Polling Periods
AP to Controller Communication
AMP
Controller
AP

These best practices are recommended when configuring hardware infrastructure:

- For legacy autonomous APs, ensure on the **Group** > **Radio** page that **Rogue Scanning** is enabled and the interval is accurate, as shown in Figure 226:

Figure 226 *Group Rogue Scanning Configuration*



Rogue Scanning: ● Enabled ○ Disabled

Rogue Scanning Interval (15-1440 min): 15

- For thin APs, ensure that the controllers are configured to gather RF information from the thin APs frequently.
- For Cisco LWAPP, navigate to **Groups** > **Cisco WLC Config** page in AMP. Navigate the tree control to the **Wireless** section, and for each PHY navigate to **RRM** > **General** section. Review the values in the **Monitor Intervals** section. These should be configured to a recommended setting of **180** for better accuracy.

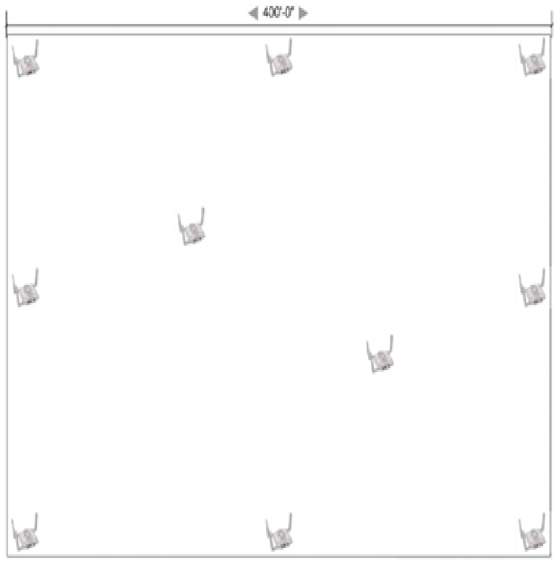
Deploying APs for Client Location Accuracy

Deploying access points for client location accuracy can be different than deploying access points for capacity. Follow these guidelines for best results:

- Ensure that at least 3 radios can hear each client devices at -85 dBm or below
- Ensure that you deploy an access point approximately every 3,500 square feet.
- For square or rectangular floor plans ensure access points are deployed on the exterior walls of each floor with access points in the middle as well.

Refer to Figure 227 for an example.

Figure 227 *Rectangular Floor Plan AP Deployment*



Using QuickView to Assess RF Environments

QuickView has four distinct views or entry points: client view, access point view, floor plan view, and network, campus, and building view.

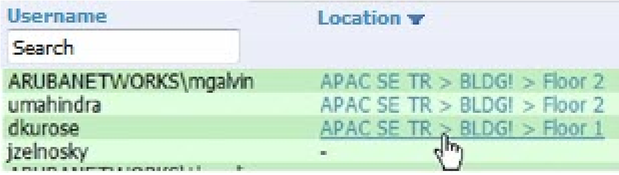
This section contains the following corresponding topics:

- "Viewing a Wireless User’s RF Environment" on page 341
- "Viewing an AP’s Wireless RF Environment" on page 343
- "Viewing a Floor Plan’s RF Environment" on page 344
- "Viewing a Network, Campus, Building’s RF Environment " on page 345
- "Viewing Campuses, Buildings, or Floors from a Tree View" on page 345

Viewing a Wireless User’s RF Environment

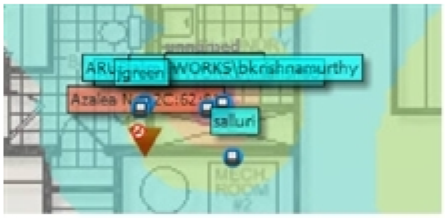
1. Navigate to **Clients** > **All**in AMP.
2. Click the link under the **Location** column for the clientof interest, as shown in Figure 228. A QuickView window of that location opens and indicates the client with a Username label, as shown in Figure 229:

Figure 228 *Link to user’s thumbnail (the Location column)*



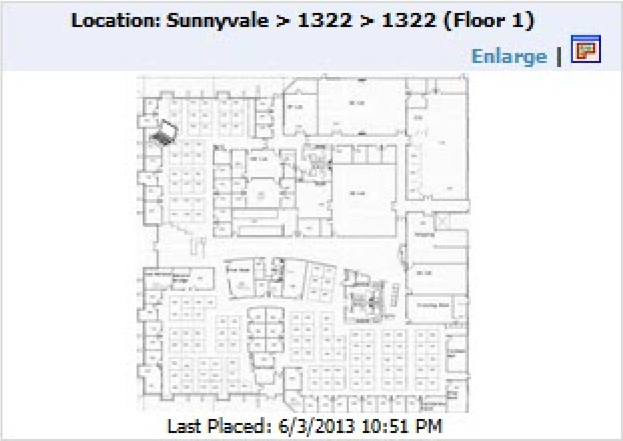
Username	Location ▼
Search	
ARUBANETWORKS\mgalvin	APAC SE TR > BLDG! > Floor 2
umahindra	APAC SE TR > BLDG! > Floor 2
dkurose	APAC SE TR > BLDG! > Floor 1
jzelnosky	-

Figure 229 *QuickView of the selected device*



You can also access this information from the **Clients** > **Client Detail** page by selecting the QuickView thumbnail, located next to the **Current Association** section of this page as shown in Figure 230:

Figure 230 *QuickView thumbnail in Clients > Client Detail*


Location: Sunnyvale > 1322 > 1322 (Floor 1)

Last Placed: 6/3/2013 10:51 PM

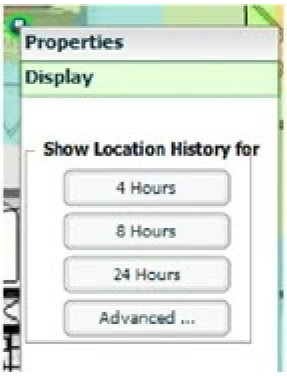
This view is focused on the wireless user enabling you quick resolution of a user's issues and therefore disables most RF objects by default.

- Users - only the user in focus is displayed
- APs - only the access point in which the focus client is associated with is displayed
- Radios - the heatmap represents only the radio to which the client in focus is associated
- Rogues - all rogues are off
- Client/Rogue Surveys - all surveys are off
- Walls - all walls are displayed
- Lines - client to AP of association
- Labels - all labels are disabled

Tracking Location History

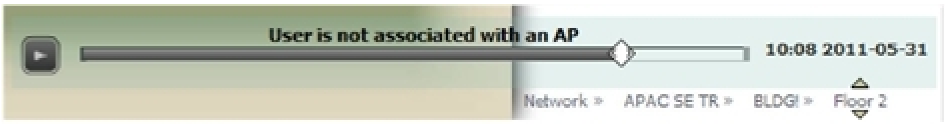
Select a client icon in the floor plan and select **Display** from the pop-up menu shown in Figure 231:

Figure 231 *Show Location History*



A location history player, illustrated in Figure 232, appears at the bottom of the QuickView window.

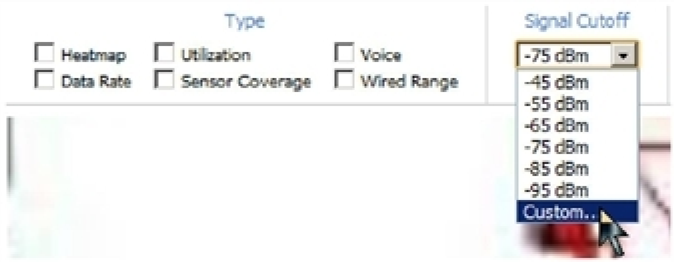
Figure 232 *Location History Player*



Checking Signal Strength to Client Location

1. On a floor plan, locate the **Signal Cutoff** menu.
2. Select the desired signal level to display, as shown in Figure 233. The heatmap updates immediately.

