Dell Networking
W-AirWave 8.2.4

DELL

User Guide

Copyright

© Copyright 2017 Hewlett Packard Enterprise Development LP. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

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

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents

Thank you for choosing W-AirWave 8.2.4. W-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.

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

- "A Unified Wireless Network Command Center" on page 13
- "Integrating W-AirWave into the Network and Organizational Hierarchy " on page 14

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

A Unified Wireless Network Command Center

Dell Networking W-AirWave 8.2.4 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, W-AirWave manages it all.

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

The components of W-AirWave are described in the next section.

W-AirWave Management Platform

The W-AirWave Management Platform (W-AirWave), provides the following functions and benefits:

- Core network management functionality, including network discovery, configuration of access points (APs) & controllers, automated compliance audits, firmware distribution, monitoring of all devices and users connected to the network, and reports showing real-time and historical trends.
- Granular administrative access that is role-based and network-based. For more information about roles, see "Administrative Roles" on page 15.
- Flexible device support for thin, thick, or mesh network architecture; multiple vendors; and current or legacy hardware.

Controller Configuration

W-AirWave supports global and group-level configuration of Dell Networking W-Series 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 Dell Networking W-Series ArubaOS, refer to the *Dell Networking W-Series ArubaOS User Guide* for your specific version.

W-AirWave consolidates and pushes global controller configurations from within W-AirWave.

Two pages in W-AirWave support controller configuration:

- **Device Setup > Dell Configuration** for global Dell Configuration. This page is available if Use Global Dell 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 Dell Networking W Configuration, refer to the *W-AirWave 8.2 Controller Configuration Guide*.

Instant Configuration

Dell Networking W-Instant (Instant) is a system of access points in a Layer 2 subnet. The Instant APs (W-IAPs) are controlled by a single W-IAP that serves a dual role as both an W-IAP and primary Virtual Controller (VC), eliminating the need for dedicated controller hardware. This system can be deployed through a simplified setup process appropriate for smaller organizations, or for multiple geographically dispersed locations without an on-site administrator.

With AirWave, IT can centrally configure, monitor, and troubleshoot Dell Instant WLANs, upload new software images, track devices, generate reports, and perform other vital management tasks, all from a remote location.

A Virtual Controller or Instant AP can authenticate to the W-AirWave server using a pre-shared key, or using two-way certificate-based authentication using an SSL certificate sent from W-AirWave to the Instant device. Virtual Controllers push data to W-AirWave via HTTPS. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, you can change the port W-AirWave uses to communicate with Instant devices.

For additional information that includes a comprehensive inventory of all pages and settings that support Instant Configuration, refer to the *Dell Networking W-Instant* in *W-AirWave 8.2 Deployment Guide*.

VisualRF

VisualRF monitors and manages radio frequency (RF) dynamics within your wireless network. Visual RF provides:

- Accurate location information for all wireless users and devices.
- Up-to-date heat maps and channel maps for RF diagnostics; it adjusts for building materials and supports multiple antenna types.
- Floor plan, building, and campus views.
- Visual display of errors and alerts.
- Easy importing 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. RAPIDs provides:

- Automatic detection of unauthorized wireless devices.
- Rogue device classification that supports multiple methods of rogue detection.
- Wireless detection, using authorized wireless APs to report other devices within range to calculate and display rogue location on a VisualRF map.
- Wired network detection of rogue APs located beyond the range of authorized APs and sensors, routers, and switches. RAPIDs ranks devices according to the likelihood they are rogues, runs multiple tests to eliminate false positive results, and identifies the switch and port to which a rogue device is connected.

Integrating W-AirWave into the Network and Organizational Hierarchy

W-AirWave generally resides in the network operations center and communicates with various components of your WLAN infrastructure. In basic deployments, W-AirWave communicates solely with indoor wireless access points (and WLAN controllers over the wired network. In more complex deployments, W-AirWave 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. W-AirWave has the flexibility to manage devices on local networks, remote networks, and networks using Network Address Translation (NAT). W-AirWave communicates over-the-air or over-the-wire using a variety of protocols.

The power, performance, and usability of W-AirWave 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 (ClearPass, Funk, FreeRADIUS, ACS, or IAS)
RADIUS Accounting	W-AirWave itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+ and LDAP	Used to authenticate W-AirWave administrative users
Routers/Switches	Provide W-AirWave with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR
Rogue APs	Unauthorized APs not registered in the W-AirWave database of managed APs

Administrative Roles

The flexibility of W-AirWave enables it to integrate seamlessly into your business hierarchy as well as your network topology. W-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.

This section contains the following procedures to deploy initial W-AirWave configuration:

> **NOTE**
> Additional configurations are available after basic configuration is complete.

Before You Begin

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

Formatting the Top Header

The Dell Networking W-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 *Dell Networking W-AirWave 8.2.4 Installation Guide*.

Figure 1: *Navigation Bar Displaying Down Device Statistics*
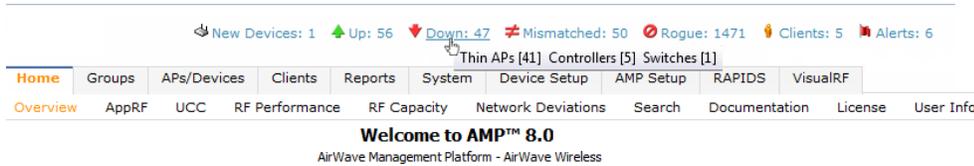
You can control the **Top Header Stats** links that appear from the **AMP Setup > General** page, as described in "Defining General W-AirWave Server Settings" on page 27. Top Header Stats can also be customized for individual users on the **Home > User Info** page. There you can select the statistics 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 User Information" on page 257 for more information.

Figure 2: *Home > User Info Top Header Stats Display Options*
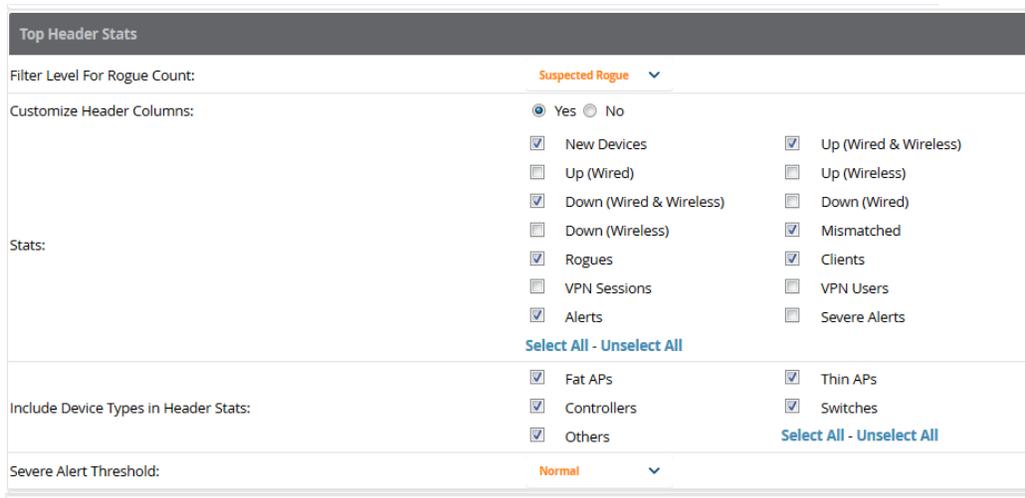
You can also set the severity level of critical alerts displayed for a user role. For details including a description of what constitutes a severe alert, see "Setting Severe Alert Warning Behavior" on page 27.

Customizing Columns in Lists

Customize the columns for any list table selecting drop-down list below the view name. Select the **New** option to create a new view with custom columns, or select **Edit** to change the columns in an existing view, as shown in the figure below.

NOTE

The default table views cannot be edited.

Figure 3: *Edit View Drop down List*
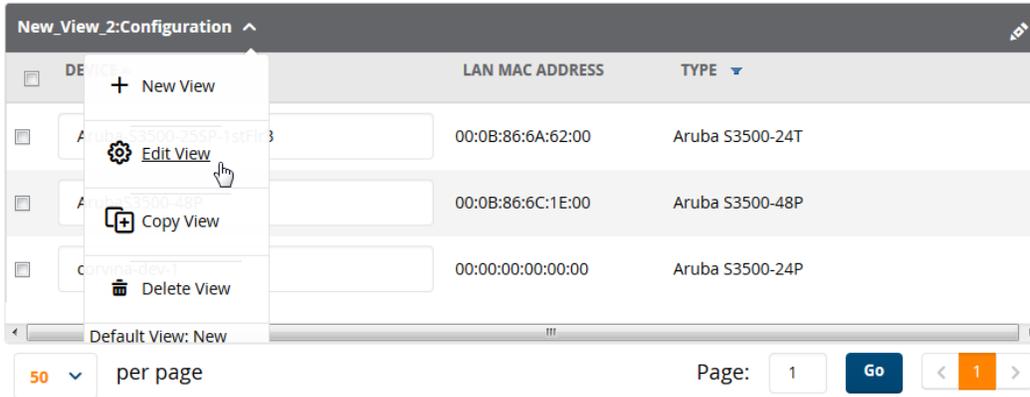
Drag and drop column headings from the **Available Columns** field to the desired location in the **Current Columns** field. The available columns vary, depending upon the list type.

Figure 4: *Selecting Available List columns*
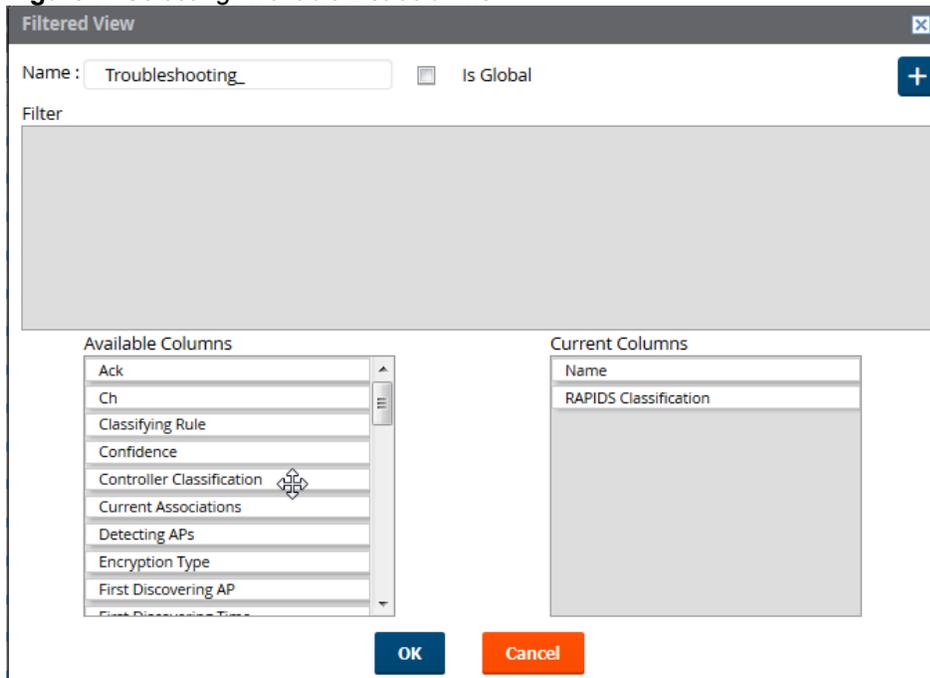
Some tables allow you to control which column heads appear for each user role. Navigate to **Home > User Info** >**Display Preferences** , and then select **Yes** in the **Customize Columns for Other Roles** field. This exposes the **Choose Columns for Roles** drop down menu in all tables that support this feature.

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 5: *Table with Choose Columns for Roles Menu Selected*

Resetting Pagination Records

To control the number of records in any individual list, select the link with **Records Per Page** mouseover text at the top left of the table, as shown in Figure 6. W-AirWave remembers each list's pagination preferences.

Figure 6: *Records Per Page Drop Down Menu*

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 7.

Figure 7: *Home > User Info > Display Preferences section*

Using the Pagination Widget

The pagination widget is located at the top and bottom of every list table, as shown in Figure 8.

Figure 8: *Pagination Widget*

Enter a page number into the **Page** field to jump to any portion of the table, or select the **>** symbol to advance to the next page, and **>|** to return to the previous page.

Using Export CSV for Lists and Reports

Some tables have a **Export CSV** (🗗) option you can use to export the data as a spreadsheet. See Figure 9 for an example of a list with the **Export CSV** icon selected.

Figure 9: *List with CSV Export Selected*
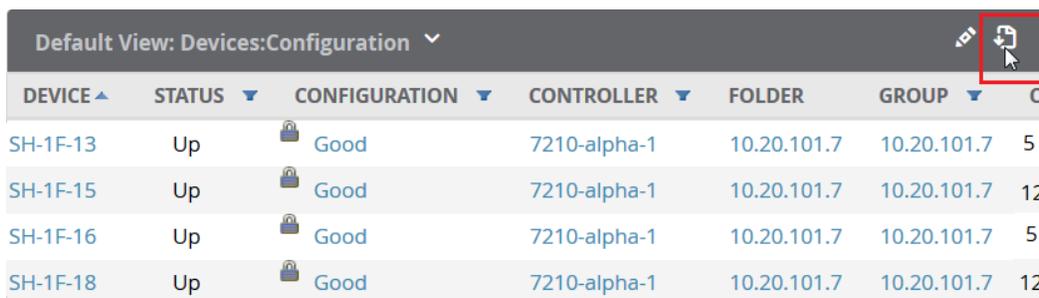
W-AirWave also enables CSV exporting of all report types. For more information, see Exporting Reports to XML, CSV, or PDF.

Defining Graph Display Preferences

Many of the graphs in W-AirWave are Highcharts, which allow you to adjust the graph settings attributes as shown in Figure 10.

Figure 10: *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 W-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 W-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 W-AirWave, these graphs appeared as separate tabs.

Customizing the Dashboard

Click ⚙ to customize the widgets that appear on your dashboard so you see only what you want in your reports. Figure 11 shows an example where you drag the "Clients by Network" widget to the dashboard.

Figure 11: *Drag a Widget to the Dashboard*
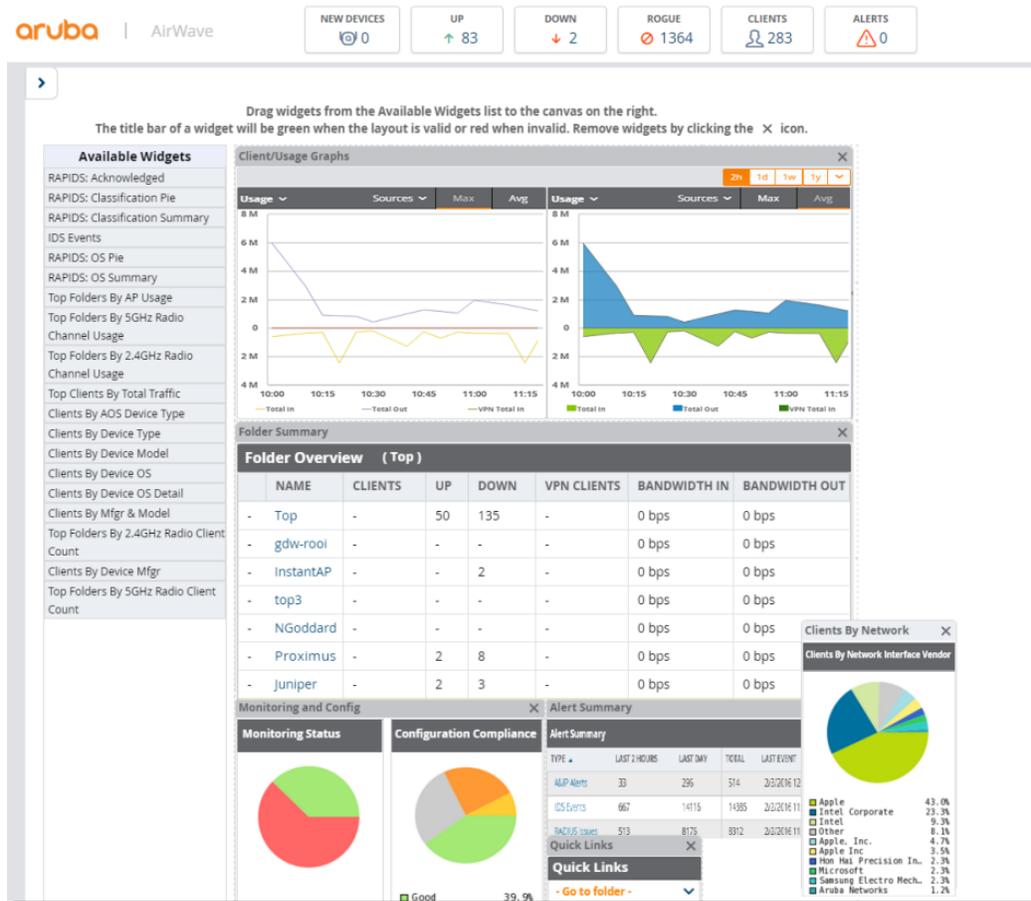
Adding Widgets

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 W-AirWave is aware of from polling the device.
	The **Usage** graph is enabled by default and, by default, shows the average 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 the SSIDs that W-AirWave 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 enabled by default and provides the number of W-AirWave alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last W-AirWave server reboot.
	● Click on **AirWave 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.

Table 2: *Available Widgets (Continued)*

Widget	Description
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 W-AirWave. 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 W-AirWave. In addition, contained rogue information will appear if **Manage rogue AP containment** is set to **Yes** on the **RAPIDS > Setup** page. 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 W-AirWave server 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 802.11a 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.

Table 2: *Available Widgets (Continued)*

Widget	Description
Top Folders By BG Radio Channel Usage	This chart shows the folders and the number of 802.11b/g 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.
Top Folders By A Radio Client Count	This chart shows the folders and the number of 802.11a 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 802.11b/g 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 W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave over the last 24 hours based on the device operating system (such as Windows or Android).

Widget	Description
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to W-AirWave 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 W-AirWave 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 pop up window rather than on the **Home > Search** page. This pop up 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 user names if that user name 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, user name, 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, user name, device name, etc). This search is case-sensitive for all searched fields.

N O T E

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

Figure 12: *Home > User Info Search Preferences*
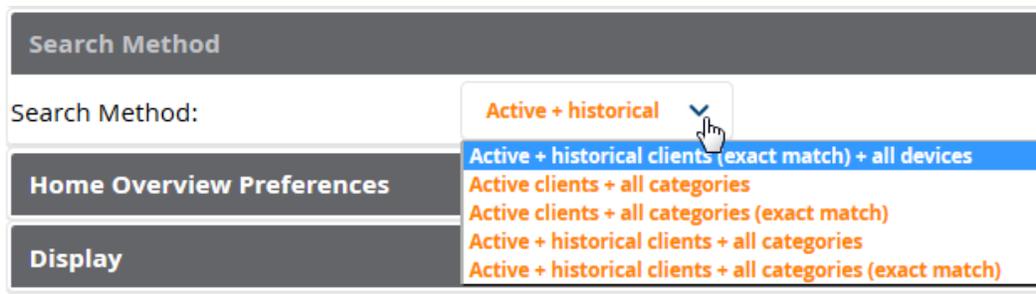
Setting Severe Alert Warning Behavior

You can control the alert levels you can see on the **Alerts** top header stats link using the **Severe Alert Threshold** drop down menu located in the **Top Header Stats** section of 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.

Defining General W-AirWave 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 27
- "Defining W-AirWave Network Settings" on page 40
- "W-AirWave User Roles" on page 44
- "Creating W-AirWave Users" on page 42
- "Configuring Login Message, TACACS+, RADIUS, and LDAP Authentication" on page 44
- "Enabling W-AirWave to Manage Your Devices" on page 53
- "Setting Up Device Types" on page 59

AMP Setup > General

The first step in configuring W-AirWave is to specify the general settings for the W-AirWave server . 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 28

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 W-AirWave server, with a maximum limit of 20 alphanumeric characters.
Default Group	Access Points	Sets the device group that this W-AirWave server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the **Groups > List** page to appear in this drop-down menu. For additional information, refer to "Configuring and Using Device Groups" on page 72.
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 W-AirWave database. If the settings do not match, the AP is flagged as mismatched and W-AirWave 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 W-AirWave detects a variance between actual device settings and the Group configuration policy in the W-AirWave database.
Help improve AirWave by sending anonymous usage data	Disabled	If enabled, W-AirWave will send anonymous data to Dell, which may be used to improve the W-AirWave software. To view an example of the data that will be sent, click the preview link.

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

Setting	Default	Description
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the local time of day W-AirWave should perform daily maintenance. During maintenance, W-AirWave cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
License APs Usage Threshold	90	Sets a threshold to display an alert on the controller monitor page when the license usage has reached this number.

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. W-AirWave 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 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.

Dell Instant Settings

A Virtual Controller can communicate with the W-AirWave server over a configurable communication port, and authenticate to the server using a pre-shared key, and/or two-way certificate-based authentication using an SSL certificate sent from W-AirWave to the Instant device.

The AMP Setup > General > Dell Instant Options page includes the following Configuration settings:

Table 5: *AMP Setup > General > Dell Instant Options Fields and Default Values*

Setting	Default	Description
Communication port (443,1000-65534):	443	By default, an Instant Virtual Controller communicates with AirWave over port 443. If your enterprise has a security policy that restricts the use of port 443 for inbound communication, use this field to change the port the Virtual Controller uses to communicate with W-AirWave.
Security method for adding new Virtual Controllers:	PSK Only	W-AirWave can use any of the following security methods to authenticate a Virtual Controller to the W-AirWave server. ● PSK Only ● PSK and Certificate ● Certificate Only If you enable certificate authentication, you are directed to the **AMP Setup > General > Upload SSL Certificate** page, where you are prompted to upload an certificate file in PEM format that contains containing both a private key and certificate.
Configuration Only	No	By default, W-AirWave will push Instant configuration settings as well as W-AirWave settings such as RAPIDS settings and traps from an W-AirWave group to a Virtual Controller assigned to that group. Select the **Yes** option to push Instant configuration settings only.

If you select a security method that includes Certificate-based authentication, you must upload the a certificate from a supported certificate authority to the W-AirWave server, as the default W-AirWave certificate will not be recognized by the Instant AP, and will cause the SSL handshake to fail. Certificate authentication also requires that the **AirWave IP address** information configured on the Instant AP is a domain name, and not an IP address.

W-AirWave supports the following trusted certificate authorities:

● **Chain 1**: Trusted Root CA: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root Intermediate CA: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA

● **Chain 2**: Trusted Root CA: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA Intermediate CA: Subject: C=US, O=Google Inc, CN=Google Internet Authority G2

● **Chain 3**: Trusted Root CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5 Intermediate CA: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3

● **Root C**A: Trusted Root CA: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

If you enable certificate authentication, you are prompted to upload an SSL certificate. you can view the current W-AirWave certificate using the **View Certificate** link on that page, or click **Change** to upload a new certificate file to the W-AirWave server.

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 pop up window rather than on the **Home > Search** page. This pop up 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, user name, 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, user name, 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 26.

Home Overview Preferences

On the **AMP Setup > General** page, locate the **Home Overview Preferences** section. Table 6 describes the settings and default values in this section.

Table 6: *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 W-AirWave. These changes affect all users and all new device groups.

Table 7 describes the settings and default values in this section.

Table 7: *AMP Setup > General > Display Fields and Default Values*

Setting	Default	Description
AP Fully Qualified Domain Name Options	No	Sets W-AirWave to use fully qualified domain names for APs instead of the AP name. For example, 'testap.yourdomain.com; would be used instead of 'testap.' 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, W-AirWave displays all Group tabs and setting options. ● **Only devices on this** AMP—When selected, W-AirWave hides all options and tabs that do not apply to the APs and devices currently on W-AirWave. ● **Selected device type**—When selected, a new field appears listing many device types. This option allows you to specify the device types for which W-AirWave displays group settings. You can override this setting.
Look up device and wireless user hostnames	Yes	Enables W-AirWave 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 W-AirWave, after which W-AirWave refreshes DNS lookup: ● 1 hour ● 2 hours ● 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 8 describes the settings and default values of this section.

Table 8: *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**.

Table 8: *AMP Setup > General > Device Configuration Section Fields and Default Values (Continued)*

Setting	Default	Description
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 Dell Configuration	No	Enables Dell Networking W configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within **Groups > Controller Config**instead of globally. **NOTE:** Changing this setting may require importing configuration on your devices. When an existing Dell Networking W 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 **AMP Features** section and adjust settings to enable or disable VisualRF and RAPIDS. Table 9 describes these settings and default values.

Table 9: *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 10 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 10: *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 11 describes the settings and default values of this section. Many settings can be set to have no expiration date.

Table 11: *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 W-AirWave stores basic information about inactive clients and VPN users. A shorter setting of 60 days is recommended for customers with high user turnover such as hotels. The longer you store inactive user data, the more hard disk space you require.
Client Association and VPN Session History (0-550 days, zero disables)	14	Defines the number of days W-AirWave 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 W-AirWave retains location history for Wi-Fi tags.
Rogue AP Discovery Events (14-550 days, zero disables)	14	Defines the number of days W-AirWave stores Rogue Discovery Events. The longer you store discovery event records, the more hard disk space you require.

Table 11: *AMP Setup > General > Historical Data Retention Fields and Default Values (Continued)*

Setting	Default	Description
Reports (0-550 days, zero disables)	60	Defines the number of days W-AirWave 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 W-AirWave retains alerts that have been automatically acknowledged. Setting this value to 0 disables this function, and alerts will never expire or be deleted from the database.
Acknowledged Alerts(0-550 days, zero disables)	60	Defines the number of days W-AirWave 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 W-AirWave 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 W-AirWave is to support any guest user. A value of **0** disables this function, and guest users will never expire or be deleted from the W-AirWave database.
Inactive SSIDs (0-550 days, zero disables)	425	Sets the number of days W-AirWave retains historical information after W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave 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" on page 219. **NOTE:** If your data table has more than 5 million rows, W-AirWave will truncate the device event retention data. In this case, the "number of days" setting becomes "number of hours."

Table 11: *AMP Setup > General > Historical Data Retention Fields and Default Values (Continued)*

Setting	Default	Description
Mesh Link History (0-550 days)	30	Sets the number of days W-AirWave retains historical information for mesh links.
Device Uptime (0-120 months, zero disables)	60	Sets the number of months W-AirWave 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 W-AirWave retains historical information for clients.
UCC Call History (1-30 days)	30	Sets the number of days that calls remain in W-AirWave's call history.
UCC Call Details (1-7 days)	2	Sets the number if days that the W-AirWave retains details for individual calls.
Partial Config Job Retention Interval (1-31 days)	31	Sets the number of days Dell Networking W-AirWave retains information about partial configuration jobs.

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 W-AirWaveTable 12 describes the settings and default values of this section.

Table 12: *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, W-AirWave upgrades the firmware for APs in **Monitor Only** mode. When W-AirWave upgrades the firmware in this mode, the desired configuration are not be pushed to W-AirWave. Only the firmware is applied. The firmware upgrade may result in configuration changes W-AirWave does not correct those changes when the AP is in **Monitor Only** mode.
Maximum Interleaved Jobs (1-20)	20	Defines the number of jobs W-AirWave runs at the same time. A job can include multiple APs. When jobs are started by multiple users, W-AirWave will interleave 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, W-AirWave 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 W-AirWave 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 13 describes the settings and default values of this section.

Table 13: *AMP Setup > General > Additional AMP Services Fields and Default Values*

Setting	Default	Description
Enable FTP Server	No	Enables or disables the FTP server on W-AirWave. 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 ArubaOS controllers to send signed and encrypted RTLS (real time locating system) packets to VisualRF; in other words, W-AirWave becomes the acting RTLS server. The RTLS server IP address must be configured on each controller. This function is used for VisualRF to improve location accuracy and to locate chirping asset tags. This function is supported only for Dell 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 W-AirWave 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 controller's value. ● **Confirm RTLS Password**—Re-enter the RTLS server password.
Use embedded Mail Server/ Mail Relay Server	Yes	Enables or disables the embedded mail server that is included with W-AirWave. 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 W-AirWave should parse client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.
Enable AMON data collection	Yes	Allows W-AirWave to collect enhanced data from Dell Networking W devices on certain firmware versions. See the *Dell Networking W-AirWave Best Practices Guide* on **dell.com/support/manuals** for more details **NOTE:** When enabling AMON, auditing should be set to **daily** and have been successful at least once to allow W-AirWave to calculate the proper BSSIDs per radio. If these BSSIDs do not exist, clients are dropped because they do not have any corresponding BSSIDs in the W-AirWave database. Auditing should be set to daily because the BSSIDs are kept in cache memory and cleared every 24 hours.
Enable Clarity Data Collection	Yes	Allows W-AirWave to collect enhanced Clarity Monitoring data from Dell Networking W devices running ArubaOS 6.4.3 and later versions
Enable AppRF Data Collection	Yes	If AMON is enabled for a controller, you can enable this flag to instruct W-AirWave to collect AppRF data from the controller. If this is enabled, then the **Home > AppRF** page will display.
AppRF Storage Allocated (Greater than or equal to 2 GB)	50	If AppRF Data Collection is enabled, specify the amount of storage to allocate.

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

Setting	Default	Description
Enable UCC Data Collection	Yes	Enables controllers to send UCC data to Dell Networking W-AirWave. For this feature to work, Dell Networking W-AirWave must be a management server on the controller, the AMON port is set up for UDP port 8211, and the controller profile has UCC monitoring enabled.
Enable UCC Calls Stitching (Heuristics)	Yes	Enables caller-to-callee call stitching for non-SDN deployments. You should turn off this option for NAT and BOC deployments.
Prefer AMON vs SNMP Polling	SNMP Polling	**Prefer AMON** is a configuration setting which causes W-AirWave to use an AMON feed to obtain client monitoring information from a controller rather than polling it via SNMP. When you enable this setting, values such as AP lists and rogue AP lists are still polled via SNMP, but the bulk of client monitoring information is delivered via AMON. Before enabling the Prefer AMON setting, please note the following: • Auditing needs to have been successful at least once to allow W-AirWave to calculate the proper BSSIDs per radio. • When **Prefer AMON** is enabled, the controller must be configured to send AMON to W-AirWave. • The network path from the controller to the W-AirWave server must allow traffic on UDP port 8211. • The controller routinely sends AMON in large UDP packets, (up to 30K bytes). Before enabling this setting, ensure the network path from the controller to W-AirWave can pass such large packets intact. • This setting should only be used in a network environment with low levels of UDP packet loss, as the loss of a single Ethernet frame will potentially result in the loss of up to 30K bytes worth of data.
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.
Require SSH host key verification	No	This setting reserved for future use.
Validate PAPI key	No	Security improvements in W-AirWave 8.2.1 and later releases allow you to specify a custom PAPI key and require PAPI key validation. If you select the Yes option, you are prompted to enter a custom PAPI key

Performance Settings

Locate the **Performance** section. Performance tuning is unlikely to be necessary for many W-AirWave deployments, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Dell support at **dell.com/support** if you think you might need to change any of these settings. Table 14 describes the settings and default values of this section.

Table 14: *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 W-AirWave to process more data per second, but it can take resources away from other W-AirWave processes. Contact Dell support at **dell.com/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 Dell support at **dell.com/support** if you think you might need to increase this setting for your network.
Maximum number of audit processes	3	Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Dell support at **dell.com/support**if you are considering increasing this setting for your network.
SNMP Fetcher Count (2-6)	2	Specify the number of SNMPv2 fetchers.
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, W-AirWave fetches SNMP data more slowly, potentially reducing device CPU load. This setting is used for networks containing legacy controllers not available through Dell. Dell recommends not enabling this setting.
Client Association Relevance Factor	0 days (disabled)	Use this setting to hide old client information from clients lists and client search results. For example, a setting of **3** limits the historical client data displayed in client lists and search results to client sessions that have been disconnected within the last three days. When this value is set to **1**, client lists and search results display only the client history for the previous day. This time range can be set from 0-550 days, where a value of zero disables this feature and makes available all historical client data. A shorter time period improves search performance and allows client lists to display more rapidly, though it will also display fewer results.
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to W-AirWave as a whole. When W-AirWave is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth usage) is not adversely impacted. The default priority is **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.

Table 14: *AMP Setup> General > Performance Fields and Default Values (Continued)*

Setting	Default	Description
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 W-AirWave Network Settings

The next steps in setting up W-AirWave are to configure the network interface, DNS settings, NTP servers, and static routes.

Figure 13 illustrates the contents of the **AMP Setup > Network** page when setting up an IPv4 interface. Optionally, you can configure an IPv6 interface. For information, see "Primary Network Interface Settings" on page 40.

Figure 13: *Network Page*

Specify the network configuration options described in the sections that follow to define the W-AirWave 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 15 describes the settings and default values.

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

Setting	Default	Description
IPv4 Address	None	Sets the IPv4 address of the W-AirWave network interface. **NOTE:** This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the W-AirWave server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.
IPv4 Gateway	None	Sets the default gateway for the network interface.
IPv6 Enabled	No	By selecting **Yes**, you can enter an optional IPv6 address and gateway address.
IPv6 Address	None	Sets the IPv6 address of the W-AirWave network interface.
IPv6 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 16 describes the settings and default values.

Table 16: *Secondary Network Interface Fields and Default Values*

Setting	Default	Description
Enabled	No	Select **Yes** to enable a secondary network interface. You will be prompted to define the IP address and subnet mask.
IP Address	None	Specify the IP address of the W-AirWave secondary network. **NOTE:** This address must be a static IP address. W-AirWave supports IPv4 and IPv6 addresses.
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 W-AirWave and your network's NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.

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

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between W-AirWave and the NTP servers creates an entry in the event log. Table 17 describes the settings and default values in more detail. For more information on ensuring that W-AirWave servers have the correct time, please see http://support.ntp.org/bin/view/Servers/NTPPoolServers.

Table 17: *AMP Setup > Network > Secondary Network Fields and Default Values*

Setting	Default	Description
Primary	ntp1.yourdomain.com	Sets the IP address or DNS name for the primary 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 W-AirWave roles.
- Complete the required configurations in this chapter before proceeding. Dell support remains available to you for any phase of W-AirWave configuration.

Creating W-AirWave Users

W-AirWave 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 W-AirWave.

> **NOTE**
>
> User name and password are not required if you configure W-AirWave to use RADIUS, TACACS, or LDAP authentication. You do not need to add individual users to the W-AirWave 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 User Roles" on page 1.

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

1. Go to the **AMP Setup > Users** page. This page displays all users currently configured in W-AirWave. Figure 14 illustrates the contents and layout of this page.

Figure 14: *AMP Setup > Users Page Illustration*

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 W-AirWave. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 15.

Figure 15: *AMP Setup > Users > Add/Edit User Page Illustration*

3. Enter or edit the settings on this page. Table 18 describes these settings in additional detail.

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

Setting	Default	Description
Username	None	Sets the user name for the user who logs in to W-AirWave. This user name is displayed in W-AirWave 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**, you should change this password. You will be logged out and asked to enter your new password.
Name	None	Allows you to define an optional and alphanumeric text field that takes note of the user's actual name.

Setting	Default	Description
Email Address	None	Allows you to specify a specific email address that will propagate throughout many additional pages in W-AirWave 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 W-AirWave pages and relevant functions.

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

What Next?

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

W-AirWave User Roles

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

User Roles and VisualRF

VisualRF uses the same user roles as defined for W-AirWave. Users can see floor plans that contain an AP to which they have access in W-AirWave, 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**, the **Restrict visibility of empty floor plans to the user that created them** configuration option allows you to restrict the visibility of empty floor plans to the role of the user who created them. By default, this setting is set to No.

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

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

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

- "Setting Up Login Configuration Options" on page 45

- "Configuring Whitelists" on page 45
- "Setting Up Certificate Authentication" on page 46
- "Setting Up Single Sign-On" on page 46
- "Specifying the Authentication Priority" on page 46
- "Configuring RADIUS Authentication and Authorization" on page 47
- "Integrating a RADIUS Accounting Server" on page 48
- "Configuring TACACS+ Authentication" on page 49
- "Configuring LDAP Authentication and Authorization" on page 50

Setting Up Login Configuration Options

On the **AMP Setup > Authentication** page, administrators can optionally configure the W-AirWave user's idle timeout or a message-of-the-day that appears on the AirWave login screen.

1. Go to **AMP Setup > Authentication > Login Configuration.**
2. Complete the fields described inTable 19:

Table 19: *Login Configuration section of AMP Setup > Authentication*

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

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

Configuring Whitelists

On the **AMP Setup > Authentication** page, you can now include a list of subnets that are able to log in to W-AirWave. If this option is enabled, then by default, the current client network will appear as the first entry in the list of subnets. Additional entries can be added, one per line, in the text entry box.

For Instant devices that are managed by W-AirWave, this option must be enabled if Certificate Authentication is also enabled.

CAUTION

Do not delete the current client network line from the W-AirWave whitelist. Doing so can result in the loss of access to the W-AirWave user interface.

Figure 16: *Enabling W-AirWave Whitelists*

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.

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 W-AirWave controllers. This allows users to log in to W-AirWave and use the IP Address or Quick Links hypertext links across W-AirWave to access the controller's WebUI 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 W-AirWave.

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.

Specifying the Authentication Priority

To specify the authentication priority for this W-AirWave server, 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 17 illustrates this page.

Figure 17: *AMP Setup > Authentication Page Illustration for RADIUS*

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 20.

Table 20: *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.

Table 20: *AMP Setup > Authentication Fields and Default Values for RADIUS Authentication (Continued)*

Field	Default	Description
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.
Authentication Method	PAP	Select one of the following authentication methods: - PAP - PEAP-MSCHAPv2 If you use the PEAP-MSCHAPv2 authentication method with the default "Read-Only Monitoring and Auditing" user role, note that the name of this role has been slightly modified in W-AirWave 8.2.3 to allow support the PEAP-MSCHAPv2 authentication method: the ampersand **(&)** symbol has been changed to the word **and**. **Role Name in 8.2.2.x and earlier releases**: *Read-Only Monitoring & Auditing* **Role Name in W-AirWave 8.2.**3: Re*ad-Only Monitoring **and** Auditing* If you used the **Read-Only Monitoring & Auditing** user role prior to upgrading to W-AirWave 8.2.3 or later releases, you must modify the user role name on the RADIUS server to ensure that the user role name on the RADIUS server exactly matches the user role name in W-AirWave.

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

Integrating a RADIUS Accounting Server

> **NOTE**
>
> W-AirWave checks the local user name 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 W-AirWave server. The only recommended user is the backup admin, in case the RADIUS server goes down.

Optionally, you can configure RADIUS server accounting on **AMP Setup > RADIUS Accounting**. This capability is not required for basic W-AirWave operation, but can increase the user-friendliness of W-AirWave administration in large networks. Figure 18 illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable W-AirWave to receive accounting records from a separate RADIUS server. Figure 18 illustrates the display of RADIUS accounting clients already configured.

Figure 18: *AMP Setup > RADIUS Accounting Page Illustration*
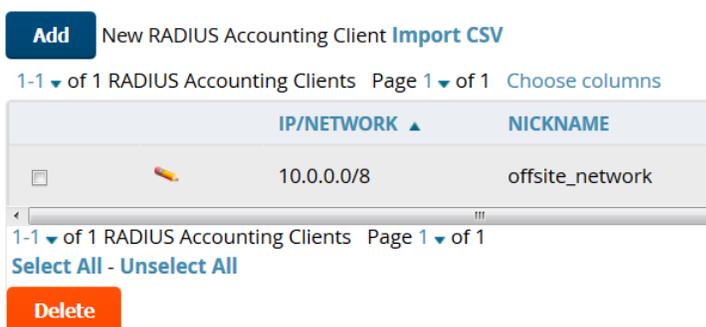
1. To define a the RADIUS authentication server or network, browse to the **AMP Setup > RADIUS Accounting** page, select **Add**, and provide the information in Table 21.

Table 21: *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 W-AirWave and the RADIUS authentication server.

2. Click Add to save your settings.

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 W-AirWave users and does not affect APs or users logging into APs.

1. Go to the **AMP Setup > Authentication** page. This page displays current status of TACACS+. Figure 19 illustrates this page when neither TACACS+, LDAP, nor RADIUS authentication is enabled in W-AirWave.

Figure 19: *AMP Setup > Authentication Page Illustration for TACACS+*

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 22.

Table 22: *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.

Table 22: *AMP Setup > Authentication Fields and Default Values for TACACS+ Authentication (Continued)*

Field	Default	Description
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 W-AirWave

To configure Cisco ACS to work with W-AirWave, 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 format: **role=**<*name_of_*AMP*_role*>. For example role=DormMonitoring.

    As with routers and switches, W-AirWave does not need to know user names.
6. W-AirWave also needs to be configured as an AAA client.
    - On the **Network Configuration** page, select **Add Entry**.
    - Enter the IP address of W-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**
>
> W-AirWave checks the local user name and password store before checking with the TACACS+ server. If the user is found locally, the local password and local role apply. When using TACACS+, it is not necessary or recommended to define users on the W-AirWave server. The only recommended user is the backup administrator, in the event that the TACACS+ 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 20 illustrates this page.

Figure 20: *AMP Setup > Authentication Page Illustration for LDAP*

3. Complete the fields described in Table 23.

Table 23: *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 W-AirWave 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.

Table 23: *AMP Setup > Authentication Fields and Default Values for LDAP Authentication (Continued)*

Field	Default	Description
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. 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 only 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 W-AirWave, 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 W-AirWave role. Users who log in to W-AirWave using this LDAP authentication will be granted permissions based on this role. Refer to W-AirWave User Roles for more information about W-AirWave User Roles.
Filter	(objectclass=*)	This option limits the object classes in which the key,role attributes would be searched.

Field	Default	Description
Add New LDAP Rule	none	The LDAP rule parameters are **Position**, **Role Attribute**, **Operation**, **Value**, and **W-AirWave** role. If you create multiple LDAP rules, rules are processed in order based on the rule position value, so the position you assign to the LDAP rule represents the order in which the LDAP rule is applied to determine the W-AirWave role. LDAP rules can only be configured and applied after LDAP authentication is enabled. The LDAP rules are similar to the rules used by the controller to derive the W-AirWave role.

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.* Dell support remains available to you for any phase of W-AirWave configuration.

Enabling W-AirWave to Manage Your Devices

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

This section contains the following procedures:

- "Configuring Communication Settings for Discovered Devices" on page 53
- "Loading Device Firmware Onto the W-AirWave Server (optional)" on page 55

Configuring Communication Settings for Discovered Devices

You can configure W-AirWave to communicate with your devices by defining default shared secrets and SNMP settings.

To define the default credentials and SNMP settings:

1. On the **Device Setup > Communication** page, enter the default credentials for each device model on your network. W-AirWave assigns default credentials to all discovered devices.

   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 W-AirWave to configure the devices. Without read-write access, W-AirWave may be able to monitor the devices but cannot apply any configuration changes.

2. Enter the SNMP timeout and retries settings. Table 24 lists the settings and default values.

Table 24: *Device Setup > Communication > SNMP Settings Fields and Default Values*

Setting	Default	Description
SNMP Timeout (3-60 sec)	3	Sets the time, in seconds, that W-AirWave waits for a response from a device after sending an SNMP request.
SNMP Retries (1-40)	3	Sets the number of times W-AirWave 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 W-AirWave does not receive an SNMP response from the device after the specified number of retries, W-AirWave 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. Click **Add** and enter the following information :

- **Username** - User name of the SNMP v3 user as configured on the controller.
- **Auth Protocol** - MD5 or SHA. The default setting is SHA.
- **Auth and Priv Protocol Passphrases** - Authentication and privilege protocol passphrases for the user, as configured on the controller.
- **Priv Protocol** - DES or AES. The default setting is DES.

The SNMP Inform receiver will restart when users are changed or added to the controller.

4. Enter or adjust the default value for the Telnet/SSH timeout. Table 25 shows the setting and default value.

Table 25: *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 26 shows the setting and default value.

Table 26: *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 27 shows the setting and default value.

Table 27: *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, W-AirWave 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 28 describes the settings and default values

Table 28: *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 W-AirWave will not modify any SNMP settings. If SNMP is not already initialized on the Symbol, Nomadix, and Cisco IOS APs, W-AirWave 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 W-AirWave.

Loading Device Firmware Onto the W-AirWave Server (optional)

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

> **NOTE**
> For more information about specifying firmware versions for devices in a group, see "Specifying Minimum Firmware Versions for Devices in a Group" on page 109.

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

The following additional pages support firmware file information:

• Firmware files uploaded to W-AirWave 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 W-AirWave-wide default firmware options.

Table 29 below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

Table 29: *Device Setup > Upload Firmware & Files Fields and Default Values*

Setting	Default	Description
Type	Dell Controller(any model)	Displays a drop-down list of the primary AP makes and models that W-AirWave supports with automated firmware distribution.

Table 29: *Device Setup > Upload Firmware & Files Fields and Default Values (Continued)*

Setting	Default	Description
Owner Role	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server. This can be FTP, TFTP, HTTP, HTTPS. or SCP.
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 W-AirWave 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 W-AirWave. The MD5 checksum is used to verify that the file was uploaded to W-AirWave 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 W-AirWave 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 W-AirWave. The MD5 checksum is used to verify that the file was uploaded to W-AirWave 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 W-AirWave

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

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Select **Add** by the **New Firmware File** option. The Add Firmware File page appears. Figure 21 illustrates this page.

Figure 21: *Device Setup > Upload Firmware and Files > Add Page Illustration*

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 Dell support at **dell.com/support** before installing non-certified firmware.

4. Enter the appropriate information and select **Add**. The file uploads to W-AirWave and once complete, this file appears on the **Device Setup > Upload Firmware & Files** page. This file also appears on additional pages that display firmware files (such as the **Group > Firmware** page and on individual **APs/Devices > Manage** pages).

5. You can also import a CSV list of groups and their external TFTP firmware servers. Table 30 itemizes the settings of this page.

Table 30: *Supported Firmware Versions and Features Fields and Default Values*

Setting	Default	Description
Type	Dell 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, or HTTPS to upload a firmware file. TFTP is recommended. If you select FTP, W-AirWave uses an anonymous user for file upload.

Table 30: *Supported Firmware Versions and Features Fields and Default Values (Continued)*

Setting	Default	Description
Use Group File Server	Disabled	If you opt to use an external firmware file server, this additional option appears. This setting instructs W-AirWave 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. W-AirWave prompts you for additional firmware information as required. For example, Intel and Symbol distribute their firmware in two separate files: an image file and an HTML file. Both files must be uploaded to W-AirWave for the firmware to be distributed successfully via W-AirWave.

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

To delete a firmware file that has already been uploaded to W-AirWave, 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 W-AirWave

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

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

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Click **Add** by the **New Web Auth Bundle** option. This page displays any existing Web Auth bundles that are currently configured in W-AirWave, and allows you to add or delete Web Auth bundles.
3. Select **Add** to create a new Web Auth bundle (see Figure 22), 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 22: *Add Web Auth Bundle Page Illustration*
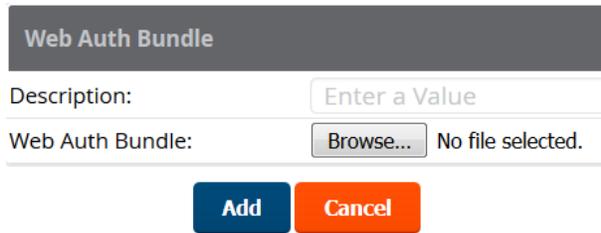
4. Enter a descriptive label in the description field. This is the label used to identify and track Web Auth bundles on the page.

5. 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.

6. 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 the **AMP Setup > Device Type Setup** page, you can define how the device types 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 clicking on a row and dragging and dropping it into a new location, as shown in Figure 23.

