AirWave 8.2.11.1

User Guide

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. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Please specify the product and version for which you are requesting source code.

You may also request a copy of this source code free of charge at: http://hpe.com/software/opensource.

AirWave is a network management platform that provides a single console where you can monitor, analyze, and configure wired and wireless networks. Whether your network is simple or a large, complex, multi-vendor installation, AirWave makes it easy to monitor your network with features like AppRF, Clarity, and VisualRF.

AirWave also provisions Aruba switches, provides CPU, memory and interface monitoring, configuration management, and upgrades switch firmware. AirWave can be used to implement zero-touch provisioning for Aruba Instant APs (IAP), Aruba switches and branch controllers.

With AirWave, you can configure:

- "Aruba Mobility Controllers" on page 16
- "Instant Access Points" on page 16
- "ArubaOS-S Switches and ArubaOS-CX Switches" on page 16

What's New

The following sections of the AirWave User Guide have been updated for this release. For a full list of new features and updates in AirWave8.2.11.1, including updates to other documents, refer to the *AirWave8.2.11.1 Release Notes*.

Table 1: *What's New in This Version of the User Guide*

Update	Description
Triggers for GRE tunnels	AirWave 8.2.11.1 introduces GRE tunnel triggers that can inform you of changes in the state or availability of tunnels, and when tunnels have the same IP address or tunnel ID.
Air Slice Client Diagnostics	Click the **Air Slice** tab on the **Clients > Diagnostics** page to view graphs showing the five applications experiencing the greatest amount of packet loss, latency, or jitter.
Topology icon	The **Devices > List** page includes a topology icon that allows you to quickly navigate to the **Home> Topology** page and view devices in the selected folder.
Generic markers in VisualRF	You can now add a generic marker to a floor plan and label it with text to mark the location of an object of interest on a floor plan, such as an IDF closet or fire extinguisher.
New Upgrade option in the CLI	The AirWave CLI added a new option to upgrade via the new Aruba Support Portal (asp.arubanetworks.com) and has deprecated support to upgrade from 8.2.11.1 via the legacy support portal at support.arubanetworks.com
Contact and Location Tracing (CLT)	Aruba NetInsight will support Contact and Location Tracing (CLT) analytics for Campus Wi-Fi customers using AirWave 8.x. This feature requires users to sign up for Aruba Central, and then use the AirWave comand-line interface to configure the CLT feature to send information to the Central cloud.

Table 1: *What's New in This Version of the User Guide (Continued)*

Update	Description
Changes to ZTP for switches	Starting with AirWave 8.2.11.1, if there is no Telnet/SSH username and password set on a group template for a factory-default switch running firmware version 16.10.008 or later, the AirWave server that creates an SSH connection to the switch will automatically reset the credentials to username: **manager** and password: **<device-serial-number>** .

Aruba Mobility Controllers

AirWave supports global and group-level configuration of Aruba mobility controllers. Several controllers can work together with APs to provide a hierarchical and redundant mobility controller system.

The mobility controller system provides:

- AP tunnel termination and translational bridging
- GRE tunnel between each AP and a mobility controller
- A virtual connection point to wireless clients
- Frame translation from 802.11 to 802.3 and 802.3 to 802.11, including encryption and decryption of wireless traffic
- Quality of service (QoS) and traffic prioritization

Working alone or in conjunction with ClearPass, the mobility controller authenticates wireless clients and includes a stateful firewall that can be configured to filter wireless traffic.

In this document, mobility controllers are also called access devices. For information about controller configuration, refer to the *AirWave 8.2.11.1 Controller Configuration Guide*.

Instant Access Points

Aruba Instant (Instant) is a system of access points in a Layer 2 subnet. The Instant APs (IAPs) are controlled by a single IAP that serves a dual role as both an 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 Aruba 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 AirWave server using a pre-shared key, or using two-way certificate-based authentication using an SSL certificate sent from AirWave to the Instant device. Virtual Controllers push data to 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 AirWave uses to communicate with Instant devices.

For additional information about Instant AP configuration, refer to the *Aruba Instant* in *AirWave Deployment Guide*.

ArubaOS-S Switches and ArubaOS-CX Switches

AirWave supports group-level configuration of ArubaOS-S Switches andArubaOS-CX Switches. These switches connect APs, wired clients and other endpoints to the network. Working alone or in conjunction with ClearPass, the ArubaOS-S Switches provide authentication, authorization and accounting.

In this document, ArubaOS-S Switches are also called access switches, and ArubaOS-CX Switches are also called core and aggregation switches. For informationabout switch configuration, refer to the *AirWave 8.2 Switch Configuration Guide*.

What's New

The following sections of the AirWave User Guide have been updated for this release. For a full list of new features and updates in AirWave8.2.11.1, including updates to other documents, refer to the *AirWave8.2.11.1 Release Notes*.

Table 2: *What's New in This Version of the User Guide*

Update	Description
Triggers for GRE tunnels	AirWave 8.2.11.1 introduces GRE tunnel triggers that can inform you of changes in the state or availability of tunnels, and when tunnels have the same IP address or tunnel ID.
Air Slice Client Diagnostics	Click the **Air Slice** tab on the **Clients > Diagnostics** page to view graphs showing the five applications experiencing the greatest amount of packet loss, latency, or jitter.
Topology icon	The **Devices > List** page includes a topology icon that allows you to quickly navigate to the **Home> Topology** page and view devices in the selected folder.
Generic markers in VisualRF	You can now add a generic marker to a floor plan and label it with text to mark the location of an object of interest on a floor plan, such as an IDF closet or fire extinguisher.
New Upgrade option in the CLI	The AirWave CLI added a new option to upgrade via the new Aruba Support Portal (asp.arubanetworks.com) and has deprecated support to upgrade from 8.2.11.1 via the legacy support portal at support.arubanetworks.com
Contact and Location Tracing (CLT)	Aruba NetInsight will support Contact and Location Tracing (CLT) analytics for Campus Wi-Fi customers using AirWave 8.x. This feature requires users to sign up for Aruba Central, and then use the AirWave comand-line interface to configure the CLT feature to send information to the Central cloud.
Changes to ZTP for switches	Starting with AirWave 8.2.11.1, if there is no Telnet/SSH username and password set on a group template for a factory-default switch running firmware version 16.10.008 or later, the AirWave server that creates an SSH connection to the switch will automatically reset the credentials to username: **manager** and password: **<device-serial-number>** .

Contacting Support

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com

End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

After you install the AirWave software, or any time you need to make changes to network settings, refer to the following procedures:

- "Defining Network Settings" on page 36
- "Configuring Cisco WLSE Rogue Scanning" on page 74
- "Configuring ACS Servers" on page 75
- "Integrating NMS Servers" on page 76
- "PCI Compliance Monitoring" on page 76
- "Deploying WMS Offload" on page 78
- "Integrating External Servers" on page 79

Defining General AirWave Server Settings

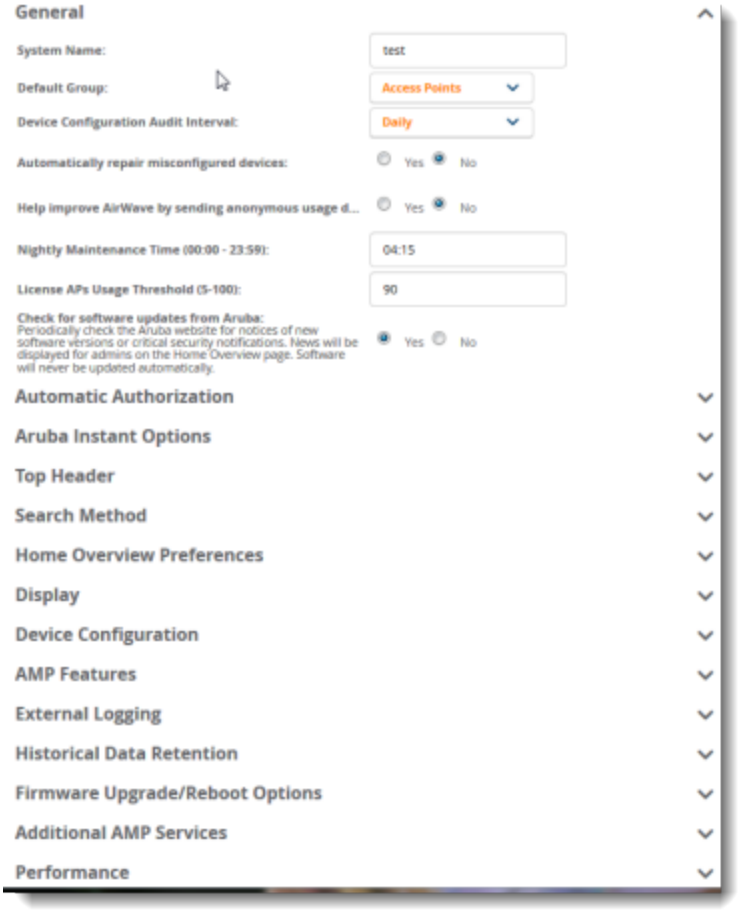
The initial tasks to configure the AirWave server include:

- "Configuring the AirWave Server" on page 19
- "Defining Network Settings" on page 36
- "Creating AirWave Users" on page 39
- "Configuring AirWave User Roles" on page 41
- "Configuring the User Login and Authentication" on page 46
- "Enabling AirWave to Manage Your Devices" on page 56
- "Managing Certificates" on page 62
- "Setting Up Device Types" on page 69

Configuring the AirWave Server

The following topics describe how to configure the general settings for the AirWave server. Figure 1 illustrates the **AMP Setup > General** page.