Figure 233 *Signal Cutoff dBm Dropdown Menu*

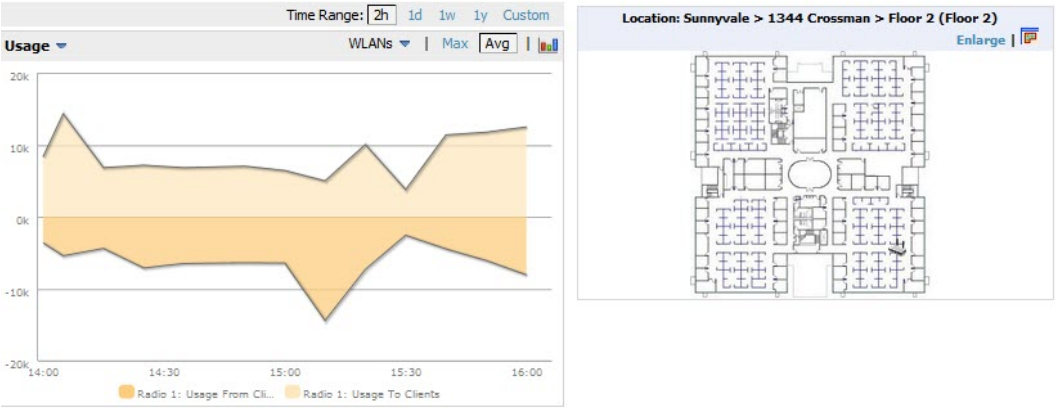


Viewing an AP's Wireless RF Environment

To view an access point's RF environment from **APs/Devices** > **Monitor** page:

1. Select a device of interest from **APs/Devices** > **List**, or any other AMP page that lists your APs. The **APs/Devices** > **Monitor** page opens.
2. Click on the QuickView thumbnail showing the location of the AP. This is located on the right side of the Monitoring graphs, as shown in Figure 234:

Figure 234 *QuickView Thumbnail in APs/Devices > Monitor page for an AP*


Time Range: 2h 1d 1w 1y Custom
Usage
WLANs
Max
Avg
20k
10k
0k
-10k
-20k
14:00
14:30
15:00
15:30
16:00
Radio 1: Usage From Cli...
Radio 1: Usage To Clients
Location: Sunnyvale > 1344 Crossman > Floor 2 (Floor 2)
Enlarge

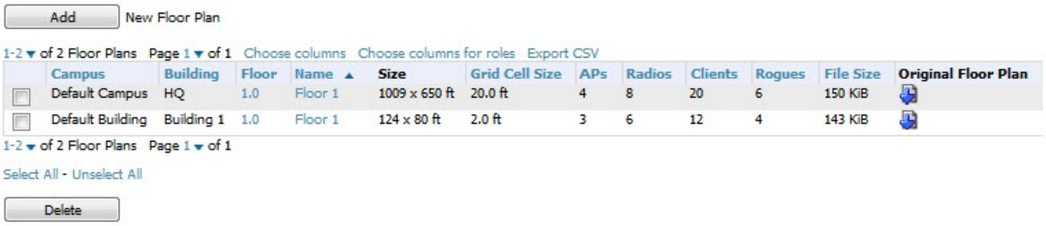
A fully interactive QuickView display opens below the graphs on the same page (not in a new window). This view is focused on enabling quick resolution of AP issues and, therefore, disables many RF objects by default as follows:

- Clients - only clients associated with radios within access point of focus are displayed
- APs - only the access point in focus is displayed
- Radios - the heatmap represents all radios within the access point of focus
- Rogues - all rogues are **off**
- Client/Rogue Surveys - all surveys are **off**
- Walls - all walls on displayed
- Lines - client to AP of association are displayed
- Labels - all labels are disabled

Viewing a Floor Plan’s RF Environment

View a floor plan's RF environment from **VisualRF** > **Floor Plans** page. This page has a fixed sorting filter of Campus, then Building, then Floor number.

Figure 235 *Floor Plans List View*



Add New Floor Plan

1-2 ▾ of 2 Floor Plans Page 1 ▾ of 1 Choose columns Choose columns for roles Export CSV

	Campus	Building	Floor	Name ▲	Size	Grid Cell Size	APs	Radios	Clients	Rogues	File Size	Original Floor Plan
□	Default Campus	HQ	1.0	Floor 1	1009 x 650 ft	20.0 ft	4	8	20	6	150 KiB	⬇
□	Default Building	Building 1	1.0	Floor 1	124 x 80 ft	2.0 ft	3	6	12	4	143 KiB	⬇

1-2 ▾ of 2 Floor Plans Page 1 ▾ of 1

Select All - Unselect All

Delete

The **VisualRF** > **Floor Plans** page provides a snapshot of how VisualRF is performing, as described in Table 160:

Table 160: *Floor Plans list columns*

Field	Description
Campus	Campus associated to the floor.
Building	Building associated to the floor.

Table 160: *Floor Plans list columns (Continued)*

Field	Description
Floor	Floor number. The decimal place can be used for mezzanine levels.
Name	Optional name of a floor. (If the name is not changed, it displays the name as Floor [Number] by default.)
Size	The height and width in feet of the floor plan, including white space.
Grid Cell Size	The size of the grid cells, in feet.
APs	The number of access points on the floor.
Radios	The number of radios associated with access points on the floor.
Clients	The number of wireless clients associated with access points on the floor. **NOTE:** Locating clients consumes significant VisualRF resources. A floor with hundreds or thousands of clients can take a long time to process.
Rogues	The number of rogue devices heard by access points on the floor. This number reflects the filters configured on the **VisualRF > Setup**. This means that while APs on the floor might hear more rogue devices, they are being filtered because of weak signal, they haven't been heard recently, or they are ad-hoc.
File Size	The floor plan background or image reported, in kilobytes. The larger the file, the longer it will take to render in the canvas.
Original Floor Plan	A link to download the original image background file.

Viewing a Network, Campus, Building's RF Environment

To view floors from a geographical perspective:

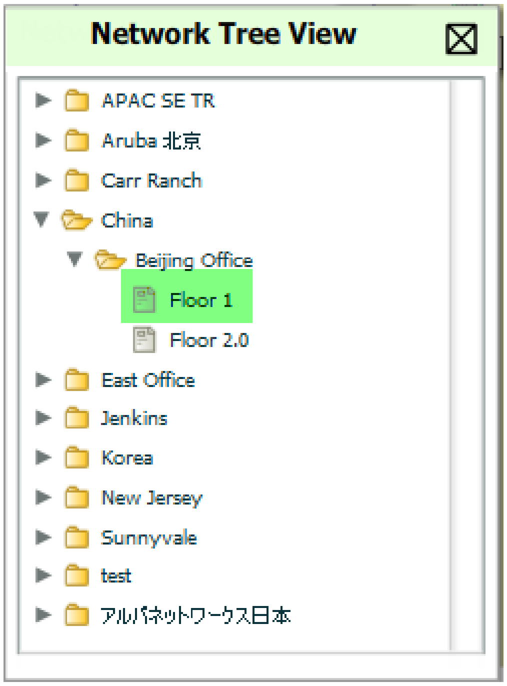
1. Navigate to the **VisualRF** > **Floor Plans** page.
2. Click on each network, campus, or building successively to drill down further until you reach the floor plan. This navigation provides information in each view as follows:
   - Network View - Contains all campuses within your WLAN
   - Campus View - All buildings within a campus
   - Building View - All floors within a building
   - Floor Plan View - All regions, wiring closets, WiFi tags within the floor

Viewing Campuses, Buildings, or Floors from a Tree View

As an alternative to using QuickView, you can use the Tree View to view floors from a hierarchical tree, as follows:

1. Navigate to the **VisualRF** > **Floor Plans** page.
2. Select the **Tree** icon (☰)at the top right of any view. The **Network Tree View** window, shown in Figure 236, appears on the screen.