Select the checkbox under the **Enabled** column to turn on device setup rules.

Refer to "Monitoring Wired and Wireless Clients" on page 1 for more information on the **Device Type** column that appears in **Clients** list tables.

Figure 23: *AMP Setup > Device Type Setup Page Illustration*

Configuring Cisco WLSE and WLSE Rogue Scanning

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

- "Introduction to Cisco WLSE" on page 60
- "Initial WLSE Configuration" on page 61
- "Configuring IOS APs for WDS Participation" on page 62
- "Configuring ACS for WDS Authentication" on page 63
- "Configuring Cisco WLSE Rogue Scanning" on page 63

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 W-AirWave to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. Table 31 describes these components.

Table 31: *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.

Table 31: *Cisco SWAN Architecture Components (Continued)*

SWAN Component	Requirements
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 W-AirWave:

- "Adding an ACS Server for WLSE" on page 61
- "Enabling Rogue Alerts for Cisco WLSE" on page 61
- "Configuring WLSE to Communicate with APs" on page 61
- "Discovering Devices" on page 61
- "Managing Devices" on page 62
- "Inventory Reporting" on page 62
- "Defining Access" on page 62
- "Grouping" on page 62

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), user name, password, and a 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 63.

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

Use these pages to make such configurations:

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

Inventory Reporting

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

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

Defining Access

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

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

Grouping

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

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

Configuring IOS APs for WDS Participation

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

- Primary WDS
- Backup WDS
- WDS Member

W-AirWave 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 user name 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 user name 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 the host name and IP address associated with the AP and 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 Cisco WLSE Rogue Scanning

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

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

1. To add a Cisco WLSE server to W-AirWave , navigate to the **AMP Setup > WLSE** page and select **Add**. Complete the fields in this page. Table 32 describes the settings and default values.

Table 32: *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 W-AirWave uses to communicate with the WLSE server.
Username	None	Defines the user name W-AirWave uses to communicate with the WLSE server. The user name and password must be configured the same way on the WLSE server and on W-AirWave. The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow W-AirWave to pull the necessary XML APIs.
Password	None	Defines the password W-AirWave uses to communicate with the WLSE server. The user name and password must be configured the same way on the WLSE server and on W-AirWave. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow W-AirWave to pull the necessary XML APIs.
Poll for AP Discovery; Poll for Rogue Discovery	Yes	Sets the method by which W-AirWave uses WLSE to poll for discovery of new APs and/or new rogue devices on the network.
Polling Period	10 minutes	Determines how frequently W-AirWave polls WLSE to gather rogue scanning data.

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

What Next?

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

Configuring ACS Servers

This is an optional configuration. The **AMP Setup > ACS** page allows W-AirWave to poll one or more Cisco ACS servers for wireless user name information. When you specify an ACS server, W-AirWave gathers information about your wireless users. Refer to "Setting Up Device Types" on page 59 if you want to use your ACS server to manage your W-AirWave users.

Perform these steps to configure ACS servers:

1. Go to the **AMP Setup > ACS** page. This page displays current ACS setup, as illustrated in Figure 24.

Figure 24: *AMP Setup > ACS Page Illustration*
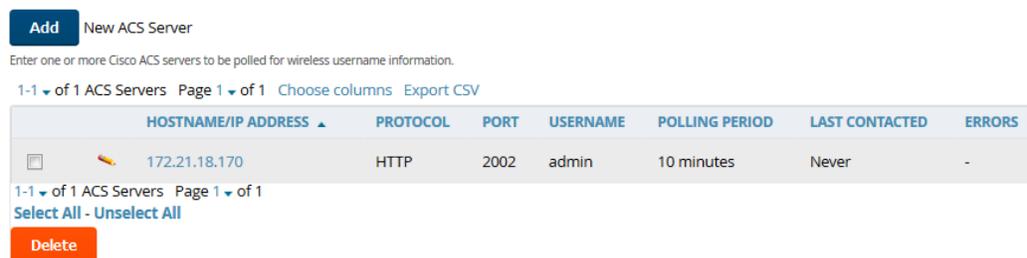
2. Select **Add** to create a new ACS server, or select a pencil icon to edit an existing server. To delete an ACS server, select that server and select **Delete**. When selecting **Add** or **Edit**, the **Details** page appears.

3. Complete the settings on **AMP Setup > ACS > Add/Edit Details**. Table 33 describes these fields:

Table 33: *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 W-AirWave uses when it polls the ACS server.
Port	2002	Sets the port through which W-AirWave communicates with the ACS. W-AirWave generally communicates over port 2002.
Username	None	Sets the user name of the account W-AirWave uses to poll the ACS server.
Password	None	Sets the password of the account W-AirWave uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently W-AirWave polls the ACS server for user name 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 include the two columns W-AirWave requires: **User-Name** and **Caller-ID**.

What Next?

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

Integrating NMS Servers

You can integrate W-AirWave with Network Management System (NMS) servers. Doing so enables W-AirWave to forward SNMP traps to the NMS.

Add an NMS Server

AirWave communicates with the NMS server using the SNMPv1, SNMPv2c, or SNMPv3 protocol over Port 162.

To integrate an NMS server with W-AirWave:

1. Go to **AMP Setup > NMS**, then click **Add**.
2. Enter the NMS server hostname or IP address.
3. Use the default port, or you can enter a new port number.
4. Select the SNMP version:
   - SNMPv1 or SNMPv2c, then enter the community string and confirm the string.
   - SNMPv3, then enter the advanced security options (authentication and privacy protocols and passphrases).
5. Click **Add**.

Download the MIB Files

The necessary AMP MIB files are available to download from the **AMP Setup > NMS** page.

> **NOTE**
>
> W-AirWave provides integration with HP ProCurve Manager (PCM). For help loading the integration files, navigate to **AMP Setup > NMS**, then click the HP ProCurve Manager Integration link.

PCI Compliance Monitoring

W-AirWave provides compliance monitoring tools that can help your organization be prepared for a PCI Data Security Standard (DSS) audit. With use of W-AirWave, your organization can monitor firewalls, network devices, and other services to show PCI compliance.

Check Compliance

The PCI compliance report displays which requirements W-AirWave monitors, provides links to device management pages, and displays any actions required to resolve compliance failures. In addition to displaying pass or fail status, W-AirWave provides diagnostic information and recommends actions required to achieve Pass status when sufficient information is available.

Figure 25: *PCI Compliance Report Example*

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

Gateway	
Host Controller IP Address	
Host Controller Name	

You can find the PCI compliance report for a device by navigating to **APs/Devices > List**, hovering the pointer over a device, and clicking **Compliance** from the shortcut menu, as shown in . If you created a PCI compliance report from the **Reports Definition** page, W-AirWave displays the report on the **Generated Reports** page when it is available. For information, see "Viewing, Running, and Deleting Reports" on page 1.

You can schedule, view, and re-run custom PCI compliance reports. For information about working with reports, see "Creating, Running, and Sending Reports" on page 264.

Enabling PCI Compliance Monitoring

When you enable PCI compliance monitoring, W-AirWave displays real-time information and generates PCI compliance reports that can be used to verify whether a merchant is compliant with a PCI requirement.

For information security standards, refer to the *PCI Quick Reference Guide*, accessible online from the PCI Security Council Document Library or see "Supported PCI Requirements" on page 68.

To enable PCI auditing:

1. Navigate to the **AMP Setup > PCI Compliance** page.
2. Find the PCI requirement that you want to monitor.

3. Click ✎ to open the Default Credential Compliance page. The compliance settings vary depending on the PCI requirement.

4. Select **Save**.

5. To view and monitor PCI auditing on the network, use generated or daily reports. See "Creating, Running, and Sending Reports" on page 264. 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.

Supported PCI Requirements

W-AirWave currently supports the PCI 3.0. requirements described in Table 34. When the requirements are disabled, W-AirWave does not check for PCI compliance or report on status.

> **NOTE**
>
> W-AirWave users without RAPIDS visibility will not see the 11.1 PCI requirements in the PCI compliance report.

Table 34: *PCI Requirements*

Requirement	Description
1.1	Establishes firewall and router configuration standards. A device fails if there are mismatches between the desired configuration and the configuration on the device.
1.2.3	Monitors firewall installation between any wireless networks and the cardholder data environment. A device fails if the firewall is not stateful.
2.1	Changes vendor-supplied default passwords before a device connects to the cardholder data environment or transmits data in the network. A device fails if the user name, passwords or SNMP credentials used by W-AirWave are on the list of forbidden default credentials. The list includes common vendor default passwords.
2.1.1	Changes vendor-supplied defaults for wireless environments. A device fails if the passwords, SSIDs, or other security-related settings are on a list of forbidden values that W-AirWave establishes and tracks. The list includes common vendor default passwords. The user can input new values to achieve compliance.
4.1.1	Uses strong encryption in wireless networks before sending payment cardholder data across open public networks. A device fails if the desired or actual configuration reflect that WEP is enabled on the network, or if associated users can connect with WEP.
11.1	Uses RAPIDS to identify unauthorized devices. A device fails when a rogue device is detected and unacknowledged, or when there are no rogues discovered in the last three months.
11.4	Uses intrusion-detection or intrusion-prevention systems to monitor traffic. Recent IDS events are summarized in the PCI compliance report or the IDS report.

Introduction to PCI Requirements

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

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

- Payment Card Industry (PCI) Data Security Standard (DSS)
  - PCI Security Standards Council 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

Deploying WMS Offload

The Dell Networking W-Series Wireless LAN Management Server (WMS) feature is an enterprise-level hardware device and server architecture with managing software for security and network policy.

WMS components include:

- Air monitor. This operating mode provides wireless IDS, rogue detection and containment.
- WMS server. This server manages devices and network activity, such as rogue detection and network policy enforcement.
- W-AirWave WebUI. This graphical user interface (GUI) provides access to the WMS offload feature.

Refer to the *Dell Networking W-W-AirWave 8.2.4 Best Practices Guide* at **dell.com/support/manuals** for additional information, including detailed concepts, configuration procedures, restrictions, ArubaOS infrastructure, and W-AirWave version differences in support of WMS Offload.

WMS Offload Configuration

WMS offload places the burden of the WMS server data and GUI functions on W-AirWave. WMS master controllers provide this data so that W-AirWave can support rigorous network monitoring capabilities.

WMS Offload is supported with ArubaOS Version 2.5.4 or later and AirWave Version 6.0 or later

Follow these steps to configure WMS offload:

1. Configure WLAN switches for optimal W-AirWave monitoring:
   a. Disable debugging.
   b. Ensure the W-AirWave server is a trap receiver host.
   c. Ensure proper traps are enabled.
2. Configure W-AirWave to optimally monitor the W-AirWave infrastructure:
   a. Enable WMS offload on the **AMP Setup > General** page.
   b. Configure SNMP communication.
   c. Create a proper policy for monitoring the W-AirWave 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:
   - Dell Networking W-Series ArubaOS
   - RF Plan

6. Use RTLS for increasing location accuracy (optional):
   a. Enable RTLS service on the W-AirWave server.
   b. Enable RTLS on ArubaOS infrastructure.

Integrating External Servers

W-AirWave supports integration with Juniper, Brocade or HPE Intelligent Management Center (IMC) servers. When a device is monitored by W-AirWave and an external server, the **APs/Devices > Monitor** page for that device provides a link to that external server.

Add a Juniper Network Director

W-AirWave supports integration with Juniper Network Director (ND) 2.0. Once integrated, the **APs/Devices > Monitor** page for that device provides access to a link the Juniper Network Director WebUI.

To integrate Juniper Network Director with W-AirWave:

1. Log in to W-AirWave, then navigate to **AMP Setup > External server**.
2. In the **Juniper Network Director** section, enter the IP address or hostname of the Juniper Network Director.
3. Click **Save**.

Add a Brocade Network Advisor

W-AirWave can monitor and secure Brocade wired networks, while Brocade Network Advisor monitors Aruba networks. Once integrated, the Brocade Network Advisor appears in the **Devices** list on the W-AirWave **APs/Devices > List** page, and the **APs/Devices > Monitor** page for that device provides access to the Brocade Network Advisor home page.

To integrate Brocade Network Advisor with W-AirWave:

1. Log in to W-AirWave, then navigate to **AMP Setup > External server**.
2. In the **Brocade Network Advisor** section, enter the IP address or hostname of the Brocade Network Advisor.
3. Click **Save**.

Add an HPE Intelligent Management Center

When a managed device is monitored by both W-AirWave and the HPE Intelligent Management Center (IMC) Enterprise Software Platform, the **APs/Devices > Monitor** page for that device includes a link to the IMC server.

Figure 26: *IMC Link on the APs/Devices > Monitor page*

To integrate an IMC server with W-AirWave:

1. Log in to W-AirWave, then navigate to **AMP Setup > External server**.

2. In the **Intelligent Management Center** section, enter the IP address or hostname of the IMC server.

3. (Optional) Click the **IMC Protocol** drop down list and select the **HTTPS** or **HTTP** protocol. The default setting is **HTTPS**.

4. (Optional) Enter a port number in the **IMC Port** field. The default port number is **8443**.

5. Enter the user name for accessing the IMC server, then confirm this password.

6. Click **Save**.

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

If the any of the **Groups** pages described in Table 35 do not appear in the navigation bar, and you want to configure settings on a hidden page, select the group from the **Groups > List** page, navigate to **Groups > Basic**, then choose the **Show Device Settings for: All Devices** option in the **Group Display Options** section of the **Groups > Basic** page. The next time you select the group from the **Groups > List** page, all available configuration options appear

Figure 27: *Subtabs under the Group tab*
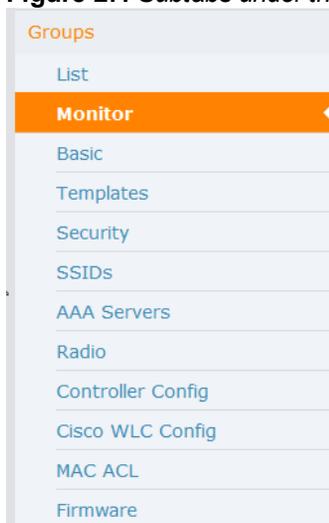
Table 35: *Groups pages*

Menu Item	Description	Refer to
List	This page is the default page in the **Groups** section of W-AirWave. It lists all groups currently configured in W-AirWave and provides the foundation for all group-level configurations.	"Viewing All Defined Device Groups" on page 75
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
Basic	This page appears when you create a new group on the **Groups > List** page. Once you define a group name, W-AirWave displays the **Basic** page from which you configure many group-level settings. This page remains available for any device group configured in W-AirWave.	"Configuring Basic Group Settings" on page 76

Table 35: *Groups pages (Continued)*

Menu Item	Description	Refer to
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, HPE, 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 87
SSID	This page sets SSIDs, VLANs, and related parameters in device groups. Use this submenu is available when you configure RADIUS servers on the **Groups > AAA Servers** page.	"Configuring Group SSIDs and VLANs" on page 92
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 86
Radio	This page defines general 802.11 radio settings for device groups.	"Configuring Radio Settings for Device Groups" on page 95
Controller Config	This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Dell Networking W-Series devices on the network. Use this page as an alternative to the **Device Setup > Dell Networking W > Configuration** page. The appearance of this page varies depending on whether W-AirWave is configured for global configuration or group configuration.	*Dell Networking W-Series Controller Configuration Guide*
Instant Config	This page manages Dell Networking W-Instant devices on the network.	*Dell Networking W-Series Instant User Guide*
Cisco WLC Config	The **Groups > Cisco WLC** page appears in the navigation bar if the you navigate to **Groups > List** and select a group that contains Cisco WLC devices. 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 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 99
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 106.

Table 35: *Groups pages (Continued)*

Menu Item	Description	Refer to
Proxim Mesh	This page defines mesh AP settings specific to Proxim devices when present.	"Configuring Proxim Mesh Radio Settings" on page 107
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 109
Firmware	This page manages firmware files for many device types.	"Specifying Minimum Firmware Versions for Devices in a Group" on page 109
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**.	"Comparing Device Groups" on page 111

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

- "Deleting a Group" on page 113
- "Changing Multiple Group Configurations " on page 113
- "Modifying Multiple Devices" on page 115
- "Using Global Groups for Group Configuration" on page 117

W-AirWave 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. W-AirWave 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:

- W-AirWave allows certain settings to be managed efficiently at the Group level, while others are managed at an individual device level.
- W-AirWave 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 W-AirWave *Global Groups* feature, which lets you create Global Groups with configurations that are pushed to individual Subscriber Groups.

The columns in the default view of the **Groups > Monitor** page is defined in Dell Networking W-AirWave and cannot be modified. However, you can create a new view of this page that returns custom information based on the filter parameters and data columns you selected when creating that new view. For more information about creating filtered views, see *Dell Networking W-AirWave 8.2.4 User Guide* .

Viewing All Defined Device Groups

To display a list of all defined groups, browse to the **Groups > List** page, illustrated in Figure 28.

Figure 28: *Groups > List Page Illustration (partial view)*

		NAME ▲	CHANGES	SSID	TOTAL DEVICES	DOWN	MISMATCHED	IGNORED	CLIENTS	USAGE	VPN SESSIONS	UP/DOWN STATUS POLLING PERIOD	DUPLICATE
	✎	Access Points		-	71	48	37	2	0	-	0	5 minutes	
	✎	IGC		-	0	0	0	0	0	-	0	5 minutes	
	✎	IGC-Test	Unapplied Changes	-	0	0	0	0	0	-	0	10 minutes	

Table 36 describes the columns in the **Groups > List** page.

Table 36: *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 76.
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 29 in "Configuring Basic Group Settings" on page 76.)
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).

Table 36: *Groups > List Columns (Continued)*

Column	Description
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 W-AirWave from a Master Console.
Global Group	Specifies which group this Subscriber Group is using as its template.
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, W-AirWave 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. (Dell configuration settings will have to be manually added back.)

NOTE: When you first configure W-AirWave, there is only one default group labeled **Access Points**. If you have no other groups configured, refer to "Configuring Basic Group Settings" on page 76.

Configuring Basic Group Settings

The first default device group set up in W-AirWave 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.

There are three ways to navigate to the Basic Group Settings page.

- Select **Add** on the **Groups > List page** to create a new group, then enter a group name and click **Add**. The **Groups > Basic** page appears.
- Navigate to **Groups > List**, select a group from the **Groups** table, then navigate to **Groups > Basic**.
- Navigate to **Groups > List** and select the **manage** (wrench) icon next to the group. If you mouse over an existing group's wrench, a pop up menu displays, allowing you to select options such as **Basic**, **Templates**,

Security, **SSIDs**, **AAA Servers**, **Radio**, **Controller Config**, **Instant Config**, and **Cisco WLC Config**. See Figure 29.

NOTE

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

Figure 29: *Pop-up When Hovering over Wrench Icon in the Groups > List Page*

Basic Configuration Settings

Table 37 describes the available settings and default values in the **Basic** section of the **Group > Basic** page.

Table 37: *Basic Group Fields and Default Values*

Setting	Default	Description
Name	Defined when first adding the group	Displays or changes the group name. As desired, use this field to set the 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 W-AirWave 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 W-AirWave, 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 W-AirWave to talk to the devices on a different IP address than the one configured on the device. **NOTE:** If enabled, the LAN IP Address listed on the **AP/Devices > Manage** configuration page under the **Settings** area is different than the IP Address under the **Device Communication** area.
Audit Configuration on Devices	Yes	Auditing and pushing of configuration to devices can be disabled on all the devices in the group. Once disabled, all the devices in the groups will not be counted towards mismatched devices.

Global Group Settings

The W-AirWave group configuration feature allows you to push configurations defined on a global group to other managed groups subscribed to that global group. describes the settings and default values of in the **Global Groups** section of the **Group> Basic** page.

Table 38: *Global Groups Fields and Default Values*

Setting	Default	Description
Is Global Group	No	If set to **Yes**, then this group can be selected in the Use Global Group drop down menu for future group configurations. For more information, refer to"Using Global Groups for Group Configuration" on page 117 .
Global Group	No	If you have defined one or more global groups, this field appears in the Global Settings for for the other (non-global) groups. Click this drop-down list select a global group to which this (non-global) group should be associated. For more information, refer to "Subscribing other Groups to a Global Group" on page 118 .

SNMP Polling Periods

Use the configuration options in the **SNMP Polling Periods** section of the **Groups > Basic** page to override default SNMP polling settings. Table 39 describes the SNMP polling options.

Table 39: *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 Period	10 minutes	Sets the interval at which W-AirWave polls for radio monitoring and 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.

Table 39: *SNMP Polling Periods Fields and Default Values (Continued)*

Setting	Default	Description
CDP Neighbor Data Polling Period	30 minutes	Sets the frequency in which this group polls the network for Cisco Discovery Protocol (CDP) neighbors.
Mesh Discovery Polling Period	15 minutes	Sets time between SNMP polls for Mesh Device Discovery.

Routers and Switches

The settings in the **Routers and Switches** section of the **Groups > Basic** page define the frequency in which W-AirWave polls all devices in the group. These options can be disabled entirely as desired. Table 40 describes the configurable poll settings for routers and switches.

Table 40: *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.
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.

Notes

Use this optional section to record additional information and comments about the group.

Group Display Options

The available W-AirWave configuration settings for a group of managed or monitored devices can vary, depending upon the type of device being configured. Use the **Group DisplayOptions** section of the **Groups > Basic** page to define the types of configuration settings that will appear for the selected group. Table 41 describes these settings and their default values.

Table 41: *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**—W-AirWave displays all Group tabs and setting options. ● **Only devices in this group**—W-AirWave 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 W-AirWave. ● **Use system defaults**—Use the default settings on **AMP Setup > General** ● **Selected device types**—Allows you to specify the device types for which W-AirWave 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.

Automatic Static IP Assignment

Use the **Automatic Static IP Assignment** section on the **Groups > Basic** configuration page to automatically assign a range of static IP addresses to new devices as they are added into the group. If you select **Yes** for the A**ssign Static IP Addresses to Devices** option, additional fields appear. Table 42 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 42: *Automatic Static IP Assignment Fields and Default Values*

Setting	Default	Description
Assign Static IP Addresses to Devices	No	Specify whether to enable W-AirWave 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 Address	none	Sets the first address W-AirWave assigns to the devices in the Group.
Number of Addresses	none	Sets the number of addresses in the pool from which W-AirWave 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.

Spanning Tree Protocol

Use the **Spanning Tree Protocol** settings on the **Groups > Basic** page to configure the Spanning Tree Protocol on Wireless LAN Controller (WLC) devices and Proxim APs. Table 43 describes the settings and default values in this section.

Table 43: *Spanning Tree Protocol Fields and Default Values*

Setting	Default	Description
Spanning Tree Protocol	No	Specify whether to enable or disable 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.

NTP

Use the **NTP Settings** section of the **Groups > Basic** page to define an NTP server and configure Network Time Protocol (NTP) settings. Table 44 describes the NTP settings and default values.

Table 44: *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 W-AirWave graphs and logs use the time set on the W-AirWave server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim section of the **Groups > Basic** configuration page.

HPE Aruba/OfficeConnect Switch Configuration

W-AirWave automates provisioning of several models of HPE OfficeConnect (Comware) switches, using template-based configuration, zero-touch provisioning (ZTP), and configuration snippets. By default, the full configuration mode is enabled whenever you create a device group. When in full configuration mode, Dell Networking W-AirWave pushes a complete set of changes using a template to the group of devices. With partial configuration mode, you can push a golden configuration to a group that contains factory-default ZTP devices. You can also push any command supported by the switch CLI to the device group regardless of their device state (factory or non-factory).

Table 45: *HPE Aruba/OfficeConnect Switch 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 W-AirWave graphs and logs use the time set on the W-AirWave server.
Daylight Saving Time	No	Enables or disables the advanced daylight saving time settings in the Proxim section of the **Groups > Basic** configuration page.

Aruba/Dell Networking W

To configure settings specific to Dell locate the **Aruba/Dell Networking W** section and adjust these settings as required. Table 46 describes the settings and default values of this section of the **Groups > Basic** page.

Table 46: *Aruba Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by W-AirWave to communicate to the AP.
Offload WMS Database	No	Configures commands previously documented in the Dell Networking W-AirWave 8.2.4 *Best Practices Guide*. When enabled, this feature allows W-AirWave 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**.
Dell Networking W-Series 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.
Manage local configuration on controllers	No	Enables or disables the management of local configuration including audit, push, and import operations.
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 ArubaOScontroller.

Dell Instant

To specify the Dell Instant settings to be applied to this group, locate the Dell Instant settings section of the **Groups > Basic** page and adjust these settings as desired. Table 47 describes the settings and default values.

Table 47: *Virtual Controller Certificate Fields and Default Values*

Setting	Default	Description
Enable Instant GUI Config	No	Select this option to configure your Instant APs via the IGC feature on the **Groups > Instant Config** pages of the W-AirWave WebUI, rather than via Instant template configuration.
Configure AirWave communication settings:	No	If the Enable Instant GUI Config setting is set to No, you can use this option to configure t6he primary (and optionally, secondary) W-AirWave server settings on an Instant AP via template configuration.
Disable auto join mode	No	If you enable the Disable auto join mode setting, then Instant APs will not automatically join a group of Instant APs in W-AirWave when that device becomes active on the network.
HTTPS timeout	5 minutes	the HTTPS timeout for Instant devices is the period for which W-AirWave waits for an Instant heartbeat message. The **Missed SNMP Poll Threshold** in the **Basic Settings** section at the top of the **Groups > Basic** page sets the number of Up/Down SNMP polls that must be missed before W-AirWave considers a device to be down. If, for example, a group of Instant APs your group settings has a **Missed SNMP Poll Threshold** of 1, then an instant AP is considered to be down if there is 1 missed heartbeat during this HTTPS timeout period, which could be anywhere between 1-30 min.
CA Cert	None	Specify a CA certificate for the Instant 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.
Captive Portal Cert	None	Specify a Captive portal certificate for the virtual controller. The fields in this drop down will populate when a certificate of type **Captive Portal Cert** is added in the **Device Setup > Certificates** page.
Captive Portal Logo	None	You can use W-AirWave to download a captive portal logo to your Instant APs. Upload the image (which must be 16k bytes or less) on the **Device Setup > Upload** page, then click the Captive Portal Logo drop down list on the Groups > Basic page to select the image to send to the W-IAPs.
RadSec Server Cert	None	Specify a RadSec 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.
RadSec CA Cert	None	Specify a RadSec 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.

Cisco IOS/Catalyst

Configure settings specific to Cisco IOS/Catalyst. Table 48 describes the settings and default values in this section of the **Groups > Basic** page.

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

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by W-AirWave to communicate to the AP.
Cisco IOS CLI Communication	Telnet	The protocol W-AirWave 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 W-AirWave 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 user name and password fields.

Cisco WLC

Use the Cisco WLC section of the **Groups > Basic** page to configure settings specific to a Cisco Wireless LAN Controllers (WLC). Table 49 describes the settings and default values in this section.

Table 49: *Cisco WLC Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	Sets the version of SNMP used by W-AirWave to communicate to WLC controllers.
CLI Communication	SSH	Sets the protocol W-AirWave 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 105.

Proxim/ Avaya

To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section of the **Groups > Basic** page and adjust these settings as required. The following table describes the settings and default values.

Table 50: *Proxim/Avaya Settings*

Setting	Default	Description
SNMP Version	1	Sets the version of SNMP used by AMP to communicate to the AP.
Enable DNS Client	No	Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select Yes for this setting, additional DNS fields display.
Primary DNS server	Blank	Sets the IP address of the Primary DNS server.

Table 50: *Proxim/Avaya Settings (Continued)*

Setting	Default	Description
Secondary DNS server	Blank	Sets the IP address of the Secondary DNS server.
Default DNS domains	Blank	Sets the default DNS domain used by the AP.
HTTP Server Port	80	Sets this port as the HTTP server port on all Proxim APs in the group.
Country Code	United States	Configures AMP to derive its time settings based on the country of location, as specified in this field.

HP ProCurve

To configure HP ProCurve specific settings, locate the **HP ProCurve** section of the **Groups > Basic** page and adjust these settings as required. The following table describes the settings and default values.

Table 51: *HP ProCurve Settings*

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

Symbol

To configure settings for Symbol controllers, , locate the **Symbol** section of the **Groups > Basic** page and adjust these settings as required. The following table describes the settings and default values.

Table 52: *Symbol Settings*

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

Juniper/3Com/Enterasys/Nortel/Trapeze

To configure SNMP settings for 3Com, Enterasys, Nortel, or Trapeze devices, locate the **Juniper/3Com/Enterasys/Nortel/Trapeze** section of the **Groups > Basic** page and click the **SNMP Version** drop-down list to define the version of SNMP to be supported. The default setting is SNMPv2c.

Universal Devices, Routers and Switches

To configure settings for universal devices on the network, including routers and switches that support both wired and wireless networks,, locate the **Juniper/3Com/Enterasys/Nortel/Trapeze** section of the **Groups > Basic** page and click the **SNMP Version** drop-down list to define the version of SNMP to be supported. The default setting is SNMPv2c.

Automatic Authorization

To control the conditions by which devices are automatically authorized into this group, locate the **Automatic Authorization** settings section of the **Groups > Basic** page and adjust these settings as required. Table 53 describes the settings and default values.

Table 53: *Automatic Authorization Fields and Default Values*

Setting	Default	Description
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.

1. 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.

2. 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.

Adding and Configuring Group AAA Servers

Configure RADIUS servers on the **Groups > AAA Servers** page. Once defined on this page, the **Groups > Security** and **Groups > SSIDs** menus appear in the navigation bar, allowing you to select and configure your RADIUS servers.

NOTE

If the **Groups > AAA Servers** page does not appear in the navigation bar, select the group from the **Groups > List** page, select the **Groups > Basic** page, then choose the **Show Device Settings for : All Devices** option in the **Group Display Options** section of the **Groups > Basic** page.

---

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.

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 54 describes the settings and default values of the **Add/Edit** page.

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

Setting	Default	Description
Hostname/IP Address	None	Sets the IP Address or DNS name for RADIUS Server. **NOTE:** IP Address is required for Proxim/ORiNOCO and Cisco Aironet IOS APs.
Secret and Confirm Secret	None	Sets the shared secret that is used to establish communication between W-AirWave and the RADIUS server. **NOTE:** The shared secret entered in W-AirWave 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.

   W-AirWave 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.

NOTE

TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Cisco WLC Security Parameters and Functions" on page 105.

Configuring Group Security Settings

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

	This page appears in the WebUI after you configure RADIUS servers on the **Groups > AAA Servers** page. Once RADIUS servers are defined, the **Groups> Security** and **Groups > SSIDs** menus appear in the navigation bar, allowing you to select and configure your RADIUS servers.

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 W-AirWave pages. Figure 30 illustrates this page and Table 55 explains the fields and default values.

Figure 30: *Groups > Security Page Illustration (partial)*

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

Setting	Default	Description
VLANs Section		

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

Setting	Default	Description
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 92. 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 90 for information on configuring Encryption.
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in W-AirWave . 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		
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	W-AirWave-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.

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

Setting	Default	Description
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, HPE 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 56 for information regarding configuring encryption.

Table 56: *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.

Table 56: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
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**.
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

Use the **Groups > SSIDs** configuration page to create and edit SSIDs and VLANs that apply to a device group. This configuration page does not appear in the W-AirWave WebUI until *after* you configure a RADIUS server using the **Groups > AAA Servers** page, as described on "Adding and Configuring Group AAA Servers" on page 86.

W-AirWave reports users by radio and by SSID. Graphs on the AP and controller monitoring pages display bandwidth in and out based on SSID. W-AirWave 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.

Perform these steps to create or edit VLANs and to set SSIDs.

The **Groups > SSID** page does not appear in the W-AirWave WebUI until *after* you configure a RADIUS server using the **Groups > AAA Servers** page, as described on "Adding and Configuring Group AAA Servers" on page 86.

N O T E

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

---

1. Go to **Groups > List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups > SSIDs** configuration page. Table 57 describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 57: *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. W-AirWave 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 explained in Table 58.
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 58 describes the settings and default values. Note that the displayed settings can vary.

Table 58: *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 59 describes the available encryption modes. Table 56 in "Configuring Group Security Settings" on page 87 describes configuration settings for each mode.

Table 59: *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 60 describes the settings and default values.

Table 60: *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 61 describes the settings and default values.

Table 61: *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 62 describes the settings and default values.

Table 62: *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.

> 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 31 illustrates this page.

Figure 31: *Groups > Radio Page Illustration*

3. Locate the **Radio Settings** area and adjust these settings as required. Table 63 describes the settings and default values.

Table 63: *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, W-AirWave automatically reboots the APs in the group when the change is implemented.

Table 63: *Groups > Radio > Radio Settings Fields and Default Values (Continued)*

Setting	Default	Description
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.
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 64 describes the settings and default values.

Table 64: *Groups > Radio > Device-Specific Fields and Default Values*

Setting	Default	Description
Load Balancing	No	If enabled, this setting allows client devices associating to an AP with two radio cards to determine which card to associate with, based on the load (# of clients) on each card. **NOTE:** This feature is only available when two 802.11b wireless cards are used in an AP-2000.
Interference Robustness	No	If enabled, this option will fragment packets greater than 500 bytes in size to reduce the impact of radio frequency interference on wireless data throughput.
Distance Between APs	Large	This setting adjusts the receiver sensitivity. Reducing receiver sensitivity from its maximum may help reduce the amount of crosstalk between wireless stations to better support roaming users. Reducing the receiver sensitivity, user stations will be more likely to connect with the nearest access point.
802.11g Operational Mode	802.11b +802.11g	This setting sets the operational mode of all g radios in the group to either b only, g only or b + g.
802.11abg Operational Mode	802.11b +802.11g	This setting sets the operational mode of all a/b/g radios in the group to either a only, b only, g only or b + g.
802.11b Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11g Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
802.11a Transmit Rate	Auto Fallback	This setting specifies the minimum transmit rate required for the AP to permit a user device to associate.
Rogue Scanning	Yes	If enabled, any ORiNOCO or Avaya 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 65 describes the settings and default values.

Table 65: *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 66 describes the settings and default values.

Table 66: *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 SSIDs for 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

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

- Navigate to **Groups > List**, then select a group that has been defined to support Cisco devices. The **Cisco WLC Config** option appears in the subtabs, as shown in Figure 32.

- Navigate to **Groups > List,** and create a new group to support Cisco devices with these steps:

   1. Navigate to the **Groups > List** page, then click **Add**.

   2. to create a new group, enter a group name, and select **Add**. W-AirWave displays the **Groups > Basic** page.

   3. In the **Groups > Basic > Cisco WLC section**, select your Cisco WLC device options.

   4. After you select **Save** or **Save and Apply**, the **Groups > Cisco WLC Config** subtab appears in the navigation pane when you select that group, as shown in Figure 32.

Figure 32: *Cisco WLC Submenu in the Navigation Bar*
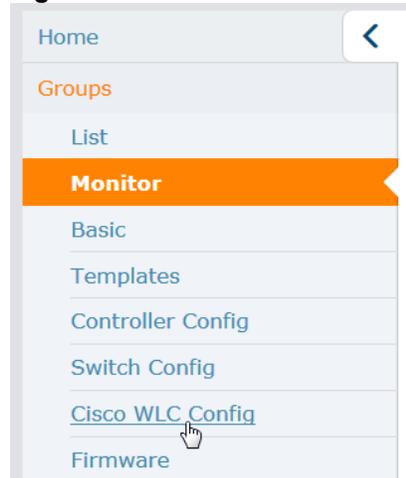
Navigating Cisco WLC Configuration

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 33 and 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 33: *Groups > Cisco WLC Config Page Illustration, collapsed view*
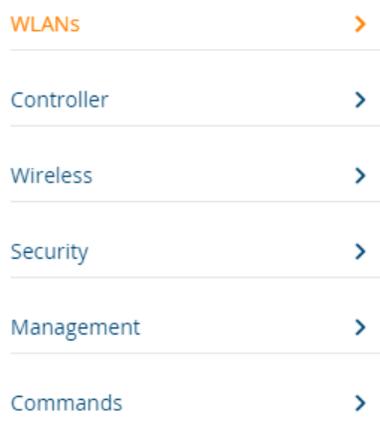
Configuring WLANs for Cisco WLC Devices

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 left navigation pane. 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. 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**, W-AirWave will display a mismatch if the WLANs in the desired config and device config differ only on the order.

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 34: *Add New SSID/VLAN > General Tab Illustration*

Figure 35: *Add New SSID/VLAN > Security Tab Illustration*

Figure 36: *Add New SSID/VLAN > QoS Tab Illustration*

Figure 37: *Add New SSID/VLAN > Advanced Tab Illustration*

Defining and Configuring LWAPP AP Groups for Cisco Devices

The **Groups > Cisco WLC Config > WLANs > Advanced > AP Groups** page allows 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 38 illustrates this page.

Figure 38: *Groups > Cisco WLC Config > WLANS > Advanced > AP Groups Page Illustration*

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 39.

Figure 39: *Groups > Cisco WLC Config > Controller Navigation*
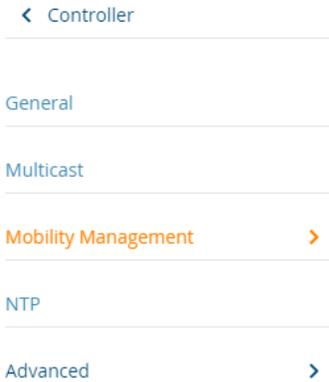
Configuring Wireless Parameters for Cisco Controllers

This section illustrates the configuration of **Wireless** settings in support of Cisco WLC controllers. Select a group with Cisco WLC devices, then navigate to **Groups > Cisco WLC Config**, expand the **Wireless** menu, then expand **Advanced**, **Mesh**, **802.11a/n** and **802.11 b/g/n** menus to display configuration settings for those categories. The navigation for Wireless settings is illustrated in .

Figure 40: *Groups > Cisco WLC Config > Wireless Navigation Illustration*
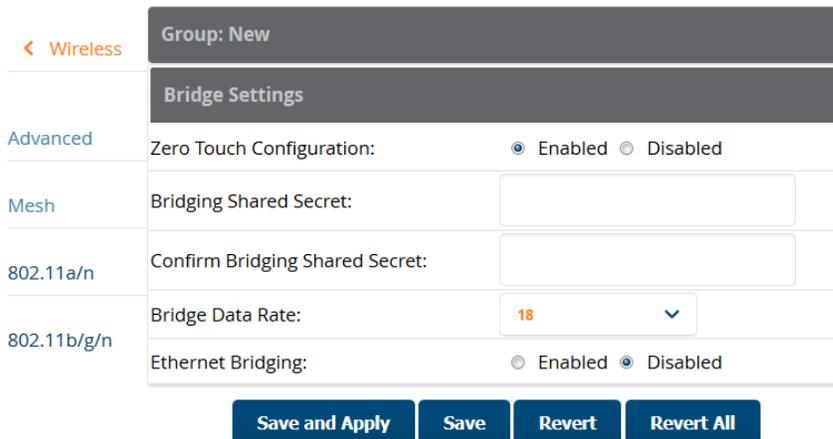
Configuring Cisco WLC Security Parameters and Functions

W-AirWave 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**

illustrates these components and this navigation:

Figure 41: *Groups > Cisco WLC Config > Security Navigation Illustration*

Configuring Management Settings for Cisco WLC Controllers

W-AirWave 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 42.

Figure 42: *Groups > Cisco WLC Config > Management Navigation Illustration*
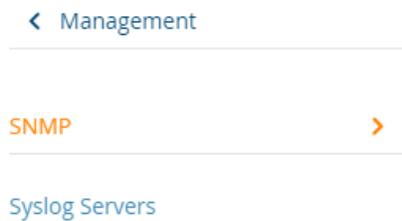
Configuring Group PTMP Settings

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 43 illustrates this page.

Figure 43: *Groups > PTMP Page Illustration*

3. Define the settings on this page. Table 67 describes the settings and default values.

Table 67: *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 44 illustrates this page. The tables that follow describe the settings and default values.

Figure 44: *Groups > Proxim Mesh Page Illustration*

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

Table 68: *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 69: *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 70 describes these settings and default values.

Table 70: *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.

Table 70: *Mesh Cost Matrix Fields and Default Values (Continued)*

Setting	Default	Description
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, W-AirWave 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 45 illustrates this page.

Figure 45: *Groups > MAC ACL Page Illustration*
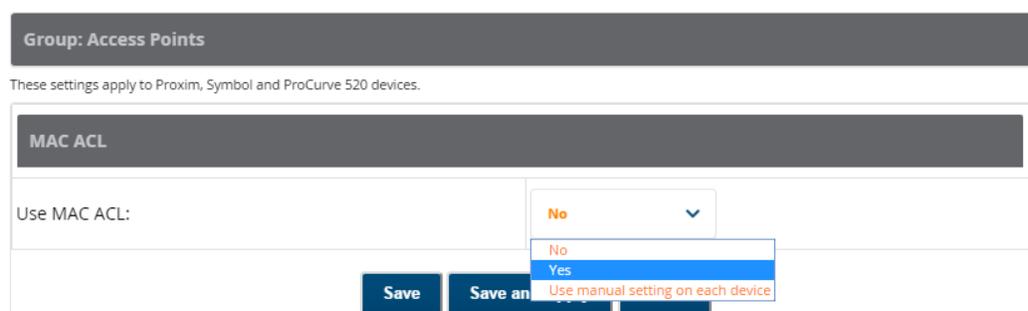
2. Select **Yes** on the **Use MAC ACL** drop-down menu. Enter all authorized MAC addresses, separated by white spaces.

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 Devices in a Group

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

When you add devices into the group in the future, you will be able to upgrade those devices manually. The firmware for an device 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 46 illustrates this page.

Figure 46: *Groups > Firmware Page Illustration (partial view)*

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 W-AirWave.

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 W-AirWave 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 W-AirWave 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.

NOTE

For more information about loading firmware on to an W-AirWave server, see "Loading Device Firmware Onto the W-AirWave Server (optional)" on page 55.

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 W-AirWave, 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 47 illustrates this page.

Figure 47: *Comparing Two Devices Groups on the **Groups > List > Compare** Page (Partial View)*

BASIC			
ACCESS POINTS			**10.20.101.8**
HTTPS Timeout	1	➡	5
Interface Up/Down Polling Period	10 minutes	➡	5 minutes
Manage local configuration on controllers	No	➡	Yes
Spanning Tree Protocol	Yes	➡	No
PTMP			
ACCESS POINTS			**10.20.101.8**
Network Name	(empty string)	➡	Wireless Network
SECURITY			
ACCESS POINTS			**10.20.101.8**
WEP Key Rotation Interval	120	➡	300
WIRELESS → 802.11A/N → CLIENT ROAMING			
ACCESS POINTS			**10.20.101.8**
802.11a Hysteresis	2	➡	3
WIRELESS → 802.11A/N → RRM → DCA			
ACCESS POINTS			**10.20.101.8**
802.11a DCA Channel 100	Disabled	➡	Enabled
802.11a DCA Channel 104	Disabled	➡	Enabled
802.11a DCA Channel 108	Disabled	➡	Enabled
802.11a DCA Channel 112	Disabled	➡	Enabled
802.11a DCA Channel 116	Disabled	➡	Enabled
802.11a DCA Channel 132	Disabled	➡	Enabled

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 W-AirWave 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.) W-AirWave 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. W-AirWave 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. W-AirWave 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. Other group configuration pages may be available, depending upon the type of devices included in that group. 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 48 illustrates the confirmation message that appears.

Figure 48: *Groups > Basic Configuration Change Confirmation Page Illustration*

5. W-AirWave 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 Dell Config changes to other groups. If the only changes on the configuration page are to Dell Networking W-Series 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**. W-AirWave takes the time zone into account for the group if a time zone other than W-AirWave 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

W-AirWave provides a very powerful utility that modifies all APs or a subset of access points unrelated to the typical W-AirWave 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 49 illustrates this page.

Figure 49: *Modify Multiple Devices Section Illustration*

3. Select one or more devices that are to share the configurations. Select the checkbox by each device you want to modify.

4. Click the **Change Device Group/Folder** drop-down menu and select any of the supported changes. Table 71 describes these actions and controls. Any action you take applies to all selected devices.

Table 71: *Modify Multiple Devices Section Fields and Default Values*

Action	Description
System Actions	
Change Device 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. When you select this option, you must also click the **Group** and/or **Folder** drop down menu and select the destination group or folder for the devices. Click **Move** and then select **Apply All** to save your changes.

Table 71: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Poll selected devices	Click **Poll Now** to poll selected devices for current user count and bandwidth data. This action overrides default poll settings for the group. Polling numerous devices may create a temporary performance load on your W-AirWave server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired W-AirWave configuration. The audit action updates the Configuration Status. **NOTE:** In versions of W-AirWave 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, W-AirWave does not show the **Audit** button in the **Modify devices** list.
Delete selected devices	Click **Delete** to remove the selected devices from W-AirWave. A new window opens and asks you to confirm your changes. Select **Apply Changes Now**. The deletions will be performed in the background and it may take a minute to remove the selected devices from the 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 266.
Update the credentials used to communicate with these devices	**Update** changes the credentials W-AirWave uses to communicate with the device. It does *not* change the credentials on the AP.
Import settings from selected devices (and discard current pre-device desired settings)	Audit updates a number of the AP-specific settings that W-AirWave initially read off of the AP including channel, power, antenna settings and SSL certifications. W-AirWave recommends using this setting if APs have been updated outside of W-AirWave. Most settings on the **APs/Devices Manage** configuration page are set to the values currently read off of the devices.
Management Level	When you select this action, you must select either **Monitor Only + Firmware Upgrade** or **Manage Read/Write** to choose new the management level for the devices.
Replace Hardware	Select the down device that will be replaced and view the list of W-AirWave 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.
Planned Downtime Mode	When you select this action, you must select either **Enable** or **Disable** to change the downtime mode for the selected devices. When this option is enabled, the selected devices are put into Planned Maintenance mode. When this mode is enabled, 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.
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.
Device Actions (Dell)	

Table 71: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Dell Networking W AP Group	When you select this option then click Update Dell Networking W AP Group, a new window opens that allows you to assign the devices to a new AP group.
Dell Networking W Instant Virtual Controller Variables	Opens the Variable Editor page for selected Dell Networking W Instant APs.
Import unreferenced Dell Networking W profiles from selected devices	Select the devices that include unreferenced profiles, then click this button to import those profiles from the selected devices.
Reprovision selected Dell Networking W devices	Configures the controller to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning.
Device Actions	
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.
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.
Reboot selected devices	Reboots the selected devices. Use caution when rebooting devices because this can disrupt wireless users.
Factory reset	Resets the selected devices back to factory-default settings.
Desired Radio Status	Enables or disables the radios on the selected device. This parameter does *not* apply to 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.

Using Global Groups for Group Configuration

The W-AirWave group configuration feature allows you to push configurations defined on a global group to the managed groups subscribed to that global group. To apply group configurations using the W-AirWave 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 50 illustrates the **Groups > List** page.

Figure 50: *Groups > List Page Illustration*

Creating a Global Group

To configure a group as a Global Group:

1. Navigate to **Groups > List**.
2. Select a the group from the **Groups** table.
3. Navigate to **Groups > Basic**. The **Global Groups** section of this page contains the **Use Global Group** option.
4. Select **Yes** for the **Use Global Group** option.

When the change is saved and applied, the group will have a checkbox next to fields. Figure 51 illustrates this configuration page.

Figure 51: *Groups > Basic Page for a Global Group (partial view)*

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.