Figure 1: *AMP Setup > General Settings*



Whenever you save changes to these settings, AirWave applies them globally across the product for all users.

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 AirWave server using alphanumeric characters.
Default Group	Access Points	Sets the device group that this AirWave server uses as the default for device-level configuration. Select a device group from the drop-down menu. A group must first be defined on the **Groups > List** page to appear in this drop-down menu. For additional information, refer to "Using Device Groups" on page 81.

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

Setting	Default	Description
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 AirWave database. If the settings do not match, the AP is flagged as mismatched and 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 AirWave detects a variance between actual device settings and the Group configuration policy in the AirWave database.
Help improve AirWave by sending anonymous usage data	Disabled	If enabled, AirWave will send anonymous data to Aruba, which may be used to improve the AirWave software.
Nightly Maintenance Time (00:00 - 23:59)	04:15	Specifies the local time of day AirWave should perform daily maintenance. During maintenance, AirWave cleans the database, performs backups, and completes a few other housekeeping tasks. Such processes should not be performed during peak hours of demand.
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.
Check for software updates	Yes	Enables AirWave to check automatically for multiple update types. Check daily for AirWave updates, to include enhancements, device template files, important security updates, and other important news. This setting requires a direct Internet connection via AirWave.

Automatic Authorization Settings

On the **AMP Setup > General** page, locate the **Automatic Authorization** section. AirWave uses the automatic authorization settings to add devices into groups and folders. Table 4 describes these settings and identifies the default values.

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 **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**.

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

Setting	Default	Description
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 Switch Mode	Manage Read/Write	This setting is mainly used to push the configuration template to ZTP devices automatically without user intervention. When a switch registers with AirWave using ZTP, AirWave automatically puts the device into Manage Read/Write mode.
Automatically Authorized Virtual Controller Mode	Manage Read/Write	By default, this setting automatically puts the Instant AP into Manage Read/Write mode.
Authorize Aruba Instant APs	All	Auto-authorizes Instant APs using a pre-shared key (PSK) to access AirWave and join a group or folder. • **Whitelist**. AirWave automatically approves devices on a whitelist. You must use the group or folder that correlates to the provisioning rule configured in Activate. After ZTP, if you want to move the device to a different group or folder, set the **Use Aruba Instant AP Configured Group/Folder** option to **Yes**. • **All**. Onboards a device using a pre-shared key (PSK). AirWave adds the device to the new devices list. After you authorize this device, AirWave auto-authorizes all subsequent devices using the same PSK and adds the devices to AirWave and the specified group.
Authorize Aruba Switches to AirWave	All	Auto-authorizes Aruba switches to access AirWave and join a group or folder. • **Whitelist**. Select this option to auto-authorize devices on a whitelist. You must use the group or folder that correlates to the provisioning rule configured in Activate. After ZTP, if you want to move the device to a different group or folder, select **Yes**. • **All**. Onboards a device using a pre-shared key (PSK). AirWave adds the device to the new devices list. After you authorize this device, AirWave auto-authorizes all subsequent devices using the same PSK and adds the devices to AirWave and the specified group.

Restrictions for Using Whitelists

There are several restrictions that apply to this feature when AirWave can't distinguish between Instant APs and switches:

- When you add new devices, AirWave displays a rejection message:
- When you import devices from a whitelist, AirWave shows whitelisted devices in the Default View on pages that list devices.
- When you push a CLI command to a whitelisted device, AirWave won't push the command to the device and displays an error message. Select **Ignore** to clear the message. This might occur even though you selected **All**

for the **Authorize Aruba Instant Aps** or **Authorize Aruba Switches to AirWave** settings on the **AMP Setup > General** page.

- When you choose to export the whitelist for Instant APs, switches, or combined devices to a CSV, AirWave exports all the whitelisted devices on the **New Device** page to a CSV regardless of your selection.

Aruba Instant Settings

A Virtual Controller can communicate with the 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 AirWave to the Instant device.

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

Table 5: *AMP Setup > General > Aruba 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 AirWave.
Security method for adding new Virtual Controllers:	PSK Only	AirWave can use the following security methods to authenticate a Virtual Controller to the AirWave server: • PSK Only • PSK and Certificate • Certificate Only If you enable certificate-based 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 both a private key and certificate.
Allow None-TPM Devices	Yes	If certificate-based authentication is enabled for the Virtual Controller, AirWave allows low assurance, non-TPM device. This setting is unavailable when PSK authentication is used.
Configuration Only	No	By default, AirWave will push Instant configuration settings as well as AirWave settings such as RAPIDS settings and traps from an 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 AirWave server, as the default AirWave certificate will not be recognized by the Instant AP, and will cause the SSL handshake to fail. Certificate authentication also requires that the **AMP IP address** information configured on the Instant AP is a domain name, and not an IP address.

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 CA**: 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 AirWave certificate using the **View Certificate** link on that page, or click **Change** to upload a new certificate file to the AirWave server.

Top Header Settings

The top header of each AirWave WebUI page displays icons that provide counts on newly discovered devices, device status, mismatches, rogues, clients, and both unacknowledged and severe alerts. These icons also provide direct links for immediate access to key system components.

Figure 2: *Header Statistics Icons*

You can configure what is displayed in the top header for all pages, or for individual AirWave users.

To change the header statistic icons:

1. Navigate to **AMP Setup > General**, then scroll down to **Top Header**.
2. Choose the statistics.
3. Choose the devices.
4. Click **Save**.

A confirmation message does not appear when you make modifications to the top header statistic icons.

To change statistics that display for an AirWave user:

1. Navigate to **Home > User Info** page, then scroll down to **Top Header Stats**.
2. Choose the statistics.
3. Choose the devices.
4. Click **Save**. These user settings will override the general settings on the AMP Setup page.

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.

- 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.
- 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.

NOTE

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

Per-user search preferences can be set in the **Home > User Info** page.

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 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 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.

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

Setting	Default	Description
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, AirWave displays all Group tabs and setting options. • **Only devices on this** AMP—When selected, AirWave hides all options and tabs that do not apply to the APs and devices currently on 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 AirWave displays group settings. You can override this setting.
Look up device and wireless user hostnames	Yes	Enables 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 AirWave, after which 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**.
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.

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

Setting	Default	Description
Use Global Aruba Configuration	No	Enables Aruba configuration profile settings to be globally configured and then assigned to device groups. If disabled, settings can be defined entirely within **Groups > Controller Config**and **Groups > Switch Config** instead of globally. **NOTE:** Changing this setting may require importing configuration on your devices. When an existing Aruba configuration setup is to be converted from global to group, follow these steps: 1. Set all the devices to Monitor Only mode before setting the flag. 2. Each device Group will need to have an import performed from the **Device Configuration** 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 for VisualRF, RAPIDS, and AirWave Glass. 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.
Enable Central Authentication Service	Yes	Toggles on or off single-sign on (SSO) authentication between AirWave and AirWave Glass.
Central Authentication Hostname		If the Central Authentication Service is enabled and the managed AMP is attached to AirWave Glass, this field is automatically populated, and you don't need to configure the hostname.

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.

For information about creating triggers in order to receive event notifications, see "Creating New Triggers" on page 308.

Table 10: *AMP Setup > General > External Logging Section Fields and Default Values*

Setting	Default	Description
Include event log messages	No	Select **Yes** to send event log messages to an external Syslog server. **NOTE:** If you enable event logging, other options to configure the Syslog server and enable logging using Common Event Format (CEF) become available.
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**.
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

Historical data retention settings affect how long AirWave retains data. The longer AirWave retains data, such as inactive client sessions and rogue discovery events, the more hard disk space you require.

Table 11 describes the historical data retention settings on the **AMP Setup > General** page and provides the default values.

Table 11: *AMP Setup > General > Historical Data Retention Settings*

Setting	Default	Description
Inactive Client and VPN User Data (1-1500 days)	60	Defines the number of days AirWave retains basic information about inactive clients and VPN users. As a best practice, configure a shorter interval, such as 60 days, for customers with high user turnover.
Client Association and VPN Session History (1-550 days)	14	Defines the number of days AirWave retains client and VPN session records.