Figure 236 ***Network Tree View** - Floor 1 highlighted*



Network Tree View

- APAC SE TR
- Aruba 北京
- Carr Ranch
- China
  - Beijing Office
    - Floor 1
    - Floor 2.0
- East Office
- Jenkins
- Korea
- New Jersey
- Sunnyvale
- test
- アルバネットワークス日本

3. Use the arrows to drill down into the folders to select the Campus, Building, or Floor. Select the folder or floor plan icon to open the view you have selected. The Network Tree View window will remain on the screen until you close it.

NOTE

> If you prefer not to use background maps for your campus or building placements, click a background and select **Auto-Arrange** to move the campuses, buildings from their placements into an alphabetically-sorted list.

Planning and Provisioning

VisualRF provides the capability to plan campuses, buildings, floors, and access points prior to the actual access point deployment. The following procedure describes the workflow:

- "Creating a New Campus" on page 346
- "Creating a New Building in a Campus" on page 347
- "Importing a Floor Plan" on page 349
- "Editing a Floor Plan Image" on page 350
- "Provisioning Existing Access Points onto the Floor Plan" on page 352
- "Automatically Provisioning APs onto a Floor Plan" on page 353
- "Tweaking a Planning Region" on page 356
- "Auto-Matching Planned Devices" on page 356
- "Printing a Bill of Materials Report" on page 356

Creating a New Campus

Floors are associated with a building, and buildings are associated with a campus. In order to create a new floor, you must first create a campus with at least one building.

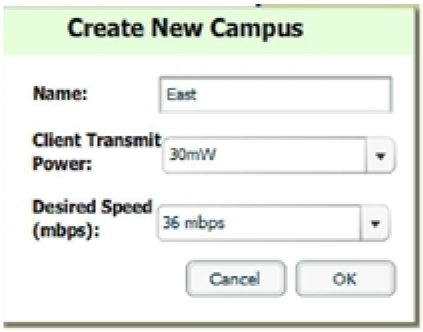
To create and place your campus, follow these steps:

1. Navigate to **VisualRF > Floor Plans**.

2. Select the **Add Campus** button located above the floor plan on the top left. The **Create New Campus** window, illustrated in Figure 237, appears.
3. Enter the following campus information:
    - **Name** of the campus
    - **Client Transmit Power** - used in auto placement of access points onto floors within this campus. The range is 30mW to 100mW.
    - **Desired Speed** (mbps)- used in auto placement of access points onto floors within this campus. The range is 6 to 200 mbps.

Buildings and floors inherit transmit power and speed from the campus.

Figure 237 *Create New Campus window*



Create New Campus

Name: East

Client Transmit Power: 30mW

Desired Speed (mbps): 36 mbps

4. Select **OK** to save. You will see a new Campus icon appear on the campus canvas.
5. Add appropriate network geographical background or upload a personalized image by right-clicking on the background.
    - Set Map - Allows you to browse with the included maps.
    - Auto Arrange Campuses -Arranges the campus in alphabetical order across the background.
6. Drag the new Campus icon to the appropriate location on the map background.

Creating a New Building in a Campus

1. Select the newly created Campus icon from the previous step. When the blank campus area opens, select the **Add New Building** icon.
2. When the New Building window appears, enter the following information:

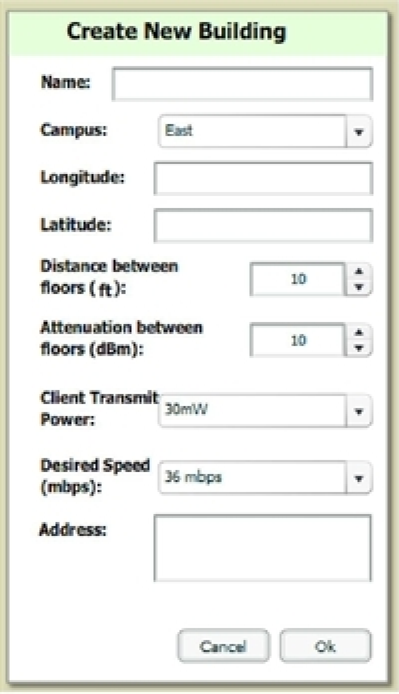
Table 161: *New Building Fields and Descriptions*

Field	Description
Name	Name of the building; located on an existing campus.
Campus	Lists all campuses configured on your AMP.
Longitude & Latitude	These fields are used to represent a building on Google Earth.
Distance between floors	The normal distance between floors in the building. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This

Table 161: *New Building Fields and Descriptions (Continued)*

Field	Description
	data element can be imported or exported to external planning tools like Ekahau. It is not currently utilized by AMP.
Attenuation between floors	Enter the attenuation loss in decibels between floors. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently utilized by AMP.
Client Transmit Power	This value is used when auto-provisioning access points onto a floor plan.
Desired Speed	Speed will determine the new access points when auto-provisioning.
Address	Building or Campus address (optional)

Figure 238 *Create New Building Window*



Create New Building

Name:	
Campus:	East
Longitude:	
Latitude:	
Distance between floors (ft):	10
Attenuation between floors (dBm):	10
Client Transmit Power:	30mW
Desired Speed (mbps):	36 mbps
Address:	

3. Select **OK** to save. A new Building icon will appear in the upper-left corner of the canvas.
4. Drag the Building icon to the appropriate location on the map background.
5. Add appropriate geographical background or upload a personalized image by right-clicking on the background in your Network or in any Campus. The **Set Map** option allows you to browse and select an included map, or you can import your own by selecting the **Custom** button. This launches the image wizard. With this wizard, you can upload an image, specify color or greyscale, and crop your custom background.

NOTE

QuickView automatically saves background map images, campus locations, building locations, and building types.

6. To change building types, navigate to the new building by selecting the Building icon. This opens the Building page. This page is a blank canvas without a background.
7. Right-click on the background of the Building page and select **Set Building Type**.
8. Select a building type of Rectangular, Circular, Rectangular Prism, or Square.

You are now ready to import your floor plan.