Subscribing other Groups to a Global Group

Once one or more global groups have been configured, other groups may subscribe to a particular Global Group. To subscribe a (non-global) group to a Global Group:

1. Navigate to **Groups > List**.
2. Select a the group from the **Groups** table.
3. Navigate to **Groups > Basic**.

4. In the **Global Groups** section of this page, click the **Global Group** drop-down list and select a global group.

5. Select **Save and Apply** to make the changes permanent. Figure 52 illustrates this page.

Figure 52: *Subscribe to a Global Group*
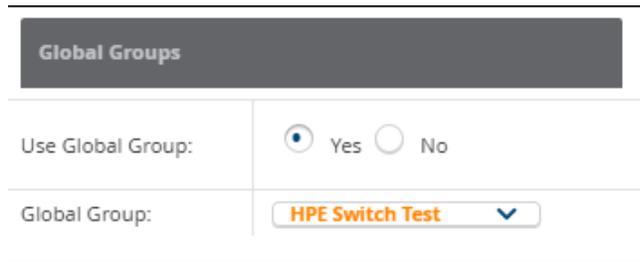
Once the configuration is pushed, the unchecked fields from the Global Group appears on the Subscriber Group as static values and settings. Only fields that had the override checkbox selected in the Global Group appear as fields that can be set at the level of the Subscriber Group. Any changes to a static 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.

Device Discovery Overview

After you have deployed W-AirWave on the network, the next step is to discover all existing devices connected to your network. W-AirWave allows device discovery through SNMP/HTTP scanning and CDP polling of Cisco switches and routers.

SNMP/HTTP Scanning Overview

In order for W-AirWave to discover devices on your network, you must first enable SNMP/HTTP scanning from the **Device Setup > Discover** page and then configure SNMP/HTTP scanning.

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

This process includes:

- "Adding Networks for SNMP/HTTP Scanning" on page 119
- "Adding Credentials for Scanning" on page 120
- "Defining a Scan Set" on page 121
- "Running a Scan Set" on page 121

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.

To add networks for SNMP/HTTP scanning:

1. Go to the **Device Setup > Discover** page.
2. Scroll down to the **Networks** section, and click **Add**.
3. Enter a network name.
4. Enter the IP network range to be scanned. Or, enter the first IP address on the network.
5. Enter the network subnet mask. The largest subnet W-AirWave supports is 255.255.255.0.

6. Click **Add**.

Figure 53 shows an example of adding a scan network called Accounting Network, where the network IP address is 10.52.0.0, and the subnet mask is 255.255.255.0.

Figure 53: *Adding a Scan Network*
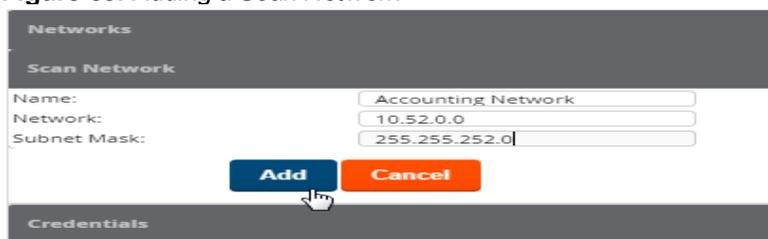
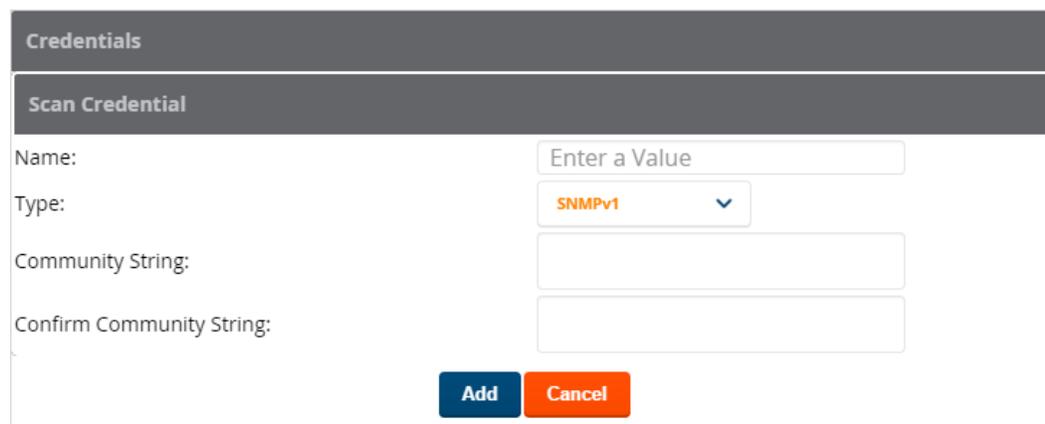W-AirWave displays all network segments in the **Network** section of the **Device Setup > Discover** page.

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 devices 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 54 illustrates this page. (Note that you may have to scroll down the page again to view this section.)

Figure 54: *Device Setup > Discover > Add/Edit New Scan Credential Section Illustration*

3. Enter a name for the credential in the **Name** field (for example, **Default**). This field supports alphanumeric characters (both upper and lower case), blank spaces, hyphens, and underscore characters.

4. Choose the type of scan to be completed (**SNMPv1, SNMPv2,** or **HTTP**). In most cases, perform scans using SNMP for device discovery, but consider the following factors in your decision:

   ● SNMPv1 and SNMP v2 differ between in their supported traps, supported MIBs, and network query elements used in device scanning.

   ● HTTP discovers devices using the HyperText Transfer Protocol in communications between servers and additional network components. HTTP is not as robust in processing network events as is SNMP, but HTTP may be sufficient, simpler, or preferable in certain scenarios.

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 W-AirWave only uses it for discovering devices. To bring devices under management, W-AirWave 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 user name and password for the scan credentials.

> **NOTE**
>
> W-AirWave 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

After you have defined at least one network and one scan credential, you can create a scan set that combines the two for device discovery.

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. W-AirWave 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, .

> **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, W-AirWave can now scan for devices.

To run a scan set:

1. Browse to the **Device Setup > Discover** page and locate the list of all scan sets that have been defined so far. Figure 55 illustrates this page.

Figure 55: *Device Setup > Discover Executing a Scan Illustration*

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 72 describes the scan results and related information.

Table 72: *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 Found	Displays the total number of APs detected during the scan that W-AirWave can configure and monitor. **Total** includes both APs that are currently being managed by W-AirWave 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 W-AirWave 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 56 illustrates this page.

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

Figure 56: *APs/Devices > New Page Illustration*

What Next?

- To authorize one or more devices to a group, see "Management Modes" on page 128.
- To delete a device altogether from W-AirWave, select the corresponding check box for each device, and select **Delete**.
- Dell Networking W-Series thin APs can have Dell Networking W 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. W-AirWave 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.

Management Modes

After W-AirWave discovers devices on your network, you need to add the devices to a group and assign them a management mode. For information about device groups, refer to "Configuring and Using Device Groups" on page 72.

There are two management modes in W-AirWave:

- **Manage Read/Write** mode. In addition to monitoring the device, W-AirWave can push configurations to the device. It does this by comparing the device's current configuration settings to the group's configuration settings, and then sending configuration changes to the device.
- **Monitor Only** mode. W-AirWave only monitors the device, updating the firmware, comparing the current configuration with the policy, and displaying discrepancies on the **APs/Devices > Audit** page. Under no circumstance does W-AirWave change the device's configuration.

⚠ **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. Before you set the management mode for the device, verify that no unexpected or undesired configuration changes will be made to the devices.

You can put devices in **Manage Read/Write** mode using the **APs/Devices > Manage** or the **Modify these devices** link on any list page. However, this procedure describes how to assign a managment mode to a newly discovered device.

To add a device to a device group and set the management mode:

1. Navigate to **APs/Devices > New**. 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 W-AirWave, go to .

> **NOTE**: If you select **Manage Select Devices**, W-AirWave 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 W-AirWave in a subsequent scan. Refer to Assigning Devices to the Ignored Page.

Manually Adding Devices

You can add devices to W-AirWave by uploading a CSV file, or from the **Device Setup > Add** page. The configuration options vary depending on the device and its features. When you select a Cisco or Dell Networking W-Series device, W-AirWave automatically adds the specific make and model information into its database. In several cases, the default values from any given device derive from the **Device Setup > Communication** page.

Table 73 describes the settings on the Add Page.

Table 73: *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 (required). W-AirWave supports IPv4 and IPv6 addresses.
SNMP Port	161	The port W-AirWave uses to communicate with the AP using SNMP.
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 user name and password combination for HTTP and Telnet. Cisco supports multiple community strings per AP.

Table 73: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
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. W-AirWave initially uses this user name and password combination to control the Cisco AP. W-AirWave 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. W-AirWave 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. W-AirWave 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 user name for existing Cisco IOS APs. W-AirWave uses the Telnet user name/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 user name 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. W-AirWave uses the Telnet user name/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 user name 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 W-AirWave to enter **enable** mode on the device.

To manually add devices to W-AirWave:

1. Go to the **Device Setup > Add** page, then select the vendor and model of the device. Figure 57 illustrates this page.

Figure 57: *Selecting the Device*
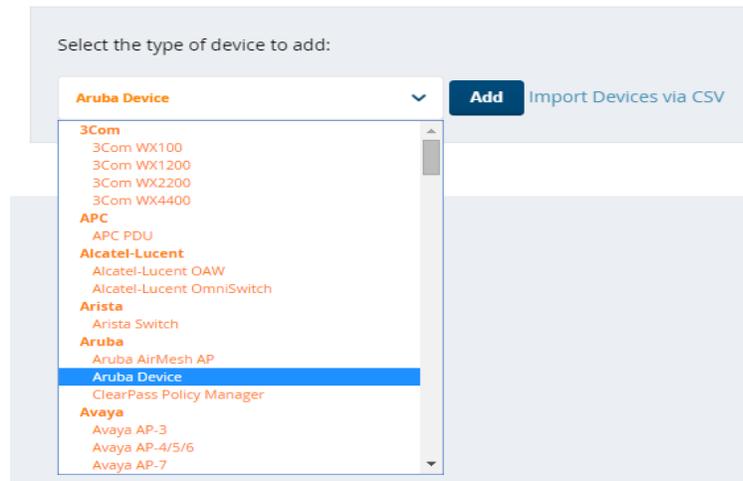
2. Select **Add**, then enter the device communications and location settings for the new device on the Add page (see Table 73 for information about the settings).

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

4. 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 "Management Modes" on page 128.

> **NOTE**
>
> If you select **Manage read/write**, W-AirWave 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.

5. 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 W-AirWave. Here you also have the option of specifying vendor name only, and W-AirWave will automatically determine the correct type while bringing up the device. If your CSV file includes make and model information, W-AirWave 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 user name
- Telnet user name
- 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 58.

Figure 58: *Device Setup > Add > Import Devices via CSV Page Illustration*

Upload a list of devices

Location	
Group:	Access Points ⌄
Folder:	Top ⌄

[Choose File] No file chosen   [Upload]

The list must be in comma-separated values (CSV) format, containing 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
IP Address is required, the others are optional.
Type is a case-insensitive string; you can view a list of device types.

Download a sample file or see the example below:
IP Address,SNMP Community String,Name,Type,Auth Password,SNMPv3 Auth Protocol,Privacy Password,SNMPv3 Privacy Protocol,SNMPv3 Username,Telnet Username,Telnet Password,Enable Password,SNMP Port
10.34.64.163,private,switch1.example.com,Router/Switch,nonradiance,md5,privacy123,aes,sv3user,telnetuser,telnetpwd,enable,161
10.172.97.172,private,switch2.example.com,router/switch,nonradiance,sha,privacy123,des,user 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 W-AirWave.

Adding Universal Devices

W-AirWave 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, W-AirWave 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 W-AirWave 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 W-AirWave that were detailed in "Manually Adding Devices" on page 124.

W-AirWave 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. W-AirWave collects this information and displays it on the **APs/Devices > Monitor** page in the **Interface** section. W-AirWave supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. W-AirWave also monitors sysUptime.

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.

W-AirWave uses SNMP or Telnet to read a device's configuration. SNMP is used for Cisco controllers. Dell Networking W-Series devices and wired routers and switches use Telnet/SSH to read device configuration. See "Individual Device Support and Firmware Upgrades" on page 175 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 W-AirWave.
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. The Audit page shows the device status and lists detailed information for all existing configuration parameters and settings for the device. Figure 1 illustrates this page.

Figure 59: *Audit Page*
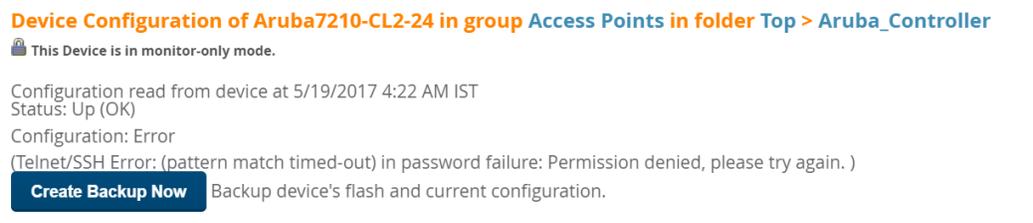
> Group configuration settings display on the right side of the page. If the device is moved from **Monitor** to **Manage** mode, the settings on the right side of the page overwrite the settings on the left.

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.

Management Modes

After W-AirWave discovers devices on your network, you need to add the devices to a group and assign them a management mode. For information about device groups, refer to "Configuring and Using Device Groups" on page 72.

There are two management modes in W-AirWave:

- **Manage Read/Write** mode. In addition to monitoring the device, W-AirWave can push configurations to the device. It does this by comparing the device's current configuration settings to the group's configuration settings, and then sending configuration changes to the device.
- **Monitor Only** mode. W-AirWave only monitors the device, updating the firmware, comparing the current configuration with the policy, and displaying discrepancies on the **APs/Devices > Audit** page. Under no circumstance does W-AirWave change the device's configuration.

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. Before you set the management mode for the device, verify that no unexpected or undesired configuration changes will be made to the devices.

You can put devices in **Manage Read/Write** mode using the **APs/Devices > Manage** or the **Modify these devices** link on any list page. However, this procedure describes how to assign a managment mode to a newly discovered device.

To add a device to a device group and set the management mode:

1. Navigate to **APs/Devices > New**. 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 W-AirWave, go to step 4 on page 129.

NOTE

If you select **Manage Select Devices**, W-AirWave 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 W-AirWave in a subsequent scan. Refer to Assigning Devices to the Ignored Page.

Ignoring Discovered Devices

You might want to ignore a discovered device. If you know that the device will be down temporarily, you can add it to the ignore list and then remove it from the ignored list when it is online again.

If W-AirWave discovers an ignored device in a subsequent scan, it doesn't display the device in the list of new devices on the **AP/Devices > New** page. However, W-AirWave lists a deleted device on this page if it discovers it again.

To ignore a device:

1. Go to the **APs/Devices > New** page.

2. Select the checkbox beside the device, and then select **Ignore Selected Devices** from the drop-down menu (see Figure 60. You can select more than one at a time.

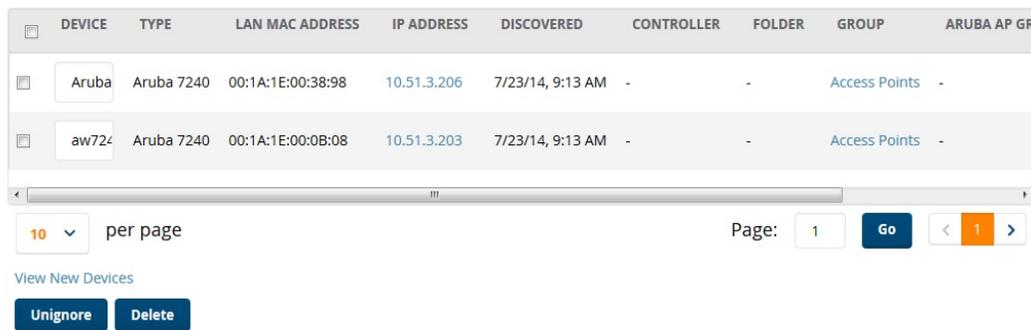**Figure 60:** *APs/Devices > New Page Illustration*
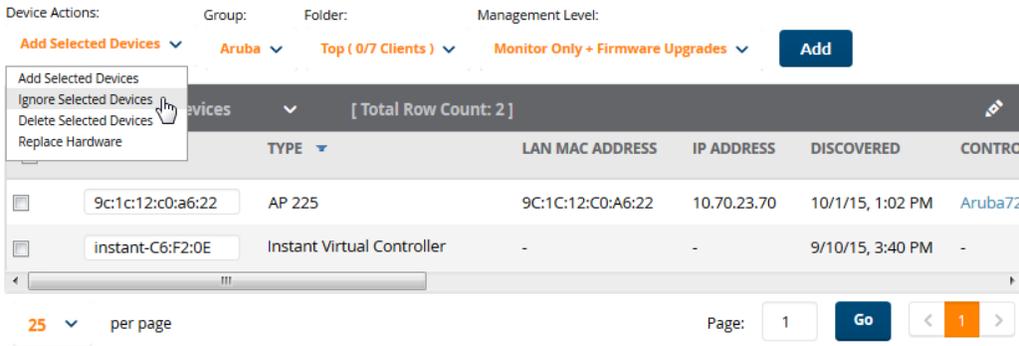
Unignoring a Device

Perform these steps 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 61: *APs/Devices > Ignored Page Illustration*

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 W-AirWave 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.

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 74:

Table 74: *Common System Messages for Down Status*

Message	Meaning
AP is no longer associated with controller	This means the AP no longer shows up in any controller's AP list (on the W-AirWave server). Either the AP was removed from the controller, or it has roamed to another controller that W-AirWave does not have visibility to, or it is offline.
Controller is Down	When a controller goes down, W-AirWave automatically marks all associated thin APs down This is because communication to thin APs are via the controller, and W-AirWave 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	W-AirWave could not fetch a configuration for the device. Usually this is because W-AirWave 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 W-AirWave.
SNMP Trap	W-AirWave 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 user name and password specified for that device is incorrect.
Unexpected LAN MAC Address found at this device's IP address	If W-AirWave 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 W-AirWave. 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 the credentials are incorrect, return to the **Device Communications** area on the **APs/Devices > Manage** page. Enter the appropriate credentials, and select **Apply**.

5. Return to the **APs/Devices > List** page to see if the device appears with a Status of **Up**.

The following sections discuss various monitoring options in W-AirWave:

- "Monitoring Basics" on page 1
- "Monitoring Access Points, Mesh Devices, and Controllers" on page 135
- "Monitoring Switches and Routers" on page 1
- "Monitoring Controller Clusters" on page 155
- "Monitoring Clients" on page 1
- "Troubleshooting Client Issues" on page 1
- "Using Topology" on page 158

Monitoring Overview

You can quickly go to any device's monitoring page by navigating to the device's folder on the **APs/Devices > List** page, and then selecting that device from the Devices List. The information shown on the **APs/Devices > Monitor** pages varies, depending on whether a page is showing information for a wired device such as a router or switch, a controller or WLAN switch, or a thin or fat AP. The information also changes if the device is a mesh device or spectrum analysis is enabled.

For details on the information the **APs/Devices > Monitor** page displays for all managed device types, refer to the following sections:

- "Device Info" on page 132
- "Alert Summary " on page 133
- "Device Events" on page 133
- "Recent AMP Events" on page 133

See also "Monitoring Access Points, Mesh Devices, and Controllers" on page 135 and "Monitoring Switches and Routers" on page 1 for information about monitoring these specific device types.

Device Info

The **APs/ Devices > Monitor** pages for all device types include a **Device Info** section at the top, displaying information such as monitoring/configuration status, serial number, total clients, and firmware version, as shown in Figure 62. The specific information shown in this section varies according to device type.

Figure 62: *Monitoring Page Top Level Data Common to All Device Types*

Alert Summary

The **Alert Summary** table shown in Figure 63 appears at the bottom of the **APs/Devices > Monitoring** page for all device types, and lists information for AMP Alerts, Intrusion Detection System (IDS) Events and RADIUS issues. Click any of these table entries to view a detailed summary of alerts for that alert type. For more information on the contents of these alert summaries, see "About Alerts" on page 229

Figure 63: *Alert Summary on the APs/Devices > Monitor page*

Alert Summary				
TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	1	1	10/12/2016 5:18 PM CST
IDS Events	162	1826	5139	10/13/2016 6:18 AM CST
RADIUS Accounting Issues	0	2	8	10/12/2016 11:12 AM CST
RADIUS Authentication Issues	205	3264	7581	10/13/2016 6:16 AM CST

Device Events

The **Device Events** table shown in Figure 64 displays all SNMP traps and syslog messages sent to W-AirWave for the selected device. Click any link in the **Source Device** column to view the **APs/Devices > Monitor** page for the device that sent the event message to W-AirWave.

Figure 64: *Device Events on the APs/Devices > Monitor page*

Recent AMP Events

The **Recent AMP 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 Event Log" on page 220).

Table 75 describes the fields in this page that display in the **Recent Events** table.

Table 75: *APs/Devices > Monitor > Recent AMP 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 W-AirWave user that submitted them. Automated W-AirWave events are logged as the **System** user.
Event	Displays a short text description of the event.

Using Device Folders

Using folders, you can group your devices in order to manage device reporting, view statistics, and identify status. You *must* use folders if you want to limit the APs and devices W-AirWave users can see.

Adding device folders

To add a device folder:

1. Go to **APs/Devices > List**, scroll to the end of the Devices List and click **Add New Folder** at the bottom of the page.
2. Enter text that describes the folder, such as *APs in Sunnyvale* if you want to organize the folders by device location.
3. Select the parent folder, then click **Add**.
4. Select the parent folder. If the parent folder contains subfolders, you can create a hierarchical structure that is manageable, for example, by location, building name, or room.

   Figure 65 shows how to create the *APs in Sunnyvale* folder.

Figure 65: *Adding a New Folder*
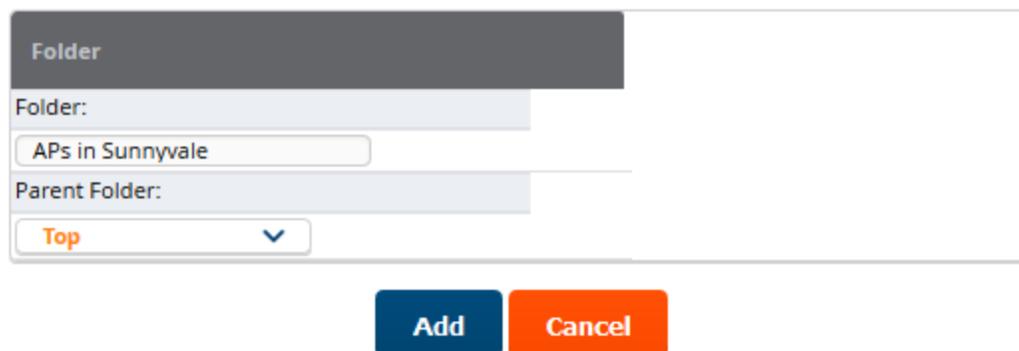
Moving folders

If you want to change the folder hierarchy, W-AirWave lets you move and rename folders.

To move folders:

1. Select the folder you want to move from **Go to folder** at the upper left of the **APs/Devices** page.
2. Scroll to bottom of the page and click 🖊 .
3. Select the new parent folder and click **Save**.

Expanding folders

If you want to see every device in a folder, select **Expand folders to show all devices**. When you expand a folder, W-AirWave displays information about all of the devices in the folder in the Devices List.

For example, if you select the **Top** folder and then click **Down** in the navigation bar, W-AirWave displays all the down devices in the Top folder.

Monitoring Access Points, Mesh Devices, and Controllers

The **APs/Devices > Monitor** page for APs, mesh devices, and controllers 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.

You can click **Poll Now** on the monitoring page to override the preset polling interval and force W-AirWave to immediately poll the network for updates.

> **NOTE**
>
> For information on the monitoring data that appears on the **APs/Devices > Monitor** page for wired devices, see "Monitoring Switches and Routers" on page 1.

Device Information for Access Points, Mesh Devices, and Controllers

> **NOTE**
>
> For descriptions about about the device information for wireless devices, see "Device Information for Switches and Routers" on page 1.

Table 76 describes the fields and information displayed in the **Device Info** section for different models and types of wireless devices.

Table 76: *Device Information for Wireless Devices*

Field	Description
Poll Now	When you select the **Poll Now** button above the **Device Info** section, W-AirWave immediately polls the device or controller. 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 W-AirWave to connect to the device. **Up** (no issue) means everything is working as it should. **Down** (SNMP get failed) means W-AirWave can get to the device but not speak with it using SNMP. Check the SNMP credentials W-AirWave is using the view secrets link on the **APs/Devices > Manage** page and verify SNMP is enabled on the device. Many APs ship with SNMP disabled. **Down** (ICMP ping failed after SNMP get failed) means W-AirWave is unable to connect to the AP using SNMP and is unable to ping the device. This usually means W-AirWave is blocked from connecting to the device or the device needs to be rebooted or reset.
Configuration	• **Good** means all the settings on the AP agree with the settings W-AirWave wants them to have. • **Mismatched** means there is a configuration mismatch between what is on the AP and what W-AirWave 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.

Field	Description
Firmware	Displays the firmware version running on the AP. Newer AirMesh APs include the new bootloader APBoot. W-AirWave helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Licenses (Appears for Dellcontrollers)	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 W-AirWave 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 W-AirWave.
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.
IP Address	Displays the IP address that W-AirWave uses to communicate to the device. W-AirWave supports IPv4 or IPv6 addresses. 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 access the device using HTTP, HTTPs, telnet or SSH. For Dellcontrollers, if Single Sign-On is enabled for your role in this W-AirWave 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.

Field	Description
Quick Links	**Open controller UI :** A drop-down menu that allows you to jump to the controller's WebUI in a new window. For Dellcontrollers, if Single Sign-On is enabled for your role in W-AirWave 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 Mesh Devices" on page 146.

W-AirWave allows you to execute show commands on some models of Aruba or HPE switches by clicking the **Run Command** drop-down list on the **APs/Devices > Monitor** page of the W-AirWave WebUI, and selecting a supported show command. For a list of devices that support show commands via the W-AirWave **APs/Devices > Monitor** page, refer to the W-AirWave*Supported Infrastructure Devices* document. For complete information about the output of each command, refer to the documentation for that switch.

Radios

Table 77 describes the information in the **Radio** table for APs.

Table 77: *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.
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.

Table 77: *APs/Devices > Monitor > Radio Fields and Descriptions (Continued)*

Field	Description
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 .

Wired Interfaces

Devices with wired interfaces (other than Dell Networking W-Instant APs) will display the **Wired Interfaces** table, which is described in Table 78:

Table 78: *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 W-AirWave is able to ping it and fetch SNMP information. If the AP is listed as **Down**, then W-AirWave 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.
Dell 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.

Graphs for Access Points, Mesh Devices, and Controllers

Figure 66 illustrates the interactive graphs available on this page. Use the drop down button next to the graph title to select a different graph.

Figure 66: *Interactive graphs for a Dell controller*
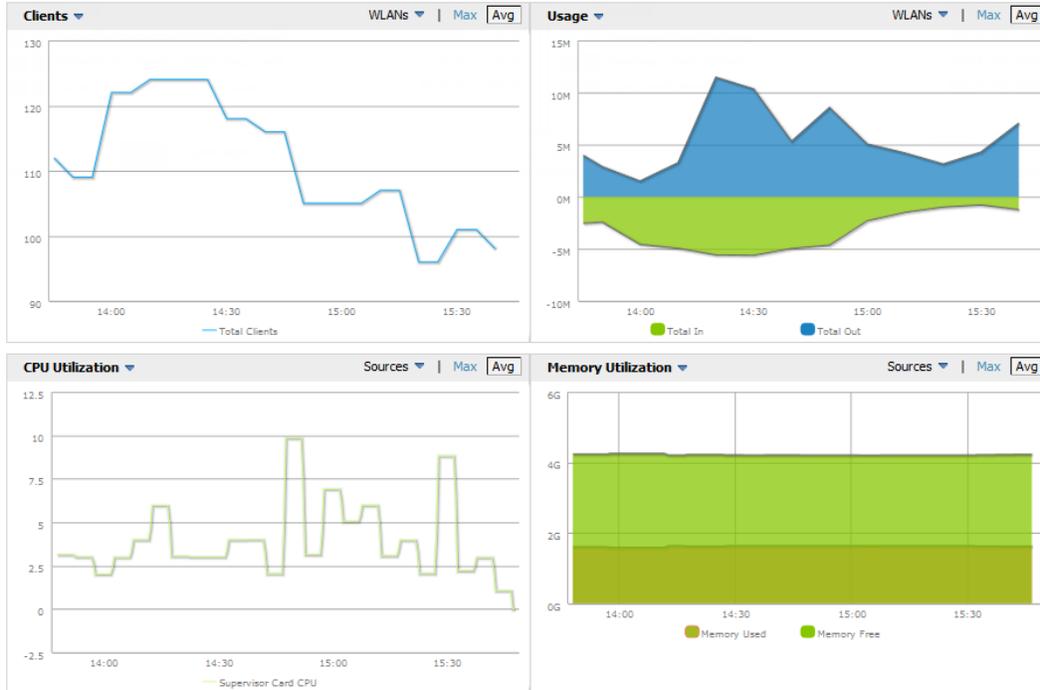
Table 79 describes the graphs on this page.

Table 79: *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 only)	Reports overall CPU utilization (not on a per-CPU basis) of the device.
Memory Utilization (controllers only	Reports average used and free memory and average max memory for the device.

Location

If the device is associated to a VisualRF map, this section of the page displays the device on the map. Click the map to open it in VisualRF.

Connected Clients

Table 80 describes the fields and information displayed for the **Connected Clients** display.

Table 80: *APs/Devices > Monitor > Connected Clients Fields and Default Values*

Field	Description
Username	Provides the name of the User associated to the AP. W-AirWave 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 59.
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 W-AirWave 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 W-AirWave provide the RADIUS Accounting Auth type • **WPA2**—Wi-Fi Protected Access 2 encryption • No Encryption W-AirWave considers all other types as not authenticated. The information W-AirWave 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 W-AirWave. 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 W-AirWave.
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 running Instant releases prior to Instant 4.1.0.
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 running Instant releases prior to Instant 4.1.0.

Table 80: *APs/Devices > Monitor > Connected Clients Fields and Default Values (Continued)*

Field	Description
Location	Displays the VisualRF box that 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. W-AirWave can gather it from the ARP cache of switches discovered by W-AirWave. 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.

RF Neighbors

This table displays information about other devices in the AP's RF neighborhood, including the name of the AP or device, and the neighboring radio channel(s) and RSSI (in dBm) detected by the AP.

CDP Neighbors

The **APs/Devices > Monitoring** page for devices that support Cisco Discovery Protocol (CDP) may display information for neighbor devices detected using CDP.

> **NOTE**
>
> Wireless controllers also include interface-specific data for wired interfaces on the **APs/Devices > Interfaces** page. For more information, see "Monitoring Wired Interface Settings" on page 1.

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 Dell 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 67.

Figure 67: *Links to the Radio Statistics page on APs/Devices > Monitoring for an AP*

Radios									
Index ▲	Name	MAC Address	Clients	Usage (Kbps)	Channel	Tx Power	Antenna Type	Role	SSID
1	802.11bgn	18:64:72:40:B7:80	0	0.00	1	15 dBm	Internal	Access	Keynote
2	802.11ac	18:64:72:40:B7:90	0	0.00	36	15 dBm	Internal	Access	Keynote

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 Dell Networking W-Series set to Spectrum mode), and summarizes major issues.

Viewing Real-Time ARM or AirMatch Statistics

Dell AP Groups that have the **Adaptive Radio Management** (**ARM**) features 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.

View additional ARM or AirMatch statistics from Dell Networking W-Series controllers via the Radio Statistics page by selecting a radio, clicking the **Run a command** drop-down menu and choosing a command, as illustrated in Figure 68.

Figure 68: *Fetch additional radio stats by running a show command*
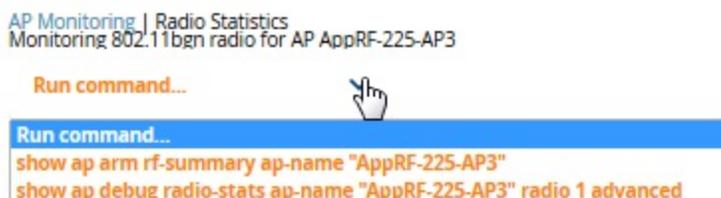
When this command is selected, a new browser window launches with the statistics in plain text. Other ARM-tracked metrics are visible in the **Radio Statistics** page for Dell Networking W-Series APs.

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 81 and illustrated in Figure 69:

Table 81: *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 69: *Issues Summary Section Illustration*

These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the 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 70.

Figure 70: *802.11 Radio Counters Summary table*

802.11 Radio Counters Summary (frames/sec)				
	CURRENT	**LAST HOUR**	**LAST DAY**	**LAST WEEK**
Unacked	5	5	7	7
Retries	0	0	1	0
Failures	0	0	0	0
Dup Frames	0	0	1	2
FCS Errors	36	148	799	1099

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 82: *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 Dell 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.
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 Dell APs, crossing the noise threshold triggers an automatic channel change.

Table 82: *Radio Statistics Interactive Graphs Descriptions (Continued)*

Graph Title	Description
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 Dell APs to dynamically adjust the power toward your acceptable Coverage Index as needed. For more information, see the Adaptive Radio Management chapter of the *Dell Networking W-Series 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	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 *Dell Networking W-AirWave Best Practices Guide* at **dell.com/support/manuals** for details. **NOTE:** (Dell Networking W and Cisco WLC thin APs on supported firmware versions only)
Goodput	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 retry effort taken for both successful and dropped frames.

Figure 71: *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 W-AirWave is enabled as a trap host (see the *Dell Networking W-AirWave Best Practices Guide* at **dell.com/support/manuals** 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 72.

Figure 72: *ARM Events Table Illustration*

The columns and values are described in .

Table 83: *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 W-AirWave 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 Dell Networking W-Series 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 . This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

Figure 73: *Detected Interfering Devices Table Illustration*

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 74. This table appears only for Dell Networking W-Series AP radios.

Figure 74: *Active BSSIDs Table Illustration*

Monitoring 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 75: *APs/Devices > Monitor page for a Mesh Device*
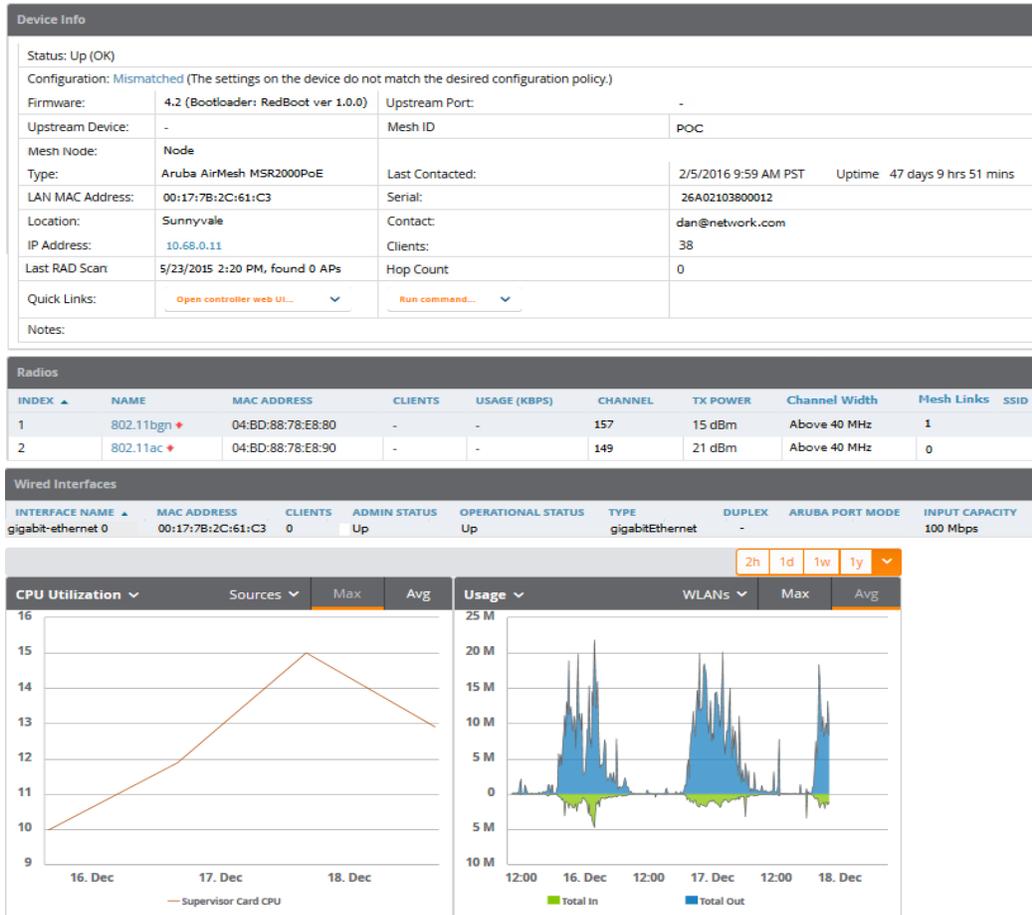
These fields are described in detail in "Viewing Device Monitoring Statistics" on page 1.

Setting up Spectrum Analysis

The spectrum analysis software modules available on many Dell Networking W-Series APs 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 Dell'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, including a list of APs that support spectrum analysis refer to the *Dell Networking W-Series ArubaOS User Guide* at **dell.com/support/manuals**.

Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in Spectrum mode in W-AirWave:

- 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.
- Dell Networking W 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 W-AirWave:

- Dell Networking W AP Groups running permanently with the default Spectrum profile
- Individual APs running temporarily in Spectrum mode while part of a Dell Networking W AP Group set to ap-mode
- Controller-level Spectrum Overrides (an alternative to creating new Dell Networking W AP groups or new radio profiles for temporary changes)

Setting up a Permanent Spectrum Dell AP Group

If you have multiple supported Dell Networking W-Series APs in multiple controllers that you want to run in Spectrum mode over the long run, you create a special Dell Networking W 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 Dell Networking W 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 Dell Networking W 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 Dell 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 76, and then select **Save**.

Figure 76: *Spectrum mode in Controller Config*
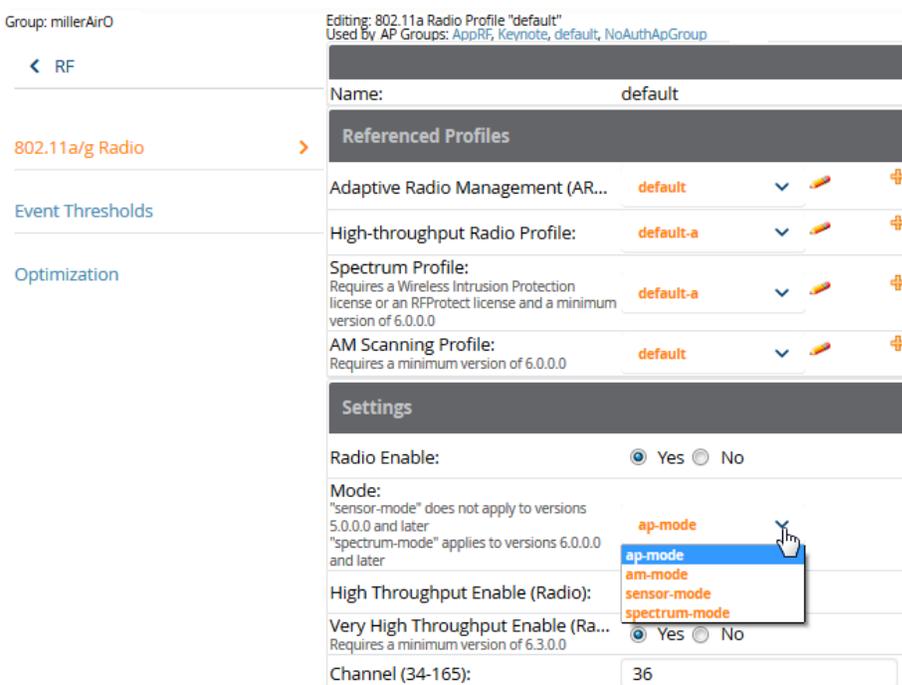
The above steps will use the defaults in the referenced **Spectrum Profile**. In most cases, you should not change the settings in the default profile. If you must change the defaults, however, navigate to **Groups > Controller Config > Profiles > RF > 802.11a/g Radio > Spectrum** page, and create a new Spectrum profile with non-default settings.

If all of the devices in this Dell Networking W 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 Dell Networking W AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Dell Networking W-Series 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 77: *Spectrum Analysis on Controller Dashboard*
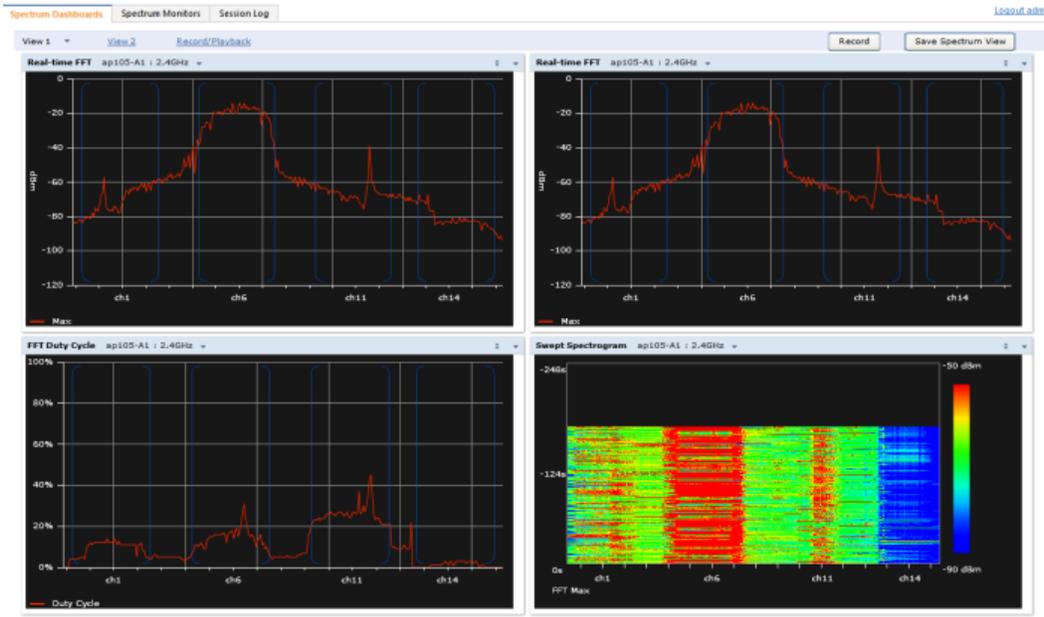
To disable Spectrum mode on this individual AP after it has collected data, return to the **APs/Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

Configuring a Controller to use the Spectrum Profile

You can use W-AirWave to customize individual fields in the profile instance used by a particular controller without having to create new Dell Networking W AP groups and new radio profiles. To do this, you can set a controller-level override for its referenced Spectrum profile on the **APs/Devices > Manage page**, as illustrated in Figure 78. This will affect all Spectrum-supported APs managed by this controller.

Figure 78: *Override Section of a Supported Controller's Manage Page*
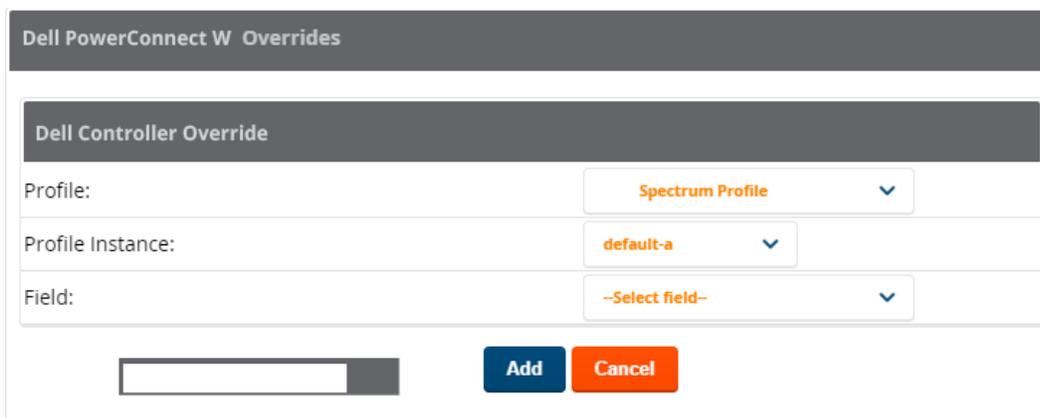
Perform these steps to override individual profile settings for a Dell Networking W-Series controller that is part of a spectrum-mode Dell Networking W AP group:

1. Select a Spectrum-supported Dell Networking W-Series 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 Dell Networking W Overrides section, click the **Add New Dell 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.

Monitor Wired Devices

The monitoring page for wired devices routers and switches includes device information, and graphs.

You can navigate to the monitoring page by selecting **APs/Devices > Monitor**. Figure 79 shows part of a monitoring page for a switch.

To change the graphs, click the arrow by the graph title and select one of the following:

- Usage.
- CPU Utilization.
- Memory Utilization.

Figure 79: *Monitoring Page for a Switch*

Monitoring Wired Interfaces

All managed wired devices also include interface-specific data on the **APs/Devices > Interfaces** tab, as shown in Figure 80.

Figure 80: *APs/Devices > Interfaces Page for Wired Devices (partial view)*

The **Interfaces** page includes a summary of all the device interface, including **Up/Down** status, client and bandwidth Information. For stacked switches, the master switch displays information for the interfaces of all the members, including its own. The physical and the virtual interfaces are displayed in separate **Physical Interfaces** and **Virtual Interfaces** tables. VLANs are listed in the **VLAN** table below the interface tables.

You can change the **Auto-Detect Interface Capacity** or the **Interface Label** settings by selecting the **Edit Interfaces** link at the top of these tables, or by clicking the edit (pencil) icon beside each interface name. Interface labels are used to group one or more interfaces for the purpose of defining interface bandwidth triggers.

> **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

View Individual Interface Statistics

Select any interface name in the **Physical Interface** or **Virtual Interface** tables on the **APs/Devices > Interfaces** page to display the **APs/Devices > Interface Monitoring** page, which displays **Usage** and **Interface Frame Counte**r charts for the selected interface, as well as a list of any connected clients.