Table 11: *AMP Setup > General > Historical Data Retention Settings (Continued)*

Setting	Default	Description
Tag History (1-550 days)	14	Defines the number of days AirWave retains location history for Wi-Fi tags.
Rogue AP Discovery Events (2-550 days)	14	Defines the number of days AirWave retains rogue discovery events.
Reports (1-550 days)	60	Defines the number of days AirWave retains reports. **NOTE:** If there are more than 1000 reports, the **Reports > Generated** page might respond slowly.
Automatically acknowledge alerts (1-550 days)	14	Defines the number days of before AirWave automatically acknowledges alerts that have not been manually acknowledged.
Acknowledged Alerts (1-550 days)	60	Defines the number of days before AirWave deletes acknowledged alerts. **NOTE:** If there are more than 2000 alerts, the **System > Alerts** page might respond slowly.
Radius/ARM/IDS Events (1-550 days)	14	Defines the number of days AirWave retains information about RADIUS, ARM, and IDS events.
Archived Device Configurations (1-100)	10	Defines the number of configurations that AirWave retains for archived devices.
Archive device configs even if they only have rogue classifications	No	AirWave archives device configurations even if the device only has rogue classifications when you select **Yes**.
Guest Users (1-550 days)	30	Sets the number of days that AirWave is to support any guest user.
Inactive SSIDs (1-550 days)	425	Sets the number of days AirWave retains historical information after AirWave last saw a client on a specific SSID.
Inactive Interfaces (1-550 days)	425	Sets the number of days AirWave retains inactive interface information after the interface has been removed or deleted from the device.
Interface Status History (1-550 days)	425	Sets the number of days AirWave retains historical information on interface status.

Table 11: *AMP Setup > General > Historical Data Retention Settings (Continued)*

Setting	Default	Description
Interfering Devices (1-550 days)	14	Sets the number of days AirWave retains historical information on interfering devices.
Device Events (Syslog, Traps) (1-31 days)	2	Sets the number of days AirWave retains historical information on device events such as syslog entries and SNMP traps. Refer to "Viewing Device Events" on page 306. **NOTE:** If your database has more than five million rows, AirWave truncates the device event retention data, and the "number of days" becomes "number of hours."
Mesh Link History (1-550 days)	30	Sets the number of days AirWave retains historical information for mesh links.
Device Uptime (1-120 months)	60	Sets the number of months AirWave retains historical information on device uptime.
Client Data Retention Interval (1-425 days)	425	Sets the number of days AirWave retains historical information for clients.
UCC Call History (1-30 days)	30	Sets the number of days that calls remain in AirWave's call history.
UCC Call Details (1-7 days)	2	Sets the number of days that the AirWave retains details for individual calls.
Config Job Retention Interval (1-31 days)	31	Sets the number of days AirWave retains information about configuration jobs.
WAN Stats History (0-550 days, zero disables)	90	Sets the number of days AirWave retains WAN monitoring statistics. If you change this setting to zero, AirWave will not delete the data.

Firmware Upgrade/Reboot Options

Locate the **Firmware Upgrade/Reboot Options** section and adjust settings as required. This section allows you to configure the default firmware upgrade behavior for AirWaveTable 12

Table 12 describes the firmware upgrade and reboot options.

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, AirWave upgrades the firmware for APs in **Monitor Only** mode. When AirWave upgrades the firmware in this mode, the desired configuration are not be pushed to AirWave. Only the firmware is applied. The firmware upgrade may result in configuration changes AirWave does not correct those changes when the AP is in **Monitor Only** mode.
Allow Rebooting Monitor Only Devices	No	If **Yes** is selected, AirWave can reboot devices in **Monitor Only** mode.
Enable firmware distribution via http	No	By default, we use HTTPS and require user log in for firmware updates. **NOTE:** For IAPs running versions earlier than Instant 3.4.0.0, set this option to "Yes" in order to get firmware updates using HTTP.
Fast Download	No	When fast download is enabled, standalone IAPs in the same RF zone are grouped so that they can download the image from each other. This assumes that the APs are behind the same firewall so that they can reach each other, thereby making the firmware download faster.
Sequential Reboot	No	When sequential reboot is enabled, the APs in the same RF zone will reboot sequentially. At any given time, only one AP is being rebooted. As a result, users can use another AP that is visible in RF and have uninterrupted service.
Maximum Interleaved Jobs (1-20)	20	Defines the number of jobs AirWave runs at the same time. A job can include multiple APs. When jobs are started by multiple users, 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, 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 AirWave pauses the upgrade process. User intervention is required to resume the upgrade process. Setting this value to **0** disables this function.
Failure timeout (5-60 mins)	60	Sets the timeout for an upgrade attempt.
DRT upgrade failure timeout (2-30 mins)	6	Sets the timeout for a Downloadable Regulatory Table (DRT) upgrade attempt.
Number of tries in failure (1-4)	1	Sets the number of retry attempts.
Periodic run failed upgrade interval	Disabled	Set the length of time AirWave retries running a failed upgrade.

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 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, 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 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	Yes	Enables or disables the embedded mail server that is included with AirWave.
Mail Relay Server	Optional	If you enable the "Use embedded mail server" option, enter information for an optional mail relay server. This field supports a **Send Test Email** button for testing server functionality. Click this button to enter valid email addresses.
Process user roaming traps from Cisco WLC	Yes	Whether AirWave should parse client association and authentication traps from Cisco WLC controllers to give real time information on users connected to the wireless network.

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

Setting	Default	Description
Enable AMON data collection	Yes	Allows AirWave to collect enhanced data from Aruba devices on certain firmware versions. See the *Best Practices Guide* on the **Home > Documentation** page for more details **NOTE:** • When enabling AMON, auditing should be set to **daily** and have been successful at least once to allow 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 AirWave database. Auditing should be set to daily because the BSSIDs are kept in cache memory and cleared every 24 hours. • To view usage data on a standalone controller or managed device, set the **Enable AMON Data Collection** option to **No** to allow usage data to be aggregated from the AP level.
Enable Clarity Data Collection	Yes	Allows AirWave to collect enhanced Clarity Monitoring data from Aruba devices running ArubaOS 6.4.3 and later versions
Enable Traffic Analysis Data Collection	Yes	If AMON is enabled for a controller, you can enable AirWave to collect Traffic Analysis data from the controller by setting this to Yes. When enabled, the **Home > Traffic Anaylsis** dashboard is available in the WebUI.
Traffic Analysis Storage Allocated (GiB)	50	If Traffic Analysis Data Collection is enabled, you can specify the amount of storage to allocate.
Enable UCC Data Collection	Yes	Enables controllers to send UCC data to AirWave. For this feature to work, 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.

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

Setting	Default	Description
Prefer AMON vs SNMP Polling	Yes	**Prefer AMON** is a configuration setting which causes 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. **NOTE:** • Auditing needs to have been successful at least once to allow AirWave to calculate the proper BSSIDs per radio. • When **Prefer AMON** is enabled, the controller must be configured to send AMON to AirWave by issuing the **controller-amon bssid-tunnel-stats** command from the command-line interface of the standalone controller or managed device (not mobility master). • To view bandwidth usage data on a standalone controller or managed device, you must set **Prefer AMON vs SNMP Polling** to **No** and also set the **Enable AMON Collection** setting to **No**. For more information, see "Enable AMON data collection" on page 33. • The network path from the controller to the 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 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 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
Configure Activate Credentials	No	When you enable this option, you can configure the username and password for the Activate user. **NOTE:** The Activate user needs to be created beforehand at: Aruba Activate
Disable TLS 1.0 and 1.1	Yes	This option is set to Yes by default. In order for Aruba switches to automatically check-in to AirWave by ZTP, you must change this option to No. If you select No, you must restart AMP.
Number of Reports to Execute in Parallel (1-10)	3	Make your reports run faster by setting a limit on how many reports can run at the same time.
AES Encryption key for Credentials		Authentication key used with the AES authentication protocol.

Performance Settings

Locate the **Performance** section. Performance tuning is unlikely to be necessary for many AirWave deployments, and likely provides the most improvements for customers with extremely large Pro or Enterprise installations. Please contact Aruba support if you think you might need to change any of these settings. Table 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 AirWave to process more data per second, but it can take resources away from other AirWave processes. Contact Aruba support if you think you might need to increase this setting for your network. Also note that the value range varies based on the number of available process cores.
Maximum number of configuration processes	5	Increases the number of processes that are pushing configurations to your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Aruba support if you think you might need to increase this setting for your network.
Maximum number of audit processes	3	Increases the number of processes that audit configurations for your devices, as an option. The optimal setting for your network depends on the resources available, especially RAM. Contact Aruba support if you are considering increasing this setting for your network.
SNMP Fetcher Count (2-6)	2	Specify the number of SNMPv2 fetchers.
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, AirWave fetches SNMP data more slowly, potentially reducing device CPU load. We recommend enabling this global setting only if your network contains a majority of much older legacy controllers (800, 2400, 5000, or controllers that use Supervisor Module II). If your network mainly uses newer controllers, we strongly recommend disabling 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.