Importing a Floor Plan

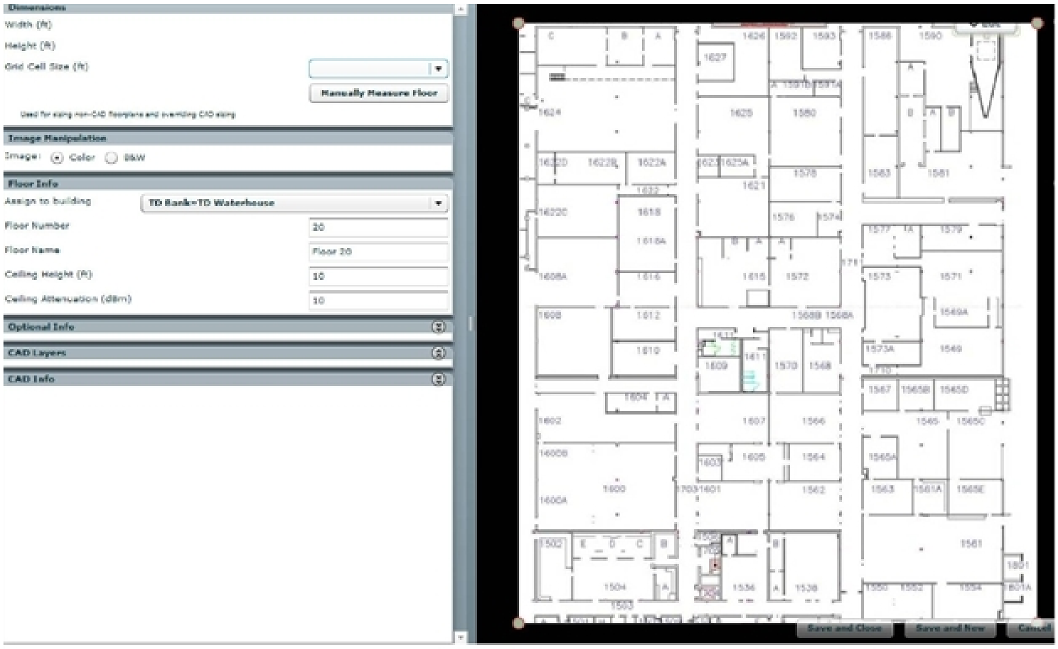
The following steps show how to import a floor plan background image file.

NOTE

When importing RF plans, be sure that the devices to be included are also available in the device catalog.

1. In **VisualRF** > **Floor Plans**, click the **Add Floorplan** icon (displays when viewing a Building) or use the **Add** button above the floor plan list at the bottom of the page.
2. Select **Choose File** to locate a floor plan image file from your hard drive. The following file types are supported:
   - CAD (**NOTE**: CAD floor plans must be generated from an AutoCAD source file.)
   - DWG (**NOTE**: DWG files that include cross-referencing bindings are not supported and may not display properly. In addition, the size limit for DWG files is currently 2880x2880 px.)
   - GIF
   - JPG/JPEG
   - PNG
   - PDF - Single page only. (**NOTE**: PDF floor plans must be generated from a source file. Other PDFs, such as those scanned from a printer, will not import properly.)
3. In VisualRF, select **Upload**. This opens the image file along with VisualRF planning tools on the left side.

Figure 239 *Floor Plan Imported into VisualRF*



Dimensions

Width (ft)

Height (ft)

Grid Cell Size (ft)

Used for sizing non-CAD floorplans and overriding CAD sizing

Image Manipulation

Image: ● Color ○ B&W

Floor Info

Assign to building: TD Bank-TD Waterhouse

Floor Number: 20

Floor Name: Floor 20

Ceiling Height (ft): 10

Ceiling Attenuation (dBm): 10

When importing RF plans, be sure that the devices to be included are also available in the device catalog.

- If the floor plan does not require cropping, sizing, or layer control, then click **Save and Close** to begin provisioning APs or **Save and New** to upload a new floor plan.
- If the floor plan does require cropping, sizing, or layer control, then proceed to the next procedure

NOTE

Floor plans can be added (imported), edited, and deleted. Currently, functionality does not exist to replace a floor plan. If you want to import a newer floor plan to replace a current one, you must first delete the original plan and then add the new plan.

Editing a Floor Plan Image

There are many ways to edit a floor plan that you have uploaded, as explained in the following topics:

- "Cropping the Floor Plan Image" on page 350
- "Sizing a Non-CAD Floor Plan " on page 350
- "Removing Color from a Floor Plan Image" on page 351
- "Assigning Campus, Building, and Floor Numbers " on page 351
- "Assigning Optional Planner, Owner, or Installer Information for the Floor Plan" on page 352
- "Controlling the Layers in the Uploaded Floor Plan (CAD only)" on page 352
- "Error Checking of CAD Images" on page 352
- "Last Steps in Editing an Uploaded Image" on page 352

Cropping the Floor Plan Image

Cropping is available from within the Upload Wizard. Use the cropping handles (red circles) to remove extra white space around the floor plan. VisualRF will calculate an attenuation grid for the entire map including white space. Reducing the white space on a floor plan will increase location accuracy and decrease the load an on the server. A good rule of thumb would be about ½ inch white space, if possible, on all sides.

VisualRF dissects each floor plan into a grid consisting of cells specified in this setting. The Core Thread service calculates the path loss for every radio to every cell on the floor plan.

By default the importation wizard allocates 2,500 grid cells to each site based on dimensions. If you have a site that is 250 ft. by 100 ft, the Floor Plan importation wizard would calculate the grid cell size at 10 feet. 250 ft. x 100 ft. = 25,000 ft. 25,000 ft. / 2,500 ft. = 10 ft.

NOTE

Decreasing the grid cell size will increase accuracy, but it also increase CPU consumption by the floor caching threads and the location caching threads. Check the **System > Performance** page to ensure your server is functioning properly when you make a change to this setting.

Other items worth noting:

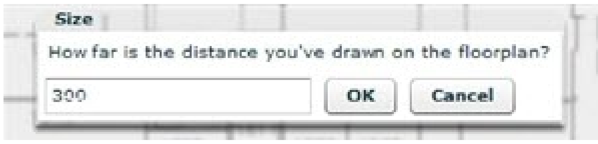
- If this is a CAD file, then the Floor Plan creation wizard will automatically inherit height and width from the drawing.
- If this is a non-CAD file, then the height and width is zero.
- CAD files are converted to a JPG with a resolution of 4096 horizontal pixels at 100% quality prior to cropping. If you crop, then you will lose clarity.
- CAD files must be generated from AutoCAD and may not exceed 10 MB.
- Metric CAD files are supported.
- Importing GIF files for floor plans can result in blank QuickView thumbnails.

Sizing a Non-CAD Floor Plan

You should not have to resize a CAD drawing unless you see nonsensical dimensions. To resize a non-CAD image if you already know the dimensions, follow these steps:

1. Select the **Manually Measure Floor** button in the **Dimensions** section. The pointer changes to a cross-hair icon.
2. Locate two points within the floor plan that you know the distance. Most door jams (door openings) are 3 feet.
3. Select and hold to establish the first point and drag your mouse to the second point and release.
4. A distance dialogue box appears. Enter the proper length in feet, as shown in Figure 240.

Figure 240 *Manually Measuring a Floor Plan*



Size

How far is the distance you've drawn on the floorplan?

300

5. Select **OK**.

Floor plans can be resized in VisualRF after they have been uploaded. Within VisualRF you will also be able to zoom in on a room or doorway to increase the accuracy of your sizing.

Removing Color from a Floor Plan Image

To remove color, locate the **Image Manipulation** section and select **B&W** in the **Image** field.

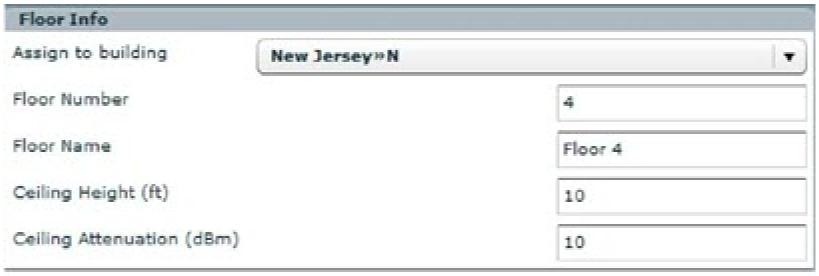
Assigning Campus, Building, and Floor Numbers

Locate the **Floor Info** Section and assign the following information, as detailed in Table 162 and illustrated in Figure 241:

Table 162: *Assigning numbers*

Setting	Default	Description
Building drop-down	N/A	Use this drop-down to associate the floor with a building which associate it to a Campus as well.
Floor Number	0.0	The floor number. You can enter negative numbers for basements. **NOTE:** Each floor plan within a building must have a unique floor number.
Floor Name	Floor [Number]	A descriptive name for the floor. It inherits the floor number as a name if nothing is entered.
Ceiling Height	10	Specifies the height from the floor to the ceiling. This will default to the ceiling height for the building, but you can override here if needed for atria or basements.
Ceiling Attenuation	20	Specifies the attenuation characteristics in dB of the ceiling or the floor above.