Figure 81: *Interface Statistics on the APs/Devices > Interface Monitoring Page*
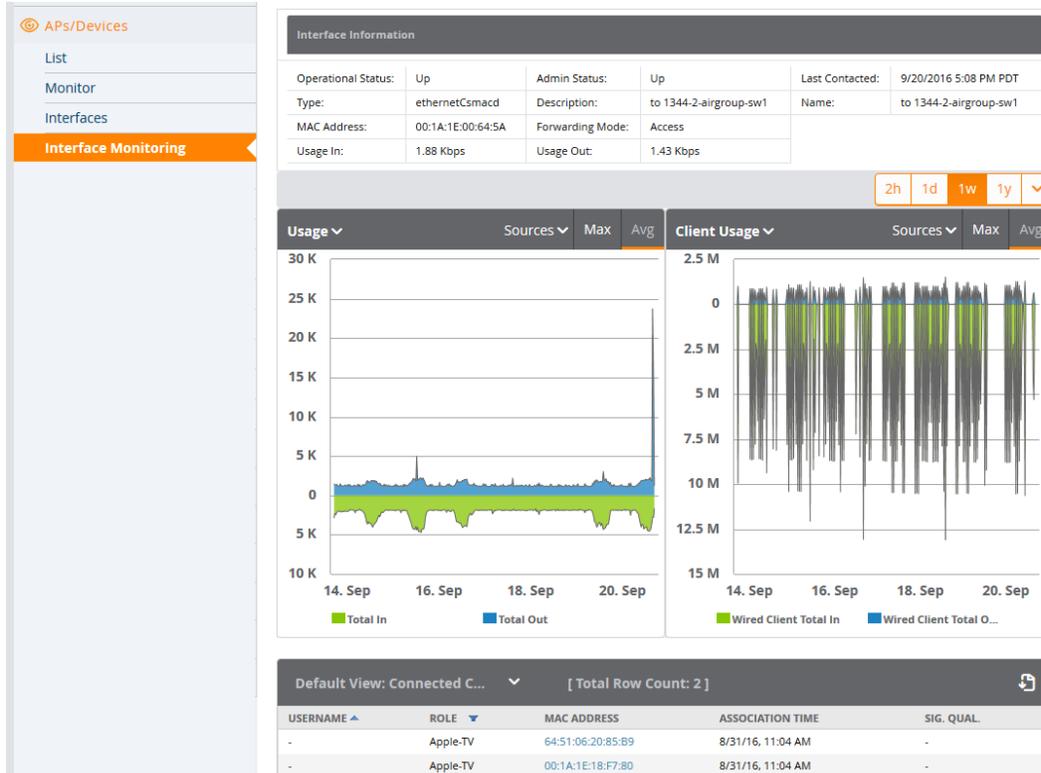
Monitoring Wired Interfaces

The **Interface Monitoring** page for a wired device is comprised of the following sections:

- Interface Information
- Usage and Interface Frame Counters graphs
- Connected Clients
- Wired Clients

To go to the monitoring page for an interface, click the **Interface** link in the Physical or Virtual Interfaces tables on a switch, as shown Figure 82.

Figure 82: *Interface Monitoring Page for a Wired Device*
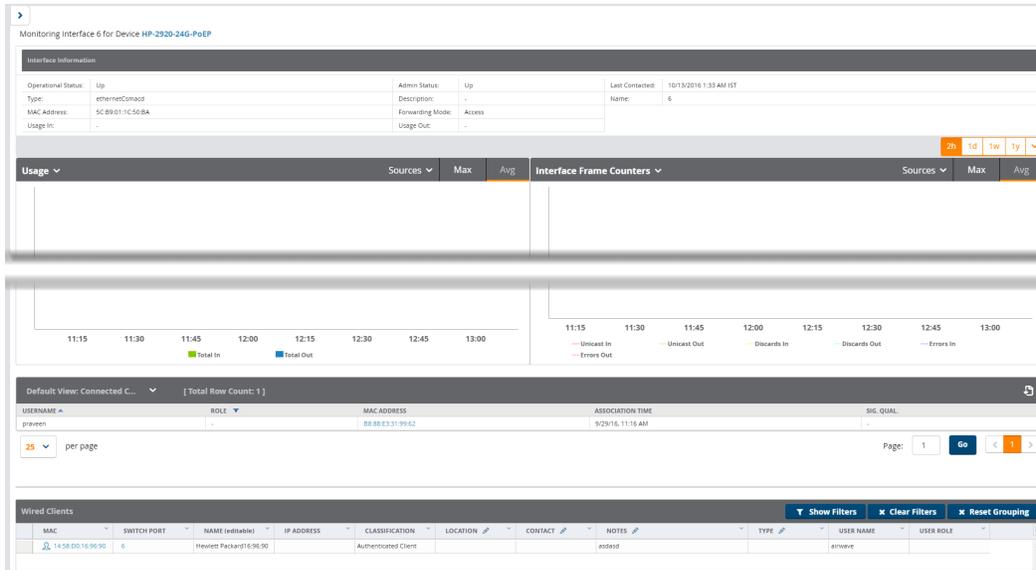
Specifics of the interface are in the Interface Information section, as depicted in Figure 83.

Figure 83: *Interface Information*

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 155 above.

Connected Clients, if any, are listed in a table below the interactive graphs.

What Next?

All device lists in W-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 163.

Monitoring Controller Clusters

The Controller Clusters dashboard displays statistics for all ArubaOS clusters. You can access the Controller Clusters dashboard by navigating to **Home > APs/Devices> Controller Clusters**. The Controller Clusters dashboard includes a **Clusters** table that displays statistics for each cluster group.

The cluster is a group of up to 12 controllers, using Layer 2 or Layer 3 connections, that work together to provide high availability to all their clients and ensure service continuity when a failover occurs. All controllers that are part of the cluster are managed by the same Mobility Master.

Mobility Master and all the controllers should be managed from the same W-AirWave server, and the controller clusters must be running Dell Networking W-Series ArubaOS 8.0.1 or later.

Figure 84: *Controller Clusters Dashboard*
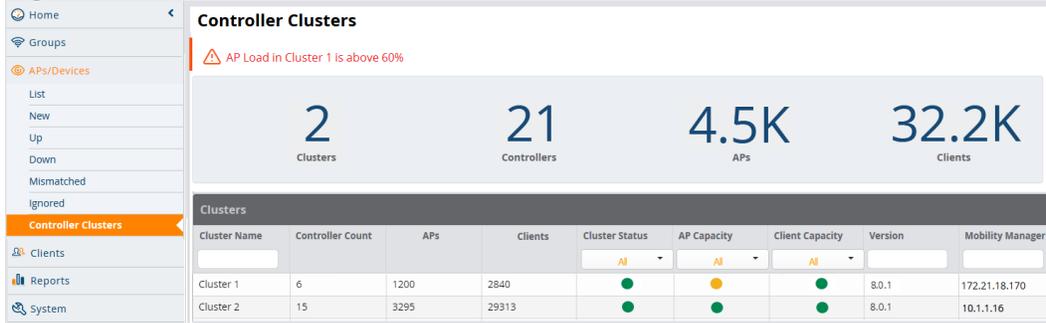
Sorting and Filtering Controller Cluster Data

Select any column heading in the Clusters table to sort the table by that value. Enter a text into the column search fields to filter the results.

Viewing Controller Cluster Details

From the Controller Clusters dashboard, select any cluster in the **Cluster** table to open the **Cluster Detail** page (see). The **Cluster Detail** page provides capacity graphs for APs and users, controller information, and cluster events.

Figure 85: *Cluster Detail Page*
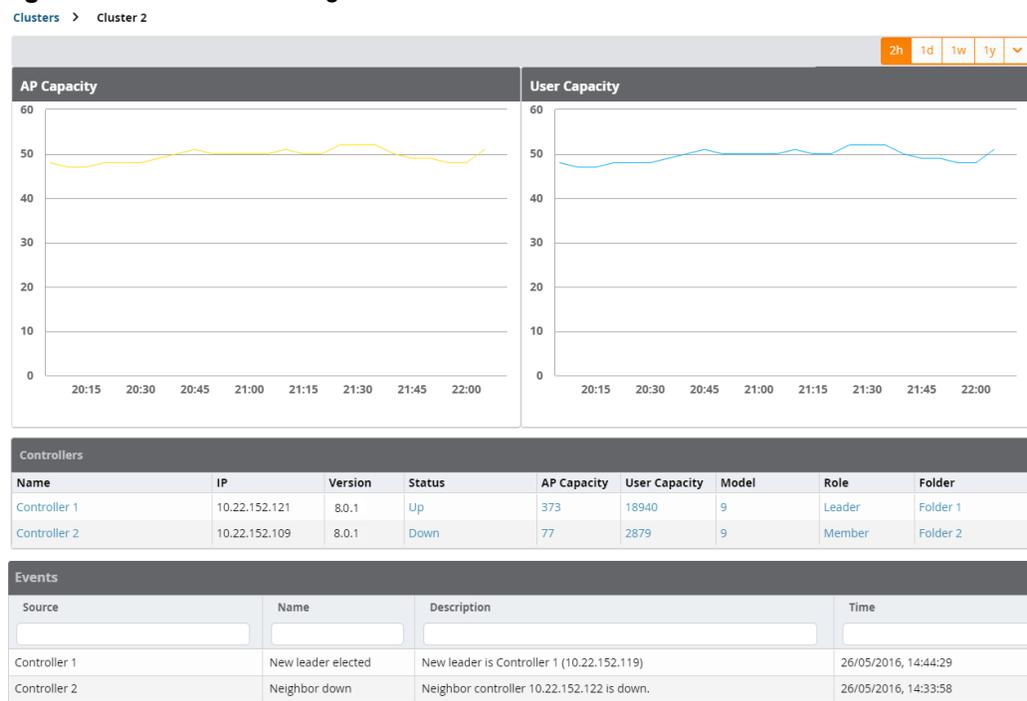
Viewing Capacity Graphs

The **Cluster Detail** page displays the following graphs:

- AP capacity. This graph shows the percentage of a cluster's total AP capacity currently in use, as well as the percentage of AP capacity currently in use on each individual controller in the cluster.

- User capacity. This graph shows the percentage of a cluster's total client capacity currently in use, as well as the percentage of client capacity currently in use on each individual controller in the cluster.

Hover your mouse over any section of these graphs to view detailed statistics for that point in the graph. To change the time interval displayed in this graphic, click the schedule toolbar above the **Client Capacity** graph.

Viewing Controller Statistics

The **Controllers** table provides statistics for the controllers in that cluster group. You can click any table heading to sort the table by that column criteria, or enter a text string into the entry field at the top of any column to filter the table by that value.

Table 84: *Controllers Table*

Column	Description
Name	Name of the controller in the cluster.
IP	IP address of the controller in the cluster.
Status	This column can display one of the following status icons: ● 🔴 = The controller is down ● 🟢 = The controller is active
AP Capacity	This column can display one of the following capacity icons: ● 🟢 = Controller is below 60% AP capacity ● 🟡 = Controller is between 60% and 80% AP capacity ● 🔴 = Controller is at greater than 80% AP capacity
Client Capacity	This column can display one of the following capacity icons: ● 🟢 = Controller is below 60% client capacity ● 🟡 = Controller is between 60% and 80% client capacity ● 🔴 = Controller is at greater than 80% client capacity
Role	Controller role within the cluster, either **leader** or **member**.
Type	Controller model type.
Version	Version of ArubaOS currently running on the controller.

Monitoring Cluster Events

The Events table displays a description and timestamp for each cluster event. For example, you will see events when a cluster member becomes inactive, crosses a capacity threshold, or changes its role within the cluster.

Where to Find Additional Cluster Information

The **APs/Devices > Monitor** page also displays cluster information for controllers and APs associated to a cluster.

- The **Device Info** section of the **APs/Devices > Monitor** page for a cluster controller includes the name of the cluster to which that controller belongs.
- The **Device Info** section of the **APs/Devices > Monitor** page for an AP associated to a cluster controller displays information about its active controller and its standby controller. Figure 86 shows the **APs/Devices > Monitor** page for an AP associated to a cluster member.

Figure 86: *APs/Devices > Monitor page for an AP in a Controller Cluster*
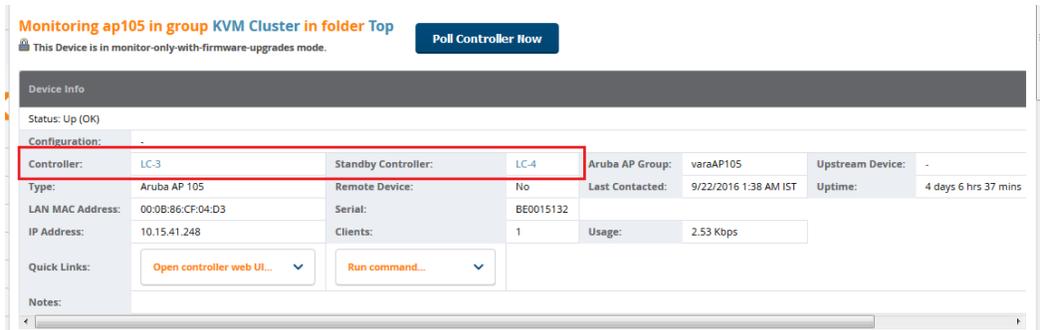
Using Topology

W-AirWave looks at the devices and links in your network and then puts them in an interactive topology map. Nodes on the map can include access points, switches, wireless controllers, and routers. By default, access points are hidden from map view so you can visualize your switching infrastructure.

Topology provides shortcuts to monitoring pages, interface information, and W-AirWave folders. Colored icons and connections help you visualize health and resource usage.

You can find Topology by navigating to **Home > Topology**.

> **NOTE**
>
> W-AirWave users with Admin roles can view and perform tasks in Topology. For information about user roles, see "User Roles" on page 1

Figure 87: *Topology Map View*
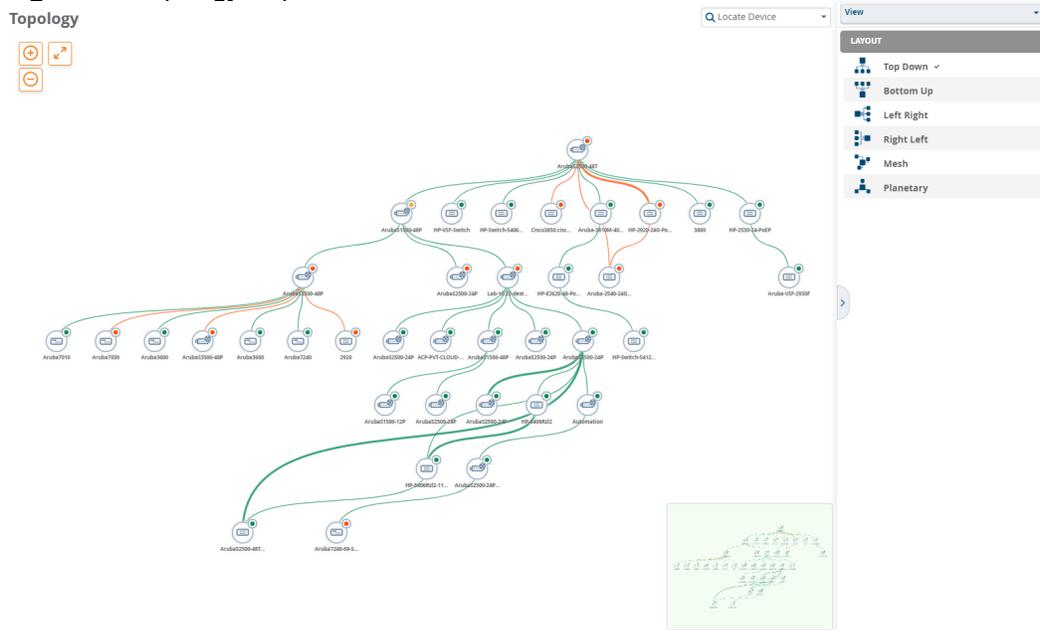
Navigate the Map

Using your mouse and keyboard, or touchscreen and trackpad, you can:

- Pan and zoom to view specific parts of the map
- Recenter your map

- Drag and drop a node (in mesh and planetary views). For information about views, see

Topology puts a bird's eye view in the lower-right corner of the map. As you move around in map view, you can see your location in the topology map in this view from above.

Change the Root Node

The first thing you might want to do is change the root node that W-AirWave places at the top of the topology map. To change the root node, right-click the device and select **Set as Root**.

If you choose **Reset the Root**, Topology selects a random node and, in the background, deletes the cached root node from browser cookies.

Figure 88: *Changing the Root Node*
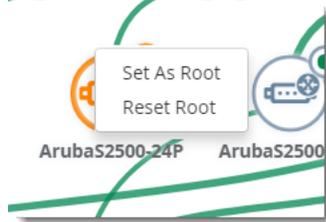
Change the Layout

You can rearrange the way the topology map displays the connections from the root node to other nodes. Some nodes might not have connections and look like islands on the map.

To change the layout, choosing from the following options in the **View** taskpane:

- Top Down. Creates a topology map that flows from top to bottom.
- Bottom Up. Creates a topology map that flows from bottom to top.
- Left Right. Creates a topology map that flows from left to right. If you select a device to reposition it on the map, the device and its connections move with it.
- Mesh. Creates a topology map that shows devices connected to a hub, spread randomly and overlapping. Dragging and dropping a device rearranges only that device on the map.
- Planetary. Creates topology map that shows devices connected to a hub, spread without overlapping. Dragging and dropping a device redistributes all devices on the map.

Search for a Device

You may want to locate a device and quickly monitor or troubleshoot it.

To search for a device:

1. Go to **Home > Topology**, then click the search field.
2. Select a device from the list. You can narrow down the list by typing at least 2 characters in the search field.

Figure 89: *Search for Device*
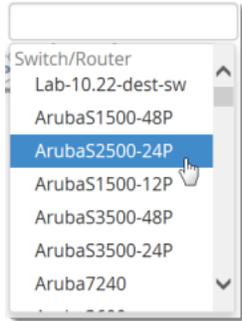
After locating the device, W-AirWave centers the device on the map, highlighting the icon in orange, and displays details about the device in the right pane.

Figure 90: *Search Result*
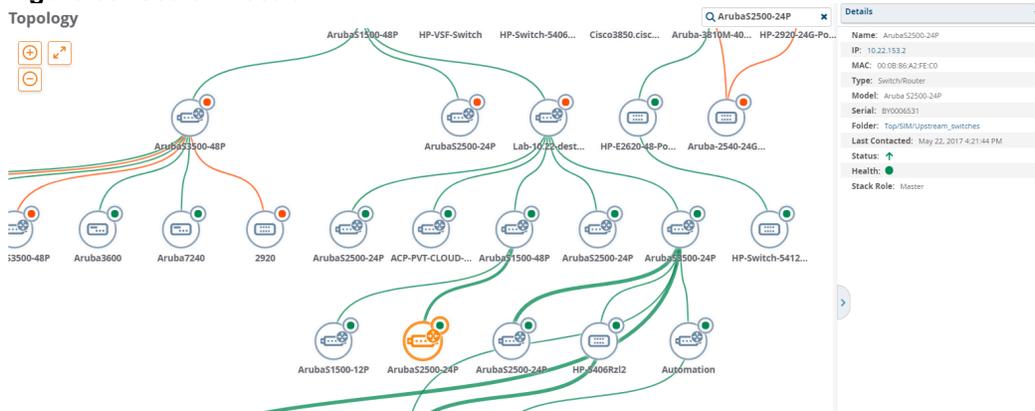
At a glance, you can see the device status and health from these details. For more information, see "Using Topology" on page 158 and "Status Icons" on page 163.

Respond to Alerts

If you see a bell icon at the upper-left corner of the topology map, there are changes to your network for you to review.

1. Hover your mouse over the bell icon to view the notification.

Figure 91: *Alert Notification*

2. Click the bell icon to review the information.

Figure 92: *Alert Messages*
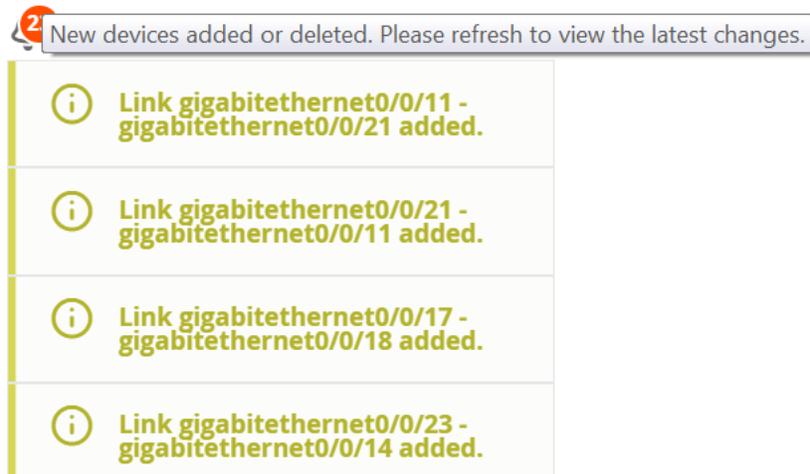
Take Action from Quick Links

Topology provides access to monitoring information from quick links in tooltips and device details in the right pane.

Tooltips

Tooltips provide quick links to the monitoring page for the device or the switch interface. Tooltips also display potential problems on a device. Alerts are colored orange in the tooltip.

To see tooltips

- Hover your mouse over a node in the topology map.
- Hover your mouse over the connection between two switches.

Device Details

Details include information, health and status indicators, and quick links to monitoring pages.

To view details for a device:

- Search for a device.
- Click a node in the map
- Click a connection in the map

In Figure 93, you can see that the health of the network connection, represented as an orange line in the topology map, is critical. Thicker lines represent multiple links between devices. By clicking on the links to the switch ports, you can troubleshoot further.

Figure 93: *Additional Details of the Connected Devices and Switch Interface*

Filter the Map

You can quickly change the topology map to monitor and visualize your network by applying filters.

> **NOTE**
>
> By default, W-AirWave hides access points from the topology map. To see access points, select AP from the filter list.

To apply a filter:

1. Select **Filter** from the task pane.

Figure 94: *Filtering Devices*

2. Hide or unhide the devices based on device type. The topology map displays only selected device types. Nodes and their connections are highlighted and shadowed in the VLAN view, as shown in Figure 95.

Figure 95: *Filtering VLANs*
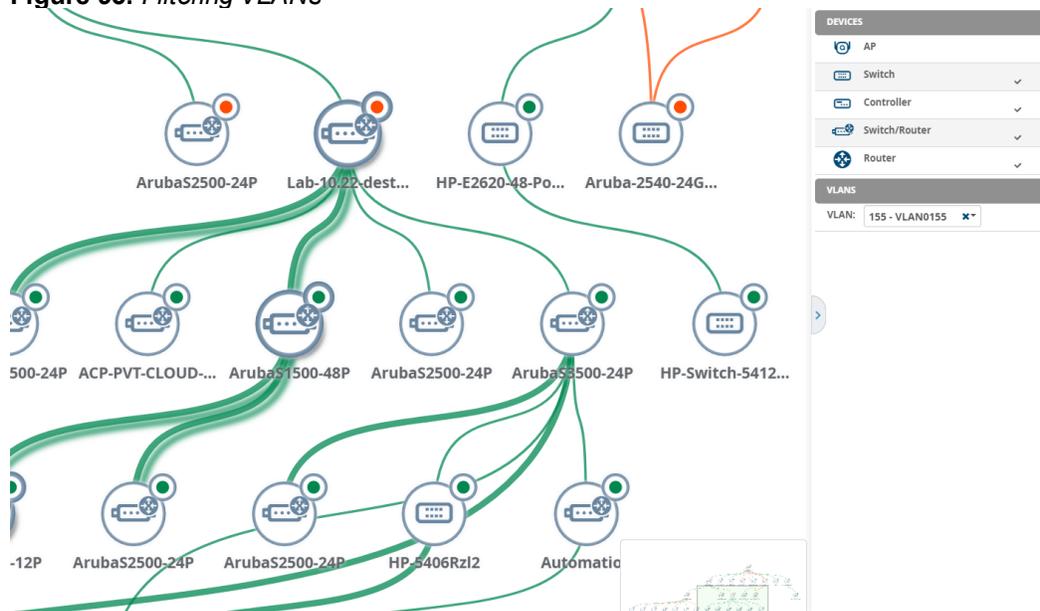
Status Icons

The colored icons show device status, number of rogues, CPU and memory utilization, and bandwidth usage. Green generally means everything is good, yellow is average, and orange requires your attention.

Table 85: *Topology Status Icons*

Icon	Meaning
🟢	There are no alerts or detected rogues. Health indicators are: • Node: more than 25% memory is available and less than 75% CPU is used. • Link: less than 70 Mbps bandwidth is used.
🟡	There are 1 to 2 alerts and no detected rogues. Health indicators are: • Node: more than 15% memory is available and less than 85% CPU is used. • Link: between 70 Mbps and 90 Mbps bandwidth is used.
🔴	There are at least 2 alerts or 1 or more detected rogues. Health indicators are: • Node: less than 15% memory is available and more than 85% CPU is used. • Link: more than 90 Mbps bandwidth is used.
—	Link is up.
—	Link is down.
↑	Device is up.
↓	Device is down.

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 164
- "Configuring AP Settings" on page 165
- "Setting a Maintenance Window for a Device" on page 173
- "Configuring Device Interfaces for Switches" on page 173
- "Individual Device Support and Firmware Upgrades" on page 175

While most device configuration settings can be efficiently managed by W-AirWave 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.

W-AirWave 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 W-AirWave pages where any mismatched settings can be configured.

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, W-AirWave will push a new configuration to the device in the event that the actual device configuration does not match the W-AirWave 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 96.

Figure 96: *APs/Devices > Manage > General Section Illustration*

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 115.

N O T E

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 mouse over the name of the device whose AP settings you want to edit. Click the **Manage** link for that device. Figure 97 illustrates one example of this page. (Note that the page and fields vary based on the device type.)

Figure 97: *APs/Devices > Manage Page Illustration (partial view)*

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 86 describes the fields, information, and settings.

Table 86: *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 W-AirWave is able to ping it and fetch SNMP information from the AP. If the AP is listed **Down** then W-AirWave 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 W-AirWave successfully contacted the AP.

Table 86: *APs/Devices > Manage > General Fields and Descriptions (Continued)*

Field	Description
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.
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. W-AirWave 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, W-AirWave 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 87 describes field settings, default values, and information for the **Settings** section of this page.

Table 87: *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)

Table 87: *APs/Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
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.
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.

Table 87: *APs/Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
Organization	Read from Device	Instant	The Organization string of the W-IAP.
Dell AP Group	default	All	Specifies the Dell AP Group in which this devices resides.
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 88 describes many of the possible fields.

> **NOTE**
> For complete listing and discussion of settings applicable only to *Dell Networking W-Series* devices, see the Dell Networking W-Series *Device Configuration Guide.*

Table 88: *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.

Table 88: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
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. **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.

Table 88: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
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)**
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. W-AirWave 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, W-AirWave 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 Dell Networking W-Series controllers in groups with Dell Networking W GUI Config disabled.

Table 89 describes field settings, default values, and additional information for this page.

Table 89: *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.
SSL Certificate	None	Cisco IOS	W-AirWave will read the SSL Certificate off of the AP when it comes UP in W-AirWave. 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 90 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by W-AirWave, refer to the Cisco WLC product documentation.

Table 90: *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

W-AirWave can automate the manual action of putting multiple devices into Manage mode at once so that changes can be applied, and after the maintenance period is over, the devices automatically revert to Monitor-Only mode.

Maintenance windows can be set as a one-time or recurring event on the **APs/Devices > Manage** and **Groups > Basic** 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 W-AirWaves.

NOTE

When a maintenance window is configured, W-AirWave 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 98: *Add New Maintenance Window in APs/Devices > Manage page*

AP Maintenance Window	
Name:	Enter a Value
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:	January 11, 2016 5:02 pm PST
Desired Start Date/Time:	Enter a Value
Duration: e.g. '10 min', '2 hours'	Enter a Value

Add **Cancel**

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

New physical and virtual interfaces are discovered using SNMP polling. 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.

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 **Interface Monitoring** window which may a slightly different appearance than Figure 99, depending on the device type, and whether you are configuring a physical or virtual interface.

Figure 99: *Editing a Switch Interface*

Editing Interface gigabitethernet0/0/1 for Device Aruba-S3500-25SP-1stFlr3

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:	Enter a Value
Mode:	Auto ⌄

Save **Cancel**

To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 100.

Figure 100: *Edit Multiple Interfaces*

🔧 Edit Interfaces

1-5 ▾ of 5 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Physical Interfaces

	INTERFACE ▲	MODE	NAME	TYPE ▾
✎	Fa0/1	Access	FastEthernet0/1	ethernetCsmacd
✎	Fa0/2	Distribution	FastEthernet0/2	ethernetCsmacd
✎	Fa0/3	Access	FastEthernet0/3	ethernetCsmacd
✎	Fa0/4	Access	FastEthernet0/4	ethernetCsmacd
✎	Fa0/5	Access	FastEthernet0/5	ethernetCsmacd

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 101.

Figure 101: *Multiple Interface Editing Page Illustration*

1-5 ▾ of 5 Interfaces Page 1 ▾ of 1 Reset filters Choose columns Export CSV

Physical Interfaces

|	INTERFACE ▲	MODE	NAME	TYPE ▾	CISCO INTERFACE TYPE	DESCRIPTION	INTERFACE LABELS
✎	Fa0/1	Auto ⌄	FastEthernet0/1	ethernetCsmacd	-		
✎	Fa0/2	Auto ⌄	FastEthernet0/2	ethernetCsmacd	-		
✎	Fa0/3	Auto ⌄	FastEthernet0/3	ethernetCsmacd	-		
✎	Fa0/4	Auto ⌄	FastEthernet0/4	ethernetCsmacd	-		
✎	Fa0/5	Auto ⌄	FastEthernet0/5	ethernetCsmacd	-		

W-AirWave 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 Dell Networking W-Series controllers. The available device communication fields will vary, depending on the brand and model of the AP.

1. Locate the **Device Communication** area on the **APs/Devices > Manage** page.
2. Specify the credentials to be used to manage the AP. Figure 102 illustrates this page.

Figure 102: *APs/Devices > Manage > Device Communication*
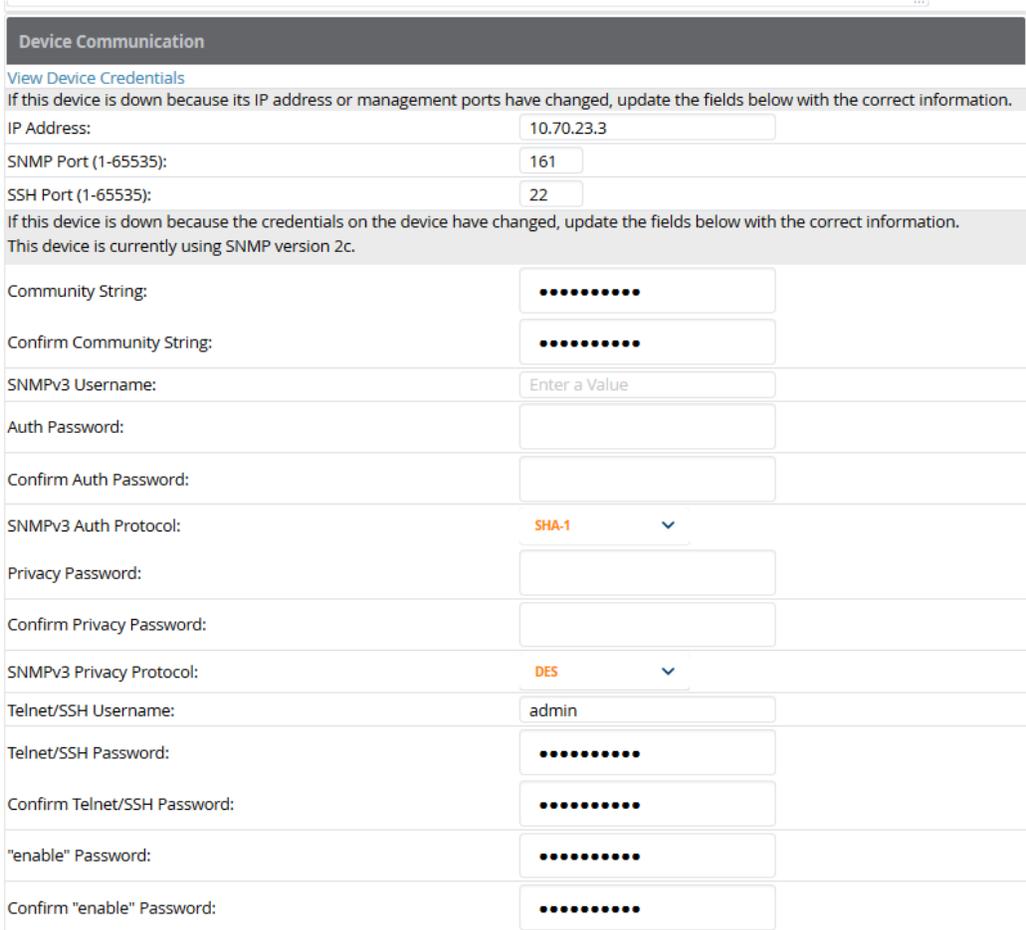
Device Communication	
View Device Credentials	
If this device is down because its IP address or management ports have changed, update the fields below with the correct information.	
IP Address:	10.70.23.3
SNMP Port (1-65535):	161
SSH Port (1-65535):	22
If this device is down because the credentials on 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:	Enter a Value
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:	••••••••••

3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. (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.
5. 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. The **Update Firmware** button only appears if the W-AirWave Administrator has enabled **Allow firmware upgrades in monitor-only mode** on the **AMP Setup > General** page, *and* you are looking at an **APs/Devices > Manage** page for a controller or autonomous AP that supports firmware upgrades in W-AirWave. See the Supported Infrastructure Devices document on the

Home > Documentation page for a list of the W-AirWave-supported devices that can perform firmware upgrades. In most cases, you cannot upgrade firmware directly on thin APs.

Figure 103 illustrates the page that opens and Table 91 describes the settings and default values.

Table 91: *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 103: *APs/Devices > Manage Firmware Upgrades*

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**.

This section provides an overview and several tasks supporting the use of device configuration templates in W-AirWave, and contains the following topics:

Group Templates

Supported Device Templates

Templates are helpful configuration tools that allow W-AirWave 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

Use the graphical Dell config feature in support of Dell Networking W-Series devices, particularly for ArubaOS 3.3.2.x and later. Refer to the *Dell Networking W-AirWave 8.2.4 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 W-AirWave 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 72.
2. From the W-AirWave navigation pane, select **Templates**. The **Templates** page appears. Figure 104 illustrates the **Groups > Templates** configuration page.

Figure 104: *Groups > Templates Page Illustration for a Sample Device Group*

Table 92 describes the columns in this image.

Table 92: *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 92: *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 W-AirWave 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 105.

Figure 105: *Groups > Templates > Add Template Page Illustration*

The settings for the **Add a Template** page are described in Table 93. Note that the fields can vary based on the Group.

Table 93: *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 195.
Name	None	Defines the template display name.

Table 93: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
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 W-AirWave applies the template, copied from the new configuration file to the startup configuration file on the AP. If **No** is selected, W-AirWave 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 184 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 W-AirWave uses to contact devices after the configuration has been pushed. If this option is enabled, then new credential information fields display.
Community String	None	If the template is updating the community strings on the AP, enter the new community string W-AirWave should use here. W-AirWave 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 user name on the AP, enter the new user name W-AirWave should use here. W-AirWave 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 W-AirWave should use here. W-AirWave updates the credentials it is using to communicate to the device after the device has been managed.

Table 93: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
enable Password	None	If the template is updating the enable password on the AP, enter the new enable password W-AirWave should use here. W-AirWave 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 user name on the AP, enter the new SNMP user name here. W-AirWave 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 user name password here. W-AirWave 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. W-AirWave 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 186, including the following sections:
  - "Using AP-Specific Variables" on page 186
  - "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 186
  - "Using Conditional Variables in Templates" on page 187
  - "Using Substitution Variables in Templates" on page 188

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. W-AirWave 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 186

   These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Dell customer support at **dell.com/support** before proceeding.

7. Specify the device types for the template. The templates only apply to devices of the specified type.

   ■ Specify whether W-AirWave should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then W-AirWave instructs the AP to copy the configuration from W-AirWave to the startup configuration file of the AP and reboot the AP.

   ■ If the **Reboot Devices after Configuration Changes** option is not selected, then W-AirWave 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 W-AirWave 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 W-AirWave.

> **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 186
- "Using Directives to Eliminate Reporting of Configuration Mismatches" on page 186
- "Using Conditional Variables in Templates" on page 187
- "Using Substitution Variables in Templates" on page 188

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 W-AirWave.

The `power` lines set the power local `cck` and `ofdm` values to the numerical values that are stored in W-AirWave.

Using Directives to Eliminate Reporting of Configuration Mismatches

W-AirWave 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, W-AirWave 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 W-AirWave from reporting mismatches for this type of variance.

W-AirWave provides two types of directives that can be used within a template to control how W-AirWave 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 W-AirWave ignores them when verifying configurations. Lines enclosed in `<ignore_and_do_not_push>` cause W-AirWave 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 W-AirWave 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 W-AirWave 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 94:

```
%if variable=value%
…
%endif%
```

Table 94: *Conditional Variable Syntax Components*

Variable	Values	Meaning
interface	Dot11Radio0	2.4GHz radio module is installed
	Dot11Radio1	5GHz external radio module is installed
radio_type	a	Installed 5GHz radio module is 802.11a
	b	Installed 2.4GHz radio module is 802.11b only
	g	Installed 2.4GHz radio module is 802.11g capable
wds_role	backup	The WDS role of the AP is the value selected in the drop down menu on the **APs/Devices > Manage** configuration page for the device.
	client	
	master	
IP	Static	IP address of the device is set statically on the AP Manage configuration page.
	DHCP	IP address of the device is set dynamically using DHCP

Using Substitution Variables in Templates

Substitution variables are used to set AP-specific values on each AP in the group. It is obviously not desirable to set the IP address, hostname, and channel to the same values on every AP within a Group. The variables in Table 95 are substituted with values specified on each access point's **APs/Devices > Manage** configuration page within the W-AirWave 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. W-AirWave would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent W-AirWave from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, W-AirWave suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way W-AirWave 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 95.

Table 95: *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 95: *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 Dell Networking W-Instant

The first Instant network that is added to W-AirWave automatically includes the default configuration that is used as a template to provision other Instant networks. Refer to the documentation that accompanies Dell Networking W-Instant for more information.

> **NOTE**
>
> 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.

W-AirWave 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 W-AirWave. W-AirWave 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:** W-AirWave 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. W-AirWave 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 W-AirWave normal **Group** configuration pages. W-AirWave 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 W-AirWave 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 191
- "WDS Settings in Templates" on page 191
- "SCP Required Settings in Templates" on page 192
- "Supporting Multiple Radio Types via a Single IOS Template" on page 192
- "Configuring Single and Dual-Radio APs via a Single IOS Template" on page 193

Applying Startup-config Files

Each of the APs in the Group copies its unique startup-config file from W-AirWave via TFTP or SCP.

- If the **Reboot Devices after Configuration Changes** option is selected, then W-AirWave instructs the AP to copy the configuration from W-AirWave to the startup-config file of the AP and reboot the AP.
- If the **Reboot Devices after Configuration Changes** option is not selected, then W-AirWave 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 W-AirWave 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 user name 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 user name 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 user name 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 W-AirWave to login to the AP must have level 15 privileges. Without them, W-AirWave 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:

```
user name Cisco privilege 15 password 7 0802455D0A16
aaa authorization exec default local
ip scp server enable
```

The `user name` line is a guideline and will vary based on the user name 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 . You can import interface information as described in this section or by fetching a template from that device, as described in .

> **NOTE**
> Just one template is used for any type of Cisco IOS device, and another is used for any type of Catalyst Switch regardless of individual model.

Configuring Symbol Controller / HPE WESM Templates

This section describes the configuration of templates for Symbol controllers and HPE WESM devices.

Symbol Controllers (RFS x000, 5100 and 2000) can be configured in W-AirWave using templates. W-AirWave 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 . 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 **alp-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
!
user name admin password 1 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
user name admin privilege  superuser
user name operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
!
!
access-list 100 permit ip 192.168.0.0/24 any rule-precedence 10
!
spanning-tree mst cisco-interoperability enable
spanning-tree mst configuration
 name My Name
!
ip dns-server-forward
wwan auth-type chap
no bridge multiple-spanning-tree enable bridge-forward
country-code us
aap-ipfilter-list no port 3333 plz
aap-ipfilter-list no port 3333 tcp plz
 deny tcp src-start-ip 0.0.0.0 src-end-ip 255.255.255.255 dst-start-ip 0.0.0.0 dst-end-ip
255.255.255.255 dst-start-port 3333 dst-end-port 3334 rule 1
%redundancy_config%
logging buffered 4
logging console 4
snmp-server engineid netsnmp 6b8b45674b30f176
snmp-server location %location%
snmp-server contact %contact%
snmp-server sysname %hostname%
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpmanager v3 encrypted auth md5 0x1aa491f4ca7c55df0f57801bece9044c
snmp-server user snmpoperator v3 encrypted auth md5 0xb03b1ebfa0e3d02f50e2b1c092ab7c9f
```

A sample Symbol Smart RF template is provided below for reference:

```
radio %radio_index% radio-mac %radio_mac%
%if radio_type=11a%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11an%
  radio %radio_index% coverage-rate  18
%endif%
%if radio_type=11b%
  radio %radio_index% coverage-rate  5p5
%endif%
%if radio_type=11bg%
  radio %radio_index% coverage-rate  6
%endif%
%if radio_type=11bgn%
  radio %radio_index% coverage-rate  18
%endif%
```

A sample Symbol thin AP template is provided below for reference and for the formatting of `if` statements.