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

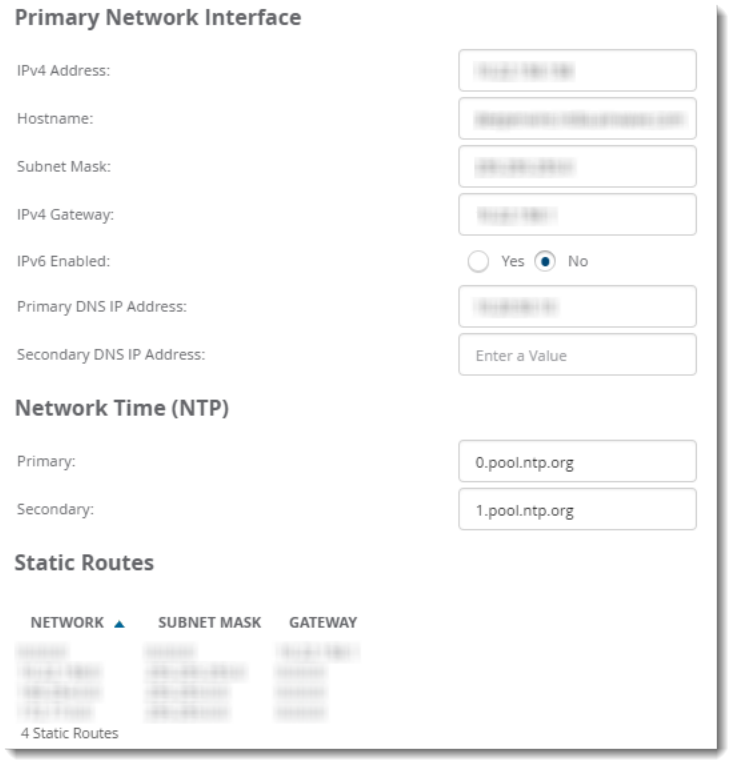
Setting	Default	Description
RAPIDS Processing Priority	Low	Defines the processing and system resource priority for RAPIDS in relation to AirWave as a whole. When AirWave is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (such as client connections and bandwidth usage) is not adversely impacted. The default priority is **Low**. You can also tune your system performance by changing group poll periods. If you select **Custom** for the priority, then also specify the RAPIDS custom process limit.
RAPIDS custom process limit (1-16)	1 when **Custom** is specified for the RAPIDS Processing Priority.	Sets the maximum number of monitoring process assigned to RAPIDS work. Note that this option is only available if **Custom** is specified for the RAPIDS Processing Priority.

Defining Network Settings

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

Figure 3 illustrates the contents of the **AMP Setup > Network** page when setting up an IPv4 or IPv6 interface. Note that you must enter an IPv4 address into the I**Pv4 address** field even if the AirWave server will use IPv6 as the primary interface, as this IPv4 address field is mandatory. For information, see "Primary Network Interface Settings" on page 37.

Figure 3: *Network Page*



Specify the network configuration options described in the sections that follow to define the 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.

Refer to the following topics for configuration information:

- "Primary Network Interface Settings" on page 37
- "Secondary Network Interface Settings" on page 38
- "Network Time Protocol (NTP) Settings" on page 38
- "Static Routes" on page 39

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 AirWave network interface. **NOTE:** This field is required, even if the primary interface uses an IPv6 address. This address must be a static IP address.
Hostname	None	Sets the DNS name assigned to the AirWave server.
Subnet Mask	None	Sets the subnet mask for the primary network interface.

Table 15: *Primary Network Interface Fields and Default Values (Continued)*

Setting	Default	Description
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 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 AirWave secondary network. **NOTE:** This address must be a static IP address. 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 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 AirWave server, not on individual access points.

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between AirWave and the NTP servers creates an entry in the event log. Table 17 describes the settings and default values in more detail. For more information on ensuring that 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.

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

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

Creating AirWave Users

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 AirWave.

NOTE

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

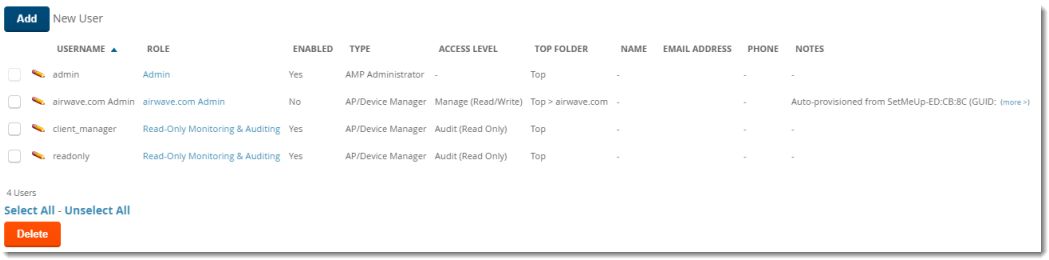
The user role defines the user type, access level, and the top folder for that user. User roles are defined on the **AMP Setup > Roles** page. Refer to the previous procedure in this chapter for additional information, "Creating AirWave User Roles" on page 41.

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

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

1. Go to the **AMP Setup > Users** page. This page displays all users currently configured in AirWave, as shown in Figure 4.

Figure 4: *AMP Setup > Users Page*

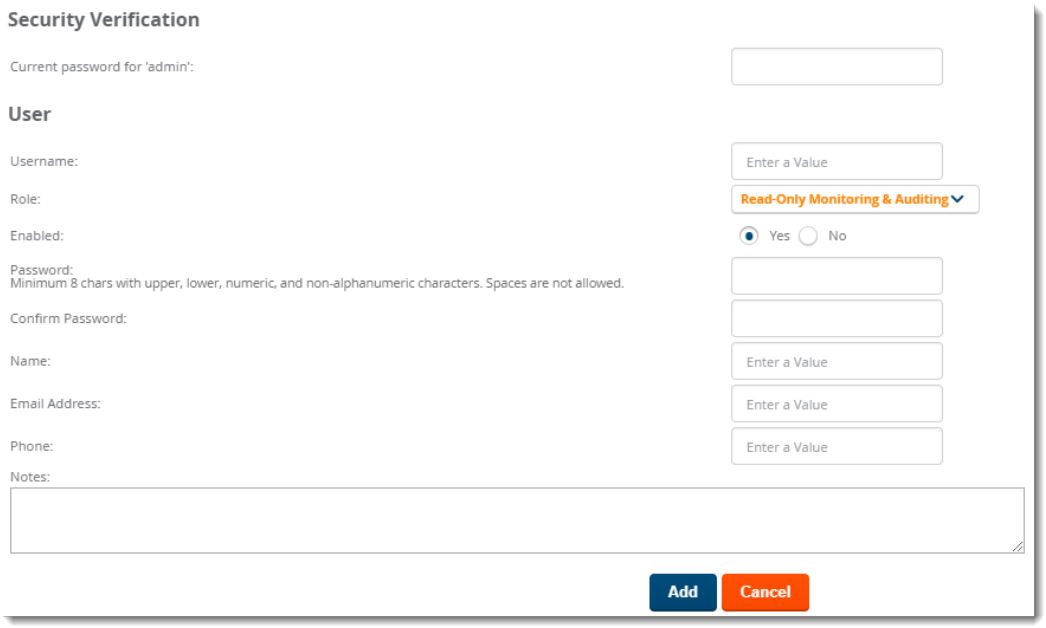


2. Select **Add** to create a new user, select the pencil icon to edit an existing user, or select a user and select **Delete** to remove that user from AirWave. When you select **Add** or the edit icon, the **Add User** page appears, illustrated in Figure 5.

NOTE

Current users cannot change their own role. The **Role** drop-down field is disabled to prevent this.

Figure 5: *AMP Setup > Users > Add/Edit User Page*



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

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 AirWave. This user name is displayed in 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. AirWave strengthens user passwords with SHA512 encryption. **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.

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

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

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

Configuring AirWave User Roles

The **AMP Setup > Roles** page defines the viewable devices, the operations that can be performed on devices, and general 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 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.

Refer to the following additional topics:

- "User Roles and VisualRF" on page 41
- "Creating AirWave User Roles" on page 41

User Roles and VisualRF

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

In **VisualRF > Setup > Server Settings**, 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 AirWave, VisualRF must be restarted for the new user to be enabled.

Creating AirWave User Roles

Roles define the capabilities a user has access to and the privileges and views available for device groups and devices in AirWave. The available configuration options differ for each role type.