Figure 241 *Entering Floor Info for the Uploaded Floor Plan Image*



Floor Info

Assign to building	New Jersey»N
Floor Number	4
Floor Name	Floor 4
Ceiling Height (ft)	10
Ceiling Attenuation (dBm)	10

Assigning Optional Planner, Owner, or Installer Information for the Floor Plan

Locate the **Optional Information** section and enter the following information in Table 163:

Table 163: *Optional Information for the Floor Plan*

Setting	Default	Description
Owner	N/A	The owner of the floor (used in diagnostics and alerts).
Planner	N/A	The person in charge of planning the RF layout for the floor.
Installer	N/A	The person in charge of installing RF equipment for the floor.

Controlling the Layers in the Uploaded Floor Plan (CAD only)

Follow these steps to controller layers in CAD images:

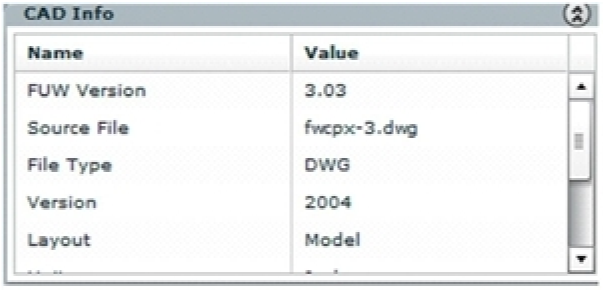
1. Find the CAD Layers section on the page.
2. Unselect the layers which are not required. There is slight delay because each request makes a round trip to the server.

Error Checking of CAD Images

VisualRF will check for errors in your uploaded CAD image. You can view any issues as follows:

1. Locate the **CAD Info** section, as shown in Figure 242.
2. Review the CAD version, units of measurement, and raw width and height numbers.

Figure 242 *Checking for CAD errors*



CAD Info

Name	Value
FUW Version	3.03
Source File	fwcpx-3.dwg
File Type	DWG
Version	2004
Layout	Model

Last Steps in Editing an Uploaded Image

Click the **Save and Close** button to begin provisioning APs or **Save and New** to upload another floor plan. After clicking **Save and Close**, you are redirected back into QuickView where you can provision APs, Wiring Closets, and wired infrastructure.

Provisioning Existing Access Points onto the Floor Plan

To provision existing AP in your network onto the floor plan you just uploaded, follow these steps:

1. Navigate to **VisualRF** > **Floor Plans**.
2. Select the floor plan you have uploaded using the floor number or name links in the list.
3. Select the **Add Deployed Device** icon in the **Edit** menu. A pop-up window list of devices in your AMP appears, as shown on Figure 243
4. Select whether to navigate by Group or by Folder in the **View By** field.

NOTE

Wired-only access device, such as RAP-5, do not have any radios and, therefore, should not be included on a floor plan.

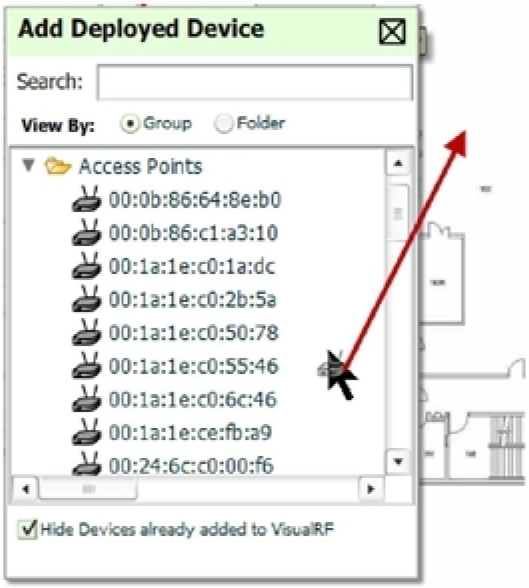
5. Select whether to navigate by Group or by Folder in the **View By** field.

NOTE

Alternatively, you can use the **Search** field.

6. Expand the Group or Folder containing the access points which need to be provisioned on this floor plan. Note that by default, devices that have already been added to VisualRF are hidden. To show them, clear the **Hide Devices already added to VisualRF** check box at the bottom of the list.
7. Click and drag an AP to its proper location on the floor, as shown in Figure 243:

Figure 243 *Provisioning APs onto the Floor Plan*



Add Deployed Device ☒

Search:

View By: ● Group ○ Folder

▼ Access Points
- 00:0b:86:64:8e:b0
- 00:0b:86:c1:a3:10
- 00:1a:1e:c0:1a:dc
- 00:1a:1e:c0:2b:5a
- 00:1a:1e:c0:50:78
- 00:1a:1e:c0:55:46
- 00:1a:1e:c0:6c:46
- 00:1a:1e:ce:fb:a9
- 00:24:6c:c0:00:f6

☑ Hide Devices already added to VisualRF

8. After all APs are provisioned on the floor plan, select **Save** (floppy disk icon) in the top right of the **QuickView** window.

NOTE

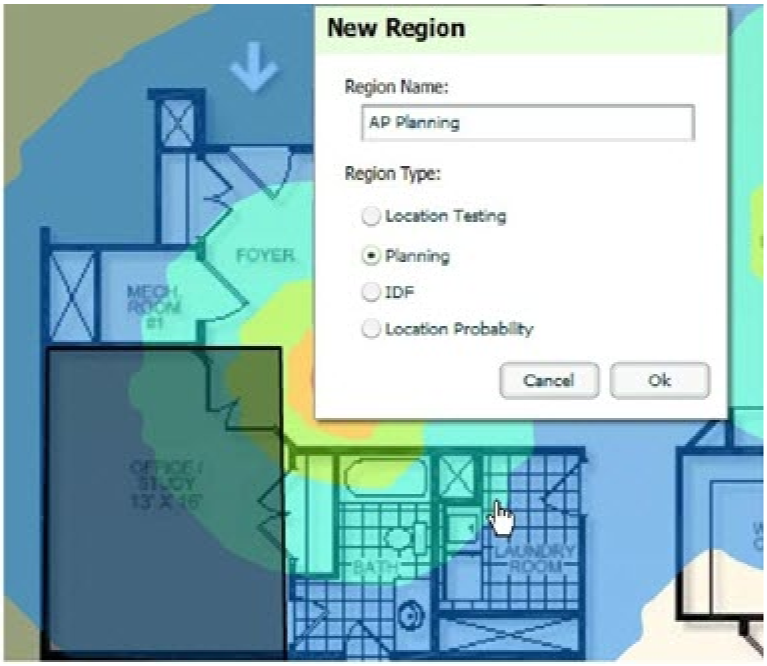
The floor is submitted to one of the core threads to recalculate path loss and then to one of the location caching threads to recalculate client locations. All changes may not be visible on a refresh until this process complete.