```
   radio add %radio_index% %lan_mac% %radio_type% %ap_type%
```

```
radio %radio_index% radio-number %radio_number%
radio %radio_index% description %description%
%if radio_type=11a%
radio %radio_index% speed  basic6 9 basic12 18 basic24 36 48 54
radio %radio_index% antenna-mode primary
radio %radio_index% self-heal-offset 1
radio %radio_index% beacon-interval 99
radio %radio_index% rts-threshold 2345
radio %radio_index% max-mobile-units 25
radio %radio_index% admission-control voice max-perc 76
radio %radio_index% admission-control voice res-roam-perc 11
radio %radio_index% admission-control voice max-mus 101
radio %radio_index% admission-control voice max-roamed-mus 11
%endif%
%if radio_type=11an%
radio %radio_index% speed  basic11a 9 18 36 48 54 mcs 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
%endif%
%if radio_type=11b%
radio %radio_index% speed  basic1 basic2 basic5p5 basic11
%endif%
%if radio_type=11bg%
radio %radio_index% speed  basic1 basic2 basic5p5 6 9 basic11 12 18 24 36 48 54
radio %radio_index% on-channel-scan
radio %radio_index% adoption-pref-id 7
radio %radio_index% enhanced-beacon-table
radio %radio_index% enhanced-probe-table
%endif%
%if radio_type=11bgn%
radio %radio_index% speed  basic11b2 6 9 12 18 24 36 48 54 mcs
0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
%endif%
radio %radio_index% channel-power indoor %channel% %transmit_power% %channel_attribute%
%detector%
%adoption_pref_id%
radio %radio_index% enhanced-beacon-table
radio %radio_index% on-channel-scan
%ap_include_4%
```

Configuring a Global Template

Global templates allow W-AirWave 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 106.

Figure 106: *Group > Templates > Add Page Illustration*

4. Use the drop-down menu to select a device from which to build the global template and click the **Fetch** button. The 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 107: *Template Variables Illustration*

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.

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 W-AirWave 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 "SNMP/HTTP Scanning Overview" on page 119.

Furthermore, RAPIDS integrates with external intrusion detection systems (IDS), as follows:

- **Dell WIP**—The Dell Networking W-Series 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)—W-AirWave 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 W-AirWave.
- **AirDefense**—Uses the W-AirWave XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from W-AirWave.

Viewing Overall Network Health on RAPIDS > Overview

The **RAPIDS > Overview** page displays a page of RAPIDS summary information (see Figure 108). Table 96 defines the summary information that appears on the page.

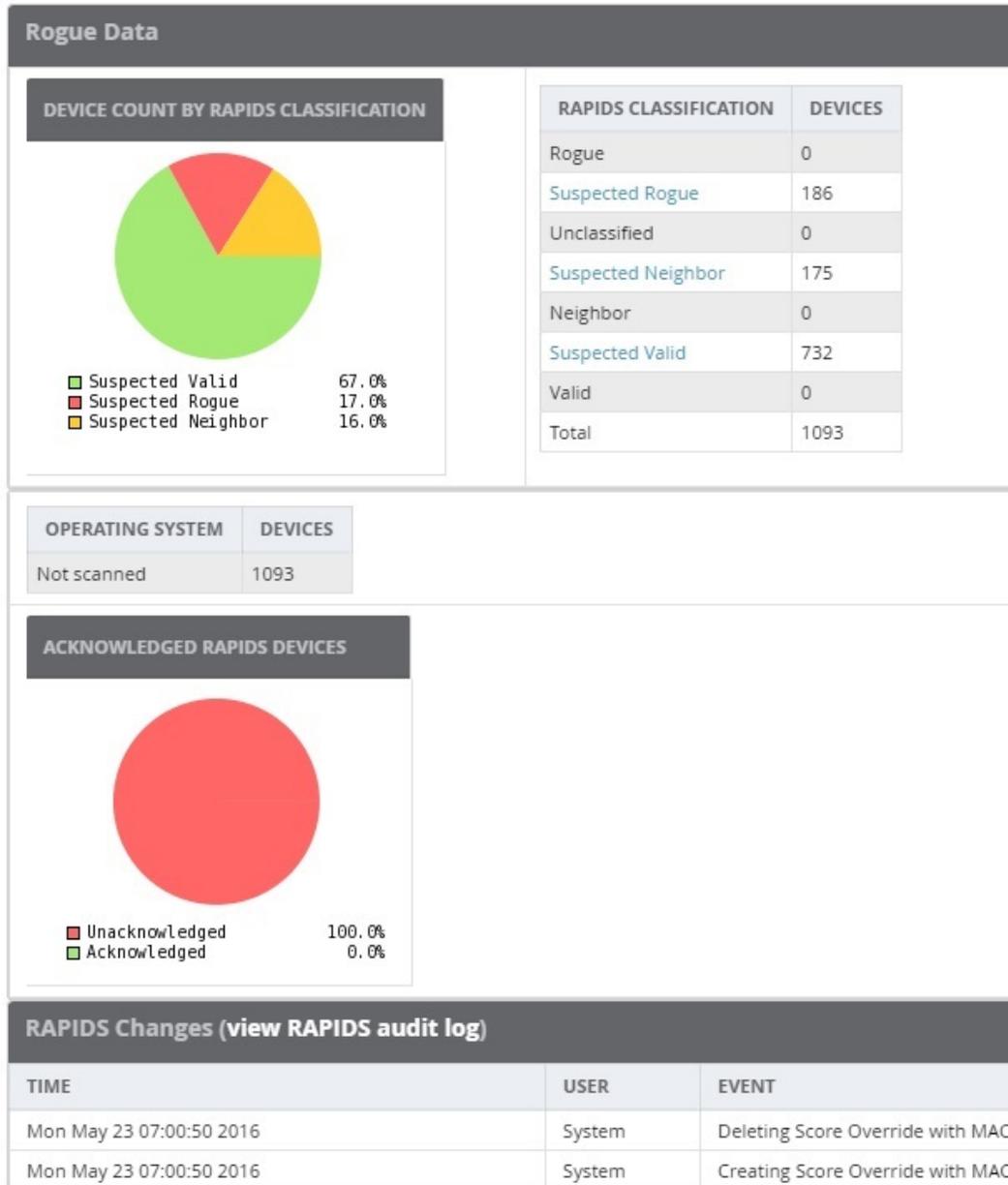**Figure 108:** *RAPIDS > Overview Page Illustration (partial view)*

Table 96: *RAPIDS > Overview Fields and Descriptions*

Summary	Description
Device Count by RAPIDS Classification	A pie chart of rogue device percentages by RAPIDS classification.

Table 96: *RAPIDS > Overview Fields and Descriptions (Continued)*

Summary	Description
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.
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 W-AirWave server for RAPIDS. Complete the settings on this page as desired, and select **Save**. Most of the settings are internal to the way that W-AirWave will process rogues.

Refer to the following sections:

- "RAPIDS Setup" on page 200
- "Additional Settings" on page 204

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 109: *RAPIDS > Setup Page Illustration*

Table 97: *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 W-AirWave, 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 98: *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, W-AirWave can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Dell Networking W-Series controllers (running ArubaOS versions 3.x and later). W-AirWave will alert you to the appearance of the rogue device and identify any mismatch between controller configuration and the desired configuration.

Table 99: *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 Dell 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 205 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 100: *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 W-AirWave 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

:Use the **AMP Setup > Roles > Add/Edit Role** page to define the ability to use RAPIDS by user role. Refer to Creating AirWaveOV3600 User Roles.

Defining RAPIDS Rules

The **RAPIDS > Rules** page is one of the core components of RAPIDS. This feature allows you to define rules by which any detected device on the network is classified.

This section describes how to define, use, and monitor RAPIDS rules, provides examples of such rules, and demonstrates how they are helpful.

This section contains the following topics:

- "Controller Classification with WMS Offload" on page 204
- "Device OUI Score" on page 205
- "Rogue Device Threat Level" on page 205
- "Viewing and Configuring RAPIDS Rules" on page 205
- "Recommended RAPIDS Rules " on page 208
- "Using RAPIDS Rules with Additional W-AirWave Functions" on page 209

Controller Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Dell Networking W-Series WLAN switches. Controller classification of this type remains distinct from RAPIDS classification. WLAN switches feed wireless device information to W-AirWave, which W-AirWave then processes. W-AirWave 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 W-AirWave and Dell Networking W-Series ArubaOS for scenarios involving WMS Offload.

Table 101: *Rogue Device Classification Matrix*

W-AirWave	ArubaOS (ARM)
Unclassified (default state)	Unknown
Rogue	Rogue
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Valid	Valid
Contained Rogue	DOS

For additional information about WMS Offload, refer to the *Dell Networking W-AirWave 8.2.4 Best Practices Guide* at **dell.com/support/manuals**.

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 102 provides list the OUI scores definitions.

Table 102: *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 W-AirWave, navigate to the **RAPIDS > Rules** page (Figure 110).
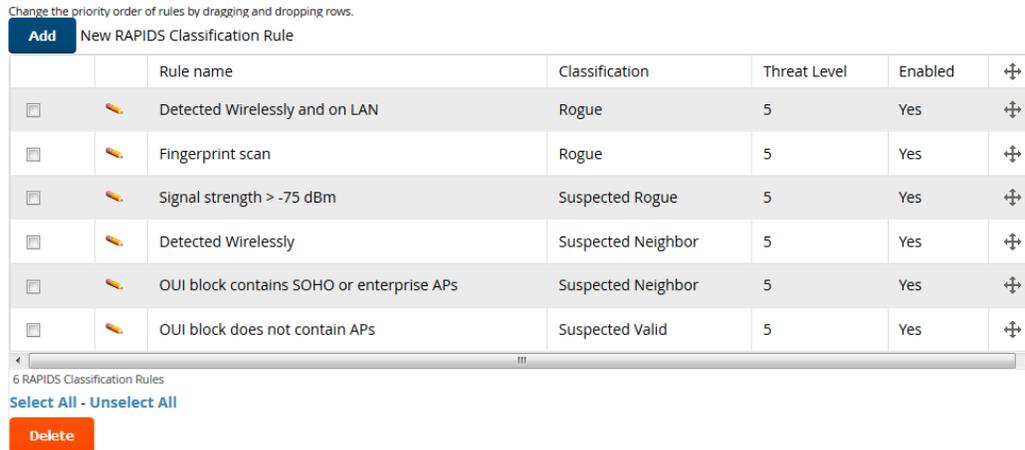
Figure 110: *RAPIDS > Rules Page Illustration*

Table 103 defines the fields in the **RAPIDS > Rules** page.

Table 103: *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 205 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 111).

Figure 111: *Classification Rule Page*

Fill in the settings described in Table 103 then select an option from the drop down menu.

Table 104 defines the drop down menu options that are at the bottom left of the RAPIDS Classification Rule dialog box (see Figure 111). After all rule settings are defined, select **Add**. The new rule automatically appears in the **RAPIDS > Rules** page.

Table 104: *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, W-AirWave processes only alpha-numeric characters and the asterisk wildcard character (*****). W-AirWave 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).
Channel	Rogue matches a specified Channel number. Enter channel numbers in the valid format to match rogue devices.
Detected Client Count	Classifies based on the number of valid clients.

Table 104: *Properties Drop Down Menu (Continued)*

Option	Description
Wireline Properties	
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.
Dell 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 111). 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 W-AirWave. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.

- **If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, then Classify as Rogue**

This rule classifies a device as a rogue when the SSID for a given device is your SSID and is not an Ad-Hoc device. Windows XP automatically tries to create an Ad-hoc network if it can not find the SSID for which it is searching. This means that user's laptops on your network may appear as Ad-Hoc devices that are broadcasting your SSID. If this happens too frequently, you can restrict the rule to apply to non-ad-hoc devices.

- **If More Than Four APs Have Discovered a Device, then Classify as Rogue**

  By default, W-AirWave tries to use Signal Strength to determine if a device is on your premises. Hearing device count is another metric that can be used.

  The important concept in this scenario is that legitimate neighboring devices are only heard by a few APs on the edge of your network. Devices that are heard by a large number of your APs are likely to be in the heart of your campus. This rule works best for scenarios in large campuses or that occupy an entire building. For additional rules that may help you in your specific network scenario, contact Dell support at **dell.com/support**.

Using RAPIDS Rules with Additional W-AirWave Functions

Rules that you configure on the **RAPIDS > Rules** page establish an important way of processing rogue devices on your network, and flagging them for attention as required. Such devices appear on the following pages in W-AirWave, with additional information:

- **RAPIDS > List**—Lists rogue devices as classified by rules.
- **RAPIDS > Rules**—Displays the rules that classify rogue devices.
- **RAPIDS > Overview**—Displays general rogue device count and statistical information.
- **System > Triggers**—Displays triggers that are currently configured, including any triggers that have been defined for rogue events.
- **Reports > Definitions**—Allows you to run New Rogue Devices Report with custom settings.
- **VisualRF**—Displays physical location information for rogue devices.

Viewing Rogues on the RAPIDS > List Page

To view a rogue AP, select the **RAPIDS > List** tab and select a rogue device type from the **Minimum Classification** drop-down menu (see Figure 112). 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.

The columns in the default view for the RAPIDS > List page is defined in Dell Networking W-AirWave and cannot be modified. However, you can create a new view for this page that returns custom information based on the filter parameters and data columns you selected when creating that new view. For more information on creating custom views, see "Creating Custom Views" on page 1.

Figure 112: *RAPIDS > List Page Illustration (partial view)*

Default View: Rogue Devices	⌄	[Total Row Count: 2114]			
ACK ▲▼	**RAPIDS CLASSIFICATION ▼**	**THREAT LEVEL**	**NAME**	**CLASSIFYING RULE ▼**	**CONTROLLER CLASSIFICATION**
No	Suspected Rogue	5	Aruba Netw-6F:7E:80	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Aruba Netw-72:A2:D0	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Aruba Netw-D4:82:00	Signal strength > -75 dBm	Suspected Rogue
No	Suspected Rogue	5	Aruba Netw-D4:23:B0	Signal strength > -75 dBm	Suspected Rogue
No	Suspected Rogue	5	Aruba Netw-C4:75:80	Signal strength > -75 dBm	Suspected Rogue
No	Suspected Rogue	5	Aruba Netw-8B:83:50	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Aruba Netw-26:55:20	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Aruba Netw-E3:2C:E0	Signal strength > -75 dBm	Suspected Rogue
No	Suspected Rogue	5	Aruba Netw-6C:57:70	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Cisco-BF:74:0C	Signal strength > -75 dBm	Suspected Neighbor
No	Suspected Rogue	5	Aruba Netw-F0:B9:B0	Signal strength > -75 dBm	Suspected Rogue

Table 105 details the column information displayed in Figure 112. For additional information about RAPIDS rules, refer to "Defining RAPIDS Rules" on page 204.

Table 105: *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 W-AirWave user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 200).
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 205. The threat level is also supported with Triggers (see "Using the System Pages" on page 218).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, W-AirWave assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. Clicking the linked name will redirect you to the **RAPIDS > Detail** page for that rogue device. Refer to "Overview of the RAPIDS > Detail Page" on page 212.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 205).
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.

Table 105: *RAPIDS > List Column Definitions (Continued)*

Column	Description
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 Dell 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.
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.

Table 105: *RAPIDS > List Column Definitions (Continued)*

Column	Description
OS	This field displays the OS of the device, as known. OS is the result of a running an OS port scan on a device. An IP addresses is required to run an OS scan. The OS reported here 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 W-AirWave. 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.
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 113).

Figure 113: *RAPIDS > Detail Page Illustration*

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 W-AirWave 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 W-AirWave processing.

Viewing Ignored Rogue Devices

The **RAPIDS > List** page allows you to view ignored rogues—devices that have been removed from the rogue count displayed by W-AirWave. Such devices do not trigger alerts and do not display on lists of rogue devices. To display ignored rogue devices, select **View Ignored Rogues** at the bottom left of the page.

Once a classification that has rogue devices is chosen from the drop-down menu, a detailed table displays all known information.

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.

- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. W-AirWave performs a port scan on the device and attempts to determine the operating system. (See "Setting Up RAPIDS" on page 200.)

  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 114, Figure 115, and Table 106 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 114: *RAPIDS > Score Override Page*
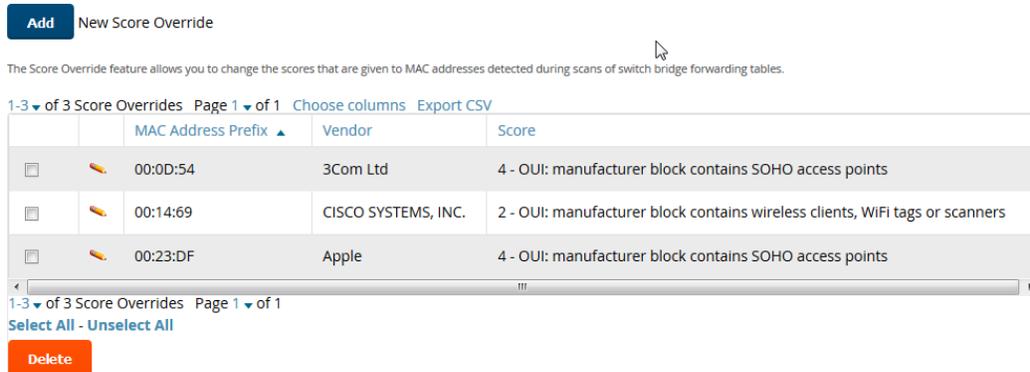
2. Click **Add** to create a new override or select the pencil icon next to an existing override to edit that override. The **Score Override** add or edit page appears (Figure 115).

Figure 115: *Add/Edit Score Override Page*

Table 106: *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 116.

Figure 116: *Audit Log Page Illustration*

Additional Resources

The following W-AirWave tools support RAPIDS:

- **System Triggers and Alerts**—Triggers and Alerts that are associated with rogue devices follow the classification-based system described in this chapter. For additional information about triggers that support rogue device detection, see to "Viewing, Delivering, and Responding to Triggers and Alerts" on page 229.

- **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 290.

For additional security-related features and functions, see the following topics in this guide.

- "Configuring Group Security Settings" on page 87
- "Configuring Cisco WLC Security Parameters and Functions" on page 105
- "Configuring Group SSIDs and VLANs" on page 92
- "Using the System Pages" on page 218

Daily WLAN administration often entails network monitoring, supporting WLAN and W-AirWave users, and monitoring W-AirWave system operations.

This chapter includes the following sections:

- "Using the System Pages" on page 218
- "Backing Up Your Data" on page 233
- "Managing Mobile Devices with SOTI MobiControl and W-AirWave " on page 239
- "About the Home Page" on page 240
- "Logging out of W-AirWave" on page 263

Using the System Pages

The **System** pages provide a centralized location for system-wide W-AirWave data and settings. System pages let you view things like syslog messages and W-AirWave events, set triggers, respond to alerts, manage configuration jobs, and monitor system performance.

Checking the Status of W-AirWave Services

From the **System > Status** page, you can:

- Get diagnostic tar files to show customer support.
- View the status of W-AirWave services. Status can **OK**, **Disabled**, or **Down**. If any service is **Down** (displayed in red) contact Dell support at **dell.com/support**.
- Access log files.
- Reboot the AirWave server. Click **Reboot System** to power cycle your W-AirWave remotely when it is needed.
- Restart W-AirWave services. Click **Restart AMP** to restart W-AirWave services without power cycling the server or reloading the OS.

About the Tar Files

The link **diagnostics.tar.gz** contains reports and logs that are helpful to Dell support in troubleshooting and solving problems. Your Dell 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 Dell support.

Important Log Files

A summary table lists logs that appear on the **System > Status** page. These are used to diagnose W-AirWave problems. Additional logs are available via SSH access in the /var/log and /tmp directories; Dell support engineers may request these logs for help in troubleshooting problems and will provide detailed instructions on how to retrieve them.
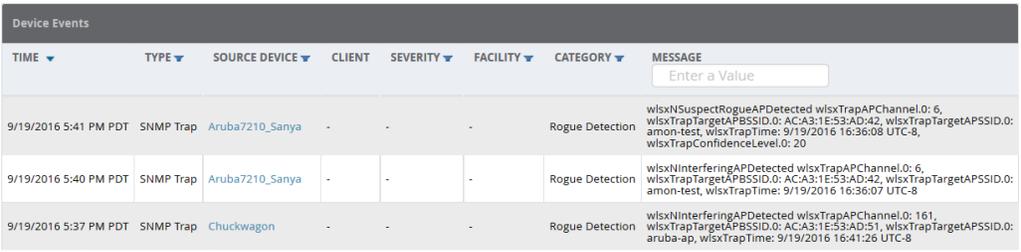
Table 107 describes some of the most important logs.

Table 107: *Important 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; send this log to Dell 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

Admins can use the **System > Syslog & Traps** page to review all syslog messages and SNMP traps that W-AirWave receives from the trigger type **Device Event**. These device events are listed by time, type, source device, AP, severity, facility, category, and message. You can filter most columns by clicking 🔽, and you can filter messages using the **Search** field, as shown in Figure 117.

You can change the historical data retention from the **Device Events (Syslog, Traps)** field in **AMP Setup > General**.

Figure 117: *Viewing Device Events*

Table 108 describes the columns and the information provided in each:

Table 108: *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 W-AirWave could not correlate the source IP.

Table 108: *System > Syslog & Traps Columns and Descriptions (Continued)*

Column	Description
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 a Dell Networking W-Series controller.
Message	The raw trap message including the AP MAC Address, time sent, and other information. For syslogs, W-AirWave does not display the numbers at the beginning of the message that indicate the severity and facility. For traps, W-AirWave will attempt to translate them to human-readable format when possible. W-AirWave will not receive processed SNMP traps into the Device Event framework if the W-AirWave 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 Event Log

The **System > Event Log** page is a very useful debugging tool containing a list of recent W-AirWave events including APs coming up and down, services restarting, and most W-AirWave-related errors as well as the user that initiated the action. Figure 118 illustrates this page, and Table 109 describes the page components.

Figure 118: *System > Event Log Page Illustration*

TIME	USER	TYPE	EVENT	DEVICE ID	FOLDER	GROUP
Tue Jan 12 16:17:08 2016	System	Device	Aruba 7210 Aruba7210 Device Monitor: update() - DBD::Pg::st execute failed: ERROR: invalid input syntax for integer: "ayadav2_FCS64X0_temp" [fo	5	Top > All Wireless Office	Aruba
Tue Jan 12 16:12:08 2016	System	Device	Aruba 7210 Aruba7210 Device Monitor: update() - DBD::Pg::st execute failed: ERROR: invalid input syntax for integer: "ayadav2_FCS64X0_temp" [fo	5	Top > All Wireless Office	Aruba
Tue Jan 12 16:07:08 2016	System	Device	Aruba 7210 Aruba7210 Device Monitor: update() - DBD::Pg::st execute failed: ERROR: invalid input syntax for integer: "ayadav2_FCS64X0_temp" [fo	5	Top > All Wireless Office	Aruba
Tue Jan 12 16:02:08 2016	System	Device	Aruba 7210 Aruba7210 Device Monitor: update() - DBD::Pg::st execute failed: ERROR: invalid input syntax for integer: "ayadav2_FCS64X0_temp" [fo	5	Top > All Wireless Office	Aruba
Tue Jan 12 15:57:08 2016	System	Device	Aruba 7210 Aruba7210 Device Monitor: update() - DBD::Pg::st execute failed: ERROR: invalid input syntax for integer: "ayadav2_FCS64X0_temp" [fo	5	Top > All Wireless Office	Aruba

Table 109: *Event Log Fields*

Column	Description
Time	Date and time of the event.

Table 109: *Event Log Fields (Continued)*

Column	Description
User	The W-AirWave user that triggered the event. When W-AirWave 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 NMS Servers" on page 65 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 W-AirWave 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

W-AirWave monitors key aspects of wireless LAN performance. When certain conditions or parameters arise that are outside of normal bounds, W-AirWave 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 221 to configure triggers.

Creating New Triggers

W-AirWave monitors key aspects of your network performance. When certain conditions or parameters arise that are outside of normal bounds, AirWave triggers alerts that enable you to address problems, often before users have a chance to report them.

To create a trigger:

1. Navigate to **System > Triggers**, then click **Add**.
2. Select the type of trigger from the drop down menu.

Figure 119: *Selecting the Type of Trigger*
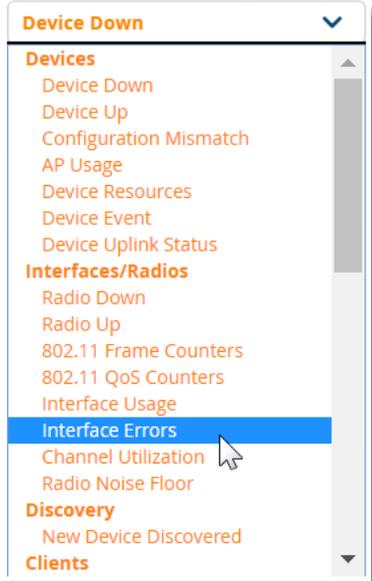
3. Select the severity level.

4. Select whether W-AirWave matches all or any trigger conditions, then click **Add**. In many cases, you must configure at least on condition setting. For more information about trigger conditions, see "Types of Triggers" on page 222.

5. Configure the trigger restrictions:

    - Folder. Limits the trigger to apply to devices in the selected folder.

    - Include Subfolders. Limits the trigger to apply to devices in the selected folder and subfolders.

    - Group. Limits the trigger to apply to devices in the selected group.

    Selecting folder and group applies the trigger to the intersection of devices in both group and folder.

6. Enter alert notifications, including a note that will be included with the alert. This note will appear with the alert on the **System > Alerts** page. Alert notification settings include:

    - Email. Enter the sender and recipient email addresses.

    - NMS. Choose one or more of the pre-defined trap destinations, which are configured on the **AMP Setup >NMS** page. This option is available if an NMS server has been added to W-AirWave.

    - Logged Alert Visibility. Choose how this trigger is distributed. The trigger can distributed according to how is it generated (triggering agent), or by the role with which it is associated.

    - Suppress Until Acknowledged. Choose whether the trigger requires manual, 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.

7. Click **Add** to save the trigger. The trigger appears the next time you go to the **System > Triggers** page.

Types of Triggers

The following sections provide information about the triggers and condition settings you can apply to each one.

- "Device Triggers " on page 223
- "Interface and Radio Triggers" on page 225
- "Discovery Trigger" on page 226
- "Client Triggers" on page 227

- "RADIUS Authentication Triggers" on page 228
- "RADIUS Accounting Triggers" on page 1
- "IDS Event Triggers" on page 228
- "Health Triggers" on page 229

Device Triggers

To set a trigger for devices, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the device triggers described in Table 110

For more information on creating a device trigger for hardware errors, see "Triggers for hardware monitoring" on page 224.

Table 110: *Device Triggers*

Name	Description and Conditions
Device Down	This type of trigger activates when an authorized, monitored AP has failed to respond to SNMP queries from W-AirWave. 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. W-AirWave 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 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.

Table 110: *Device Triggers (Continued)*

Name	Description and Conditions
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 W-AirWaves, W-AirWave creates two default trigger definitions for Device Events: ● SNMP Trap Category of **Hardware** or **Software** ● Event Type is **Syslog** and **Syslog Severity** >= **Critical** For help creating these triggers, see "Triggers for hardware monitoring" on page 224
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.

Triggers for hardware monitoring

W-AirWave provides triggers that alert you to hardware failures to your APs, Dell switches, and hardware components.

To create a trigger for device hardware failures:

1. Navigate to the **System > Triggers** page, then create trigger as a device event.

2. Select the event severity: None, Minor, Major, or Fatal.

3. Add the trigger condition in W-AirWave with the trigger conditions shown in Figure 120.

Figure 120: *Example Trigger Conditions*

4. Configure the switch for sending syslog messages:

```
HP-Switch-5406Rzl2(config)# logging facility syslog
HP-Switch-5406Rzl2(config)# logging <Airwave _IP>
```

The hardware triggers display in the Triggers table, as shown in Figure 121.

Figure 121: *Hardware Triggers*

Interface and Radio Triggers

To set a trigger for interfaces and radios on monitored devices, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the interface or radio triggers described in Table 111.

For more information on creating a new trigger, see "Creating New Triggers" on page 221.

Table 111: *Interface and Radio Triggers*

Name	Description and Conditions
Radio Down	Indicates that a device's radio is down 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.
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**.
Interface Errors	Indicates that errors have occurred while transmitting and receiving traffic over the selected interface, device, or interface label. Available conditions are **Device Type**, **Interface Errors Combined (%)**, **Interface Errors In (%)**, **Interface Errors Out (%)**, **Interface Label**, **Interface Mode**, **Interface Name**, and **Interface Type**. For information about creating these triggers, see "Triggers for Interface Errors" on page 226.

Table 111: *Interface and Radio Triggers (Continued)*

| Name	Description and Conditions
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 a specified period of time.

Triggers for Interface Errors

You can create alerts to help you monitor interface errors by setting criticial thresholds depending on the interface type.

To create a trigger for interface errors:

1. Navigate to **System > Triggers**, select **Interface Errors** from the list, as shown in Figure 122.

Figure 122: *Selecting the Interface Error Trigger*
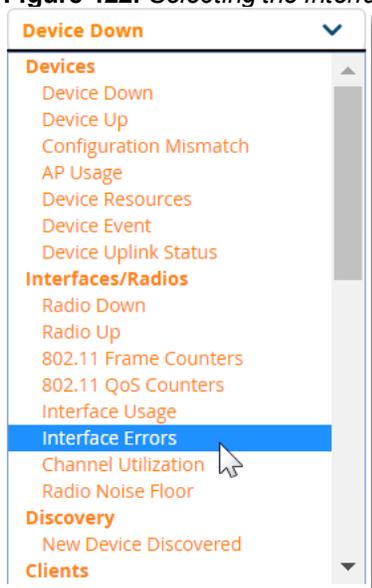
2. Apply match conditions. Figure 123 shows an alert for a switch interface that is showing 1% or more input errors for 5 minutes.

Figure 123: *Interface Errors Trigger*

Discovery Trigger

To set a discovery trigger, click the **Type** drop-down list on the **System > Triggers > Add** page and select the New Device Discovered trigger. Table 112 describes the trigger.

For more information on creating a new trigger, see "Creating New Triggers" on page 221.

Table 112: *Discovery Trigger*

Name	Description and Conditions
New Device Discovered	This trigger type flags the discovery of a new AP, router, or switch connected to the network (an device that W-AirWave 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)

Client Triggers

To set a user-related trigger for clients, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the client triggers described in Table 113.

For more information on creating a new trigger, see "Creating New Triggers" on page 221.

Table 113: *Client Triggers*

Name	Description and Conditions
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 user names 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).

Table 113: *Client Triggers (Continued)*

Name	Description and Conditions
Inactive Tag	This trigger type flags events in which an RFID tag has not been reported back to W-AirWave 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.
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.

RADIUS Authentication Triggers

To set a trigger for RADIUS authentication issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the RADIUS authentication triggers described in Table 114.

For more information on creating a new trigger, see .

Table 114: *RADIUS Authentication Triggers*

Name	Description and Conditions
Client RADIUS Authentication Issues	This trigger type sets the threshold for the maximum number of failures before an alert is issued for a user. The **Option**, **Condition**, and **Value** fields allow you to define the number of authentication issues per client that will trigger an issue.
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 number of authentication issues per device that will trigger an issue.
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.

IDS Event Triggers

To set a trigger for Intrusion Detection System (IDS) events, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the IDS event triggers described in Table 115.

For more information on creating a new trigger, see .

Table 115: *IDS Event Triggers*

Name	Description and Conditions
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 Condition** to specify the count characteristics that trigger an IDS alert.

Name	Description and Conditions
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 198 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.

Health Triggers

To set a trigger for W-AirWave server health issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the health triggers described in Table 116.

For more information on creating a new trigger, see "Creating New Triggers" on page 221.

Table 116: *Health Triggers*

Name	Description and Conditions
Disk Usage	This trigger type is based on the disk usage of W-AirWave. This type of trigger indicates that disk usage for the W-AirWave 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 W-AirWave suffers performance degradation due to lack of disk space.
System Resources	For the System Resources trigger, you must configure at least one matching condition before you save the new trigger. The available matching conditions are **CPU Utilization Percentage**, **Disk I/O Utilization Percentage**, and **Memory Utilization Percentage**.

Viewing, Delivering, and Responding to Triggers and Alerts

This section describes triggers and alerts and contain the following topics:

- "Viewing Triggers" on page 232
- "Delivering Triggered Alerts" on page 233
- "About Alerts" on page 229
- "Responding to Alerts" on page 233

W-AirWave monitors key aspects of wireless LAN performance. When certain parameters or conditions arise that are outside normal bounds, W-AirWave generates (or triggers) alerts that enable you to address problems, frequently before users have a chance to report them.

About Alerts

You can find the **Alert Summary** table by responding to the **Alerts** or **Severe Alerts** icons that appear in the status bar at the top of all W-AirWave pages, or by navigating to one of the following pages:

- **APs/Devices > List**
- **APs/Devices > Monitor**
- **Groups > Monitor**
- **Home > Overview**

- **Clients > Connected or Client Detail**
- **System > Alerts**

Clicking any of the hyperlinks in the **Type** column opens a detailed view for the selected alert.

Figure 124: *Alert Summary on the APs/Devices > Monitor page*

Alert Summary				
TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	1	1	10/12/2016 5:18 PM CST
IDS Events	162	1826	5139	10/13/2016 6:18 AM CST
RADIUS Accounting Issues	0	2	8	10/12/2016 11:12 AM CST
RADIUS Authentication Issues	205	3264	7581	10/13/2016 6:16 AM CST

> **NOTE**
>
> For information about setting the severe alert threshold, see "Setting Severe Alert Warning Behavior" on page 27.

Types of Alerts

AMP Alerts

Click the AMP Alerts link shown in Figure 124to open the **AMP Alerts** page. This page includes a **Summary** table that describes the AirWave (AMP) Alert type, and the number of times that event occurred over the past 2 hours and the last 24 hours. The **Alerts** table appears below the **Summary** table, and includes the following information for each AMP Alert:

- Trigger Type: Name of the AMP Alert trigger
- Trigger Summary: Description of the AMP Alert trigger
- Triggering Agent: MAC address of the device that triggered the alert
- Severity: Alert severity level
- Time: Timestamp for the alert

IDS Events

Click the IDS Events link shown in Figure 124 to open the **IDS Events** page. This page includes a **Summary** table that describes the Intrusion Detection System (IDS) event type, and the number of times that event occurred over the past 2 hours and the last 24 hours. The **IDS Events** table appears below the **Summary** table, and includes the following information for each IDS eventt:

- Severity: Event severity level
- Category: IDS category for the event
- Scope: Indicates of the scope of the IDS event impacts an *AP*, *Client or AP*, *Client* or *Probe*.
- Attack: Name of the IDS Event
- Detail: Details about the IDS Event type, if available
- Attacker: MAC address of the device that triggered the IDS event
- Target: MAC address of the device that was the target of the IDS attack
- Time: Timestamp for the event

RADIUS Events

Click the RADIUS Authentication Issues link, or the RADIUS Accounting Issues link, shown in Figure 124 to open the **RADIUS Issues** page. This page includes a summary table that describes the event type, and the number of times that event occurred over the past 2 hours and the last 24 hours.

The **RADIUS Authentication issues** table and the **RADIUS Accounting issues** table appear below the **Summary** table. You can view the following information for each RADIUS event:

- Event: Name of the RADIUS event
- Username: user name of the device that triggered the event
- Client MAC Address: MAC address of the client that triggered the event
- Client IP address: IP address of the client that triggered the event
- AP/Device: AP or device to which the client is associated
- BSSID: BSSID of the AP radio
- Radio: PHY type of the AP radio (e.g., 802.11a, 802.11ac, etc.)
- Controller: Name of the Controller to which the device is associated
- RADIUS Server/RADIUS IP: Server name and IP address of the RADIUS server
- Time: Timestamp for the event

Viewing System Alerts

Open the **System > Alerts** page by navigating to **System > Alerts**, or by selecting the **Alerts** or **Severe Alerts** icon on the status bar at the top of the W-AirWave WebUI. Figure 125 illustrates the **System > Alerts** page.

Figure 125: *System > Alerts Page Illustration*

1-21 ▾ of 21 Alerts   Page 1 ▾ of 1   Choose columns   Export CSV

	Trigger Type	Trigger Summary	Triggering Agent	Time ▾
☐	Device Down	Device has rebooted: Device uptime value changed (current: (more...)	1341-AP118	1/11/2016
☐	Device Down	Device has rebooted: Device uptime value changed (current: (more...)	1341-AP118	1/11/2016
☐	Device Down	Device has rebooted: Device uptime value changed (current: (more...)	1341-AP118	1/11/2016
☐	Device Down	Device Type is Access Point	1344-1-AP16	1/9/2016 7
☐	Device Down	Device Type is Access Point	1344-1-AP16	1/9/2016 7

View Acknowledged Alerts

For each new alert, the **System > Alerts** page displays the information described in Table 117.

Table 117: *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.

Table 117: *System > Alerts Fields and Default Settings (Continued)*

Field	Description
Severity	Displays the severity code associated with that trigger
Details	Displays additional details for alerts.

Viewing Triggers

W-AirWave provides default triggers to help you monitor your devices, hardware, and disk usage. Using syslog messages, W-AirWave monitors devices for hardware failures and alerts you to problems on the **System > Triggers** page, as shown in .

Click any of the column headings in this table to sort the data.

Figure 126: *Triggers Table*

describes the fields that you see in the **Triggers** table.

Table 118: *Triggers Fields and Descriptions*

Field	Description
Type	Trigger type
Trigger	Condition that generated the trigger alert
Additional Notification Options	This column indicates whether the alert will be distributed via email, to a network management system (NMS), or to both.
NMS Trap Destinations	The NMS server to which the trigger is sent. NMS trap destinations are configured on the **AMP Setup >NMS** page. Note that this option is only available if an NMS server has been added to W-AirWave.
Severity	Severity level assigned to the trigger
Folder	Indicates if the trigger applies only to APs/Devices in the specified folder. . **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.
Group	Indicates if the trigger applies 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.
Include Subfolders	Indicates if the trigger applies only to APs/Devices in the specified folder, or to that folder and all of its subfolders.

Table 118: *Triggers Fields and Descriptions (Continued)*

Field	Description
Logged Alert Visibility	Indicates if the trigger is distributed according to how is it generated (triggering agent), or by the role with which it is associated.
Suppress Until Acknowledged	Options include: ● **No**. A new alert will be created every time the trigger criteria are met. ● **Yes**. An alert will be received the first time the criteria is met, and a new alert for the device is not created until the initial one is acknowledged.

Refer to for additional information.

Delivering Triggered Alerts

W-AirWave uses Postfix to deliver alerts and reports via email because it provides a high level of security and queues email locally until delivery. If W-AirWave 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 Your Data

W-AirWave 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 W-AirWave only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. W-AirWave 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 W-AirWave settings.

For information about running a backup and restoring from a backup, see "AMP Command Line Interface" on page B.

Viewing and Downloading Backups

To view current W-AirWave backup files, go to the **System > Backups** page. Figure 127 illustrates this page.

Figure 127: *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** pop up 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 W-AirWave data and save the file as nightly_data00[1-4].tar.gz. In previous W-AirWave versions, the scripts created both config backup and data backup files. In order to restore the W-AirWave data, it is only necessary to have most recent data backup file, and W-AirWave no longer uses or supports the config backup file, effective as of W-AirWave 6.3.2.

Manage Configuration Change Jobs

Schedule configuration change jobs are summarized in the **Scheduled Events** table on the **System > Configuration Change Jobs** page, illustrated in Figure 128. Select a AP or group in the **Device** or **Group** columns in this table to go to the monitoring page for that device or group. Select a folder in the **Folder** columns to go to the **AP's/Devices > List** page for that folder.

To edit an existing configuration change job:

1. Click the description of a change job in the **Description** column of the **Scheduled Events** table. The **System > Configuration Change Job Detail** window opens.

2. On the **System > Configuration Change Job Detail** window 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.

   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.

Figure 128: *System > Configuration Change Jobs and System > Configuration Change Jobs Detail*

Monitoring Firmware Upgrade Jobs

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 W-AirWave.

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 129: *System > Firmware Upgrade Jobs Page Illustration*

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 .

  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.

Refer also to .

Monitoring System Performance

The **System > Performance** page displays basic W-AirWave hardware information as well as resource usage over time. W-AirWave 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 W-AirWave over time.

Figure 130: *System > Performance Page Illustration (Partial Screen)*

Table 119 describes the system information, performance graphs, and statistics for AMON, RabbitMQ, Redis, database, and disk displayed on System page.

Table 119: *System Performance Page Graphs*

Field	Description
System Information	
Current Time	Displays the current time on the W-AirWave server.
CPU(s)	Basic CPU information as reported by the operating system.

Table 119: *System Performance Page Graphs (Continued)*

Field	Description
Memory	The amount of physical RAM and Swap space seen by the operating system. Refer to the *Dell Networking W-AirWave Server Sizing Guide* at **dell.com/support/manuals** 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 W-AirWave 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 W-AirWave 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 W-AirWave 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 W-AirWave. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If your W-AirWave 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, W-AirWave 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 (W-AirWave services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (W-AirWave, VisualRF and web server).
CPU Utilization by Worker/by Service	Displays reads and writes for workers (W-AirWave services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (W-AirWave, VisualRF and web server).
System Network Usage	All traffic in and out measured in bits per second of your primary network interface (Eth0 being the most common).

Table 119: *System Performance Page Graphs (Continued)*

Field	Description
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 inbound packets, and inbound packet processing rates, message processing rates, PAPI CPU utilization, and PAPI packet loss in your network. **NOTE:** W-AirWave can use DTLS to secure AMON traffic. If configured to do so, you will see inbound DTLS PAPI packets in the **AMON Packet Arrival / Processing Rate** widget. For information about uploading the DTLS certificate, see "CLI Options" on page B.
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.
Redis Statistics	
Redis Activity	Use this chart under the supervision of Dell support to troubleshoot Redis activity. Click any point in the chart to view Redis activity over the past day, week, month or year.
Redis Used Memory	Use this chart under the supervision of Dell support to troubleshoot Redis memory issues. Click any point in the chart to view the total number of bytes used by the Redis process over the past day, week, month or year.
Redis Keyspace	Use this chart under the supervision of Dell support to troubleshoot Redis keys. Click any point in the chart to view Redis Key usage over the past day, week, month or year.
Database Statistics	
Top 5 Tables (by row count)	The five largest tables in W-AirWave. 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 W-AirWave 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	

Table 119: *System Performance Page Graphs (Continued)*

Field	Description
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.

Troubleshoot System Performance

There are several initial steps that you can take to troubleshoot W-AirWave performance problems, including slow page loads and timeout errors. Initial troubleshooting steps includes 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 *Dell Networking W-AirWave Server Sizing Guide* or contact Dell support at **dell.com/support** for the latest recommendations.

Managing Mobile Devices with SOTI MobiControl and W-AirWave

Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Apple, and Android devices, has been integrated into W-AirWave to provide direct access to the MobiControl Web Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Refer to the following for additional information:

- "Prerequisites for Using MobiControl with W-AirWave" on page 239
- "Adding a Mobile Device Management Server for MobiControl" on page 240
- "Accessing MobiControl from the Clients > Client Detail Page " on page 240

Prerequisites for Using MobiControl with W-AirWave

In order to use the MobiControl integration in W-AirWave, the following is required:

- An W-AirWave 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 W-AirWave 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 W-AirWave, you must first add your MDM server and designate it as a MobiControl.

Adding a Mobile Device Management Server for MobiControl

1. To add an MDM server to W-AirWave, navigate to **AMP Setup > MDM Server** and click **Add**. Complete the fields on this page. Table 120 describes the settings and default values:

Table 120: *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, W-AirWave will connect to port 80 of the SOTI server; with HTTPS, W-AirWave 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 W-AirWave. 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 W-AirWave polls the MDM server. The default is 5 minutes.

2. When finished, select **Add.**

The list page for the MDM server also displays:

- **Last Contacted –** The last time W-AirWave was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, W-AirWave 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 W-AirWave, follow these steps:

1. Navigate to a page that lists clients. This can include:
   - **Clients > Connected** or **Clients > All**
   - Search results that display user MAC 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.

About the Home Page

The **Home** page provides customizable dashboard views, where you can monitor the health of your network services, mobile app usage, RF issues, UCC traffic, and Clarity data. It is also where you can access product documentation, manage W-AirWave licenses, and customize your user information and search preferences.

Monitoring Your Network Health

To view your overall network health, navigate to **Home > Overview**. The top header of the page display the status of your network, while the navigation pane on the left side of the page allows you to navigate through the W-AirWave WebUI.

Table 121 describes the sections and charts that appear in the Overview page.

Table 121: *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.
Client Health	This graph shows the percentage of clients with good, fair, and poor health. To view the new graph from the Home page, select **Client Health** from the **Clients** menu.
	The client health metric displayed in these charts is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting call data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries.
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 229). 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.

Section	Description
Quick Links	The **Quick Links** section provides drop-down menus that enable you to move to the most common and frequently used pages in W-AirWave as follows: ● **Go to folder**—This menu lists all folders defined in W-AirWave from the **APs/Devices List** page. See "Using Device Folders" on page 134. ● **Go to group**—This menu lists all groups defined in W-AirWave, 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 72. ● **View Latest Reports**—W-AirWave 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 Sending Reports" on page 264. ● **Common Tasks**—This menu lists quick links to the most heavily used task-oriented pages in W-AirWave, to include the following: ■ **Configure Alert Thresholds**—This link takes you to the **System > Triggers** page. See "Viewing Triggers" on page 232. ■ **Configure Default Credentials**—This link takes you to the **Device Setup > Communication** page. See "Configuring Communication Settings for Discovered Devices" on page 53. ■ **Discover New Devices on Your Network**—This link takes you to the **Device Setup > Discover** page. See "Device Discovery Overview" on page 119. ■ **Supported Devices and Features**—This link displays a PDF that summarizes all supported devices and features in chart format for W-AirWave. ■ **Upload Device Firmware**—This link displays the **Device Setup > Upload Firmware & Files & Files Upload** page. See "Loading Device Firmware Onto the W-AirWave Server (optional)" on page 55. ■ **View Event Log**—This link displays the **System > Event Log** page. See "Using the Event Log" on page 220.

You can add or remove widgets to change what W-AirWave reports on your dashboard. See "Customizing the Dashboard" on page 21 for more information.

Monitoring with AppRF

The **Home > AppRF** page displays mobile app usage and performance statistics to network administrators. Non-admin users can view information for the devices and folders to which they have access.

The AppRF dashboard provides a comprehensive overview on the different widgets available for AppRF. Each widget is presented as a directive, with various functions to view in-depth details on the users and applications within a widget.

Figure 131: *AppRF Dashboard*
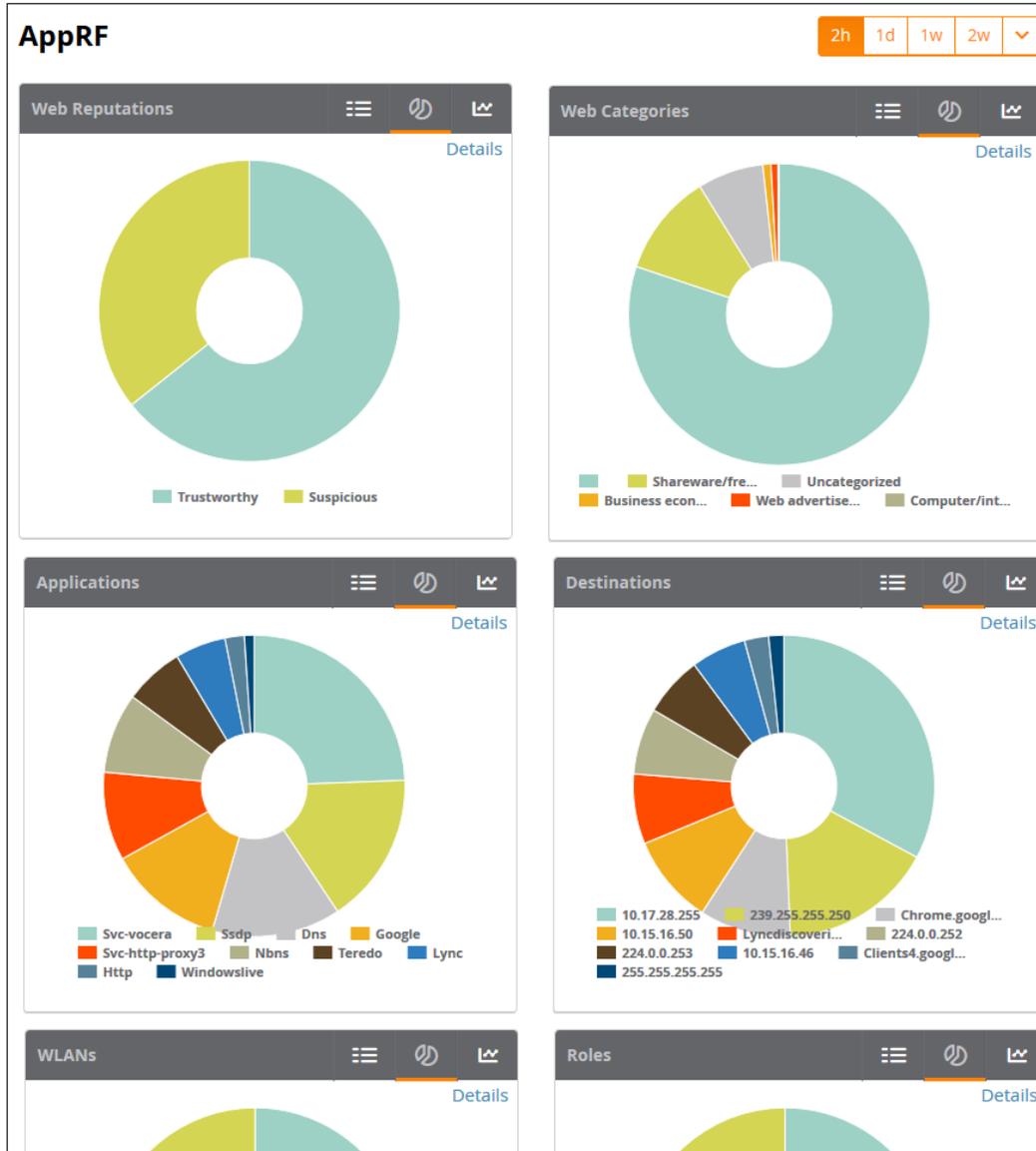
Each widget contains toggle buttons to switch between the following views:

- ▤ - List showing all the categories within the widget
- ⊘ - Donut chart representing the proportional usage of categories
- ⮑ - Usage graph displaying usage (in MB) over time

Widget Directives

The AppRF dashboard displays each widget as a directive, containing the following functions:

- **List**: List of categories available for each specific widget (for example, Application Categories: Social Media, Torrent, Chat Protocols, Games, Web Development Tools, Ad Blocker).
- **Details Link**: Link to the **Details** page, where you can view the following information for each category:
  - **Category**: Name of the user
  - **Bytes**: Total usage in bytes (MB)
  - **Packets**: Total number of packets transmitted/received

- **Web Reputation**: Web reputation, indicating the safety of the site
- **Web Category**: Website type
- **Destination**: Number of destinations reached through the given category
- **User Role**: Number of roles assigned to the user
- **Devices**: Number of devices connected to the given category
- **User Name**: Name of the user
- **Device MAC**: MAC address of the user
- **WLANs**: Number of WLANs to which the user is connected
- **Category Details**: Under the **Details** page of each widget, you can select a category to view details for the individual category.
- **Donut Chart**: Chart representing the proportional usage of categories within a widget. Hover your mouse above each section of the chart to view the category name and usage, in KB and percentage (%).
- **Usage Graph**: Graph displaying usage over time.

Using the UCC Dashboard

The UCC dashboard in W-AirWave displays charts that show UCC trends to network administrators. Non-admin users can view information for the devices and folders to which they have access.

Viewing Call Details

You can view call details by clicking the **Call Details** link at the lower-left of each graph. Information, such as the operating system of the client device, protocol used to complete the call, and connectivity type are all displayed in the table view. You can look for any device issues that are detected during the call in the **End-to-End Quality** field, or network quality issues in the **Mean Opinion Score (MOS)** field. The MOS is updated after a call has ended.

By default, the data in this table is displayed by the call start time, with the most recent call at the top of the list.

To change how the data is displayed, do any of the following:

- Click the column heading to sort the data.
- Click ▼ at the top of column headings to filter the data.
- Click the Show link to add parameters like Protocol to the table view.

Tips for Filtering Calls

If you want to reduce the amount of calls that appear as unknown, you can filter the results by call types. When you select **Voice**, the UCC dashboard shows only voice calls and conference calls. When you select **Others**, any other type of call, such as video and desktop sharing, is reported.

The UCC dashboard also displays calls based on the end-to-end call quality. When you select **WLAN**, information displayed is based on the UCC score of the calls.

> **NOTE:** If Heuristics is enabled in W-AirWave and there is no end-to-end call quality information, W-AirWave will display information based on UCC call quality (see "Additional AMP Services" on page 36).

Viewing UCC Charts, Graphs, and Tables

W-AirWave aggregates UCC call data and presents them in charts, graphs, and tables. Hovering over the charts displays details about the highlighted section of that chart.

Call Quality

Call quality is measured by a metric called the UCC score. This metric takes into account delay, jitter, and packet loss. W-AirWave obtains these metrics from RTCP messages sent from the client (if the client is capable of sending them). For audio calls, W-AirWave obtains these metrics from the Dell AP that inspects the RTP flows.

The following table describes the UCC scores and quality indications.

Table 122: *UCC Quality Levels*

UCC Score	Quality Indication
71 or greater	Good quality seen by the network
31 to 70	Fair quality seen by the network
0 to 30	Poor quality seen by the network

To view call quality information, click the following hyperlinks:

- Trend. This chart shows the number of calls with good, fair, or poor client health over the selected time period.
- Distribution. This graph shows the relative proportions of calls with each quality type.
- APs. This chart shows information about APs that supported poor quality calls.
- Folder. This table view shows all folders that carried calls and, for each folder, the percentage of calls that were rated poorly by UCC.

Quality Correlation

These graphs display the correlation between call quality and client health. The client health metric displayed is the efficiency at which that AP transmits downstream traffic to a particular client. W-AirWave determines this value by comparing the amount of time the AP spends transmitting call data to a client to the amount of time that would be required under ideal conditions at the maximum Rx rate supported by client, without data retries.

For example, a client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or is sending 3 extra transmissions to that client for every packet.

To view quality correlation information, click one of the following hyperlinks:

- Trend. This chart shows the number of calls with good, fair, or poor client health over the selected time period.
- Scatterplot. This chart shows a historical view of the call quality and client health of each individual call. To view call details for a specific client, click on a call session (see "Viewing End-to-End Call Details" on page 246).
- Connectivity. This table view shows the number of calls of each quality level (good, fair, poor, and unknown) by connectivity type (wired to Wi-Fi, wired to external, wired to wired, Wi-Fi conference, Wi-Fi to external, and Wi-Fi to Wi-Fi).

Call Volume

To view call volume information, click one of the following hyperlinks:

- Trend. This graph and table displays the number of calls made during the selected time period using a UCC application, such as SIP, Lync, and FaceTime.
- APs. This graph displays the names of the APs that supported these calls.

Devices

These graphs display information about the calls made by different device types, such as Windows 7, Mac OS X, iPhone, or Android devices.

- Trend. This graph show the numbers of calls by each platform type over the selected time period.
- Distribution. This chart shows the relative proportion of calls that originated form each device type.
- Quality. This graph shows the numbers of calls at each quality level made by each device type.

Viewing End-to-End Call Details

For an end-to-end view about a call, go to **Home > UCC > Call Quality > Call Details** and click the magnifying glass icon in the **Details** column. Overall client health is rated good, fair, or poor (see "Quality Correlation" on page 245 for information about the UCC score).

Client information, such as a description of the client device (shown as the operating system of the device in Figure 132), the signal-to-noise (SNR) ratio for the call on the client's connection, speaker and microphone glitch rate, and transaction rates, are provided in this table view.

Figure 132: *End-to-End View*
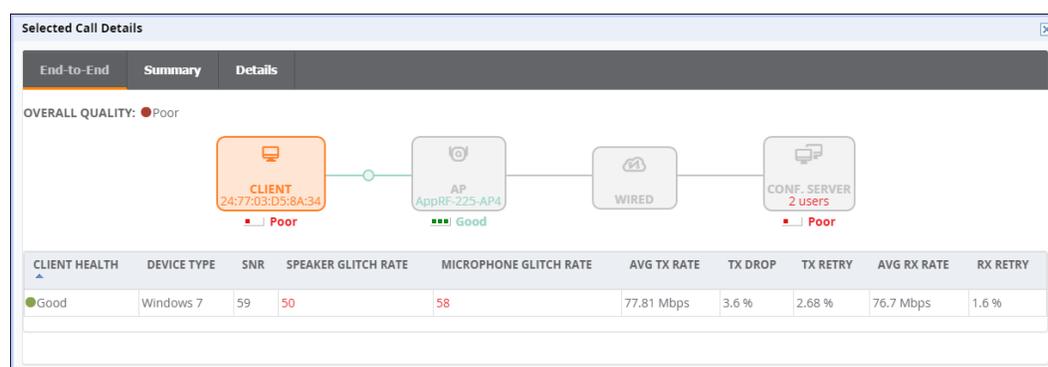
Figure 133: *AP Details in the End-to-End View*
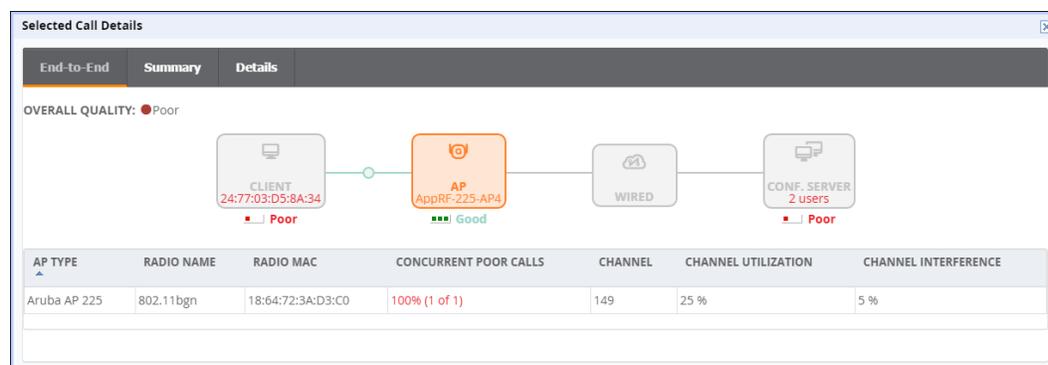
Table 123: *AP Details*

Column Name	Description
AP Type	The type of AP to which the client is connected.
Radio Name	The AP's radio being used for the call (802.11bgn or 802.11ac)
Radio MAC	The AP radio's MAC address.

Table 123: *AP Details (Continued)*

Column Name	Description
Concurrent Poor Calls	The number of poor calls occurring simultaneously with the call being viewed.
Channel	The channel used for the call.
Channel Utilization	The used channel's utilization as a percentage.
Channel Interference	The interference impacting the used channel as a percentage.

Get Call Summary

Use the **Summary** tab to see more call details and a graph displaying the quality of the call as it progressed. Hovering over the graph displays a snap-shot of the call at two-minute intervals, which can help you identify when changes occurred during the call.

Figure 134: *Call Summary Information*
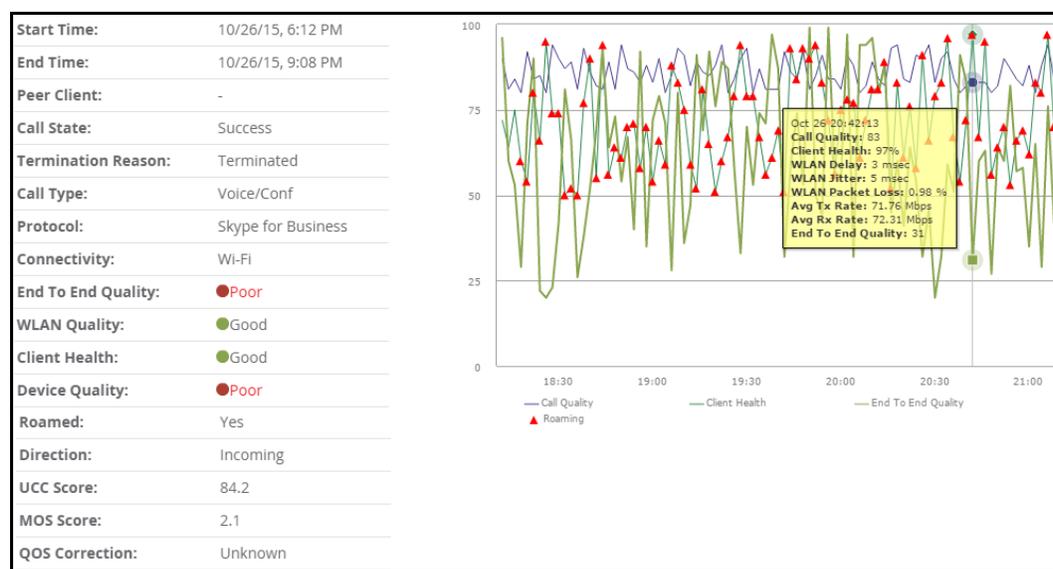
To view more details about a call, click the **More** link at the lower right of the Summary tab.

- Microphone Details. This information about the client's microphone includes manufacturer and model, the capture device driver, glitch rate, and audio microphone error.
- WLAN. This information repeats some of that shown on the End-to-End tab, in addition to WLAN delay, jitter, and packet loss.
- End To End. This information, about the connection between the caller and receiver, includes MOS, delay, jitter, packet loss, and burst gap details.
- End Point Details. This information about the device used by the caller includes IP address, Wi-Fi device driver, CPU details, and OS.
- Speaker Details. This information describes the type of speaker used by the caller.

For a granular look at a specific call, click the Details Tab. It shows the same information found on the Summary tab in table divided into two-minute intervals.

Using the UCC Report

The UCC report provides an overall look at UCC activity on your network in the specified time period. This information is displayed in a series of tables representing the top connectivity types, call types, application types, device types, folders, APs, and clients with the highest percentage of poor quality calls.

Table 124: *UCC Report Fields*

Field	Description
Quality Metric	The metric used to determine the quality of calls.
Connectivity Type	The type of connection (such as Wi-Fi to Wi-Fi or Wi-Fi to external) used to complete calls.
Call Type	The type of call, such as voice or video.
Application Type	The software application used to complete a call.
Device Type	The client device used to complete a call. The device type is displayed as the device's operating system.
% of Poor Calls	The percentage of poor calls completed on the specified metric such as device type, application type, etc.
Poor Calls	The number of poor calls completed on the specified metric such as device type, application type, etc.
Total Calls	The total number of calls completed on the specified metric such as device type, application type, etc.
Folders	The device folder from which calls were completed.
APs	The APs that carried calls.
Clients	The clients who completed calls. This is displayed by MAC address and user name.
% of Poor Calls by MOS Score	The percentage of poor calls completed by a folder, AP, or client based on the MOS Score.
% of Poor Calls by UCC Score	The percentage of poor calls completed by a folder, AP, or client based on the UCC Score.
Average Client Health (Poor Calls)	The average client health when completing a call.
Total Calls	Total number of calls from a folder, AP, or client.
Total Call Time	Total call time of all calls from a folder, AP, or client.

Viewing RF Performance

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 Dell Networking W-Series devices that support AMON. The Health graph and chart are only populated with information from controllers running ArubaOS 6.3 or greater.

Figure 135: *Home > RF Performance*

Clients

CLIENTS ▲	2.4 GHZ	5 GHZ
a	-	2
ac 20 MHz	-	12
ac 40 MHz	-	328
b	6	-
n 20 MHz	44	30
n 40 MHz	0	152
Total	**50**	**524**

Least Healthy Clients

CLIENT	HEALTH (%) ▲
lioneljohn.gabrillo	3
rildo.oliveira	4
giovanni.anele	5
karine.ceita	7
vlam	10

Lowest SNR Clients

CLIENT	SNR (DB) ▲
gchittipedhi	8
leonardo.setani	14
giovanni.anele	14
ttrotter	15
karine.ceita	16

Lowest Speed Clients

CLIENT	SPEED (MBPS) ▲
sailaja.brahmandam	1
-	1
pguda	6
gchittipedhi	6
prakash.guda	6

You can click on a value in any of the graphs to view the associated list of clients.

Figure 136: *Drill down to view all clients*
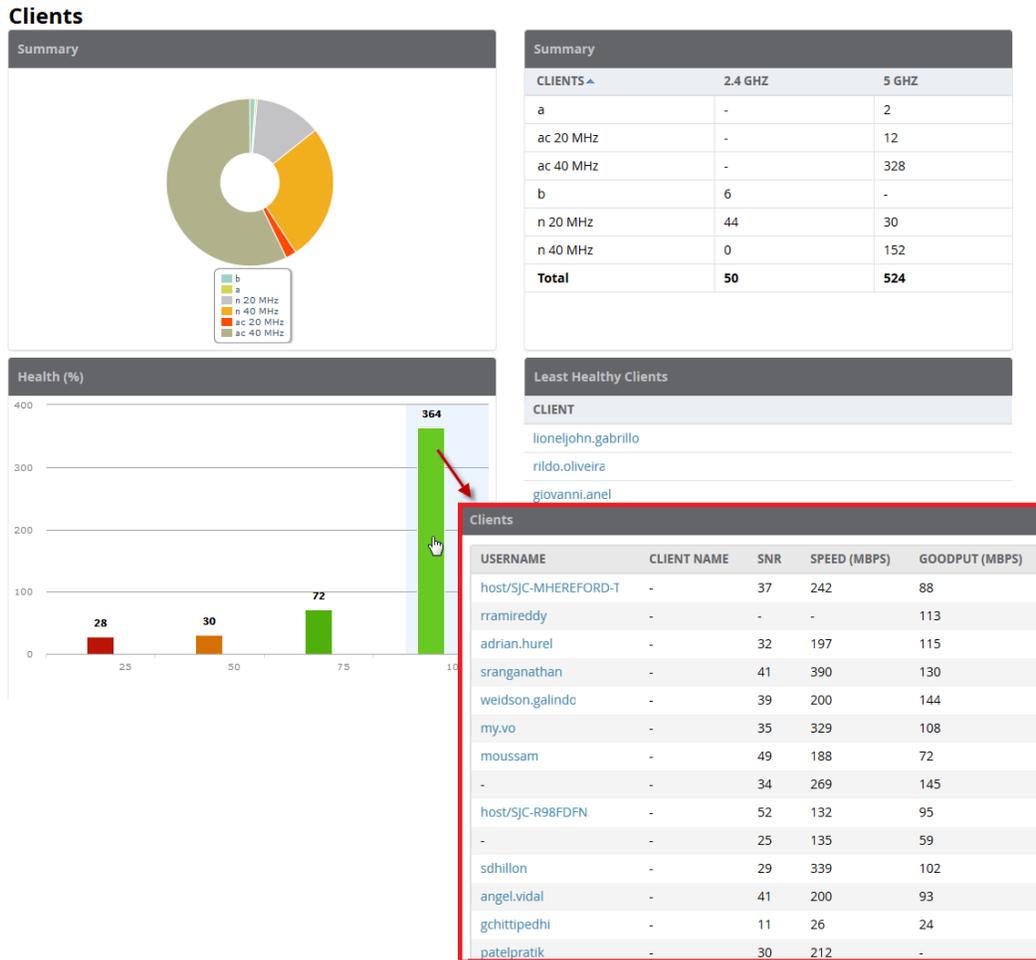
When the client information is displayed, an additional drill down is available to view information for a specific client, device, or location.

> **NOTE**
>
> When you click on a user name 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 RF Capacity

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 137: *The Home > RF Capacity page*
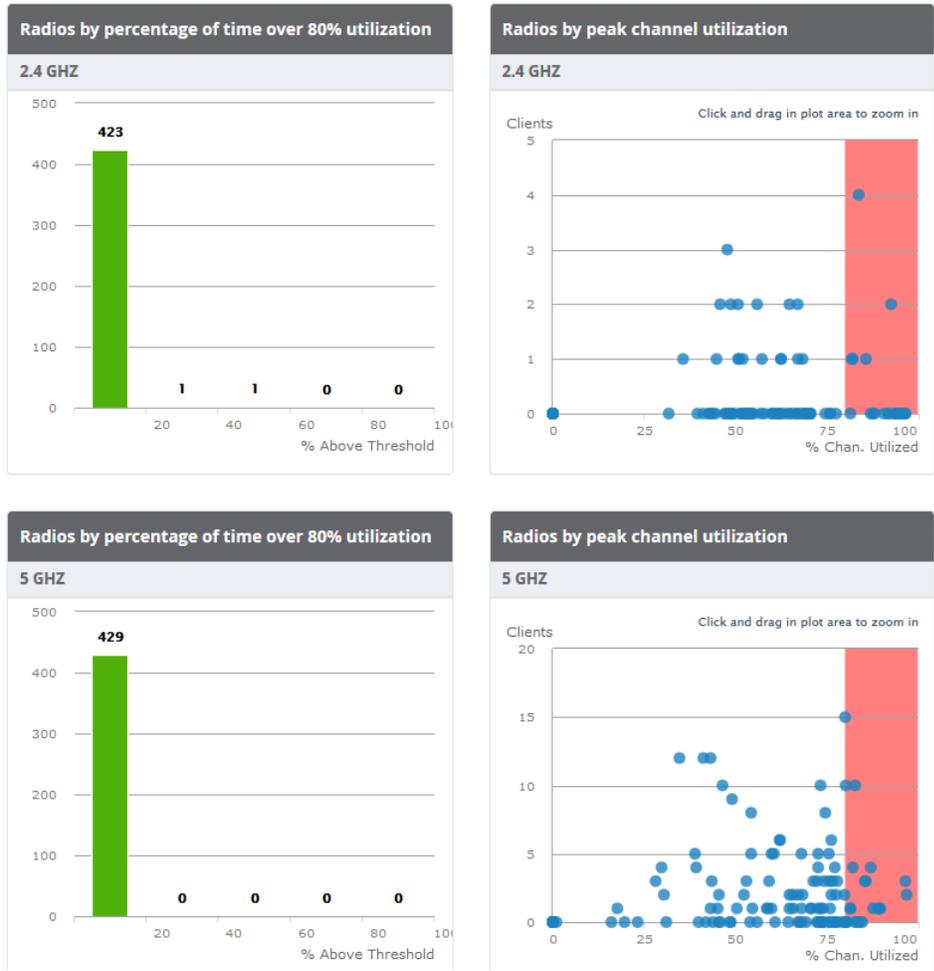
You can click on a bar in the upper graphs to view a pop up showing a detailed list of the devices that connected in the week before the RF Capacity page was run. This pop up includes additional drill downs to the device, the controller, and the folder. You can also search in this pop up.

Figure 138: *Example of 2.4 GHz radio pop up*

APS/DEVICES	MAX. UTILIZATION ▼	% OF TIME ABOVE THRESHOLD	AP TYPE	CONTROLLER	AP FOLDER
1341-AP127	96.4567	14.13	AP 325	Chuck	Top > HQ
1341-AP117	96.4567	11.14	AP 325	Chuck	Top > HQ
1341-AP102	96.063	4.17	AP 325	Chuck	Top > HQ
1341-AP112	96.063	5.89	AP 325	Chuck	Top > HQ
1341-AP126	95.6693	9.81	AP 325	Chuck	Top > HQ
1341-AP124	95.6693	7.7	AP 325	Chuck	Top > HQ
1341-AP129	95.6693	4.16	AP 325	Chuck	Top > HQ
1341-AP116	95.6693	7.14	AP 325	Chuck	Top > HQ
1341-AP115	95.6693	5.03	AP 325	Chuck	Top > HQ
1341-AP108	95.6693	9.86	AP 325	Chuck	Top > HQ
1341-AP99	95.2756	5.16	AP 325	Chuck	Top > HQ
1341-AP105	95.2756	0.59	AP 325	Chuck	Top > HQ
1341-AP104	95.2756	2.15	AP 325	Chuck	Top > HQ
1341-AP106	95.2756	0.8	AP 325	Chuck	Top > HQ

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 139: *Example pop up showing channel utilization*
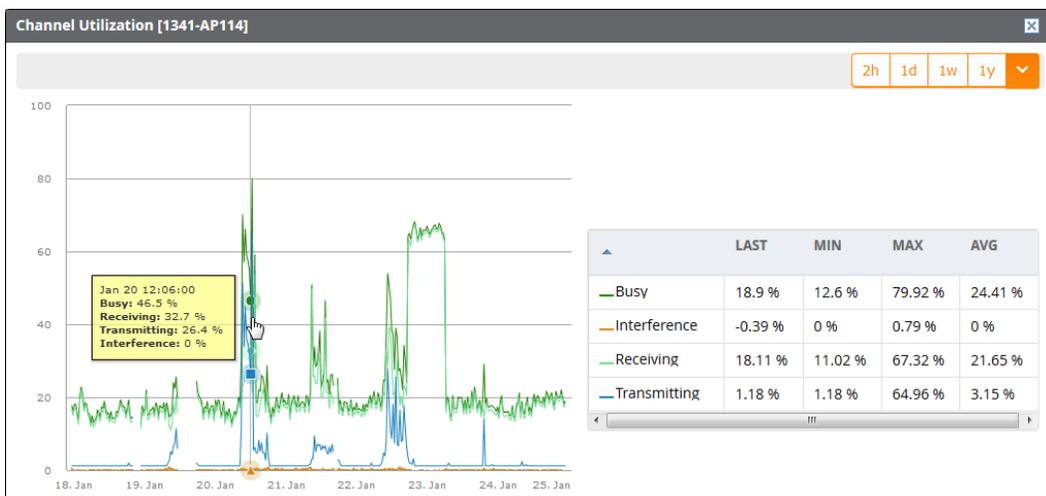
Viewing Network Deviations

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 W-AirWave 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 W-AirWave.

Figure 140: *Home > Network Deviations page*
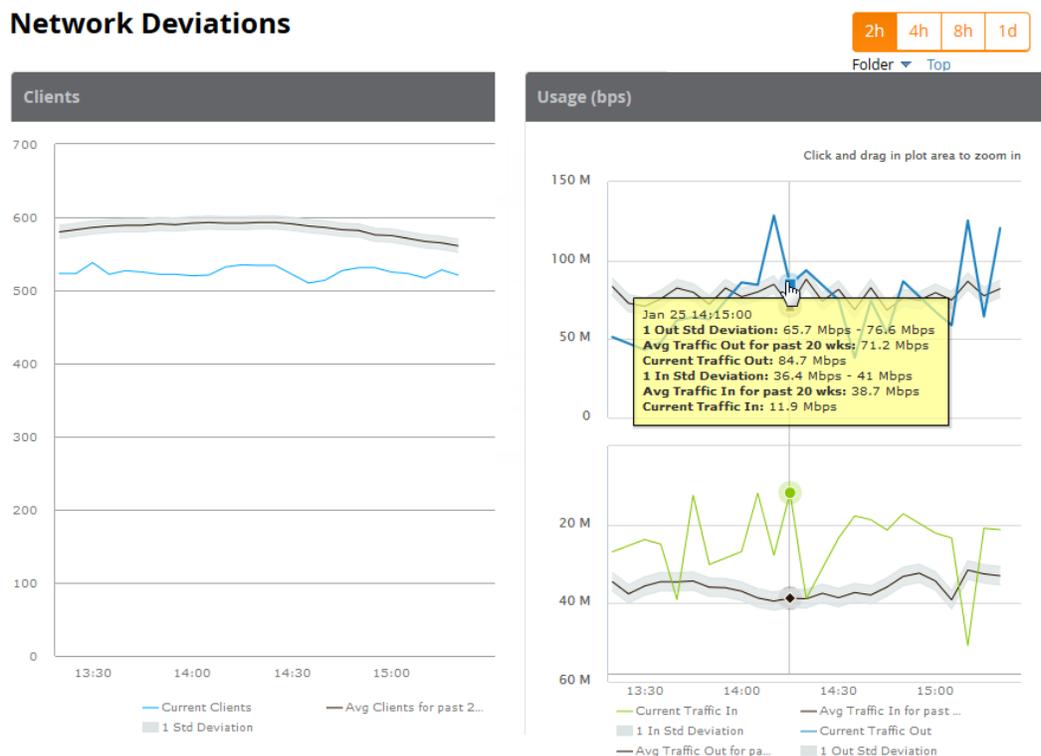
The first time this page is launched, the graphs will display information for all devices in the Top folder. To specify a different folder, simply select one from the folder drop down in the upper-right corner, and then refresh the page. W-AirWave will remember the new setting the next time that the page is launched.

By default, the graphs display average and standard deviation information for the current time over the last 40 weeks. Click the **gear icon** in the upper right corner to change these defaults. W-AirWave 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 141: *Network Deviations Threshold*
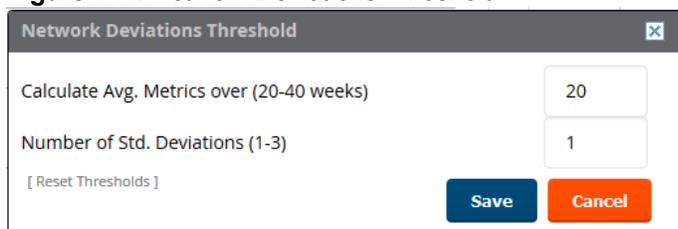
How Standard Deviation is Calculated

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.

How to Use Search

The **Search** field at the top of every W-AirWave page provides a simple way to find devices, clients, groups, and rogues. You can search for things like notes, versions, serial numbers, IP addresses (IPv4 or IPv6), and MAC addresses.

To find something using the Search field:

1. Click .

2. In the Search field, type a keyword or the first few letters and numbers. For example, Figure 142 shows the the search results for "00:".

3. Select one of the following search methods:

- Press Enter. You can change this default search method preference in the **Home > User Info** page.

- Click the down arrow and select a method from the list of search options.

- Click [Q] to see quick search results, showing connected clients, which might already be your default search method.

Results include hypertext links to additional pages, and the **Filter** icon over some columns allows for additional filtering of search returns.

Figure 142: *Home > Search Page Illustration with Sample Hits on 00: (partial view)*
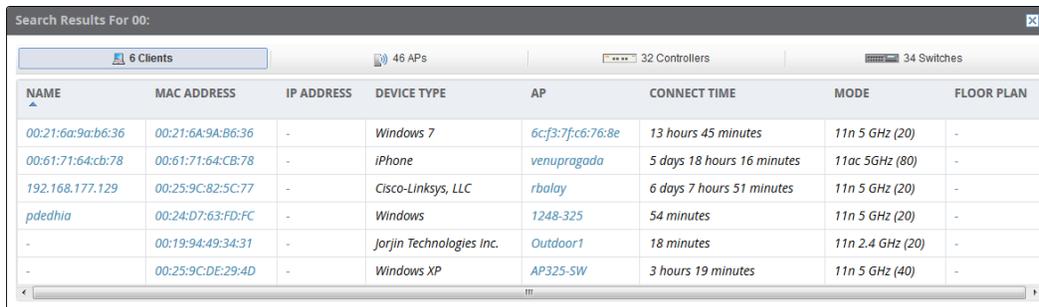
NAME	MAC ADDRESS	IP ADDRESS	DEVICE TYPE	AP	CONNECT TIME	MODE	FLOOR PLAN
00:21:6a:9a:b6:36	00:21:6A:9A:B6:36	-	Windows 7	6c:f3:7f:c6:76:8e	13 hours 45 minutes	11n 5 GHz (20)	-
00:61:71:64:cb:78	00:61:71:64:CB:78	-	iPhone	venupragada	5 days 18 hours 16 minutes	11ac 5GHz (80)	-
192.168.177.129	00:25:9C:82:5C:77	-	Cisco-Linksys, LLC	rbalay	6 days 7 hours 51 minutes	11n 5 GHz (20)	-
pdedhia	00:24:D7:63:FD:FC	-	Windows	1248-325	54 minutes	11n 5 GHz (20)	-
-	00:19:94:49:34:31	-	Jorjin Technologies Inc.	Outdoor1	18 minutes	11n 2.4 GHz (20)	-
-	00:25:9C:DE:29:4D	-	Windows XP	AP325-SW	3 hours 19 minutes	11n 5 GHz (40)	-

For information on how to customize your search results, see .

Accessing W-AirWave Documentation

The **Home > Documentation** page provides easy access to all relevant W-AirWave documentation. All of the documents on this page are hosted locally by your W-AirWave 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 Dell support at **dell.com/support**.

Licensing in W-AirWave

You can view current licenses, verify your license count, and add new licenses from the **License** page. When you add switches to a stack, one W-AirWave license covers the switch stack.

Figure 143 illustrates this page, and Table 125 describes the contents.

Figure 143: *Home > License Page Illustration*
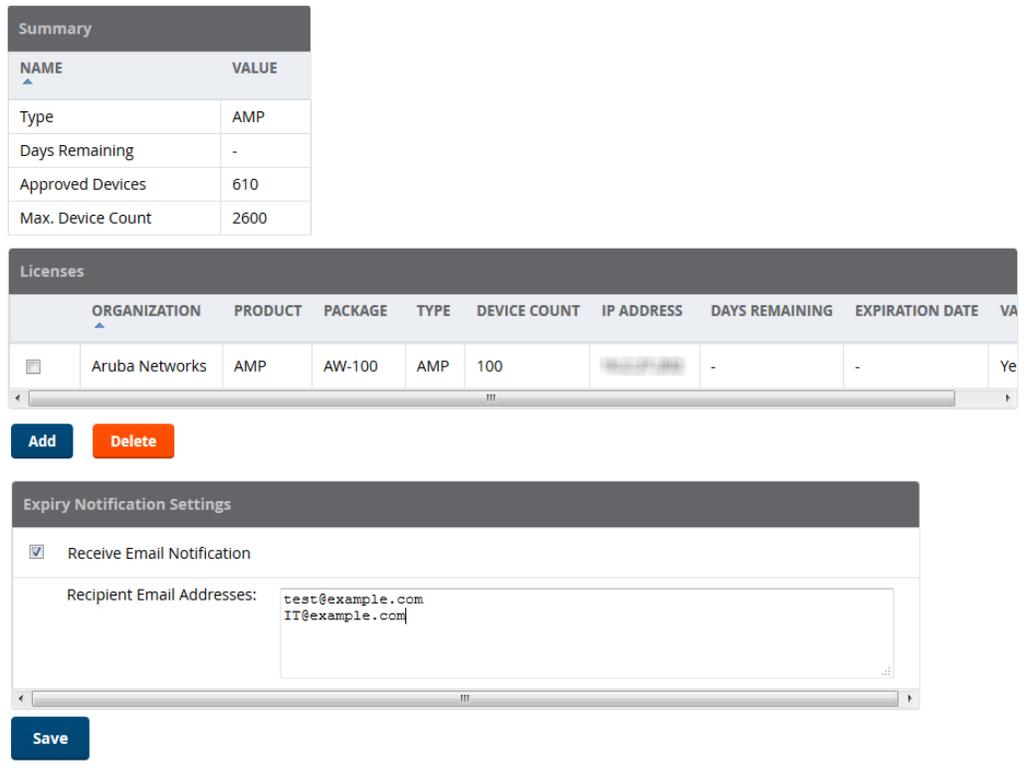
Adding licenses

To add a license:

1. Open the email containing your license key, and select and copy the text of that license.

2. From the **Home > License** page, click **Add**. A pop up window opens.

3. Paste the text of the license into the pop up window, and click **Add**. The Dell End-User License Agreement appears.

4. Review the license agreement, then click **I Accept**. The newly added license displays in the License table.

Viewing licenses

You can click in the license table to view a pop up that shows details of any license key.

Table 125: *License Table Fields and Descriptions*

Field	Description
Organization	Displays the organization listed on your license key.
Product	This product description is read directly from the license key.
Package	Displays the license type. For example, this could be a license for an enterprise W-AirWave server, or a smaller license to support additional devices.
Type	Shows whether the license is for a Master Console, an AirWave server, or a failover server.
Device Count	Number of devices supported by the license.

Table 125: *License Table Fields and Descriptions (Continued)*

Field	Description
IP Address	IP address of the W-AirWave server using the license. This address is read directly from the license key.
Days Remaining	Remaining number of days on a trial license.
Expiration Date	Expiration date of the temporary or evaluation license.
Valid	Indicates that the license is valid and active.

Configuring License Expiration Email Notifications

For licenses with an expiration date, the administrator can configure email messages to notify specified parties of when a license is set to expire. W-AirWave sends an expiration notification email six months, three months, one month, and one week prior to expiration. Additionally, the email lists time remain for each expiring license installed on the W-AirWave server. This feature is disabled by default.

To configure Expiry Notifications:

1. Navigate to **Home > License > Expiry Notification Settings**.
2. Check the **Receive Email Notifications** check box to enable.
3. Insert any number of email addresses separated by spaces, commas, or semicolons.
4. Click **Save**.

Configuring Your User Information

You can update your contact information, authentication information on the **User Information** page. You can also customize how W-AirWave displays header statistics, searches for data, and refreshes its display. Figure 144 illustrates the **Home > User Info** page.

Figure 144: *Home > User Info Page Illustration*

admin is logged in as a local database user with role Admin and Administrator access to RAPIDS.

Change Password

Current password for 'admin':
Password:
Minimum 8 chars with upper, lower, numeric, and non-alphanumeric characters.
Confirm Password:
Changing your password will log you out.

User Information

Name: Enter a Value
Email Address: Enter a Value
Phone: Enter a Value
Notes:

Top Header Stats

Filter Level For Rogue Count: Suspected Rogue
Customize Header Columns: Yes ○ No ●

Search Preferences

Search Method: Use system defaults

Display Preferences

Default Number of Records per List: 25 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
Default Client Chart Mode: Max
Timezone for UI Charts/Tables: Use system defaults

Save   Revert

Table 126 describes the settings on the User Information page.

Table 126: *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 204.
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 W-AirWave screen.
Stats	Select the specific data you would like to see in the Top Header Stats. Refer to the "Status Section" topic in the *Dell Networking W-AirWave 8.2.4 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.

Table 126: *Home > User Info Fields and Descriptions (Continued)*

Field	Description
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 pop up window rather than on the **Home > Search** page. This pop up 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, user name, 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, user name, device name, etc). This search is case-sensitive for all searched fields.
Display Preferences	
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 W-AirWave automatically ends the user session. This setting only the logged-in user of this W-AirWave. The default is 60 minutes. To set the max idle timeout for all users of this W-AirWave, see "Setting Up Login Configuration Options" on page 45.

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 W-AirWave.

- **Email Address**—Enter the email address to be used for alerts, triggers, and additional W-AirWave 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 W-AirWave users or administrators to understand the functions, roles, or other rights of the user being created.

Supporting Multiple W-AirWave Servers

You can monitor multiple W-AirWave servers using the Master Console. After you add the W-AirWave servers to Master Console, they will be polled for basic W-AirWave information.

The **Overview** page in the Master Console provides summary statistics for the entire network at a glance.

- Reports can be run from the **Master Console** to display information from multiple W-AirWave 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 W-AirWave 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 W-AirWave 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.

If you have the Master Console license, you can also monitor your multiple W-AirWave servers using AirWave Glass. For more information, see the *AirWave Glass 1.0.0 User Guide*.

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 W-AirWave. This feature is disabled by default for security reasons; no W-AirWave 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 . The URL of the public portal will be https://your.AMP.name/public. When you upgrade to the latest version of W-AirWave, the public portal is disabled by default, regardless of the type of license.

Figure 145: *Public Portal Page Illustration*
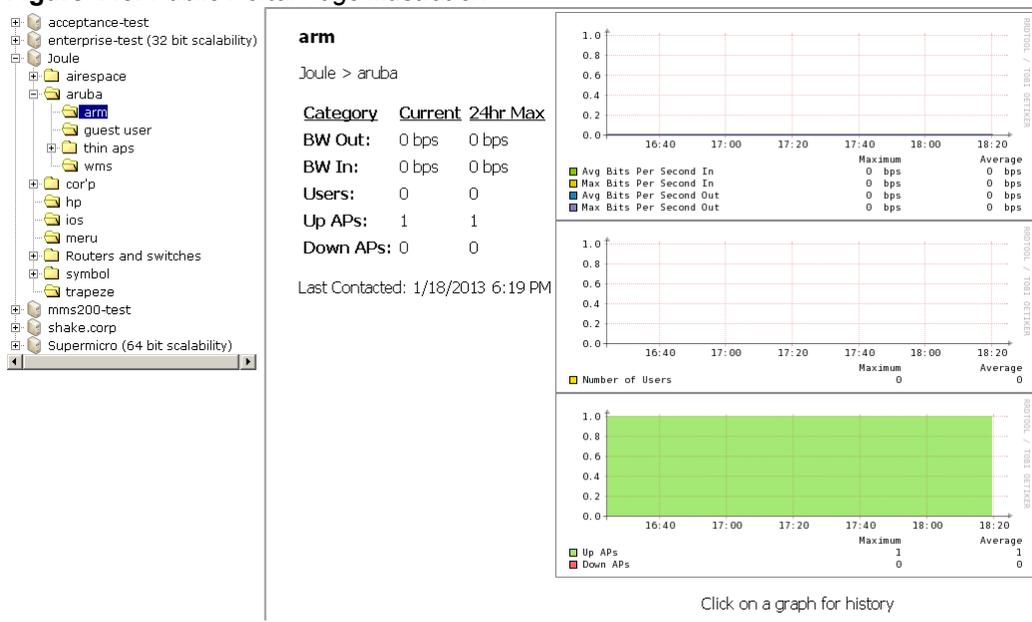
The Public Portal supports configuration of the iPhone interface, which can be configured using the Master Console W-AirWave page.

Adding a Managed AMP with the Master Console

Perform the following steps to add a managed W-AirWave 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 127.

Table 127: *Managed AMP fields and default values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the W-AirWave server to be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed W-AirWave server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed W-AirWave server.
Username	N/A	The user name used by the Master Console to login to the managed W-AirWave server. The user needs to be an AP/Device Manager or W-AirWave Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console to login to the managed W-AirWave server.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed W-AirWave server.

Table 127: *Managed AMP fields and default values (Continued)*

Field	Default	Description
Manage Group Configuration	No	Defines whether the Master Console can manage device groups on the managed W-AirWave 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 W-AirWave 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 templates chapter of the W-AirWave User Guide, except that there is no process by which templates can be fetched from devices in the subscriber group on managed W-AirWave servers. 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 W-AirWaves, 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 W-AirWave servers; make sure that the **Manage Group Configuration** option is enabled for each managed W-AirWave.

Once Global Groups have been configured on the **Master Console**, groups must be created or configured on the managed W-AirWave servers 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 W-AirWave. 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 W-AirWave 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 the **Configuring and Using Device Groups** chapter of the W-AirWave User Guide"Configuring and Using Device Groups" on page 72.

Controller Backups and Restoration

You can create a backup on demand by creating and collecting a flash backup from the controller. Daily backups are also created. At a minimum, there are four backup files:

- Two daily backups
- One backup from last week
- One backup from last month

The backup saved from a firmware upgrade is automatic and requires no manual intervention. All backups can be saved or restored and are displayed on the **Audit** page. You can only perform a backup on a device if the firmware version of the device and the backup image are identical. After you click **Restore**, the device on which the restoration is being performed automatically switches from monitor mode to maintenance mode. After you restore a backup image to a device, you must restart the controller.

Logging out of W-AirWave

To log out of W-AirWave, select the **Logout** link on the upper right hand corner of every W-AirWave page.

You will be logged off automatically based on the number of minutes set in the **Idle Timeout** setting of **Home > User Info**. Refer to "Setting Up Login Configuration Options" on page 45.

Reports in W-AirWave are powerful tools for network analysis, user configuration, device optimization, and network monitoring. All reports can be printed, emailed, or exported.

What You Can Do With Reports

W-AirWave includes 20 default reports and runs them daily. You can access these reports after they have run, through hyperlinks on the **Generated Reports** page. You might want to keep only the reports that you need and delete, or reschedule, others to optimize your disk space. For information about working with reports, see "About the Default Reports" on page 266.

W-AirWave populates the default reports with pre-defined fields. Some default reports don't span a period of time, taking snapshots of your device inventory and configurations. Commonly used reports include: inventory, configuration audit, and client sessions.

If these reports don't have the details you need, you can build a custom report with the help of widgets. By changing the restriction settings, you can isolate a folder, group, or period of time. For information about report customization, see "Creating Reports" on page 297.

Track licenses

- License. Use this report to track licenses on the devices in your network. The report includes the license type, quantity, percentage used, installation dates, expiration dates, and license keys. For information, see "Using the License Report" on page 268.

Improve Network Efficiency and User Experience

- Capacity Planning. Use this report to track device bandwidth capacity and throughput in groups, folders, and SSIDs. Based on interface-level activity, you can use it to analyze device capacity and performance on the network. For information, see "Using the Capacity Planning Report" on page 273.
- Memory and CPU Utilization. Use this report to view the top percentage of memory utilization and usage for devices and CPUs. You can use filters by specific devices, such as controllers, switches, and APs. For information, see "Using the Memory and CPU Utilization Report" on page 268.
- Network Usage. Use this report to track network-wide information by usage and clients. You can narrow information by groups and folders, or summarize by usage and client count for folders. For information, see "Using the Network Usage Report" on page 269.
- Port Usage. Use this report to find all the ports and switches in your network and view traffic patterns. The histogram identifies unused ports and switches. For information, see "Using the Port Usage Report" on page 271.
- RF Health. Use this report to monitor 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 helps pinpoint the most problematic devices on your network, and lists the top devices by problem type. For information, see "Using the RF Health Report" on page 272.
- UCC. Use this report to monitor UCC activity on your network. This information includes the top connectivity types, call types, application types, device types, folders, APs, and clients with the highest percentage of poor quality calls. For information, see "Using the UCC Report" on page 248.

Monitor Clients and Devices

- Client Inventory. Use this report to view information about clients that connected to your network. You can use filters and match criteria to customize your report. Information reported includes include manufacturer make and model, OS summary, asset category and group, and authentication type. For information, see "Using the Client Inventory Report" on page 275.

- Client Session. Use this report to view information for each time a user connects to your network. You can use filters and match criteria to customize your report. Information reported includes MAC address, user name, role, and SSID. For information, see "Using the Client Session Report" on page 277.

- Configuration Audit. Use this report to see a network snapshot of your device configurations. You can get an inventory one device at a time, one folder at a time, or one device group at a time. The report includes hypertext links to device configuration pages. For information, see "Using the Configuration Audit Report" on page 279.

- Device Summary. Use this report to see which devices are used the most or least, as well as get an inventory of all devices. You can also use this report to establish more equal bandwidth distribution across multiple devices. For information, see "Using the Device Summary Report" on page 280.

- Device Uptime. Use this report to monitor device performance and availability. This report covers average uptimes by SNMP and ICMP protocols, device groups and folders, or SSID information. You can add time restrictions so W-AirWave only generates the report during a planned maintenance period or business days. For information, see "Using the Device Uptime Report" on page 282.

- Inventory. Use this report to track all devices in your network. For example, you could use the report to find Cisco devices and break down the list by model and device type. For information, see "Using the Inventory Report" on page 283.

- Rogue Containment Audit. Use this report to see whether your rogue containments are failing. For information, see "Using the Rogue Containment Audit Report" on page 285.

Show Compliance

- PCI Compliance. Use this report to view PCI configurations and show compliance during an audit. For information, see "Using the PCI Compliance Report" on page 286.

Troubleshoot Device and Network Issues

- IDS Events. Use this report to respond to IDS events on the network involving APs or controller devices. W-AirWave reports on devices that have had the most events in the prior 24 hours. The report includes hypertext links to device configuration pages. You can use filters to show IDS events for specific devices, such as controllers and APs. For information, see "Using the IDS Events Report" on page 286.

- Match Event. Use this report to track matching events that occurred on devices. For example, you could use the report to find sticky client problems and break down the information by folder, AP, and client. For information, see "Using the Match Event Report" on page 288.

- New Clients. Use this report to see new clients that W-AirWave discovered on the network during the time duration of the report. Information reported includes user identifier, associated role when known, and device information. You can use filters to find specific devices and users, matching criteria, or view all information. For information, see "Using the New Clients Report" on page 289.

- New Rogue Devices. Use this report to find rogues device on your network. Before W-AirWave can run the report, you must define the restrictions. For information, see "Using the New Rogue Devices Report" on page 290.

- RADIUS Authentication Issues. Use this report to find the top 10 issues with controllers, RADIUS servers, and users. The report includes the number of total failures and the first and most recent event times. For information, see "Using the RADIUS Reports" on page 292.

- RADIUS Accounting Issues. Use this report to find the top 10 issues by device, controller, RADIUS server, and client. For information, see "RADIUS Accounting Issues" on page 293.
- Rogue Clients. Use this report to track the number of valid users that connected to rogues in the specified time frame. You can filter results by rogue classification, and you can include ad-hoc devices and client details. By default, the minimum RAPIDS classification is suspected rogue, and the maximum is contained rogue. For information, see "Using the Rogue Clients Report" on page 294.
- VPN Session. Use this report to view summary or detailed information about VPN activity by sessions. You can use filters or narrow results with match criteria. You can also specify device types to include in the report. For information, see "Using the VPN Session Report" on page 296.

Sorting Reports

By default, the **Reports > Generated** page lists reports ordered by generation time. You can sort reports by any column header, or choose columns to display. Clicking the report title opens the report.

Table 128 describes each column for the **Reports > Generated** page.

Table 128: *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.

About the Default Reports

This section describes the default reports in W-AirWave that run daily. You can access these reports from the **Reports > Generated** page. If you need to customize a report, see "Creating Reports" on page 297.

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 146. In this figure, a custom VPN Session report is being created for viewing VPN data for VLANs and Users.

Figure 146: *Custom Options Page Illustration*
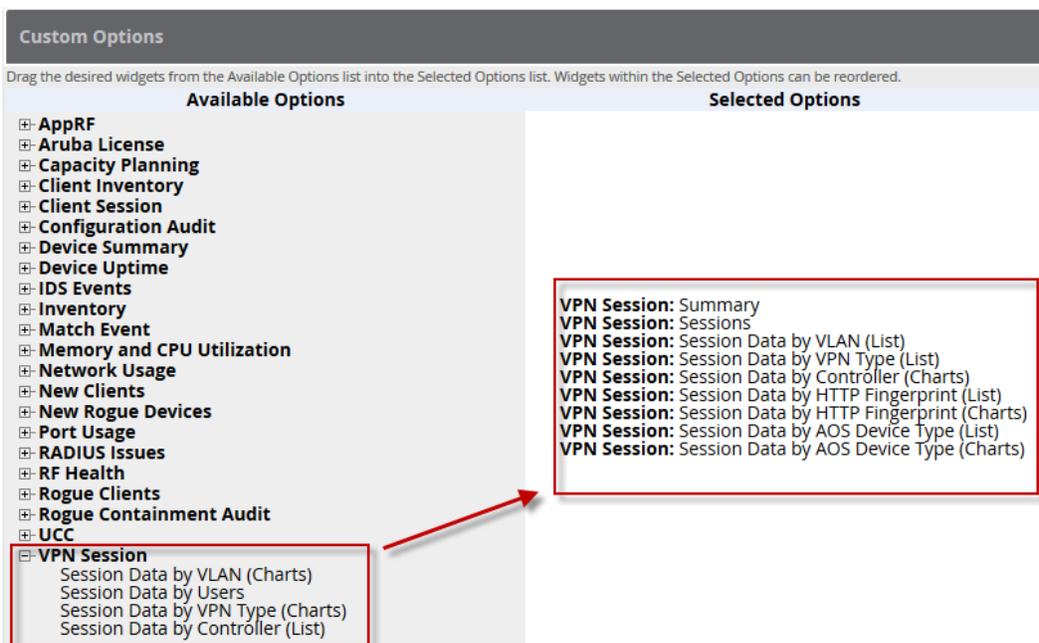
The left pane of the **Custom Options** section lists all available data that can be included in the report. Drag the desired data from the **Available Options** list on the left to the **Selected Options** pane on the right.

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 License Report

The Dell Networking W License Report tracks licenses on Dell 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 147: *Dell Networking W Detail Page*

Using the Memory and CPU Utilization Report

The Memory and CPU Utilization report, as shown in Figure 148, displays the top percentage of memory utilization and usage for devices and CPUs. You can filter this report by specific devices (controllers, APs, etc.), or to report on any number of IDS events for each specified device type.

Figure 148: *Daily Memory and CPU Usage Report*

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, as shown in , 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.

You can select an option to include tabular information below each graph, and then choose which columns display in the tables.

Figure 149: *Network Usage Report*
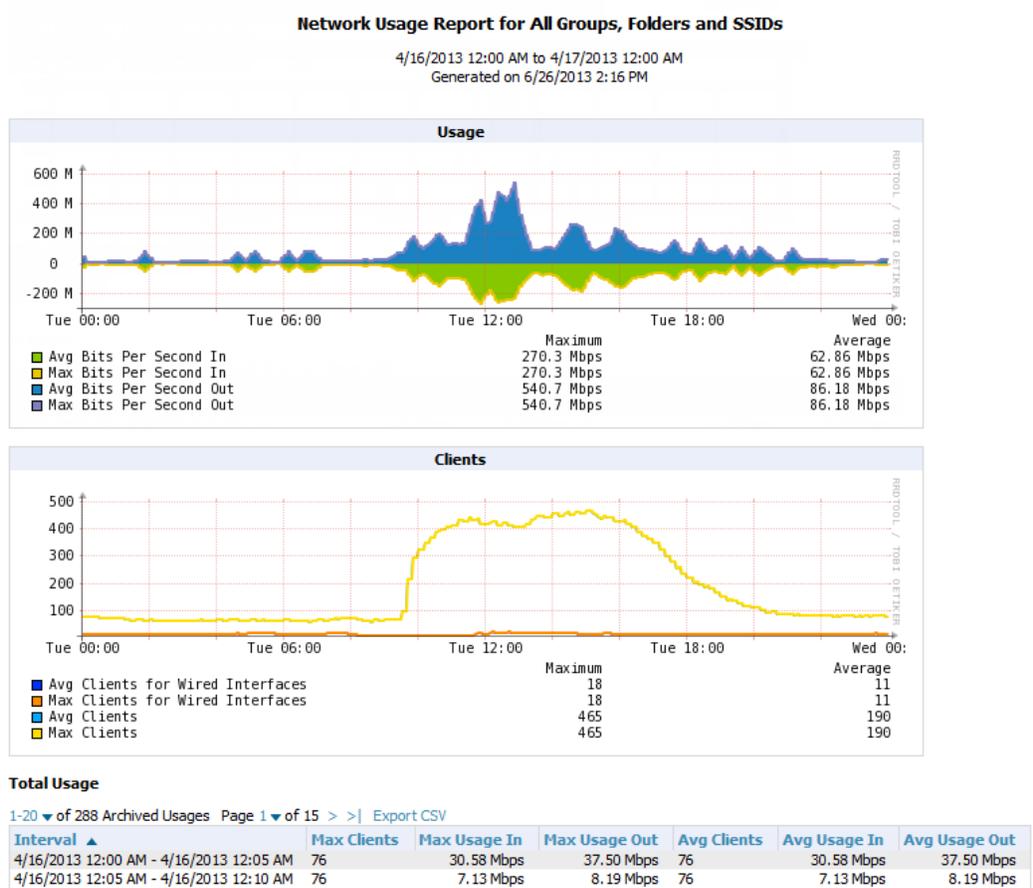
Table 129: *Network Usage Report Fields and Descriptions*

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 Port Usage Report

The Port Usage report includes the following statistics: all the switches and ports in your network by folder, unused ports, access and distribution ports, most used switches, and most used ports. This report, as shown in Figure 150, also provides a histogram of unused ports vs. unused switches by type (access or distribution).

Figure 150: *Port Usage Report*
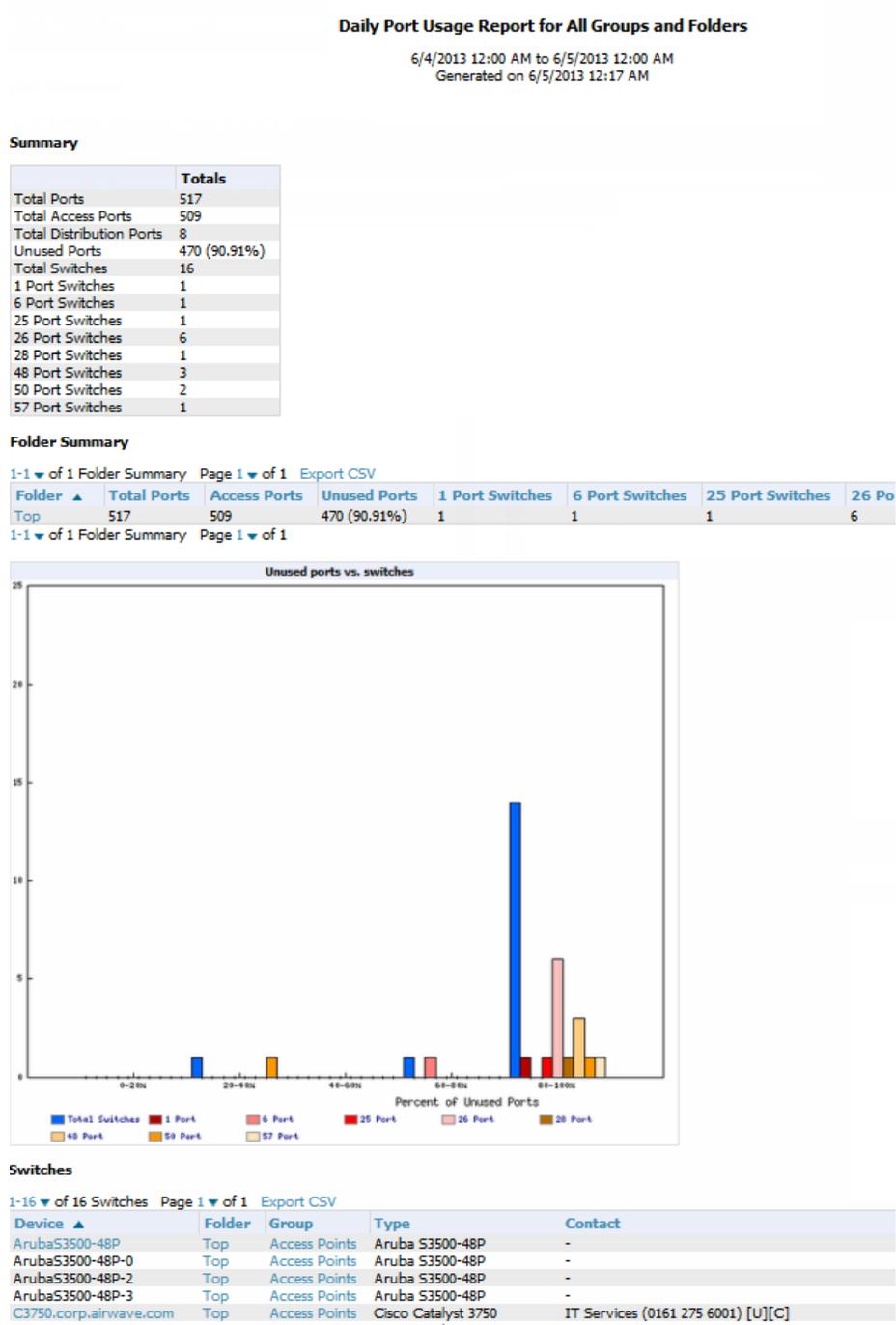
Table 130 describes the fields in the Switches table that is in this report.

Table 130: *Switch Table Fields and Descriptions*

Field	Description
Device	The name of the device
Folder/Group	The folder and group that this devices belongs to
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 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 141.)

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.

Additionally, a report can be summarized by:

- Top Folders By Worst Client and Radio Statistics Combined 2.4 GHz and 5 GHz
- Client and Radio Statistics by Folder - Combined 2.4 GHz and 5 GHz
- Top Folders By Worst Client and Radio Statistics 2.4 GHz
- Client and Radio Statistics by Folder - 2.4 GHz
- Top Folders By Worst Client and Radio Statistics 5 GHz
- Client and Radio Statistics by Folder - 5 GHz

The statistics displayed can be Client Health, Client SNR, Radio Noise, Radio Utilization, or Radio Interference. The thresholds for the statistics are defined in the corresponding fields below. These thresholds are defined by a specified percentage (0-100%) or dBm (-110-0 dBm) for Radio Noise Threshold. To select a new summary method:

1. Log in to W-AirWave.
2. Navigate to **Reports > Definitions**.
3. Select **Daily RF Health Report**.
4. Check any options under **Summarize report by**.
5. Select the statistics to be displayed from the **Top Folder Sorting Column** drop-down menu.

6. Define any thresholds appropriate to your report.

7. Click **Save and Run** or **Save**.

If an RF Health Report has not been generated before, you can create it by following the instructions on the "Creating Reports" on page 297 section of this chapter.

Figure 151 illustrates a sample RF Health Report.

Figure 151: *Daily RF Health Report Page Illustration (partial view)*

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.

W-AirWave 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 W-AirWave validates reports so you can only run them over a 366-day duration.

Using the Capacity Planning Report

The Capacity Planning Report tracks device bandwidth capacity and throughput in device groups, folders, and SSIDs. With this report, you can achieve network efficiency and an improved user experience. For information

about bandwidth information, see "Using the Network Usage Report" on page 269.

Example Custom Report

The following example creates a 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. Any setting omitted from this example remains the default value.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.
2. Enter the title, "Capacity Planning Report 1% for Group HQ".
3. Select **Capacity Planning** from the **Type** drop-down menu.
4. Select "HQ" from the **Groups** drop down menu.
5. Set the capacity threshold to 1.
6. Set the minimum time above the threshold to 5.
7. Set the maximum time above the threshold to 100.
8. Enter a 2-hour time interval for the report to run.
9. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 152.

Figure 152: *Capacity Planning Report*
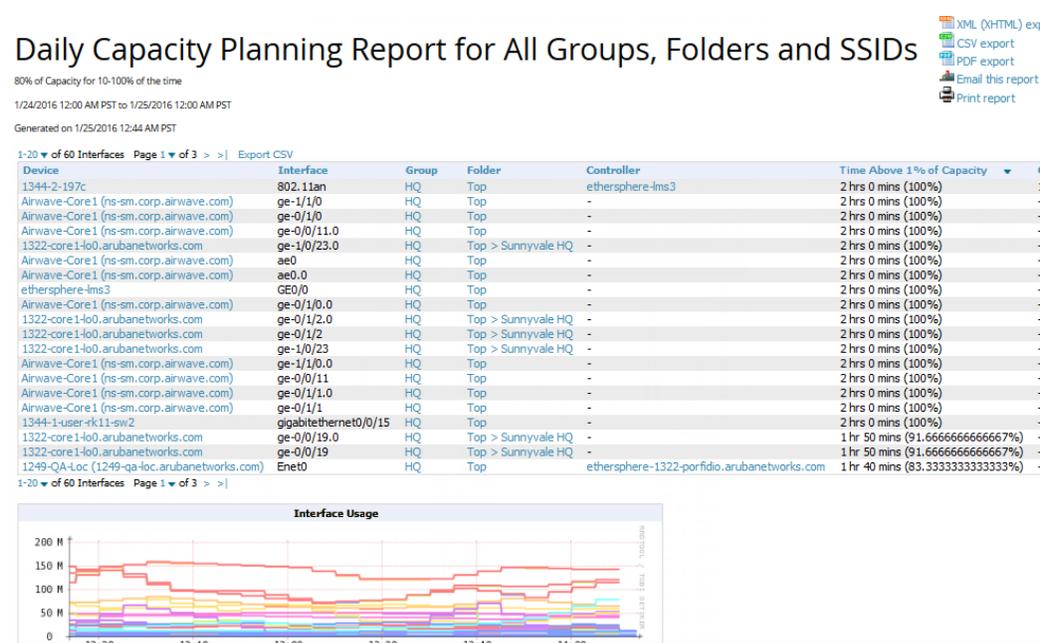
Table 131 describes the fields in the Capacity Planning Report.

Table 131: *Capacity Planning Report Fields and Descriptions*

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.

Table 131: *Capacity Planning Report Fields and Descriptions (Continued)*

Field	Description
Folder	Displays the folder with which the device is associated.
Controller	Displays the controller with which a device operates.
Time Above 1% of Capacity	Displays the time duration in which the device has functioned above 0% of capacity. A low percentage of use in this field may indicate that a device is under-used or poorly configured in relation to its capacity, or in relation to user needs.
Capacity Combined (b/s)	Displays the combined capacity in and out of the device, in bits-per-second.
Usage While > Threshold (Combined)	Displays the time in which a device has functioned above defined threshold capacity, both in and out.
Overall Usage (Combined)	Displays the overall usage of the device, both combined in and out traffic.
Usage While > Threshold (in)	Displays device usage that exceeds the defined and incoming threshold capacity.
Overall Usage (In)	Displays overall device usage for incoming data.
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 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 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 Custom Report

The following example creates a summary report of Apple devices on your network. The report also displays the last connection mode and the last SSID for all devices to help determine how and where the devices are connecting.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.
2. Enter the title, called "Client Inventory - iPhone, iPod, iPad."
3. Select **Client Inventory** from the **Type** drop-down menu.
4. In the Summarize Report By section, select the AOS Device Type Summary, Device Type Summary, Last Connection Mode Summary, and Last SSID Summary options.
5. Specify "Matching" in the Model section for iPads, iPhones, and iPods.
6. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 153.

Figure 153: *Reports > Generated > Client Inventory (partial)*
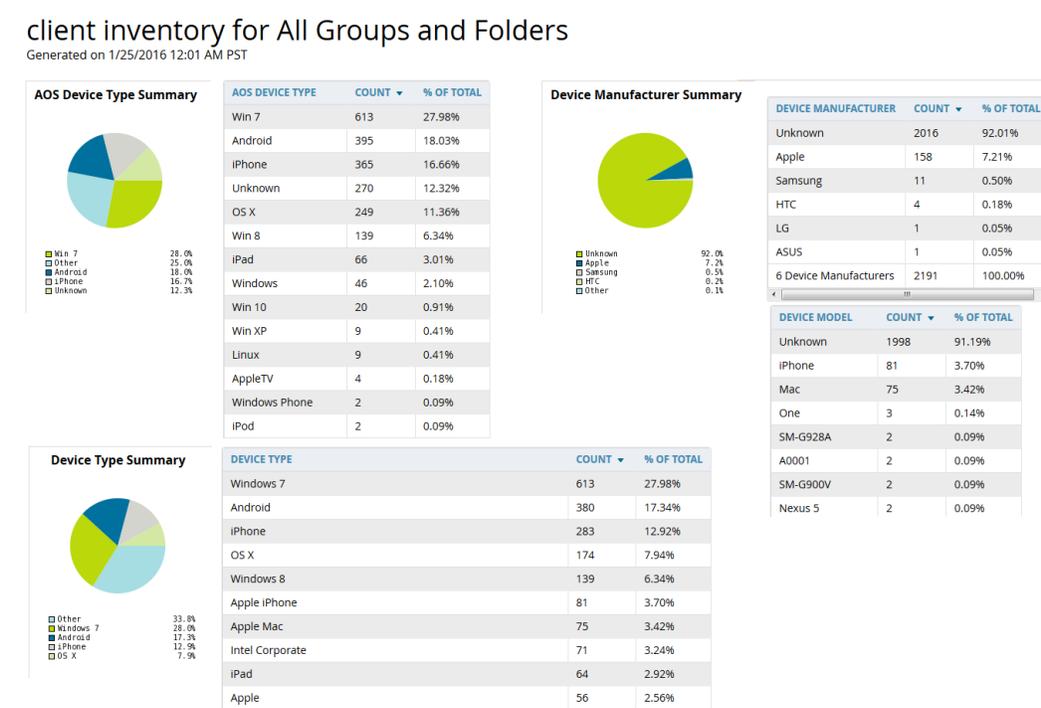
The fields on this report are described in Table 132.

Table 132: *Client Inventory Report Fields and Descriptions*

Field	Description
AOS Device Type	Displays the device type or name.
Count	The total number of each device current included in the client inventory.
% of Total	The percentage of each of the devices that are included in the client inventory.
Last SSID Summary	The SSID most recently connected to by each device. This includes the total number of clients and the percentage of each of those devices that connected to the SSID.
Last Connection Mode	The most recent connection mode used by that each device .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 itemizes user-level activity by session, meaning any instance in which a user connects to the network. In list and chart format, this report displays session information, such as: cipher; connection mode; role; SSID or VLAN ID, top clients by total MB used; device type; asset category and group; EAP supplicant; manufacturer; model; network chipset, driver, and interface vendor; and OS.

NOTE

The period of time in which the client remains connected to the network is typically calculated as a single session. However, if a client roams between APs, the periods of time the client connected to the different APs may be calculated as separate sessions.

Each report can be filtered based SSID, Device Type, Manufacturer, Model, and more.

You can specify the details that you want to include in the Sessions information, such as the MAC Address, user name, role, and SSID.

Figure 154: *Client Session Detail*

Daily Client Session Report for All Groups, Folders, SSIDs and Roles

1/14/2016 12:00 AM PST to 1/15/2016 12:00 AM PST
Generated on 1/15/2016 12:19 AM PST

1-7 ▾ of 7 OSs Page 1 ▾ of 1 Export CSV

Session Data by OS

OS	CLIENTS ▾	% OF CLIENTS	TIME	% OF TIME	BYTES USED (MB)	% OF MB USED	AVG SIGNAL QUALITY	AVG SIGNAL (DBM)	SESSIONS
-	251	60.05%	4 days 4 hrs 6 mins	36.21%	653.54	9.88%	36.01	-58.95	1225
Mac OS X	50	11.96%	2 days 11 hrs 42 mins	21.60%	2352.73	35.59%	39.92	-53.29	73
iOS	48	11.48%	1 day 15 hrs 21 mins	14.23%	311.29	4.71%	31.81	-65.60	282
Windows 7	44	10.53%	2 days 5 hrs 25 mins	19.32%	2994.56	45.29%	41.46	-52.30	78
Android	20	4.78%	16 hrs 24 mins	5.93%	16.21	0.25%	30.87	-60.74	108
Windows	4	0.96%	6 hrs 0 mins	2.17%	244.19	3.69%	37.98	-57.16	5
Windows XP	1	0.24%	1 hr 30 mins	0.54%	38.99	0.59%	44.00	-49.89	1
7 OSs		100.00%	11 days 12 hrs 29 mins	100.00%	6611.51	100.00%			1772

1-7 ▾ of 7 OSs Page 1 ▾ of 1

Clients by OS	Time Spent by OS	MB Used by OS
□ unknown 60.0%	□ unknown 36.2%	□ Windows 7 45.3%
■ Mac OS X 12.0%	■ Mac OS X 21.6%	■ Mac OS X 35.6%
□ iOS 11.5%	□ Windows 7 19.3%	□ unknown 9.9%
■ Windows 7 10.5%	□ iOS 14.2%	□ iOS 4.7%
□ Other 6.0%	□ Other 8.6%	□ Other 4.5%

1-25 ▾ of 65 OS Details Page 1 ▾ of 3 > >| Export CSV

Session Data by OS Detail

OS DETAIL	CLIENTS ▾	% OF CLIENTS	TIME	% OF TIME	BYTES USED (MB)	% OF MB USED	AVG SIGNAL QUALITY	AVG SIGI
	255	61.00%	4 days 6 hrs 1 min	36.90%	657.86	9.95%	35.94	-59.03
9.1 (13B143)	19	4.55%	21 hrs 8 mins	7.65%	41.76	0.63%	30.68	-65.81
10_10_5	19	4.55%	18 hrs 34 mins	6.72%	1195.71	18.09%	41.47	-51.90
Windows NT 6.1; WOW64	12	2.87%	13 hrs 29 mins	4.88%	116.61	1.76%	40.87	-52.48

Each Client Session Report includes a Client Session Summary section. Table 133 describes the fields that display in this summary.

Table 133: *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.
Total traffic In (MB)	The total amount of traffic that passed in the network.
Total traffic Out (MB)	The total amount of traffic that passed out of the network.

Table 133: *Client Session Summary Fields and Descriptions (Continued)*

Field	Description
Avg traffic per session (MB)	The average amount of traffic generated by each session.
Avg traffic in per session (MB)	The average amount of traffic in generated by each session.
Avg traffic out per session (MB)	The average amount of traffic out generated by each session.
Avg traffic per client (MB)	The average amount of traffic generated by each client.
Avg traffic in per client (MB)	The average amount of traffic in generated by each client.
Avg traffic out per client (MB)	The average amount of traffic out 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 a snapshot of your device configurations on the network. You can get an inventory one device at a time, one folder at a time, or one device group at a time. Reports include hypertext links to additional configuration pages.

Follow these steps to view the current audit report and configure a 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 155 and Table 134 illustrate and describe the general Configuration Audit report and related contents.

Figure 155: *Daily Configuration Audit Report Page, partial view*

Daily Configuration Audit Report for All Groups, Folders and SSIDs
Generated on 1/25/2016 12:24 AM PST

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

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

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 134: *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 W-AirWave. 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 W-AirWave. 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 156 and Table 135 illustrate and describe the Device Summary Report.

Figure 156: *Daily Device Summary Report Illustration (partial view)*

Table 135: *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.

Table 135: *Daily Device Summary Report Unique Fields and Descriptions (Continued)*

Field	Description
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 157: *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 136: *Device Uptime Report Unique Fields and Descriptions*

Field	Description
SNMP Uptime	Displays the percentage of time the device was reachable via ICMP. W-AirWave 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. W-AirWave 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 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 Custom Report

The following example creates a report of all Cisco devices on your network. Any field omitted from this example remains the default value.

1. Navigate to **Reports > Definitions**, then click **Add New Report Definition**.
2. Enter the title "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 **Type Summary**. This option will categorize the Cisco devices found in your network by device type.

6. Click **Save and Run**. The report displays on the Generated Reports page when it is available, as shown in Figure 158.

Figure 158: *Inventory Report*
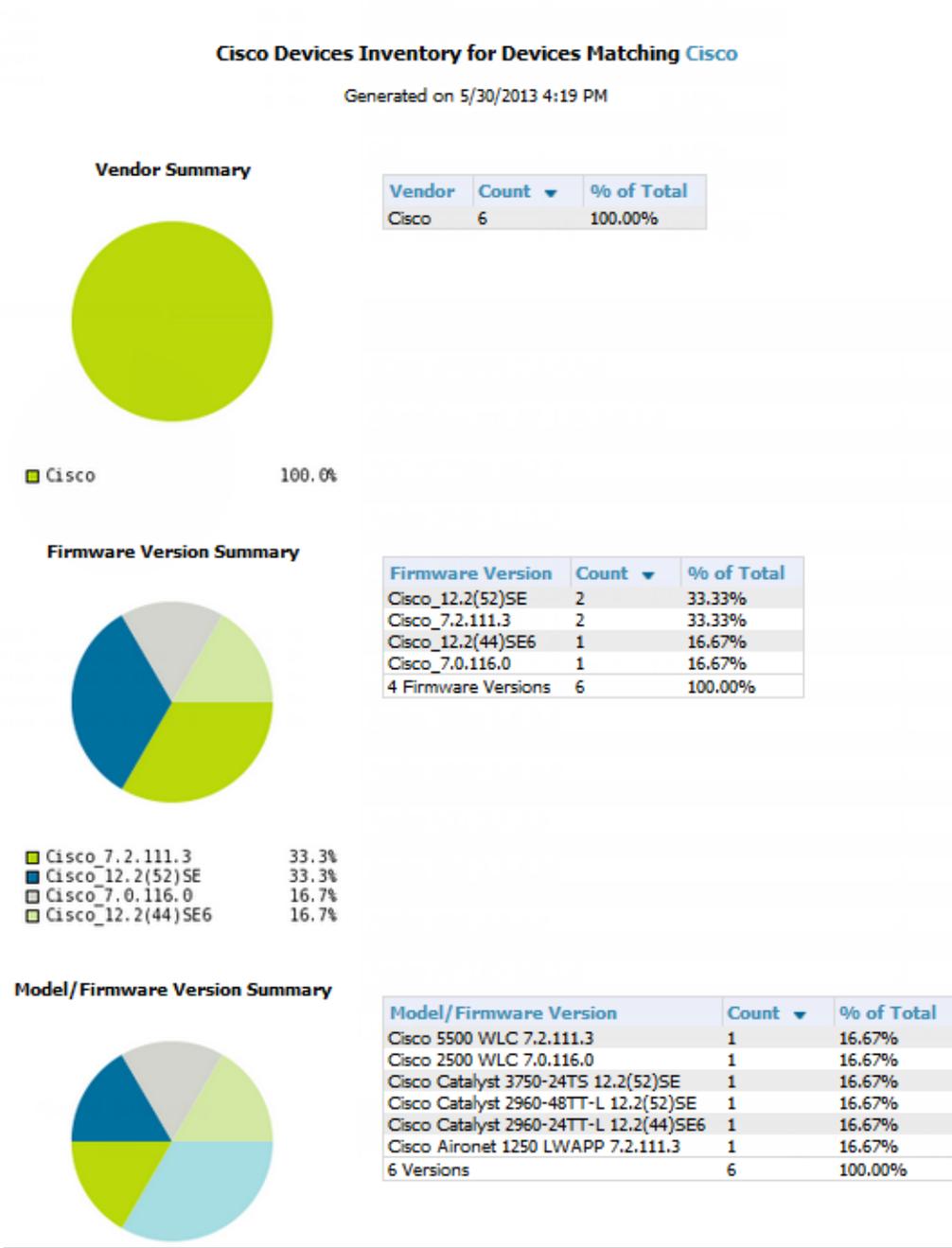
Table 137: *Inventory Report Fields and Descriptions*

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.
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 Rogue Containment Audit Report

The Rogue Containment Audit report that lets you know if any containment is failing. Figure 159 illustrates the output of this report, and Table 138 describes the fields available in the report.

Figure 159: *Rogue Containment Audit Report Page Illustration*

Table 138: *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 PCI Compliance Report

W-AirWave supports PCI requirements in accordance with the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI compliance report, shown in Figure 1, displays current PCI configurations and status. This report provides recommendations to resolve issues when possible.

Figure 160: *PCI Compliance Report*

For information about turning on this feature, see "Enabling PCI Compliance Monitoring" on page 67.

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

The **Home > Overview** page also cites IDS events. Triggers can be configured for IDS events. Refer to "Creating New Triggers" on page 221 for additional information.

Figure 161 and Table 139 illustrate and describe the IDS Events Detail report. Selecting the AP device or controller name takes you to the **APs/Devices > List** page.

Figure 161: *IDS Events Report Illustration*
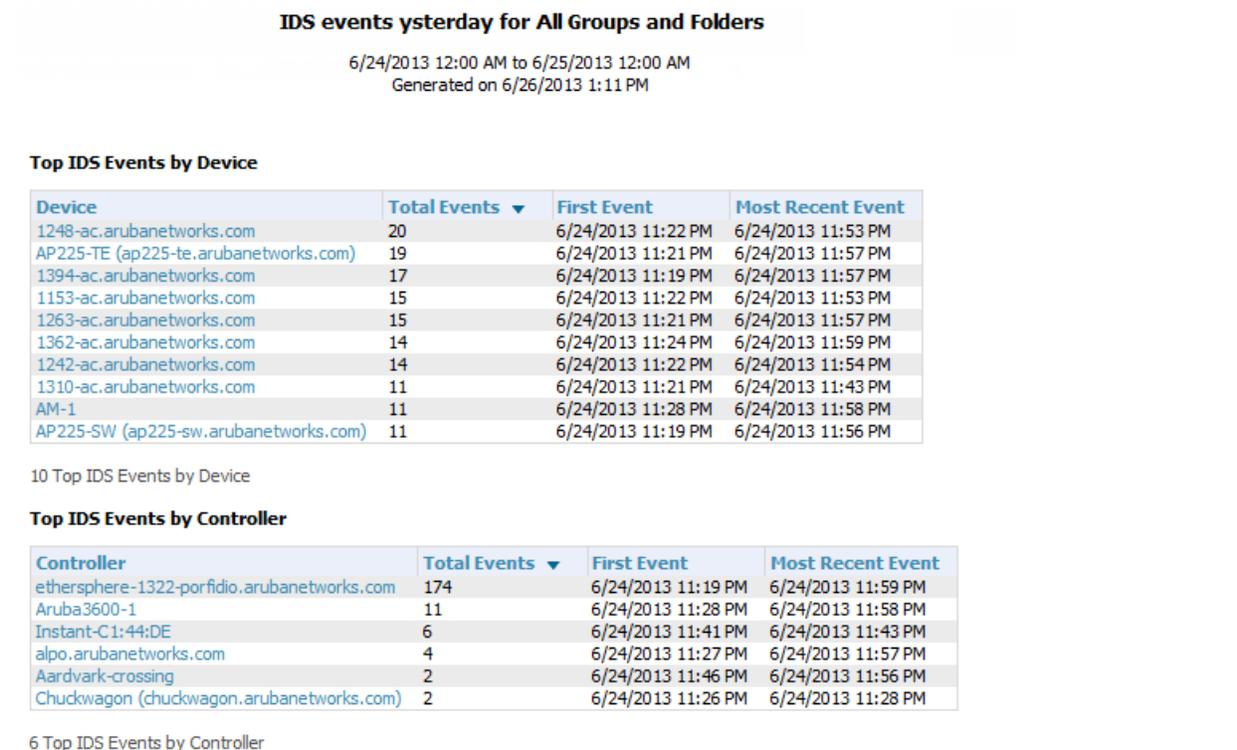
Table 139: *IDS Events Detail Unique Fields and Descriptions*

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.
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.

Field	Description
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 Match Event Report

Use the Match Events report to track matching events that occurred on devices. For example, you could use the report to find sticky client problems and break down the information by folder, AP, and/or client, as shown in Figure 162.

Figure 162: *Example of a Match Event Report*

Table 140: *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 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
- Dell 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 163 illustrates the fields and information in the New Clients Report. The fields that display on this output are described in Table 141.

Figure 163: *New Clients Report Illustration (split view)*

Table 141: *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 198
- 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 wirelessly, with extensive device parameters and hyperlink interoperability to additional W-AirWave pages

- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional W-AirWave pages
- Detailed and text-based table of discovery events pertaining to the discovery of rogue devices with extensive parameters and hyperlink interoperability to additional W-AirWave pages

This report is not run by default, but is available after you define it.

Refer to Figure 164 for a sample illustration of this report.

Figure 164: *New Rogue Devices Report Illustration (partial view)*
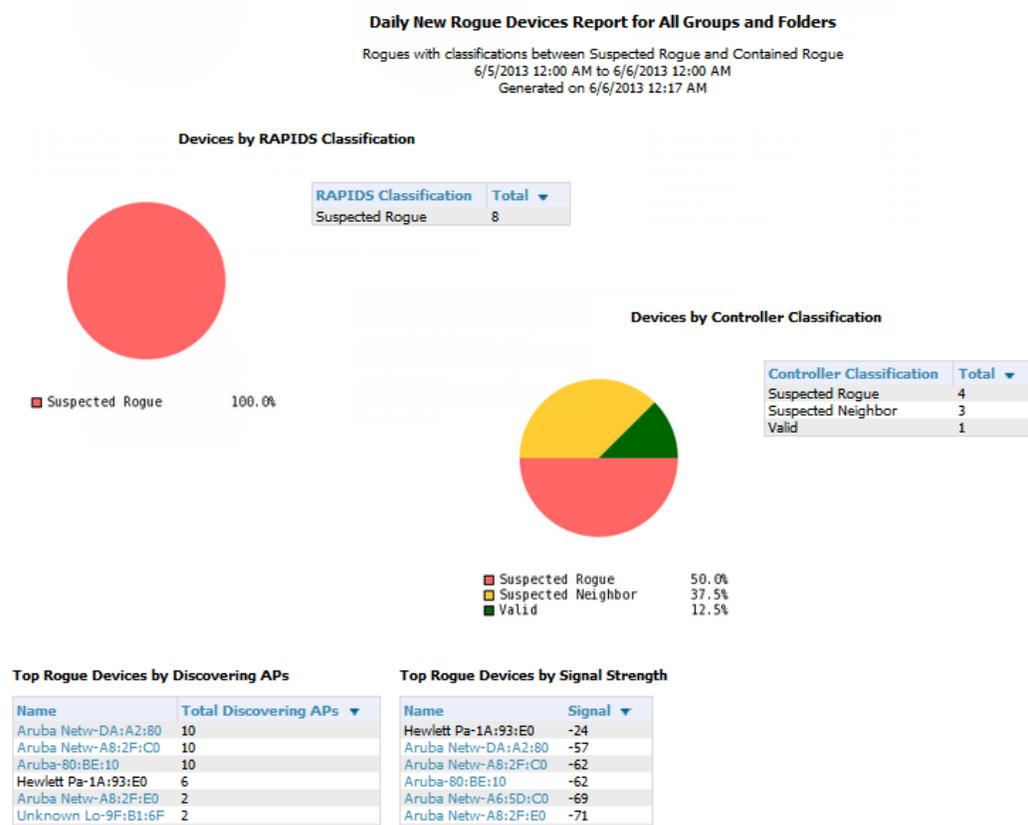
The rogue device inventories that comprise this report contain many fields, described in Table 142.

Table 142: *New Rogue Devices Report Fields*

Field	Description
Name	Displays the device name, if it can 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 198 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 198 for additional information.
Ack	Indicates whether the device has been acknowledged with the network.

Table 142: *New Rogue Devices Report Fields (Continued)*

Field	Description
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.
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 RADIUS Reports

These reports display issues that may appear with controllers, RADIUS servers, and users, or about RADIUS accounting issues.

RADIUS Authentication Issues

This report include the number of total failures and the first and most recent event times. This report shows the top 10 RADIUS authentication items in each table. You can change this value to anything other than 0.

You can filter this report by BSSID, or view detailed information about RADIUS failures. By selecting RADIUS failures, W-AirWave summarizes authentication issues for each event.

Figure 165: *RADIUS Authentication Issues Report*

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

RADIUS Accounting Issues

In order to run this report, you need to create a custom report that includes RADIUS accounting information. From the **Reports>Definitions**page, click **Add** to open the new report template. The **Custom Options** list will include options for RADIUS Accounting, as well as RADIUS Authentication.

To view a generated RADIUS accounting report, navigate to **Reports > Generated** and select the name of a report that includes RADIUS accounting details.

Figure 166: *RADIUS Accounting Issues Report*

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 167: *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 143: *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 user name (if available) and the number of misassociations.
Rogue Clients	
MAC Address	The MAC address of the rogue client
Username	The user name of the rogue client, if available
SSID	The SSID of the rogue client
First Heard	The date/time when the rogue client was first detected on the network

Table 143: *Rogue Clients fields and descriptions (Continued)*

Field	Description
Ch BW	The channel bandwidth of the client, if available
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
Location	The location of the rogue client, if available
RAPIDS Classification	The current classification of the rogue client

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 168: *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
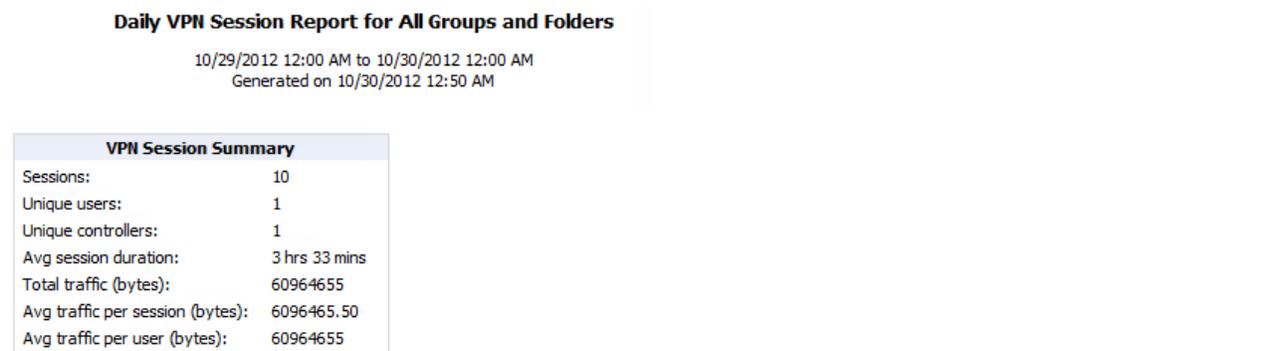
Table 144 describes the fields that display when "Summarize Report By" list information is selected for the following tables:

- 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 144: *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.

Creating Reports

You can customize reports to meet your needs. In order to do so, you need admin privilege to create reports and view all report information. W-AirWave reports and information displayed in the WebUI varies depending on configurations, user roles, and folders.

Follow these steps to create a report:

1. Navigate to **Reports > Definition**, then click **Add**. Or click   to edit a report.

2. Enter the name of the report in the **Title** field.

3. Add report widgets:

   ▪ For a default report, select the report widget from the available options, then press and hold the mouse while you drag it to the selected options. Or, you can double-click the widget.

   ▪ For a custom report, click the down arrow next to select a report from the drop-down list.

   Change the order in which the report displays data by dragging the widget to reorder it.

4. Complete the **Report Restrictions** section. All reports allow you to restrict based on a group, folder, and type of device. When you select custom options to include in a report, additional restrictions will become available.

5. Click **Yes** to schedule a report, then enter how often the report should run and when the report starts and ends. If these fields are not available, the report provides a snapshot of current status rather than spanning a period of time.

6. If you want non-admin users to see a generated reports, choose **By Subject**. By default, any report can be seen by an W-AirWave admin.

7. Click **Yes** if you want to email the report. They can be sent in HTML, PDF, and CSV formats.

8. Click **Yes** to you want to share the report by FTP or SCP to an external server.

9. Click **Add** to save your report. The report displays on the **Report Definition** page.

Tips for Restricting Time Ranges

Custom reports require extra consideration. Some reports, like client session data, are always restricted by a time range. Other reports, like client inventory, defaults to show all data. As a result, you might see conflicting device counts in these reports. To configure the time range, you must select **Limit to active devices** from the drop-down menu, and then select **Active during report timeframe** option.

Sending Reports

All reports contain links to export, email, and print reports. Graphics and links are included with exported reports. When sending reports to multiple email addresses, separate them with commas.

Figure 169: *Report*

Sending Reports to a Smart Host

W-AirWave uses Postfix to deliver alerts and reports via email, because it provides a high level of security and locally queues email until delivery. If W-AirWave sits behind a firewall, which prevents it from sending email directly to the specified recipient, use the following procedure to forward email to a smart host.

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 smart host.

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
   ```