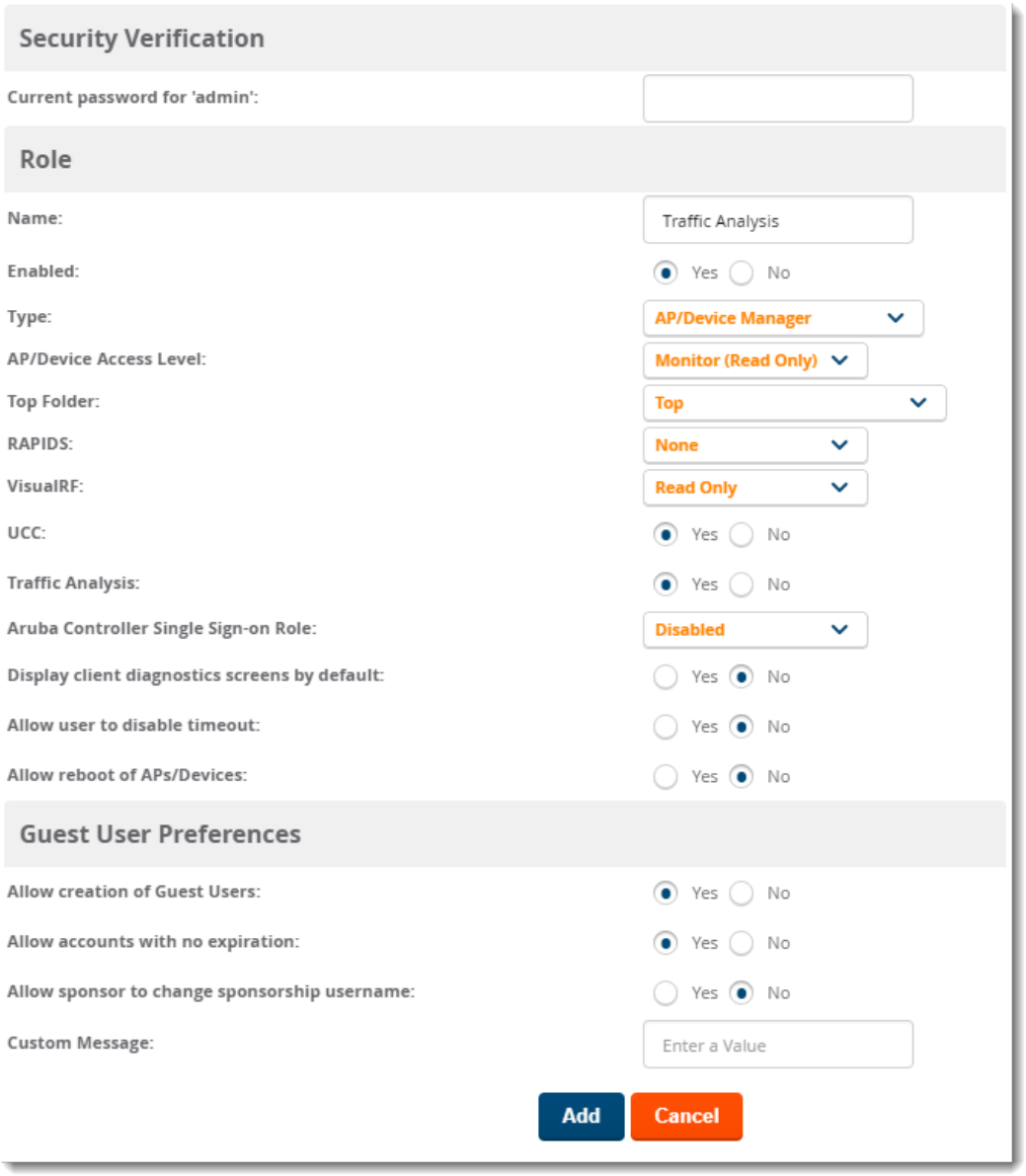
Most users will see two sections on this page: **Role** and **Guest User Preferences**. The **Guest User Preferences** section appears only if **Guest User Configuration** is enabled in **AMP Setup > General**.

If you want to create a user role, log in to AirWave as admin and follow these steps:

1. Go to the **AMP Setup** > **Roles** and click **Add**.

2. Enter a name for the user role, select options, and click **Add**. Figure 6 shows a role named Traffic Analysis being created.

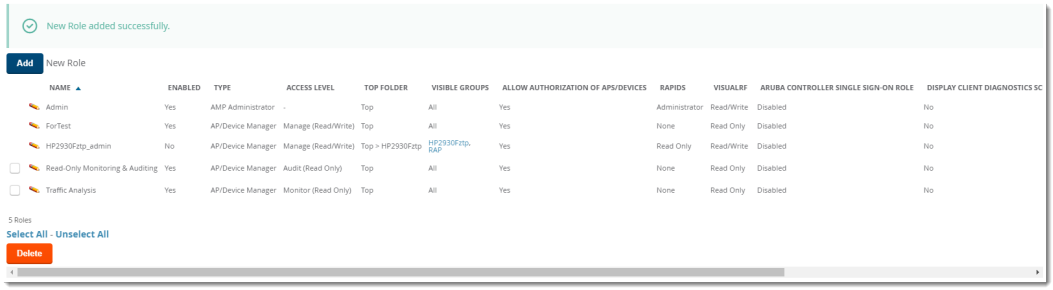
Figure 6: *Adding a Non-Admin Role Named Traffic Analysis*



3. Enter additional settings on this page.

Figure 7 shows the newly created Traffic Analysis Admin role in the Role page.

Figure 7: *Newly Created Traffic Analysis Admin Role*



AMP Administrator Role

The following table describes the available settings and default values for the AMP Administrator role.

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

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

Table 20: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for Device Manager Role*

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

Table 20: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for Device Manager Role (Continued)*

Setting	Default	Description
Type	Device Manager	Defines the type of role. **Device Manager**—Provides access to a limited number of devices and groups based on the Top folder and varying levels of control based on the Access Level.
Access Level	Monitor (Read Only)	Defines the privileges the role has over the viewable device. AirWave supports three privilege levels, as follows: • **Manage (Read/Write)**—Provides the capability to modify, remove, and view information for devices and groups. Selecting this option causes a new field, **Allow authorization of Devices**, to appear on the page, and is enabled by default. • **Audit (Read Only)**—Provides the capability to view devices and groups and the **Device Configuration** page, which may contain sensitive information like AP passwords. • **Monitor (Read Only)**—Provides the capability to view devices and groups and VisualRF.
Top Folder	Top	Defines the highest viewable folder for the role. The role is able to view all devices and groups contained by the specified top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** AirWave enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support *a subset of accounts or sites* within a single AirWave deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow Authorization of Devices	Yes	**NOTE:** This option is only available when the **AP/Device Access Level** is specified as **Manage (Read/Write)**.
RAPIDS	None	Sets the RAPIDS privileges. This field specifies the RAPIDS privileges for the user role and includes these options: • **None**— Cannot view the RAPIDS tab or any rogue devices. • **Read Only**—The user can view the RAPIDS pages but cannot make any changes to rogue devices or perform OS scans. • **Read/Write**—The user may edit individual rogues, classification, threat levels and notes, and perform OS scans. • **Administrator**—Has the same privileges as the Read/Write user, but can also set up RAPIDS rules, override scores and is the only user who can access the **RAPIDS > Setup** page.
VisualRF	Read Only	Sets the VisualRF privileges, which are set separately from the Devices: • **Read Only**—The user can view the VisualRF pages but cannot make any changes to floor plans. • **Read/Write**—The user may edit individual floor plans, buildings, and campuses.

Table 20: *AMP Setup > Roles > Add/Edit Roles Fields and Default Values for Device Manager Role (Continued)*

Setting	Default	Description
UCC	Yes	Permits access to UCC views and tables. Monitoring and managing privileges are set at the device level.
Traffic Analysis	Yes	Permits access to Traffic Analysis views and tables. Monitoring and managing privileges are set at the AP/Device level.
Aruba Controller Single Sign-On Role	Disabled	If enabled, the user has read-only or root access to Aruba controller UIs from quick links without having to enter credentials for the controller.
Display Client Diagnostics Screens By Default	No	Sets the role to support helpdesk users with parameters that are specific to the needs of helpdesk personnel supporting users on a wireless network.
Allow User to Disable Timeout	No	Whether a user can disable AirWave's timeout feature.
Allow Reboot of Devices	No	Allows user to reboot devices in AirWave.
Allow Creation of Guest Users	Yes	If this option is enabled, users with an assigned role of Monitoring or Audit can be given access to guest user account creation along with the option to allow a sponsor to change its user name. **NOTE:** This option is not available if the **AP/Device Access Level** is specified as **Manage (Read/Write)**.
Allow Accounts With No Expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow Sponsor to Change Sponsorship User Name	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

Guest Access Sponsor Role

The following table describes the available settings and default values for the Guest Access Sponsor role.

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

Setting	Default	Description
Name	None	Sets the administrator-definable string that names the role. The role name should indicate the devices and groups that are viewable, as well as the privileges granted to that role.
Enabled	Yes	Disables or enables the role. Disabling a role prevents all users of that role from logging in to AirWave.
Type	AP/Device Manager	Defines the type of role. **Guest Access Sponsor**—Limited-functionality role to allow helpdesk or reception desk staff to grant wireless access to temporary personnel. This role only has access to the defined top folder.
Top Folder	Top	Defines the Top viewable folder for the role. The role is able to view all devices and groups contained by the Top folder. The top folder and its subfolders must contain all of the devices in any of the groups it can view. **NOTE:** AirWave enables user roles to be created with access to folders within multiple branches of the overall hierarchy. This feature assists non-administrator users who support *a subset of accounts or sites* within a single AirWave deployment, such as help desk or IT staff. User roles can be restricted to multiple folders within the overall hierarchy, even if they do not share the same top-level folder. Non-administrator users are only able to see data and users for devices within their assigned subset of folders.
Allow user to disable timeout	No	Whether a user can disable AirWave's timeout feature.
Allow accounts with no expiration	Yes	Specifies whether to allow accounts that have no expiration set. If this is set to **No**, then enter the amount of time that can elapse before the access expires.
Allow sponsor to change sponsorship user name	No	Specifies whether a sponsor can change the sponsorship user name.
Custom Message	none	A custom message can also be included.

Configuring the User Login and Authentication

AirWave uses session-based authentication with a configurable login message and idle timeout. As an option, you can set AirWave to use an external user database to simplify password management for AirWave administrators and users.