Automatically Provisioning APs onto a Floor Plan

To automatically provision your access points onto your floor plan:

1. Select **Draw Region** from the **Edit** menu. A new provisioning popup appears as shown in the following figure.

Figure 244 *Planning Region Drawing and Selection Illustration*



New Region

Region Name: AP Planning

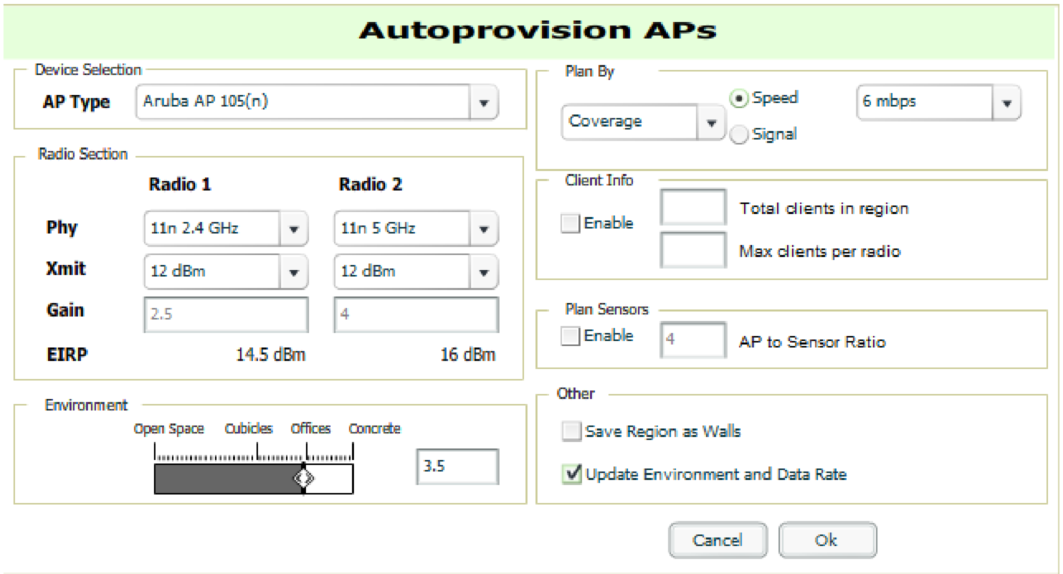
Region Type:

○ Location Testing
● Planning
○ IDF
○ Location Probability

Cancel | Ok

2. Draw your polygon as follows:
   - Left-click to initiate the process. The tool will automatically shade in your provisioning area.
   - Complete the polygon by double-clicking.
3. Once you have finished drawing the region, enter a name for the region and select a Region Type of **Planning**, and then click **OK**. The following image displays.

Figure 245 *Autoprovisioning APs*



Autoprovision APs

Device Selection

AP Type: Aruba AP 105(n)

Radio Section

	Radio 1	**Radio 2**
Phy	11n 2.4 GHz	11n 5 GHz
Xmit	12 dBm	12 dBm
Gain	2.5	4
EIRP	14.5 dBm	16 dBm

Environment

Open Space · Cubicles · Offices · Concrete: 3.5

Plan By

Coverage; ● Speed ○ Signal; 6 mbps

Client Info

□ Enable; Total clients in region; Max clients per radio

Plan Sensors

□ Enable; 4 AP to Sensor Ratio

Other

□ Save Region as Walls
☑ Update Environment and Data Rate

Cancel | Ok

4. Enter the following information into the **Autoprovision APs** window as described in Table 164:

Table 164: *Fields in the Autoprovision APs Window*

Field	Description
Device Selection	
AP Type	The type of AP used in this planning region.
Radio Section	
Phy	Whether they PHY is set to 11n or no radio.
Xmit	Transmit power of the APs.
Gain	Gain of the APs.
EIRP	EIRP of the APs.
Environment	A range from 1-4 that best describes whether the environment is related to an office space, cubicles, offices, or concrete. Decimal points are allowed.
Plan By Section	
Coverage	Plan Coverage by Speed or Signal.
Location	Plan for location accuracy. This mode will result in additional APs placed near the edge of the region to aid in location calculation.
Number of APs	Number of APs to place in the planning region.
Client Info Section	
Enable	Whether to enable planning by user capacity.
Total clients in region	Set the anticipated number of clients that will be stationed in a region.
Max clients per radio	The maximum number of clients supported by each radio.
Plan Sensors Section	
Enable	Whether to enable to plan sensors into the region.
AP to Sensor Ratio	Specify the number of sensors per AP to use when planning the region.
Other Section	
Save Region as Walls	Whether to save the edges of the planning region as walls.
Update Environment and Data Rate	Whether to update the environment and data rate in case of changes.

5. When you are finished selecting the desired options, click **OK**.

Tweaking a Planning Region

If the planning layout does not meet your expectations, you can edit by right-clicking within the region to see the following options:

- **Delete Planned APs in the Region** - Deletes only provisioned APs in the region
- **Reprovision APs** - Remove all planned APs inside this region and prompts for new information to replan the region
- **Delete the Region** - Deletes the region and all planned APs
- **Edit the region** - Change the name of the region
- **Copy the Region to floors above** - Will copy the region and auto plan for floors above.

NOTE

The starting floor will add one to the highest floor in the building and the ending floor defaults to 10 more than the starting floor.

To replicate a floor plan, follow these steps:

1. Navigate back to the Building view by clicking on the navigation tags in the bottom-right corner of the window.
2. Right-click the floor and select **Duplicate**.
3. Enter the following information:
   - Starting and ending floors
   - Select the toggles to copy walls, regions, data rates (speeds), and AP placement

NOTE

The starting floor will add one to the highest floor in the building and the ending floor defaults to 10 more than the starting floor.

4. Select **OK** to save your changes.
5. Manually refresh page and your is redirected to the **VisualRF > Floor Plan** page. The Building view will reflect the new floors.

NOTE

You should see all replicate floors with matching number of access points.

Auto-Matching Planned Devices

You can right-click a campus, building, or network icon and select the **Auto-Match Planned Devices** option to efficiently match planned APs to managed APs. If you select this option for a campus, then all planned APs in that campus are checked. If used on a building, then all the APs in that building are checked. If used on a floor, then all APs on that floor are checked.

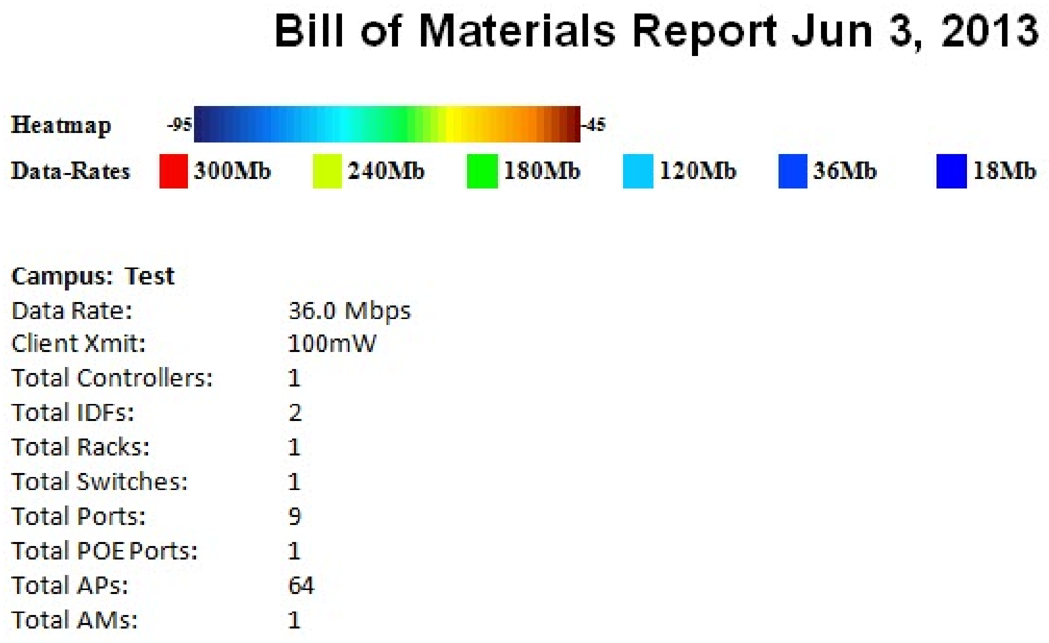
Planned devices first attempt to auto-match on MAC address, and then by name. The VisualRF MAC address checks against all of the LAN MAC addresses of a deployed AP.