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 170: *Example VisualRF Page Showing all networks*
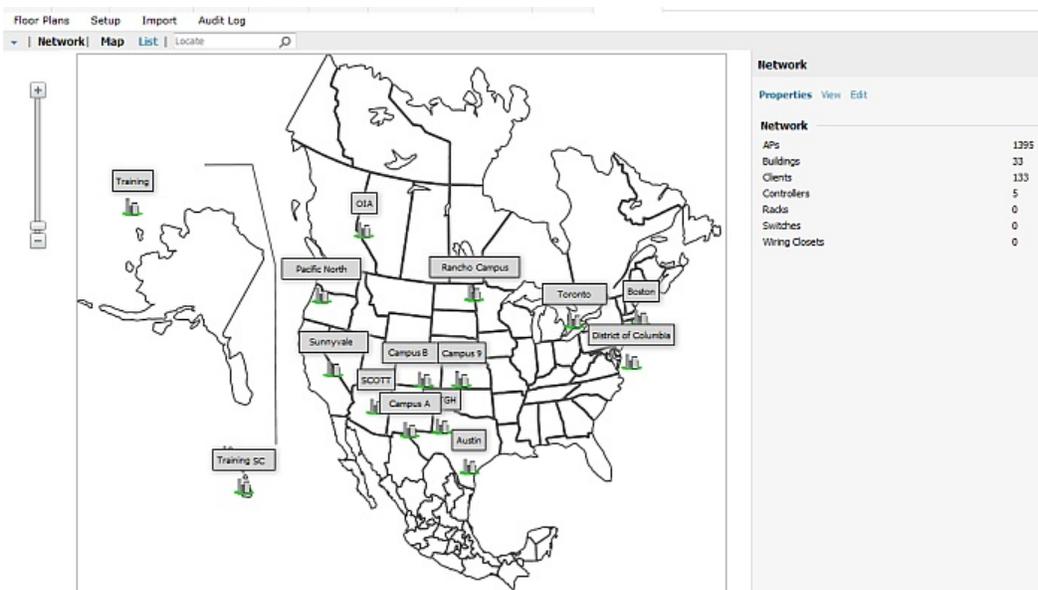
Features

- Mesh monitoring page specially for viewing Dell 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 data speed at every location on a floor plan.
- 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 predefined thresholds.
- Location playback viewer which allows visual tracking of up to 24 hours of location history.
- Dynamically recalculated path loss and device locations based on real-time data from your wireless LAN, for increased location accuracy.
- Calibrated 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. W-AirWave uses these signal strength readings to dynamically attenuate floor plans to increase the accuracy of client locations and heat maps.
- **Clients** - Clients are end-user devices that access the network through other devices monitored or managed by W-AirWave.
- **Client Health** - The client health metric compares the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.
- **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. W-AirWave 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.
- **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.
- **Session** - A session is an instance when a client connects to the network. The period of time in which the client remains connected to the network is typically calculated as a single session. However, if a client roams between APs, the periods of time the client connected to the different APs may be calculated as separate sessions.
- **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. W-AirWave also uses these signal strength readings to more accurately place these unassociated clients.
- **VisualRF** - The W-AirWave service that calculates location, calculates path loss, and provides floor plan editing capabilities.
- **VisualRF Plan** - Makes the planning portions of VisualRF available in an offline software package that does not require a server. For more information about VisualRF Plan, see "About VisualRF Plan" on page 337.

Starting VisualRF

In order to launch VisualRF, **AMP Setup > General** settings must be configured to display the VisualRF tab, and the VisualRF engine must be enabled using the **VisualRF > Setup** menu. Both of these pages are only visible to users logged-in with administrators credentials. 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 VisualRF Navigation

The top-level VisualRF menu shows only the **Network** view, as shown in Figure 171.

Figure 171: *Default VisualRF Top Level Menu - Network View*

The top-level Network view can display network campuses on a map, or in a list. You can toggle between these two displays by clicking the **Map** or **List** links at the top of the Network view.

Network View Navigation

The Network view provides page specially for viewing campuses, buildings and floors within your network.

You can select any campus or building to view the numbers of APs and clients at that location. Figure 172 displays an example of a campus view with a building icon selected:

Figure 172: *Viewing a Campus Networks in VisualRF*
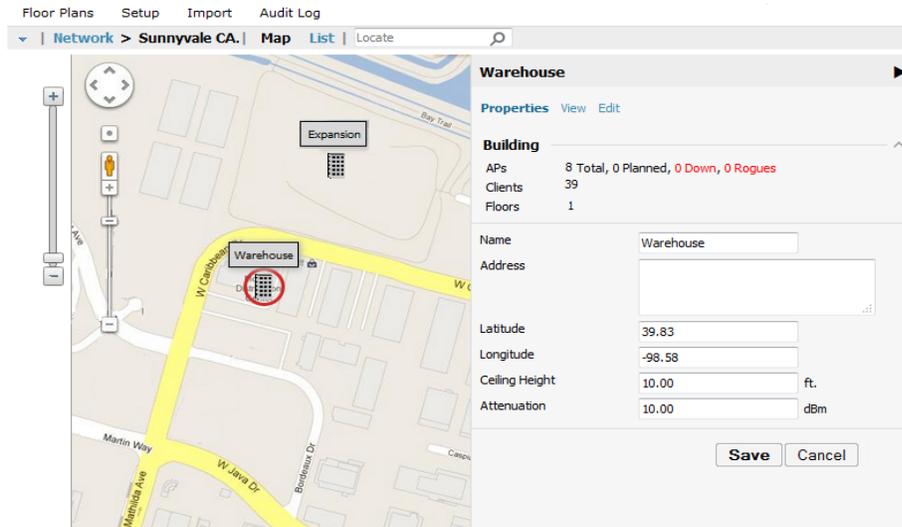
Click on an building within the selected campus, then select a floor to display the APs and clients on that floor. Select an AP or client to view detailed information about that device, as shown in Figure 173

Figure 173: *Viewing a Floor Plan in VisualRF*
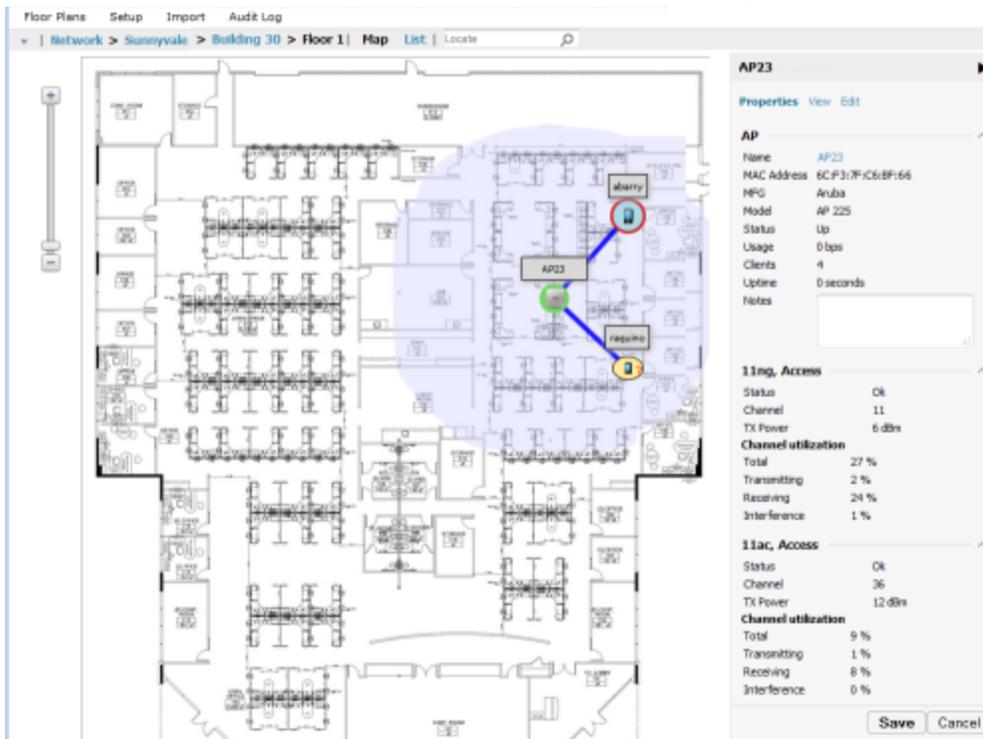
Customize Your Floor Plan View

You can customize your floor plan view by selecting the devices, client and AP overlays, display lines, and floor plan features from the **View** tab.

Devices

Click the following device options:

- **APs**, then click ▶ to select an option, such as planned or deployed, air monitors, channel, and transmit power.
- **Clients**, then click ▶ to select the size of the icon displayed for wireless users.
- **Interferers**, then click ▶ to select the size of the icon displayed for sources of Wi-Fi interference. This option works for Dell Networking W-Series ArubaOS devices running 6.1 or greater that have run the **mgmt-server type** W-AirWave command and have APs performing spectrum analysis through hybrid scanning or dedicated spectrum monitors.
- **Rogues**, then click ▶ to select the size of the icon displayed for rogue devices.
- **Tags**, then click ▶ to select the size of the icon to display Wi-Fi tags.

Client Overlays

Click the following client overlay options:

- **AppRF**, then click ▶ to customize thresholds based on your network and view the top 10 apps used in the last 2 hours. In the floorplan, hover your mouse over a client icon to see user and device details.
  You can edit the following color presets:
  - Green indicates that a client used between 0 and 20 MB in the past two hours.
  - Yellow indicates that a client used between 20 MB and 1GB in the past two hours.
  - Red indicates that a client has used more than 1 GB in the past two hours.
- **Client Health** to view metrics for controllers running Dell Networking W-Series ArubaOS 6.3 or greater. For more information on how this value is calculated, see "Useful Terms" on page 301.
- **UCC**, then click ▶ to select an option, such as Protocol, Type, or Quality.

AP Overlays

The channel utilization, channel, heatmap and speed overlays display information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Besides the current floor, you can view all floors, or data from APs located on the floor above or below.

Click the following device overlay options:

- **Ch. Utilization**, then click ▶ to select an option, such as Current, Dataset, Frequency, Floors, or whether to show the overlay as a grid. Airtime usage is a good indication of how busy an area is.
- **Channel**, then click ▶ to select an option, such as Signal Cutoff, Band, Channel, or Floors. This overlay identifies regions covered by specific channels, or regions with overlapping coverage on one selected channel or all channels in the 2.4 Ghz or 5 Ghz radio band. Hover your mouse over coverage areas for details about the APs.
- **Heatmap**, then click ▶ to select an option, such as Signal Cutoff, Frequencies, Floors, or whether to show the overlay as a grid.
- **Speed**, then click ▶ to select an option, such as Client TX, Rate, Frequencies, Floors, or whether to show the overlay as a grid. This overlay provides the highest data rate a user will receive for all areas of a floor plan. transmit power value for the overlay.
- **Voice**, then click ▶ to select an option, such as Signal Cutoff, Frequencies, Floors, or whether to show the overlay as a grid. This overlay uses color-codes to indicate the number of radios covering each grid cell based on the selected signal cutoff.