This section contains the following procedures to be followed in **AMP Setup > Authentication**:

- "Configuring the User Login" on page 47
- "Configuring Whitelists" on page 47
- "Setting Up Single Sign-On" on page 48

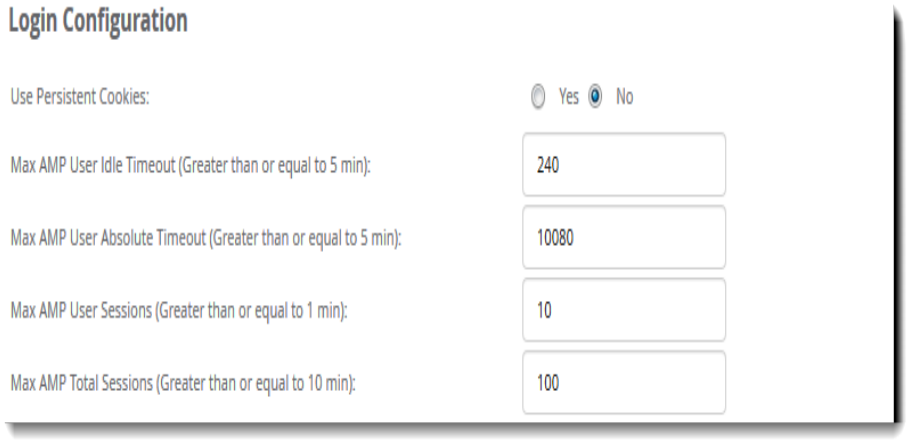
Configuring the User Login

Follow these steps to configure the login banner message, idle timeout, and persistent cookies which are session-based:

To configure user login:

1. Navigate to **AMP Setup > Authentication > Login Configuration**.
2. To clear information such as user logins, select **No** for the "Use Persistent Cookies" option.
3. Enter the length of time that passes before AirWave ends an idle user session. 5 minutes is the lowest idle setting.

Figure 8: *Example Settings for the Login Configuration Page*



4. In the **Login Message** and **Click Through Agreement** fields, type the login banner message and login agreement message that will display before the user logs in to AirWave, requiring the user to accept the terms of usage before granting full access to the WebUI.
5. Click **Save** at the bottom of the page.

Configuring Whitelists

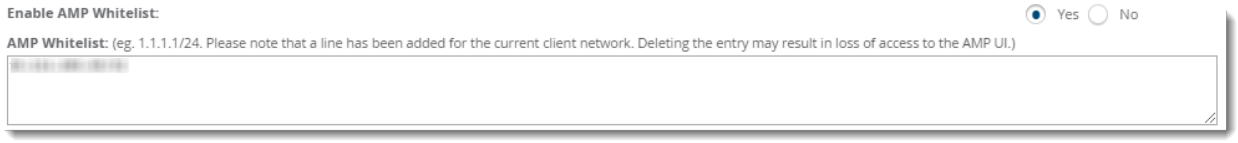
By adding subnets to a whitelist, you can limit AirWave access to users on a list of trusted subnets.

Do not delete the current client network from the AirWave whitelist, or you might lose access to the AirWave WebUI.

To configure the whitelist:

1. Navigate to AMP Setup > Authentication.
2. In the Login Configuration section, select **Yes** for the "Enable AMP Whitelist" option. When you enable this functionality, AirWave displays the whitelist with the current client network as the first entry.

Figure 9: *Enabling Whitelists*



3. To enter additional subnets, add the additional subnets on the same line, separated by commas. (For example, 192.168.0.13/32,172.16.0.0/24)
4. Scroll down the page, then click **Save**.

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 AirWave controllers. This allows users to log in to AirWave and use the IP Address or Quick Links hypertext links across 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 **Devices > Monitor** page in the **Device Info** section, and on device list pages.

Perform the following steps to enable this feature for this 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 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.

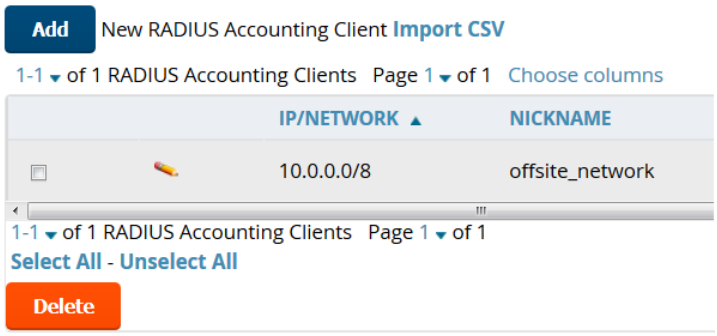
Integrating a RADIUS Accounting Server

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 AirWave server. The only recommended user is the backup admin, in case the RADIUS server goes down.

Optionally, you can configure RADIUS server accounting on **AMP Setup > RADIUS Accounting**. This capability is not required for basic AirWave operation, but can increase the user-friendliness of AirWave administration in large networks. Figure 10 illustrates the settings of this optional configuration interface.

Perform the following steps and configurations to enable AirWave to receive accounting records from a separate RADIUS server. Figure 10 illustrates the display of RADIUS accounting clients already configured.

Figure 10: *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 22.

Table 22: *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 AirWave and the RADIUS authentication server.

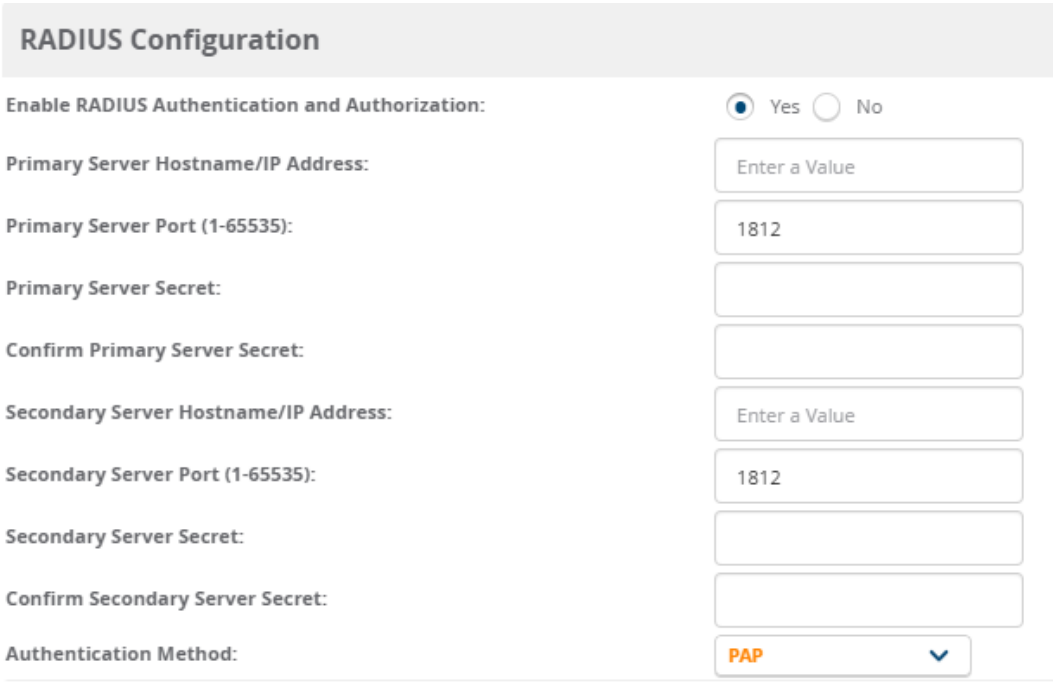
2. Click Add to save your settings.

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 11 illustrates this page.

Figure 11: *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 23.

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

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

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

Field	Default	Description
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 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 AirWave 8.2.**3: R*ead-Only Monitoring **and** Auditing* If you used the **Read-Only Monitoring & Auditing** user role prior to upgrading to 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 AirWave.

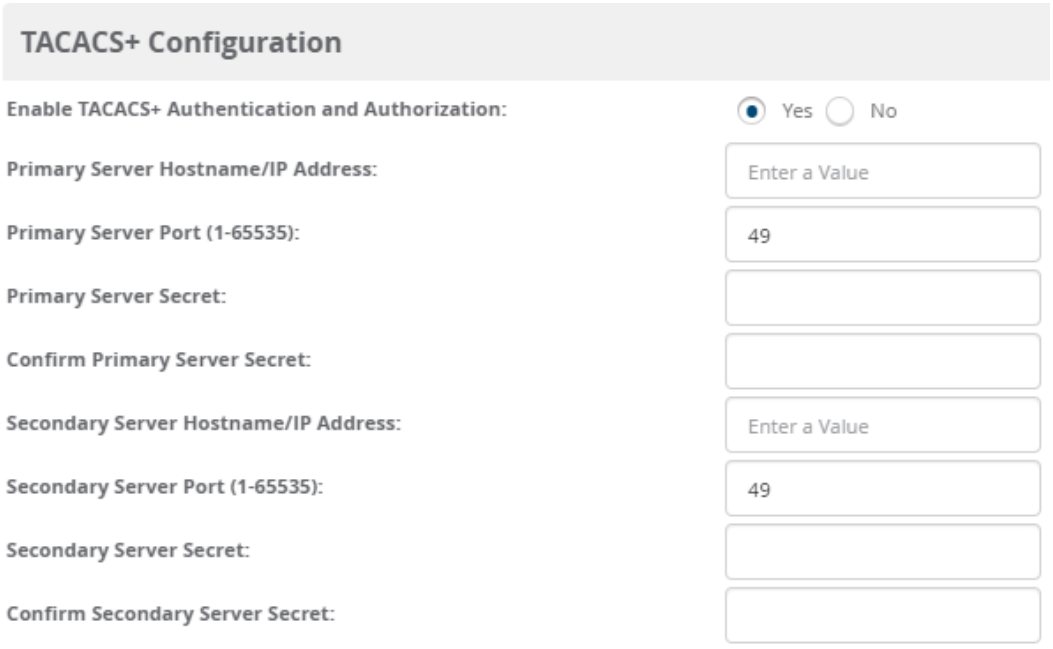
3. Select **Save** to retain these configurations, and continue with additional steps in the next procedure.