Printing a Bill of Materials Report

You can generate a Bill of Materials (BOM) Report from within VisualRF in Word format. Follow these steps:

1. Navigate back to the Network view.
2. Right select Campus icon and select **Show Bill of Materials**. A generating report popup appears.
3. Select options such as heatmap, speed, sensor coverage, wired range, and summary.
4. Select **OK**. A BOM report appears in Microsoft Word as illustrated in Figure 246:

Figure 246 *Bill of Materials Report Illustration*



Bill of Materials Report Jun 3, 2013

Heatmap -95 -45

Data-Rates 🟥 300Mb 🟨 240Mb 🟩 180Mb 🟦 120Mb 🟦 36Mb 🟦 18Mb

Campus: Test	
Data Rate:	36.0 Mbps
Client Xmit:	100mW
Total Controllers:	1
Total IDFs:	2
Total Racks:	1
Total Switches:	1
Total Ports:	9
Total POE Ports:	1
Total APs:	64
Total AMs:	1

Importing and Exporting in VisualRF

Exporting a campus

To export a campus from VisualRF so you can import it into another AMP, follow these steps:

1. Navigate back to the **Network** view.
2. Right-click the **Campus** icon.
3. Select **Export**. An object selection window appears.
4. Select the objects to export and select **Export**. A **File Download** window appears.
5. Select **Save** and save the zipped file to your local hard drive for importation to another AMP.

At this point, you are ready to deploy a production AMP and manage devices by importing your exported campus and matching the access points to your plan.

Importing from CAD

The Floor Plan Upload Wizard (FUW) should inherit all pertinent information from your CAD file if you follow this procedure:

1. Determine UNITS - all modern CAD versions (2001 and newer) support UNITS
2. Determine MEASURE - Legacy CAD versions (2000 and older) used a Imperial or Metric system.
   - If UNITS are 0 or undefined, then the standard dictates defaulting to MEASURE value
   - If MEASURE is 0 or undefined, then the standard dictates defaulting to English and inches
3. Find MODEL VIEW - If the drawing contains multiple views the FUW will default to the Model view
4. Determine Bounding Box - FUW will encompass all lines and symbols on the drawing and create a bounding box which is generally smaller than entire drawing. It is based on the UNITS or MEASUREMENT above.
5. Convert to JPG - FUW will convert the bounding box area to a JPG file with a resolution of 4096 horizontal pixels at 100% quality.
6. Start Web UI of FUW Step #1 - This is the cropping step.

This and all subsequent steps use the converted JPG file. The greater the floor plan dimensions, the less clarity the background image provides.

Batch Importing CAD Files

This process provides the ability to automatically upload many CAD files and auto provision existing walls and access points, and contains the following topics:

- "Requirements" on page 358
- "Pre Processing Steps" on page 358
- "Upload Processing Steps" on page 358
- "Post Processing Steps" on page 359
- "Sample Upload Instruction XML File" on page 359
- "Common Importation Problems" on page 359

Requirements

- Operating System: Client machine must be Windows XP, Windows Vista, or Windows 7
- Flash: Version 9 or later

Pre Processing Steps

1. Increase Memory Allocation in **VisualRF > Setup** as follows:
   - 25 floors or less - 512 MB
   - 25 to 75 floors - 1 GB
   - More than 75 floors - 1.5 GB
2. Massage the output data.
3. Increase the **Location Caching Timer** to 1 hour so that VisualRF does not overload the server calculating client locations while calculating path loss and process floor plan images.

Upload Processing Steps

1. Create CAD XML files which contain drawing filename, dimensions and optional information like device manufacture and model, device coordinates, wall coordinates and building material. This step is usually performed by your facilities or CAD department. The output of AutoCAD will not be properly formed XML, so you may need to massage the output data.
2. Copy all CAD drawings and corresponding XML files into a single directory on Windows machine. All files must be in a single directory.
3. Compress all files into a single *.zip file.
4. Open your browser and navigate to your AMP : https://<AMP_NAME>/visualrf/site_batch.
5. Select **Browse** to launch the File Explorer Window.
6. Select the zip file containing the upload instructions and click the **Open** button. The **File Explorer** Window will disappear you will return to the **Batch Floor Upload Wizard**.
7. Select **Next**.
8. The application validates the following information
   - Well-formed XML
   - All drawing files are accessible
   - All APs are present
   - All Building and Campuses are present
9. If there are any errors, none of the floor plans are created.

Post Processing Steps

1. Decrease the Location Caching Timer to previous value.
2. Review the **VisualRF > Floor Plans** page to ensure server is keeping up.

Sample Upload Instruction XML File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<visualrf:site_batch xmlns:visualrf="http://www.airwave.com" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" version="1" origin="lower-left">
        <floor name="1st Floor" number="43" building-name="Library" campus-name="University">
                <image filename="blueprint1.dwg"/>
                <access-points>
                        <access-point name="ART.1.1" x="190.26" y="222.31"/>
                        <access-point name="ART.1.2" x="136.12" y="208.60"/>
                        <access-point name="ART.1.3" x="75.02" y="221.47"/>
                        <access-point name="ART.1.4" x="73.41" y="132.48"/>
                        <access-point name="ART.1.9" x="196.67" y="98.34"/>
                        <access-point name="ART.1.8" x="179.07" y="55.97"/>
                        <access-point name="ART.1.7" x="119.64" y="56.12"/>
                        <access-point name="ART.1.6" x="74.53" y="56.36"/>
                        <access-point name="ART.1.5" x="59.18" y="38.01"/>
                </access-points>
        </floor>
        <floor name="2nd Floor" number="44" building-name="Library" campus-name="University">
                <image filename="blueprint2.dwg"/>
                <access-points>
                        <access-point name="ART.2.12" x="196.31" y="92.19"/>
                        <access-point name="ART.2.11" x="204.82" y="55.78"/>
                        <access-point name="ART.2.10" x="133.08" y="55.81"/>
                        <access-point name="ART.2.9" x="73.79" y="55.78"/>
                        <access-point name="ART.2.8" x="73.72" y="104.26"/>
                        <access-point name="ART.2.7" x="73.91" y="134.88"/>
                        <access-point name="ART.2.6" x="73.83" y="162.72"/>
                        <access-point name="ART.2.5" x="73.82" y="183.61"/>
                        <access-point name="ART.2.4" x="63.74" y="125.48"/>
                </access-points>
        </floor>
</visualrf:site_batch>
```

Common Importation Problems

- Improper or undefined UNITS or MEASURE
- Text embedded into the Model view which causes an inconsistent bounding box
- Large dimensions which cause grainy resolution upon zoom
- Legacy CAD versions prior to Release 15 or AutoCAD 2000.

Importing from an Aruba Controller

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into an Aruba controller.

Pre-Conversion Checklist

Prior to importing floor plans, ensure that VisualRF's memory allocation is sufficient for the anticipated number of floor plans.

To change the memory allocation, navigate to the **VisualRF > Setup** page and configure the memory allocation accordingly. Memory allocation should equal .5 GB for 1-75 floor plans, 1 GB for 76-250 floor plans, 1.5 GB for 251-500 floor plans, and 2 GB for 501-1,000 floor plans.

NOTE

Importing a large number of floor plans can impact performance of the AMP server. VisualRF must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. This can cause the **VisualRF > Floor Plans** page to be unresponsive.

Process on Controller

1. On the controller's UI, navigate to the **Plan > Building List** page.
2. Select the buildings to be exported and select **Export**.
3. When the dialog box appears, make sure that you have included all images and select **Save to a file**.

Process on AMP

1. Navigate to **VisualRF > Import**.
2. Select the **Import floor plans from an Aruba/ Controller** link.
3. Select the **Begin Importing Floor Plans** link.
4. When prompted for input file, use the file saved from the controller process.

VisualRF Location APIs

VisualRF provides the following location APIs:

Site Inventory: **`https://[amp_host]/visualrf/site.xml?site_id=...`**

- You can find the site_id from the Floor Plan List query defined on the XML API page
- This interface provides floor details including access points, walls, regions, surveys, etc.
- The corresponding example XML and schema are attached in visualrf_site_inventory.*

Device Location: **`https://[amp_host]/visualrf/location.xml?mac=...`**

- Provide the radio MAC of the client to locate.
- The corresponding site where the user was placed is provided along with the dimensions
- If a client is heard on multiple floors, it will only be placed on the floor that contains the AP it is associated with.

Sample Device Location Response