Relation Lines

Click the following relation line options:

- **APs** to view AP neighbor lines, which show the APs that hear each other.
- **Client Association** to view client to AP lines. The thicker lines designate AP of association, and the thinner lines show the APs that hear the client. This overlay uses color-codes to represent the radio band.
- **Client Neighbors** to view lines between a client and radios that hear the client , excluding the radio of association.
- **Interferers** to view lines between sources of Wi-Fi interference and the radios that have discovered them. For interferers, there is no radio of association.
- **Rogues** to view rogue AP to radio lines.
- **Surveys** to view lines between an AP and a client heard during a client survey. The ability to define a client survey was deprecated in W-AirWave 8.2, but surveys created in previous 7.x and 8.x releases can still be displayed on a VisualRF floor plan.
- **Tags** to view lines between Wi-Fi tags and radios which hear the tags. For tags, there is no radio of association.

Floor Plan Features

You can display floor plan features, such as Grid Lines, Labels, Origin, Regions, Walls, or Wiring Closets. If you created a client survey in W-AirWave 8.0.x and earlier, they also display on the floor plan when you select Surveys from the options.

To customize your grid lines, click ▶ to select Gridsize or Color.

To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. VisualRF uses the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position.

Mesh View Navigation

Mesh view provides a visual Mesh monitoring page specially for viewing Dell AirMesh devices. It automatically renders Mesh APs based on GPS coordinates.

You can mouse over each mesh network icon to view the numbers of APs and clients, and network usage in Mbps. Figure 174 displays an example of a Mesh Network view with a mouseover above a network icon:

Figure 174: *Viewing Mesh Networks in VisualRF*
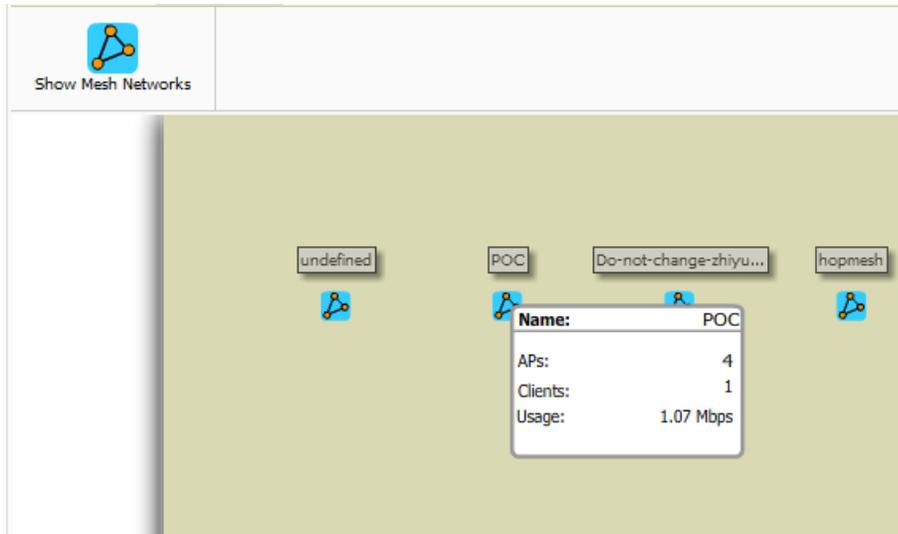
Click on an AirMesh network to display the APs with labels, as shown in Figure 175

Figure 175: *APs in a mesh network*

Select an AirMesh AP icon to bring up the pop up 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.

The top-level Mesh view includes the Refresh, Site Tree, Preferences and Help icons. Table 145 describes these icons and their functions in the VisualRF Mesh view.

Table 145: *Top Level Icons and Descriptions*

Operation	Icon	Description
Refresh		Refresh the floor plan to see changes.
Open Site Tree		Display the Network Tree View Window on top of the floor plan.
Preferences		Configure personal viewing preferences. The Preferences menu allows you to configure user preferences

Table 145: *Top Level Icons and Descriptions (Continued)*

Operation	Icon	Description
Help	ⓘ	Launch the online help. **NOTE:** This User Guide currently contains the most up-to-date help information for the VisualRF interface.

Figure 176: *Properties for a Mesh Gateway Illustration*
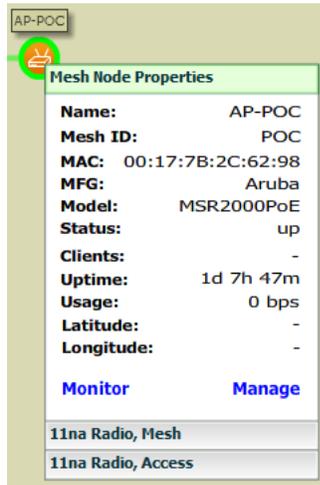
For radio-level status information on an AirMesh device in your network, select the menus in the AP's pop up window for each radio (**11na Radio**, **Access**; **11na Radio, Mesh**; and so forth).

Advanced VisualRF Settings

You can configure advanced settings for VisualRF on the **Setup** page (see). These settings can impact your server's performance and location accuracy.

> When you click **Save**, VisualRF will restart, causing a delay that might take a minute to 30 minutes, depending on the size of your VisualRF database.

Server Settings

To enable VisualRF and tune memory and performance, navigate to the **Server Settings** section on the **VisualRF > Setup** page.

Figure 177: *Server Settings*

The server settings are detailed in Table 146.

Table 146: *Server Settings*

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.

Table 146: *Server Settings (Continued)*

Setting	Default	Description
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 VisualRF, as well as W-AirWave-to-VisualRF communication. **NOTE**: If users experience timeout errors while using VisualRF, allocate additional WebUI Threads.
Synchronization Timer	15 minutes	This timer indicates how often VisualRF will synchronize with the APs within W-AirWave. 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, click [image] to access the location settings on the **VisualRF > Setup** page.

Figure 178: *Location Settings*

The location settings are detailed in Table 147

Table 147: *Location Settings*

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.

Table 147: *Location Settings (Continued)*

Setting	Default	Description
Maximum Rogue APs per Floor Plan	20	Sets the maximum number of rogues W-AirWave 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

You can configure VisualRF to calculate client locations by setting timers on the **VisualRF > Setup** page.

Figure 179: *Location Calculation Timer Settings*

Location Calculation Timer Settings	
Legacy Laptop Min/Max (sec):	90/360
Legacy Laptop Number of Samples:	3
Laptop Min/Max (sec):	90/360
Laptop Number of Samples:	3
Phone Min/Max (sec):	60/240
Phone Number of Samples:	3
RFID Min/Max (sec):	30/120
RFID Number of Samples:	4
Scale Min/Max (sec):	500/2000
Scale Number of Samples:	3
Printer Min/Max (sec):	120/480
Printer Number of Samples:	3
Rogue Min/Max (sec):	500/2000
Rogue Number of Samples:	3
Default Min/Max (sec):	90/360
Default Number of Samples:	3

The location calculation timer settings are described in Table 148

Table 148: *Location Calculation Timer Settings*

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.

Table 148: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
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 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	

Table 148: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
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.
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	This timer determines how often to calculate the locations of clients
Default Number of Samples	3	This quantity indicates how many samples are taken to calculate the location and place the client on the floor plan. The default is 3 samples.

Wall Attenuation Settings

Signal attenuation is the loss of signal strength during transmission. You can indicate the causes of attenuation using attenuation settings on the **VisualRF > Setup** page.

> **NOTE**
>
> 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.

VisualRF provides default attenuation settings for individual floor plans that you cannot change.

Figure 180: *Wall Attenuation Settings*
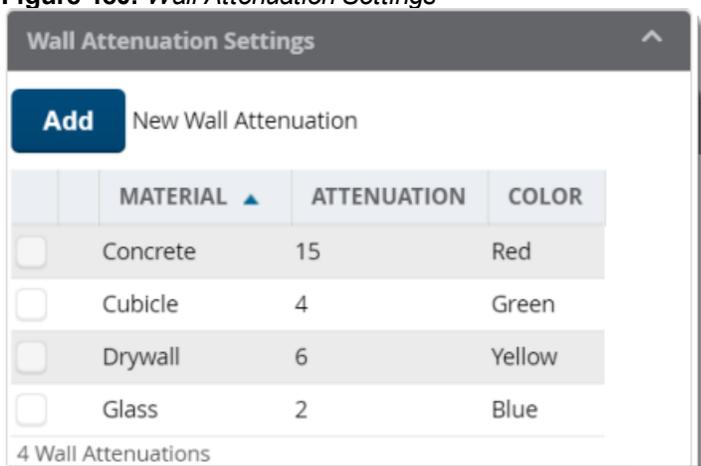
The default wall attenuation settings are described in Table 149.

Table 149: *Default Wall Attenuations*

Item	Description
Material	Type of material that reduces the signal strength, including concrete, cubicle, dry wall, and glass.
Attenuation	Signal loss represented in decibels (dB).
Color	Color representation in the floor plan.

Adding a Wall Attenuation

Follow these steps to create a wall attenuation:

1. Navigate to **VisualRF > Setup**, then click **Add**.
2. Enter the wall material.
3. Enter the attenuation in decibels.
4. Select the color used to represent the attenuation on the floor plan.

   Figure 181 shows an example of RF signal power decreasing by 3 db of attenuation for brick walls.

Figure 181: *Adding a Wall Attenuation*
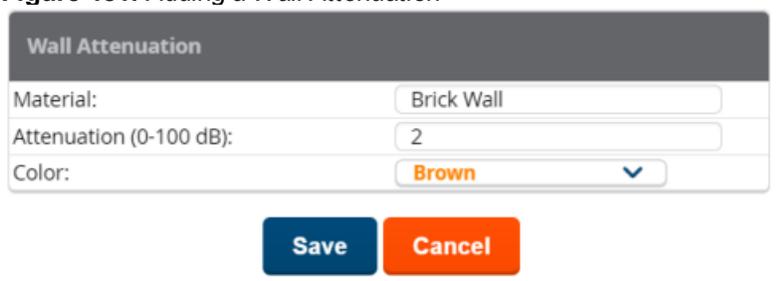
5. Click **Save**. The brick wall attenuation you added in Step 4 displays in the Wall Attenuation table.

Figure 182: *Wall Attenuation*

	MATERIAL ▲	ATTENUATION	COLOR
☐ ✎	Brick Wall	2	Brown
☐	Concrete	15	Red
☐	Cubicle	4	Green
☐	Drywall	6	Yellow
☐	Glass	2	Blue
5 Wall Attenuations			

You can later change the attenuation by clicking ✎ next to the material in the Wall Attenuation table.

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.

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 314
- "Creating a New Building" on page 315
- "Adding a Floor Plan" on page 316
- "Editing a Floor Plan Image" on page 317
- "Defining Floor Plan Boundaries" on page 318
- "Defining Floor Plan Regions" on page 318
- "Editing a Planning Region" on page 319
- "Adding Deployed Access Points onto the Floor Plan" on page 320
- "Adding Planned APs onto the Floor Plan" on page 321
- "Editing a Planning Region" on page 319
- "Auto-Matching Planned Devices" on page 322
- "Printing a Bill of Materials Report" on page 322

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:

1. Navigate to **VisualRF > Floor Plans**.
2. Navigate to the **Add Campus** menu.
3. Select **Edit** from the toolbar on the right window pane of the Network view, then click **Add campus**.
4. Enter the name of the campus, then click **Save**. A new campus icon appears on the campus background.
5. Select an appropriate network geographical background or upload a personalized image by right-clicking on the background, and selecting one of the following options:
   - **World Map**: browse and select any of the included maps.
   - **Custom Image**: upload your own image as the map background.
6. Drag the new campus icon to the appropriate location on the map background, or right-click the background and select **Auto Arrange Campuses** to arrange the campus in alphabetical order across the background.

Creating a New Building

1. Select the icon for the campus created in the previous procedure.
2. When the campus area opens, add the new building. Select **Edit** from the toolbar on the right window pane of the Network view, then click **Add building**.
3. When the **New Building** window appears, enter the following information:

Table 150: *New Building Fields and Descriptions*

Field	Description
Name	Name of the building located in an existing campus.
Address	Building or Campus address
Longitude & Latitude	These fields are used to represent a building on Google Earth.
Ceiling Height	The normal distance between floors in the building. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. This data element can be imported or exported to external planning tools like Ekahau. It is not currently used by W-AirWave.
Attenuation	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 used by W-AirWave.

NOTE

The WebUI also includes fields to configure client transmit power and desired speed values used for automatic placement of APs into floors within this campus. These fields are located in the **Advanced** section of the floor **Properties** menu.

Figure 183: *Create New Building Window*
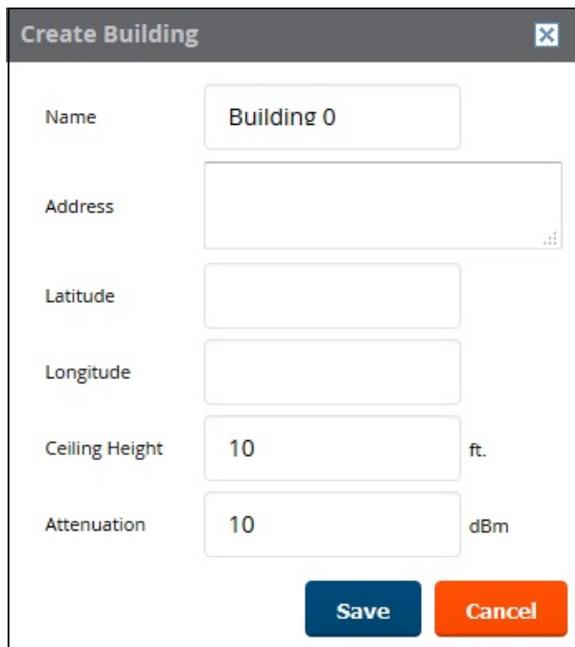
4. Select **Save**. A new building icon will appear in the upper-left corner of the background canvas.

5. Drag the Building icon to the appropriate location on the map background.

You are now ready to import your floor plan.

Adding a Floor Plan

Floor plans can be added (imported), edited, and deleted. 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 floor plan.

VisualRF supports floor plans in CAD, DWG , GIF, SVG, JPEG, PNG, and PDF format. Consider the following guidelines:

- CAD files must be generated from Autodesk's AutoCAD® software.
- The floor size is restricted to 800 X 800 meters.
- If the files include cross-referencing bindings, they might not display properly.
- PDF files must be generated from an original source file. Altered PDF files, such a scanned file, will not import properly.

NOTE

When importing a floor plan, ensure that the devices to be included are also available in the device catalog.

To add a floor plan:

1. Navigate to **VisualRF > Floor Plans**, and drill down into the network and campus maps to select the building for which you want to import a new floor plan.

2. Select **Edit** from the toolbar on the right window pane of the Network view, then click **New Floorplan**. If an incomplete floor plan is in floor wizard mode, it will appear as a windowless floor in the building icon. Double-click that floor to open the floor in the **New Floorplan** window.

3. Click **Browse** and find the floor plan file in your hard drive.

4. If your network has multiple campuses or buildings, select the campus and building. You can also rename the floor and floor number.

5. Click **Save**. The floor plan opens in VisualRF, with planning tools on the side navigation bar.

Editing a Floor Plan Image

There are several ways to edit a floor plan that you have uploaded, as explained in the following topics:

- "Cropping the Floor Plan Image" on page 317
- "Sizing a Non-CAD Floor Plan " on page 317

Cropping the Floor Plan Image

Cropping is available from within the VisualRF Floor Upload Wizard.

1. Launch the Floor Upload wizard, as described in "Adding a Floor Plan" on page 316.

2. Use the cropping handles (circles at the corners of the image) 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 not more than 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.

<table>
<tr>
<td>NOTE</td>
<td>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.</td>
</tr>
</table>

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 VisualRF thumbnails.

Copying a Floor Plan in the Same Building

When you want to create a duplicate floor plan , simply copy an existing floor plan in the same building. To do this, use the Floor plan **Duplicate** option.

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 the procedures below.

To resize a Non-CAD floor plan:

1. In the **Scale** section of the floor upload wizard, click the **Measure** button. 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. Use the slider bar at the upper left corner of the upload wizard to zoom in to a section of the floor plan, if necessary.

3. Select and hold to establish the first point and drag your mouse to the second point and release.

4. An **Enter Distance** dialogue box appears. Enter the proper length in feet, as shown in Figure 184.

5. Click **OK**.

Figure 184: *Manually Measuring a Floor Plan*
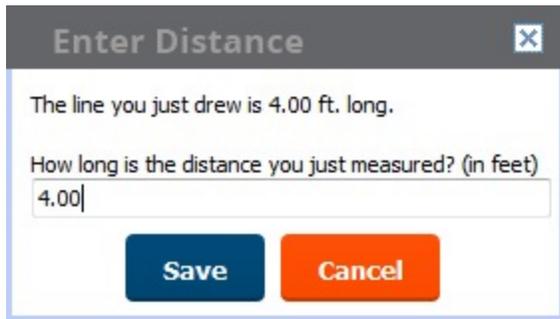
Defining Floor Plan Boundaries

Use the **Floorplan Boundary** section of the Floor Upload Wizard to refine the floor plan to remove whitespace, or to create a floorplan based on a portion of the interior of the graphic, such as an atrium.

To define a floorplan boundary:

1. Click the **Define Floorplan Boundary** button. The pointer changes to a cross-hair icon.

2. Click on the floor plan graphic to define the boundaries of the floor plan. Use the slider bar at the upper left corner of the upload wizard to zoom in to a section of the floor plan, if necessary.

3. If your floor plan has regions with different requirements than the rest of the floorplan, continue to Defining Floor Plan Regions below. Otherwise, click **Next**.

Defining Floor Plan Regions

Define regions within a floor plan that have different wireless networking requirements than the rest of the floor. For example, you can use the planning regions tool to define two small regions of high density clients within a larger floor plan with lower client density. You can define regions on a new floor plan using the Floor Upload wizard, or edit a an existing floor plan to add a new region.

Adding Region to a New Floor using the Floor Upload Wizard

You can define a floor plan region when you create a new floor plan using the Floor Upload Wizard.

1. Launch the Floor Upload wizard as described in "Adding a Floor Plan" on page 316.

1. Click the **Define Planning Regions** button. The pointer changes to a cross-hair icon.

2. (Optional) Enter a name for the region in the **Name** field.

3. Click on the floor plan graphic to define the boundaries of the region. Use the slider bar at the upper left corner of the wizard to zoom in to a section of the floor plan, if necessary.

4. Repeat steps 1-2 to create an additional regions, as required.

5. Once you have defined all necessary regions on your floor plan, click **Next** to continue to the Access Points section of the Floor Upload Wizard, as described in "Adding Planned APs onto the Floor Plan" on page 321 and "Adding Deployed Access Points onto the Floor Plan" on page 320.

Adding a Region to an Existing Floor Plan

To add a region to an existing floor:

1. Select the floor to which you want to add a region.
2. Click **Edit** in the navigation bar to open the Edit menu.
3. Click **Draw Region**. The pointer changes to a cross-hair icon.
4. Click on the floor plan graphic to define the edge of the new region. Use the slider bar at the upper left corner of the wizard to zoom in to a section of the floor plan, if necessary.
5. Once the floor plan region is defined, select the region and click the **Properties** menu. The **Name** field shows the current name for that region. You can rename a region by entering a new name into this field.
6. Click **Type** to specify a region type .
   - **Boundary**: This option creates a region that defines the boundaries of an area.
   - **Planning**: This option creates a region to plan for new access points, and define transmit power and PHY types for AP radios.
   - **Probability**: Define the location probability for the region. Location probability regions are optional regions that can be used to increase the accuracy of device location. VisualRF can calculate device locations based on probability, and use this information to place the device into regions where they are more likely to be located, like conference rooms and cubical farms, or pull users out of regions where they are less likely to be, like parking lots and courtyards.
   - **AirPlay/AirPrint**: Reserved for future use.
7. Click **Save** to save your region.

Table 151: *Fields in the Region Properties Window*

Planning Region Type	
AP Type	The type of AP used in this planning region.
Count	Number of APs of the selected type to provision onto the selected region.
Phy	Whether they PHY is set to 11n or no radio.
Tx Power	Transmit power of the AP radio, in dBm.
Gain	This read-only parameter displays the AP antenna gain in dBi.
Planned Air Monitors	Enter the number of Air Monitors to be deployed in this region
Environment	A range from 1-4 that best describes whether the environment is related to an office space, cubicles, offices, or concrete.
Probability / Location Probability Region Type	
Probability	Click and drag this slider to specify if users are likely to be in this region. A location probability of **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%.

Editing a Planning Region

You can edit a region by right-clicking within the region to see the following options:

- **Select All** - Selects all regions on the floorplan.

- **Draw Walls Around Region** - This action surrounds the region with walls of the last used wall type (concrete, cubicle, drywall or glass). For information on defining different wall types, see Adding Exterior Walls.
- **Bring to Back**, **Send to Front** - If one region is within the boundaries of another region, or two regions overlap, you may not be able to select the desired region until that region is brought to the front, or the overlapping region is sent to the back.
- **Delete Planned Devices** - Deletes all planned APs within the region.
- **Remove** - Delete the region. Any planned devices within the region will stay on the floor plan.

Floor Plan Properties

You can edit an existing floor plan by changing the floor plan properties described in Table 152. To access the **Properties** menu:

1. Navigate to **VisualRF> Floor Plans**.
2. Open the floor plan in Network view.
3. Click the **Properties** link to open the **Properties** menu.

Table 152: *Floor Plan Properties*

Setting	Default	Description
Floor Name	Floor [Number]	A descriptive name for the floor. It inherits the floor number as a name if nothing is entered.
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.
Width Height	N/A	These fields display the current width and height of the floor plan. To change these settings, click the **Measure** icon and measure a portion of the floor. For details, see Sizing a Non-CAD Floor Plan .
Gridsize	5 x 5 feet	Decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy.
Advanced		
Client TX	30mW	Client transmit power, used in auto placement of access points onto floors within this campus. The range is 30mW to 100mW.
Speed	200 Mbps	The data transmission speed used in auto placement of access points onto floors within this campus. The range is 6 Mbps to 1.3 Gbps.
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. For details on defining attenuation values, see Wall Attenuation Settings.

Adding Deployed Access Points onto the Floor Plan

You can provision existing APs in your network onto a new floor plan using the Floor Upload wizard, or edit an existing floor plan to add new APs using the **Properties** menu for that floor.

W-AirWave recalculates path loss and client locations after adding a deployed AP. All changes may not be visible on a refresh until this process complete.

1. Determine if you want to add APs to a new floor plan, or an existing floor plan.

   - To add APs to a new floor plan using the Floor Upload wizard, click **Access Points** in the wizard navigation bar, then select **Add deployed APs**.

   - To add APs an existing floor plan, select that floor plan, click the **Edit** menu in the navigation bar, then click the **Add Deployed AP** icon

2. A list of devices in your W-AirWave appears, as shown in Figure 185.

3. Select whether to view APs by **Group** or by **Folder**. You can also use the **Search** field to identify APs to add to the floor.

4. 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.

5. Click and drag an AP (or a Group or Folder of APs) to its proper location on the floor.

6. If you are adding APs to a floor using the Floor Upload wizard, click the **Finish** button. Otherwise:

   - Remove a device from the floor plan by right-clicking that device then clicking **Remove.**

   - Return to an earlier section of the Floor Upload wizard by clicking **Previous**.

   - Add existing devices to the floor plan. See "Adding Deployed Access Points onto the Floor Plan" on page 320.

Figure 185: *List of Deployed APs*
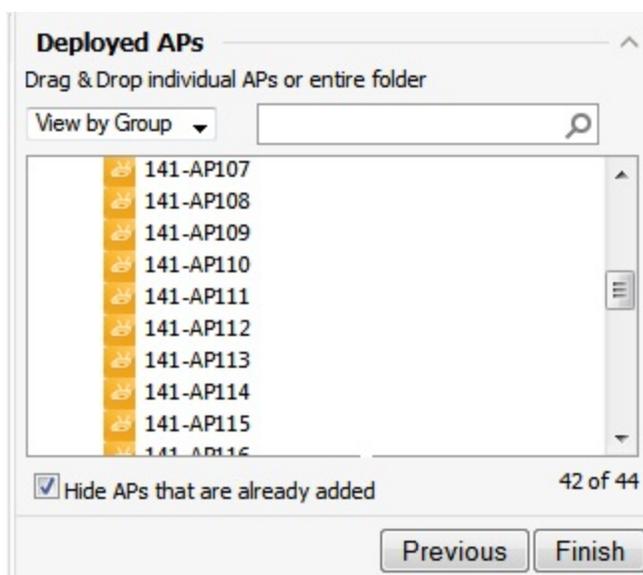
Adding Planned APs onto the Floor Plan

You can plan for and provision new APs onto a new floor plan using the Floor Upload wizard, or add new APs to an existing floor plan using the **Properties** menu for that floor.

1. Determine if you want to plan for APs on a new floor using the Floor Upload wizard, or plan for APs on an existing floor plan.

   - To add APs to a new floor plan using the Floor Upload Wizard, click **Access Points** in the wizard navigation bar, then select **Plan APs**.

   - To add APs to an existing floor plan, open the selected floor plan, then click **Edit** menu in the navigation bar.

2. Click the **Type** drop-down list and select a device type from the list of available devices.

3. In the **Count** field, enter the number of devices of that type to add to the new floor.

4. (Optional) Click and drag the **Deployment Type** slider bar to adjust data rates for a high-density or low-density environment.

5. (Optional) Click the **Advanced** link and configure the advanced deployment options
   - **Service level**: Select **Speed** or **Signal** to plan coverage by adjusting data rate requirements (Speed) or AP signal strength settings. Click **Calculate AP** count to recalculate the suggested number of APs based on these advanced settings.
   - **Client Density**: In the **Max Clients** field, set the anticipated number of clients that will be stationed in the floor. in the **Clients per AP** field, enter the maximum number of clients supported by each radio. Click **Calculate AP** count to recalculate the suggested number of APs based on these advanced settings.

6. Click **Add APs to Floorplan**.

7. Click and drag the device, to the desired location.

8. If you are done creating the floor plan, click the **Finish** button. Otherwise:
   - Remove a planned device from the floor plan by right-click that device then clicking **Remove.**
   - Return to an earlier section of the Floor Upload wizard by clicking **Previous**.
   - Add existing devices to the floor plan. See "Adding Deployed Access Points onto the Floor Plan" on page 320

Auto-Matching Planned Devices

You can right-click a floor plan or 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-click a campus icon, a building icon, or a builiding floor and select **Show Bill of Materials**. A generating report pop up 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 186:

Figure 186: *Bill of Materials Report Illustration*
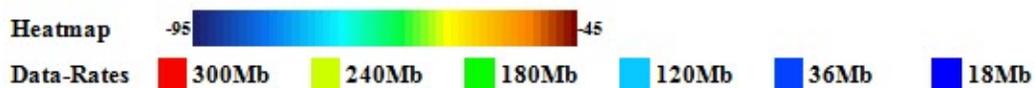
Increasing Location Accuracy

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 153:

Table 153: *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
Dell	Yes	Yes	Yes	Yes
Cisco LWAPP	Yes	Yes	Yes	Yes
Cisco IOS	Yes	No	No	With WLSE
Cisco VxWorks	Yes	No	No	No
Trapeze	Yes	No	No	Yes
Meru	No	No	No	Yes

Table 153: *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
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

W-AirWave provides four main methods to increase accuracy once your access points are deployed:

- Adding Exterior Walls - increases location accuracy by reducing the statistical probability of placements outside the office confines. See "Adding Exterior Walls" on page 324.
- 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 Defining Stationary Devices.
- 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 "" on page 1.
- Location Probability Regions - Probability regions will increase or decrease the chances of a device being located within the region. See Defining Floor Plan Regions.

Adding Exterior Walls

Because VisualRF utilizes much existing RF information, generally only external walls are required for accurate client locations. The VisualRF 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. Navigate to **VisualRF>Floor Plans** and select a floor plan.
2. Select the **Draw Wall** button in the **Edit** menu.
3. The cursor changes to a crosshair icon, indicating that the view is in wall editing mode. Use this cursor to draw the wall directly over the floor plan, as shown in Figure 187.

Figure 187: *Drawing a wall*

4. (Optional) Change the attenuation of a wall by selecting the appropriate building material for that wall.To define the wall material , select the wall, click the **Properties** tab, then select the building material type from the **Material** drop-down list.

5. When you are done creating walls, click the **Draw Wall** button again to exit the wall editing mode.

You can edit or remove a wall at any time. 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 188.

Figure 188: *Moving and resizing an existing wall*
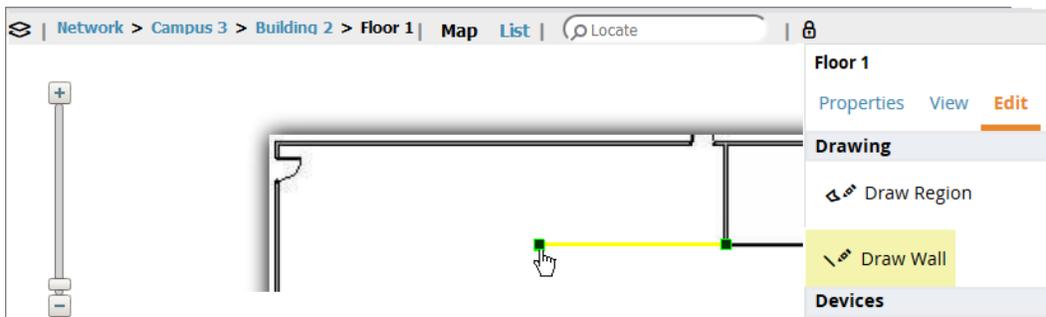
To delete a wall, select the wall and press the **Delete** key. You can also right-click on a wall and select **Delete** from the pop up menu.

> Best practices is to draw only outside walls. If you are seeing inaccurate client locations or heat maps after entering exterior walls, proceed to Client Surveys. If you still experience problems, then consider adding interior walls.

Defining Stationary Devices

VisualRF provides the ability to statically assign a permanent location 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 on the floor plan.

2. To select the client and mark it as static device, click the **Properties** link in the navigation bar, and select **Location for this client is static**.

3. Click the **Add** button for Static Training, as shown in Figure 189:

Figure 189: *Marking a Device as Static*

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 W-AirWave.

Decreasing Grid Size

Decreasing the grid size will enable the location to place clients in a small grid, which will increase accuracy. Select the floor plan, click the Properties menu, then click the **Gridsize** drop-down list.

Enabling Dynamic Attenuation

The dynamic attenuation feature (which is enabled by default) instructs the location service to sample the current RF environment and to dynamically adjust Path Loss. This feature can be enabled or disable in the **VisualRF>Setup** page.

Configuring Infrastructure

Fine-tune location services to 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 W-AirWave queries those MIB entries, and how often VisualRF service queries W-AirWave for this RF information.

Figure 190: *Timing Factors Impacting Location Accuracy*
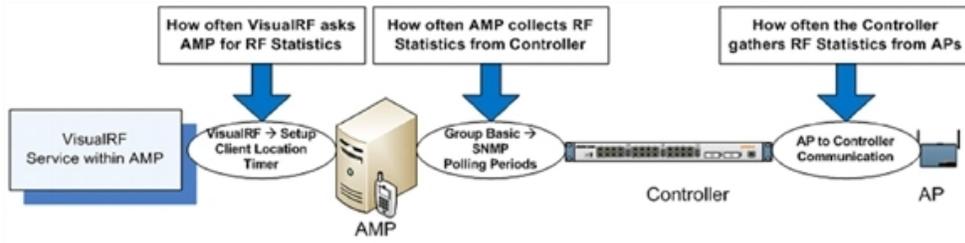
These best practices are recommended when configuring hardware infrastructure:

● For legacy autonomous APs, ensure on the **Group > Radio** page that **Rogue Scanning** is enabled and the interval is accurate, as shown in Figure 191:

Figure 191: *Group Rogue Scanning Configuration*

● For thin APs, ensure that the controllers are configured to gather RF information from the thin APs frequently.

● For Cisco LWAPP, navigate to **Groups > Cisco WLC Config** page in W-AirWave. 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 192 for an example.

Figure 192: *Rectangular Floor Plan AP Deployment*
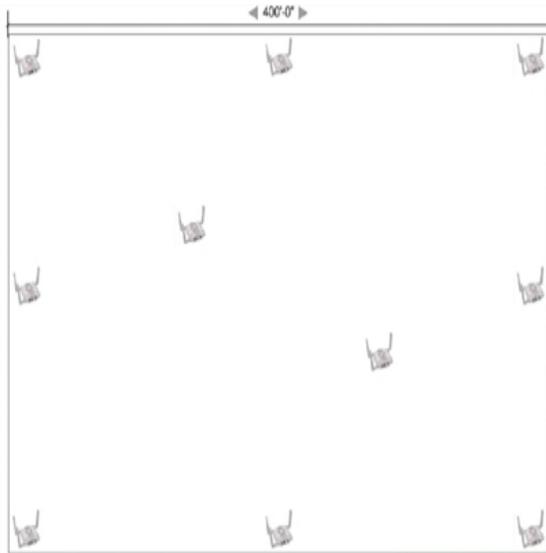
Using VisualRF to Assess RF Environments

VisualRF 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 328
- "Viewing an AP's Wireless RF Environment" on page 330
- "Viewing a Floor Plan's RF Environment" on page 331
- "Viewing a Network, Campus, Building's RF Environment " on page 332
- "Viewing Campuses, Buildings, or Floors from a List View" on page 332

Viewing a Wireless User's RF Environment

You can use Visual RF to view information about a user's RF environment.

1. from the **Clients > Client Detail** page for the client whose RF environment you want to view, select the VisualRF thumbnail, located next to the **Current Association** section at the bottom of the of this page (as shown in Figure 193):

Figure 193: *VisualRF thumbnail in Clients > Client Detail*

Location: Sunnyvale > 1322 > 1322 (Floor 1)

Enlarge |

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

The VisualRF Location History tracker can display the location history for the selected user by indicating on the floor plan the locations to which that user traveled over the selected time period.

1. To view location tracking, select a client icon in the floor plan, click the **View** link in the right navigation pane, then select **Replay Location History**.

2. Select the period of time over which you want to track that client's movements, and the optionally, the frequency of sample times. Longer sample times will impact animation speeds, and location smoothing. When the animation smoothing feature is turned off or set to a lower value, the tracking history displays smaller client movements. When the smoothing value is set to higher values, these small movements are not displayed, and only larger location movements are animated.

The location history settings, illustrated in Figure 194, appears at the bottom of the VisualRF window.

Figure 194: *Location History Player*
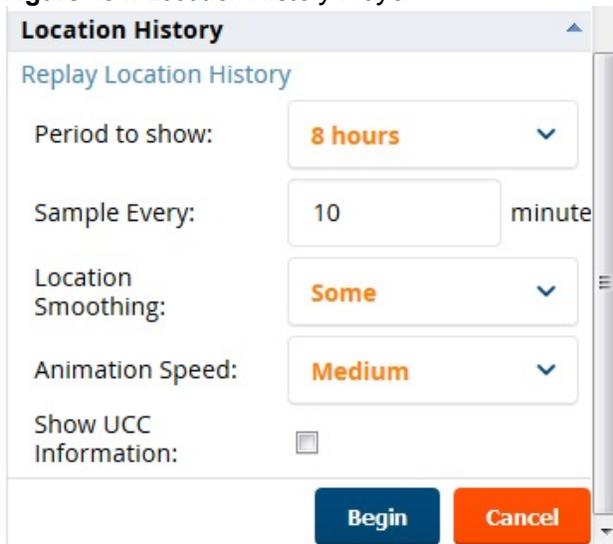
Checking Signal Strength to Client Location

1. Open a floor plan in the **VisualRF > Floor Plans** page.
2. Click the **View** tab.
3. In the **AP Overlays** section of this tab, select the **Channel** option.
4. Click the **Signal Cutoff** drop-down list.
5. Select the desired signal level to display, as shown in Figure 195. The heatmap updates immediately.

Figure 195: *Signal Cutoff dBm Dropdown Menu*
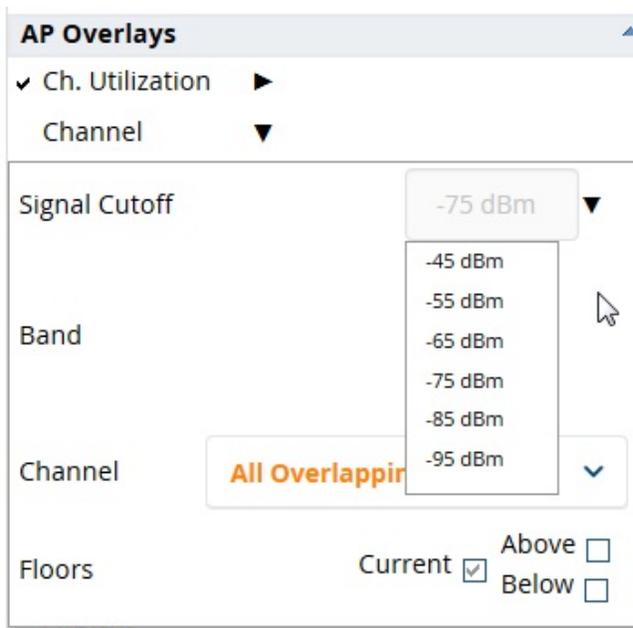
Viewing an AP's Wireless RF Environment

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 W-AirWave page that lists your APs. The **APs/Devices > Monitor** page opens.

2. If the AP is associated with a floor plan, the page displays a VisualRF thumbnail showing the location of the AP. Click this thumbnail to open the floor plan in VisualRF.

Figure 196: *VisualRF Thumbnail on the **APs/Devices > Monitor** page*
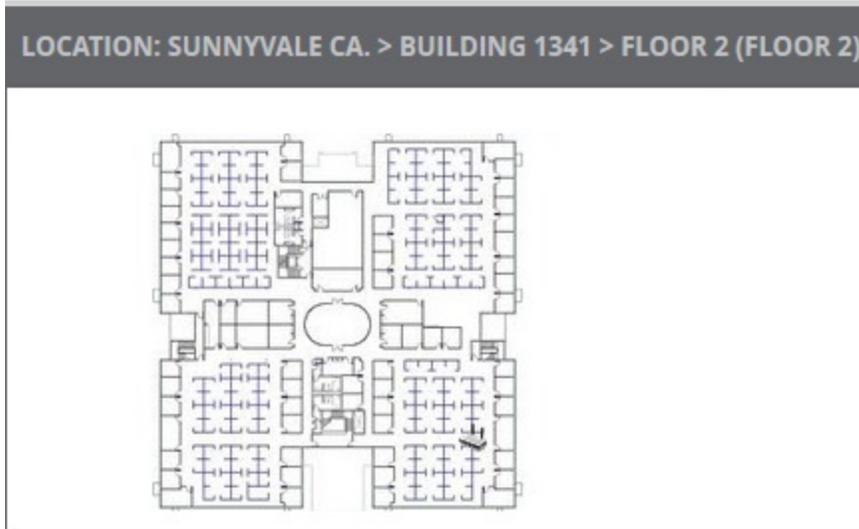
Viewing a Floor Plan's RF Environment

To view a floor plan's RF environment, navigate to the **VisualRF > Floor Plans** page. Click the **List** link at the top right of the **Floor Plans** page to view a sortable, clickable list that allows you to select and instantly view any campus, building or floor in the network.

Figure 197: *Floor Plans List View*

The **VisualRF > Floor Plans** page provides a snapshot of how VisualRF is performing, as described in Table 154:

Table 154: *Floor Plans list columns*

Field	Description
Campus	Campus associated to the floor.

Table 154: *Floor Plans list columns (Continued)*

Field	Description
Building	Building associated to the floor.
Floor	Floor number. The decimal place can be used for mezzanine levels.
Name	Optional name of a floor. (If the name is not changed, it displays the name as Floor [Number] by default.)
Size	The height and width in feet of the floor plan, including white space.
Grid Cell Size	The size of the grid cells, in feet.
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, Wi-Fi tags within the floor

Viewing Campuses, Buildings, or Floors from a List View

The WebUI supports a List View that displays a sortable, clickable list that allows you to select and instantly view any campus, building or floor in the network:

1. Navigate to the **VisualRF > Floor Plans** page.

2. Click the **List** link at the top right of any view. The **Network List View** window, shown in Figure 198, appears on the screen. If a floor is in floor upload wizard mode, it appears in the list with an asterisk (*) by the floor name.

Figure 198: *Network List View*

3. Click any of the links to view that location, or click a column heading to sort the list by that column criteria. The **Original Floor Plan** column contains links to download the floor plan graphic for the selected floor.

4. To return to the Map view, click the **Map** link at the top right of the page.

Importing and Exporting in VisualRF

Exporting a campus

To export a campus from VisualRF so you can import it into another W-AirWave, 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 W-AirWave.

At this point, you are ready to deploy a production W-AirWave 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 WebUI 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

- 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 W-AirWave : https://<W-AirWave_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 a Dell Networking W-Series Controller

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into a Dell Networking W-Series controller.

Pre-Conversion Checklist

Prior to importing floor plans, ensure that the VisualRF memory allocation is sufficient for the anticipated number of floor plans.

To change the memory allocation, navigate to the **VisualRF > Setup** page and configure the memory allocation accordingly. Memory allocation should equal .5 GB for 1-75 floor plans, 1 GB for 76-250 floor plans, 1.5 GB for 251-500 floor plans, and 2 GB for 501-1,000 floor plans.

Importing a large number of floor plans can impact performance of the W-AirWave 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 WebUI , 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 W-AirWave

1. Navigate to **VisualRF > Import**.
2. Select the **Import floor plans from an Aruba/Dell Networking W 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.'

When interacting with the W-AirWave API, the system requires that clients send the 'X-BISCOTTI' header along with posts. The value of the header is provided as a part of the response when a client authenticates against /LOGIN. A X-BISCOTTI token lasts as long as authentication session.

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 W-AirWave service on the Web. You can use VisualRF Plan to do basic planning procedures like adding a floor plan, provisioning APs, and generating a Bill of Materials (BOM) report. VisualRF Plan is free to use for anyone with aDell support account. No license is required.

The client can be downloaded from download.dell-pcw.com, Tools & Resources.

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 Dell 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 155: *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	
VisualRF preferences	X	
Resource utilization	X	
Add external walls	X	X
Client surveys	X	
Wiring Closet	X	X
View deployed switches	X	
View signal strength	X	
Planning and provisioning	X	X
Import and Export	X	X

Enabling FIPS 140-2 Approved Mode

Users who are subject to government or industry regulations must enable FIPS 140-2 approved mode when using W-AirWave. When FIPS 140-2 approved mode is on, users can connect to the W-AirWave server using FIPS 140-2 approved functions (ciphers).

To enable FIPS 140-2 approved mode:

1. Open a console window, then log into the system.
2. In the window, enter 9-5 to enable FIPS.

   The W-AirWave server reboots automatically after it turns on FIPS mode.

About the Command Line Interface

W-AirWave provides a modular command line interface (CLI) that allows you to run a finite set of management tools and configuration tasks. Some of these tasks include transferring files, enabling support connections, enabling FIPS security, upgrading software, and configuring network interfaces.

CLI Access

A change introduced in W-AirWave 8.2.4 prevents the root user from being able to connect to the CLI. You can access the CLI through an SSH connection by logging in to the W-AirWave server with the admin user created when you install or upgrade your software to W-AirWave 8.2.4. For information about the admin user, see "Step 4: Checking the W-AirWave Installation" and "Upgrading the Software" in the *W-AirWave 8.2.4 Installation Guide*.

Custom Modules

W-AirWave provides a selection of custom modules that is available by customer support request.

To get the module key:

1. Log in to the CLI as the admin user.
2. Select **9** to open the Security menu.
3. Select **7** to get the module key. A message asks you to show or save the module key for later. If you choose to save the module key, go to the next step.
4. Go back to the main menu and select **2** to download the module key to an SCP reachable destination.
5. Send module key to technical support.
6. After you receive the module, select **1** to upload the module.
7. Select **10** to add the module to your CLI custom modules menu.

How to Reset Your Password

If you forgot your password used to access the CLI, you can log in using the amprecovery credentials and reset the password.

To reset your password:

1. From a local terminal, or the VM host console, log in to the CLI:
   ```
   <AMP server> login: amprecovery
   Password: recovery
   ```
2. Select **1** to change the OS password.

   W-AirWave finds the users created after the AMP CLI installation and lists the users in the menu.
3. Select **1** to select the user.

CLI Options

Table 156 lists the CLI commands that are available in W-AirWave 8.2.4. If there are other important tasks that you can't do from the CLI, contact technical support for help.

Table 156: *CLI Options*

Option	Description
1 Upload File	Uploads a file to the AirWave server you're currently logged in to using SCP for Unix.
2 Download File	Downloads a file from the local AMP to another server using SCP for Unix.
3 Delete File	Deletes a file from the AirWave server. Files shown for deletion might include downloaded files, temporary files, and backup files.
4 Backup	Displays AMP Backup options.
4-1 Backup Now	Runs the back up now.
4-2 Configure Automatic Transfer	Sets the destination for the nightly backup files.
4-3 Local Backup Retention	Changes how many backups W-AirWave retains (maximum of 4).
5 Restore	Restores the AMP server from an on-demand, nightly, or imported backup that you select.
6 Support	Displays support options.
6-1 Show Tech Support	Displays information about the AMP server to show technical support.
6-2 Generate Diagnostic Tarball	Displays the compressed log collection for sending to customer support.
6-3 Initialize Support Connection	Loads the **support_connection.tar** file provided by customer support and creates the support user (by default, awsupport) and password.
6-4 Start Support Connection	Toggles on and off the support connection.
6-5 Delete Support User	Deletes the **awsupport.gpg** file.
6-6 Show contents of awsupport.gpg	Displays the encrypted support credentials.
7 Upgrade	Displays upgrade options.
7-1 Upgrade W-AirWave Management Platform	Runs the W-AirWave software upgrade.
7-2 Upgrade OS Kernel	Runs the kernel upgrade (requires rebooting the AirWave server).
8 Advanced	Displays system options.
8-1 Restart Application	Restarts the AirWave services.
8-2 Reboot System	Reboots the AirWave server.
8-3 Configure Network Settings	Configures network settings.
8-4 Set Hostname	Sets the hostname of the AirWave server.
8-5 Shutdown System (halt)	Shuts down the AirWave server gracefully.

Option	Description
9 Security	Displays security options.
9-1 Reset Web admin Password	Resets the Web UI log in password for admin.
9-2 Change OS User Password	Changes the CLI log in password.
9-3 Add SSL Certificate	Installs the SSL certificate, used to establish secure web sessions, on your AirWave server.
9-4 Add DTLS Certificates	Installs the DTLS certificates, used to encrypt secure AMON traffic, on your AirWave server.
9-5 Enable FIPS	Toggles on or off FIPS 140-2 Approved Mode (reboot required action).
9-6 Show EngineID	Displays the SNMPv3 engine ID.
9-7 Module Key	Displays module key options.
9-7-1 Show	Displays the PGP key used to create a custom module.
9-7-2 Save	Saves the PGP key.
10 Custom Commands	Displays custom command option.
10-1 Add New Menu Module	Adds a new CLI menu module that you select (requires requesting module encrypted with a module key from customer support).
b >> Back (or Ctrl+c)	Returns to the previous menu.
c >> Cancel	Cancels the key request.
q	Exits the CLI session.