Configuring TACACS+ Authentication

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

1. Go to the **AMP Setup > Authentication** page. This page displays current status of TACACS+. Figure 12 illustrates this page when neither TACACS+, LDAP, nor RADIUS authentication is enabled in AirWave.

Figure 12: *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 24.

Table 24: *AMP Setup > Authentication Fields and Default Values for TACACS+ Authentication*

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

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

Configuring Cisco ACS to Work with AirWave

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

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 AirWave server. The only recommended user is the backup administrator, in the event that the TACACS+ server goes down.

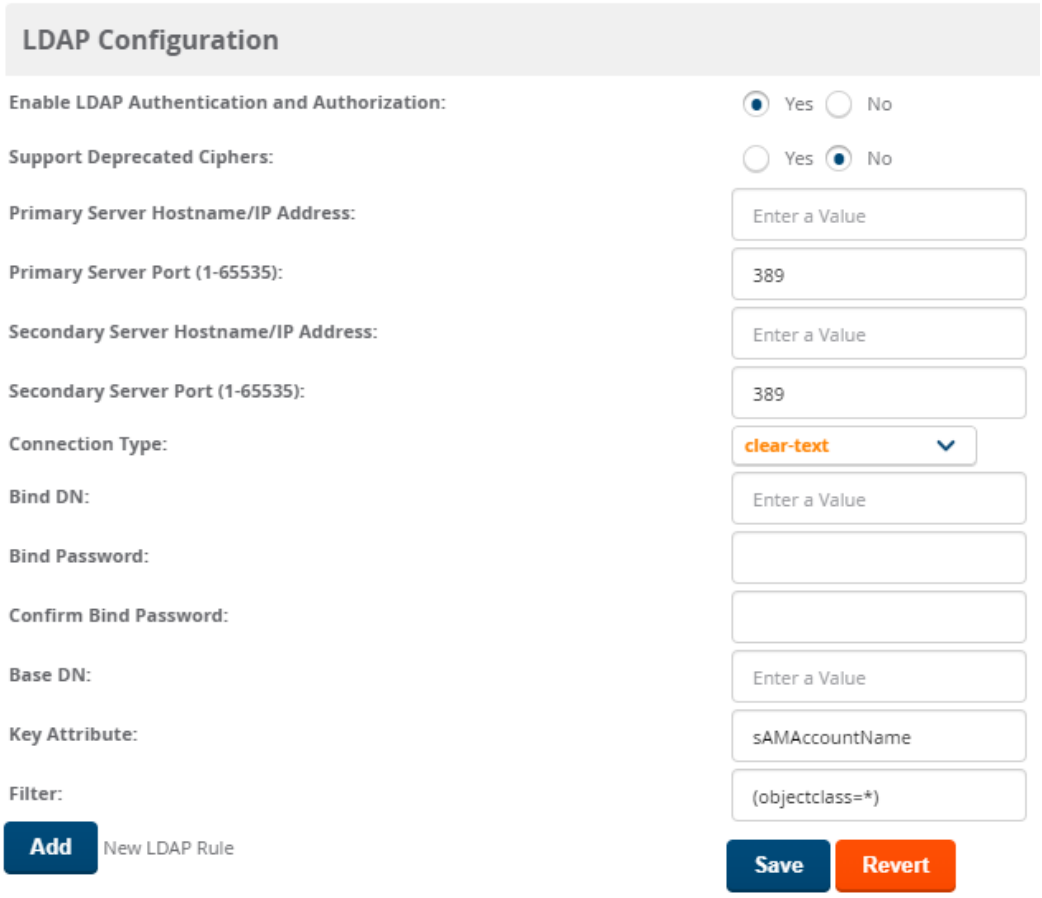
Configuring LDAP Authentication and Authorization

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 13 illustrates this page.

Figure 13: *AMP Setup > Authentication Page Illustration for LDAP*



3. Complete the fields described in Table 25.

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

Field	Default	Description
Support Deprecated Ciphers	Disabled	By default, AirWave supports the following strong ciphers. • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 Enable this **Support Deprecated Ciphers** option to allow AirWave to also use following legacy ciphers: • AES128-SHA • AES256-SHA • DES-CBC3-SHA • DHE-DSS-AES128-SHA • DHE-DSS-AES256-SHA • EDH-DSS-DES-CBC3-SHA • EDH-RSA-DES-CBC3-SHA • KRB5-DES-CBC3-MD5 • KRB5-DES-CBC3-SHA **NOTE:** AirWave does not recommend using legacy ciphers for an extended length of time.
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 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 25: *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 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 AirWave role. Users who log in to AirWave using this LDAP authentication will be granted permissions based on this role. Refer to Configuring AirWave User Roles for more information about AirWave User Roles.
Filter	(objectclass=*)	This option limits the object classes in which the key,role attributes would be searched.

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

Field	Default	Description
Add New LDAP Rule	none	The LDAP rule parameters are **Position**, **Role Attribute**, **Operation**, **Value**, and **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 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 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.* Aruba support remains available to you for any phase of AirWave configuration.

Enabling AirWave to Manage Your Devices

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

This section contains the following procedures:

- "Configuring Communication Settings for Newly Discovered Devices" on page 56
- "Uploading Firmware and Files" on page 57

Configuring Communication Settings for Newly Discovered Devices

You can configure AirWave to communicate with your devices by defining default shared secrets and SNMP settings. In order for AirWave to configure the devices, community strings and shared secrets must have read-write access.

To modify the credentials for existing devices, go to **Devices > Manage**, or go to **Devices > List** and click **Modify Devices**.

To configure communication settings for newly discovered devices:

1. Go to **Device Setup > Communication** page, then scroll down the page.
2. Enter the following SNMP settings:

- **SNMP Timeout**. The length of time (three to 60 seconds) that AirWave waits for a response from a device after sending the device an SNMP request. The default time is three seconds.
- **SNMP Retries**. The number of times (one to 40) that AirWave polls a device when the device doesn't respond to an SNMP request. Optionally, AirWave uses the number of times set for the device group by the **Missed SNMP Poll Threshold** option. AirWave will classify the device as being down if the device doesn't respond after reaching this number. If an SNMP library has a limit of 20 retries, AirWave will stop at 20. The default is three times.

3. Click **Add**, then enter the following information for the SNMPv3 user:
    - **Username**. User name of the SNMPv3 user, as it is configured on the controller. The SNMP Inform receiver will restart when users are changed or added to the controller.

- **Auth Protocol**. MD5 or SHA. The default setting is SHA.
- **Auth Passphrase**. Authentication and privilege protocol passphrase for the SNMPv3 user, as it is configured on the controller. Re-enter the passphrase.
- **Priv Protocol**. The symmetric-key algorithm used to encrypt data, Data Encryption Standard (DES) or Advanced Encryption Standard (AES). The default standard is DES.
- **Priv Protocol Passphrase**. Privilege protocol passphrase for the SNMPv3 user, as it is configured on the controller. Re-enter the passphrase.

4. For the **Telnet/SSH Timeout** option, enter the timeout period (zero to 600 seconds) to apply when performing Telnet and SSH commands. The default timeout is 10 seconds.
5. For the **HTTP Timeout** option, enter the timeout period (three to 120 seconds) used when running an HTTP discovery scan. The default timeout is five seconds.
6. For the **Attempt to ping devices that were unreachable via SNMP** option, select **No** if ICMP is disabled on the network. By default, this option is enabled. When there are more than 100 devices, and many are unreachable by ICMP, the timeouts will impede network performance, and you should turn off this option.
7. For Symbol 4131 and Cisco IOS devices that don't have SNMP initialized, select one of the following options:
   - **Do not modify SNMP settings**. AirWave will not modify any SNMP settings for these devices when you select this option. By default, this option is enabled.
   - **Enable read-write SNMP**. AirWave will manage these devices using SNMP when you select this option. By default, this option is disabled.