```
<visualrf:device_location version="1" xmlns:visualrf="www.example.com">
 <device mac="00:13:02:C2:39:28" name="Peter"
    site_id="4f674301-4b47-4ac6-8417-4eba3f7df3a6"
    site_name="NewYork">
    <site-width>124.51</site-width>
    <site-height>161.14</site-height>
    <x>82.50</x>
    <y>37.50</y>
 </device>
</visualrf:device_location>
```

Sample Site Inventory Response

```
<amp:amp_site_inventory version="1"
    xmlns:amp=http://www.example.com
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <site id="b45e7a49-23b5-4db0-891a-2e60bff90d2c" version="677">
    <name>Remax</name>
    <uom>ft</uom>
    <width>314.45</width> <height>425.88</height>
    <property name="site_owner" value="" format="" />
    <property name="name" value="Remax" format="" />
    <property name="installer" value="" format="" />
    <property name="planner" value="" format="" />
    <image type="background">
      <filename>/var/example/snapshot/b45e7a49-23-2e6d2c.677/background.jpg</filename>
      <relative-url>/snapshot/b423b5-4db0-891a2e0d2c.677/background.jpg</relative-url>
      <pixel-width>1151</pixel-width>
      <pixel-height>1557</pixel-height>
    </image>
    <image type="thumbnail">
      <filename>/var/example/snapshot/b45e7a49891af90d2c.677/thumb.jpg</filename>
      <relative-url>/snapshot/b45e7a49-23b5-4db0-891a2c.677/thumb.jpg</relative-url>
      <pixel-width>230</pixel-width>
      <pixel-height>311</pixel-height>
    </image>
    <ap id="12615" name="AP-4000M-1">
      <x>118.97</x> <y>130.38</y>
      <total-bandwidth>0</total-bandwidth>
      <total-clients>0</total-clients>
      <status>down</status>
      <uptime>0.0</uptime>
      <radio index="1" phy="g" mac="00:20:A6:5A:63:66" beamwidth="0.0"
          gain="1.5" antenna="" orientation="0.0" mount="Ceiling" valid="false">
        <discovering-radio id="11276" index="1" dBm="-85" />
        <discovering-radio id="11828" index="1" dBm="-93" />
      </radio>
    </ap>
  </site>
</amp:amp_site_inventory>
```

About VisualRF Plan

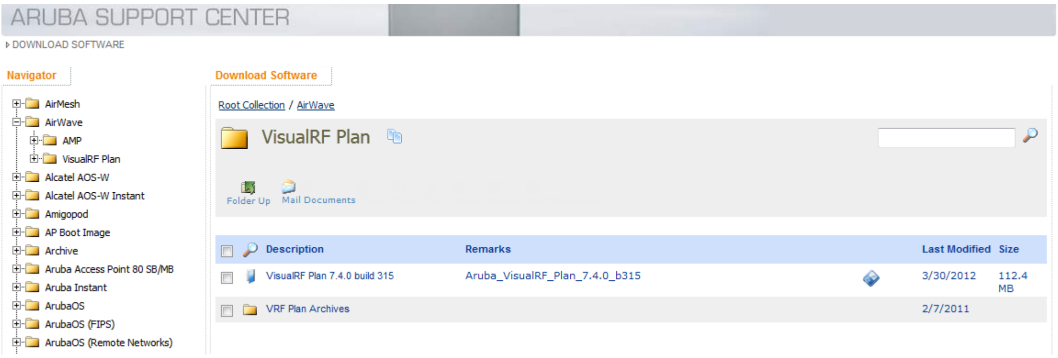
Overview

VisualRF Plan is a standalone Windows client that can be used for planning sites that do not yet use the AMP service on the Web. You can use VisualRF Plan to do basic planning procedures like adding a floor plan, provisioning APs, and generating a Bill of Materials (BOM) report.

VisualRF Plan is free to use for anyone with an Aruba support account. No license is required.

The client can be downloaded from the Aruba Support Center. On http://support.arubanetworks.com, select the **Download Software** link, which will display a tree view of Aruba software. Select the AirWave directory, and then the VisualRF Plan sub directory. The figure below shows the page that displays.

Figure 247 *VisualRF Plan Download Location Page Illustration*



	Description	Remarks	Last Modified	Size
□	VisualRF Plan 7.4.0 build 315	Aruba_VisualRF_Plan_7.4.0_b315	3/30/2012	112.4 MB
□	VRF Plan Archives		2/7/2011	

The latest version of the VisualRF Plan client will display in this folder -- earlier versions are located under the VisualRF Plan Archives subdirectory. Select the.exe file you want to download.

After VisualRF Plan has finished downloading, launch the installer.

Minimum requirements

VisualRF Plan must be installed on a Windows machine with the following minimum specifications:

- 250 MB Hard drive storage space
- 2 GB RAM
- 2.0 GHz dual-core CPU

NOTE

If installing VisualRF Plan on a VMware virtual machine hosted by a Mac computer, you must disable **Folder Sharing.**

VisualRF Plan Installation

After you have downloaded VisualRF Plan from the Aruba support site, the installer will prompt you for the location of the data directory. You must have access to the directory you choose for the installation. Also choose a directory for auto-backup. (The default is the user directory.) Follow the rest of the instructions on your installation screen.

Differences between VisualRF and VisualRF Plan

Table 165: *VisualRF vs. VisualRF Plan*

Feature	VisualRF	VisualRF Plan
Hardware sizing		X
Installation required		X
How to plan a site	X	X
Navigation	X	X
Track users	X	
Track interferers	X	
VisualRF APIs	X	
Location accuracy	X	
QuickView preferences	X	
Resource utilization	X	
Add external walls	X	X
Client surveys	X	
Wiring Closet	X	X
View deployed switches	X	

Table 165: *VisualRF vs. VisualRF Plan (Continued)*

Feature	VisualRF	VisualRF Plan
View signal strength	X	
Planning and provisioning	X	X
Import and Export	X	X