Uploading Firmware and Files

AirWave automates firmware distribution to the devices on your network. Once you have downloaded the firmware from the vendor, you can upload the firmware to AirWave for distribution to devices from the **Upload Firmware & Files** page. After you upload the firmware, AirWave lists them in the Firmware Files table on this page.

For more information about specifying firmware versions for devices in a group, see "Specifying the Minimum Firmware Version for Device Groups" on page 128.

Table 26 below itemizes the contents, settings, and default values for the **Upload Firmware & Files** page.

Table 26: *Device Setup > Upload Firmware & Files Fields and Default Values*

Setting	Default	Description
Type	Aruba Networks Controller(any model)	Displays a drop-down list of the primary AP makes and models that AirWave supports with automated firmware distribution.
Owner Role	None	Displays the user role that uploaded the firmware file. This is the role that has access to the file when an upgrade is attempted.
Description	None	Displays a user-configurable text description of the firmware file.
Server Protocol	None	Displays the file transfer protocol by which the firmware file was obtained from the server. This can be FTP, TFTP, HTTP, HTTPS. or SCP.

Table 26: *Device Setup > Upload Firmware & Files Fields and Default Values (Continued)*

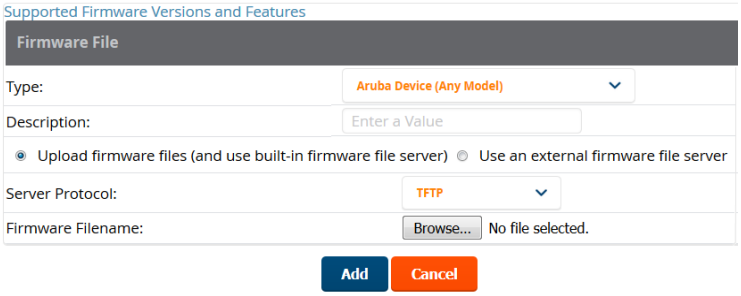
Setting	Default	Description
Use Group File Server	None	If enabled, displays the name of the file server supporting the group.
Firmware Filename	None	Displays the name of the file that was uploaded to AirWave and to be transferred to an AP when the file is used in an upgrade.
Firmware MD5 Checksum	None	Displays the MD5 checksum of the file after it was uploaded to AirWave. The MD5 checksum is used to verify that the file was uploaded to AirWave without issue. The checksum should match the checksum of the file before it was uploaded.
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 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 AirWave. The MD5 checksum is used to verify that the file was uploaded to AirWave without issue. The checksum should match the checksum of the file before it was uploaded.
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 AirWave

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

1. Go to the **Device Setup > Upload Firmware & Files** page.
2. Select **Add** by the **New Firmware File** option. The Add Firmware File page appears. Figure 14 illustrates this page.

Figure 14: *Device Setup > Upload Firmware and Files > Add Page*



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

NOTE

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

4. Enter the appropriate information and select **Add**. The file uploads to 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 **Devices > Manage** pages).
5. You can also import a CSV list of groups and their external TFTP firmware servers. Table 27 itemizes the settings of this page.

Table 27: *Supported Firmware Versions and Features Fields and Default Values*

Setting	Default	Description
Type	Aruba Networks controller	Indicates the firmware file is used with the specified type. With selection of some types, particularly Cisco controllers, you can specify the boot software version.
Firmware Version	None	Provides a user-configurable field to specify the firmware version number. This open appears if **Use an external firmware file server** is enabled.
Description	None	Provides a user-configurable text description of the firmware file.
Upload firmware files (and use built-in firmware)	Enabled	Allows you to select a firmware from your local machine and upload it via TFTP or FTP.
Use an external firmware file server	N/A	You can also choose to assign the external TFTP server on a per-group basis. If you select this option, you must enter the IP address on the **Groups > Firmware** page. Complete the **Firmware File Server IP Address** field.
Server Protocol	TFTP	Specify whether to use a built-in TFTP server or FTP, HTTP, or HTTPS to upload a firmware file. TFTP is recommended. If you select FTP, AirWave uses an anonymous user for file upload.

Table 27: *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 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.

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

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

Deleting FirmWare Files

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

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

Adding Web Auth Bundles

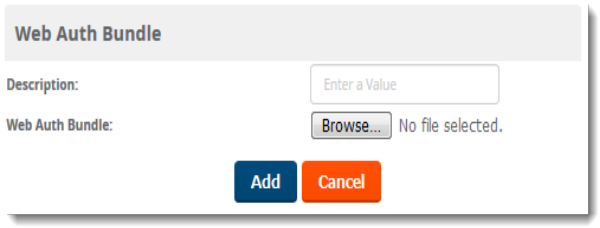
Web authentication bundles are configuration files that support Cisco WLC wireless LAN controllers. This procedure requires that you have local or network access to a Web Auth configuration file for Cisco WLC devices.

To add or edit a Web Authentication Bundle:

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 authentication bundles that are currently configured in AirWave.

3. Select **Add** to create a new bundle (see Figure 15), or select the pencil icon next to an existing bundle to edit. You may also delete a bundle by selecting that bundle with the checkbox, and selecting **Delete**.

Figure 15: *Adding a Web Auth Bundle*



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

For additional information about using web authentication bundles with Cisco WLC controllers, refer to the Wireless LAN controller Web Authentication Configuration Example, Document ID: 69340 on Cisco's Web site.

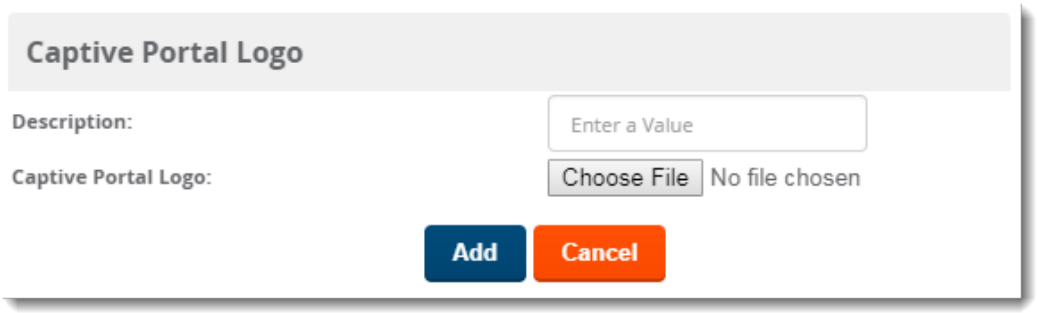
Adding a New Captive Portal Logo

If you want to use a company logo for a guest account that uses a captive portal for network authentication, you upload the logo to AirWave and then set a group of devices to use the captive portal logo.

To upload a company logo image file:

1. Click **Add** at the bottom of the Upload Firmware & Files page next to New Captive Portal Logo.

Figure 16: *Adding a Captive Portal Logo*



2. Enter a logo description.
3. Click **Choose File** to select the image file, then click **Open**.
4. Click **Add**. AirWave displays the newly added image file in the Firmware Files table.

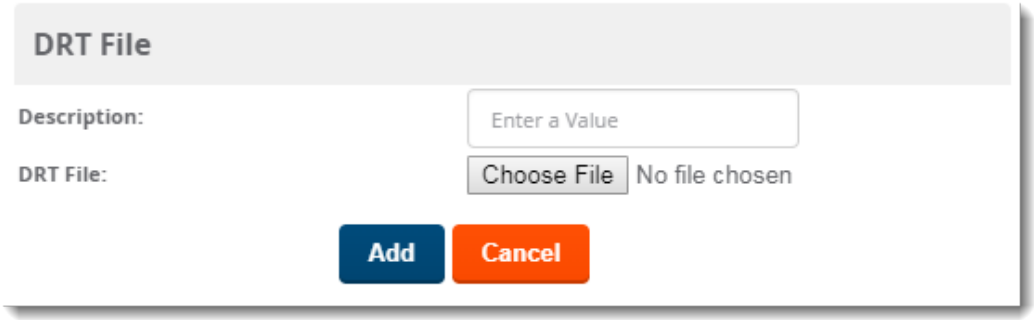
Adding a New DRT File

You can use the downloadable regulatory table (DRT) to update country domain options without upgrading the ArubaOS software version on an AP.

To add a DRT file to AirWave:

1. Click **Add** at the bottom of the Upload Firmware & Files page next to New DRT File.

Figure 17: *Adding a DRT File*



2. Enter a DRT file description.
3. Click **Choose File** to select the DRT file, then click **Open**.
4. Click **Add**. AirWave displays the newly added DRT file in the Firmware Files table.

Managing Certificates

After installing AirWave, you can install a new SSL certificate, or generate a CSR to install a signed certificate from the AMP CLI. Some certificate management tasks can only be done using the AMP CLI while others can be done using the WebUI, and the tasks are described in the following topics:

Uploading Certificates

AirWave can help you manage your certificates when you upload them to the AirWave server. AirWave verifies basic certificate information before accepting the certificate and pushing it to a device.

WebUI

You can upload the following certificates from the WebUI:

- CRL
- Intermediate Certificate Authority (CA)
- Online Certificate Status Protocol (OCSP) Responder
- OCSP Signer
- Public certificates
- Server certificates
- Trusted CA certificates
- Captive Portal (CP) certificates

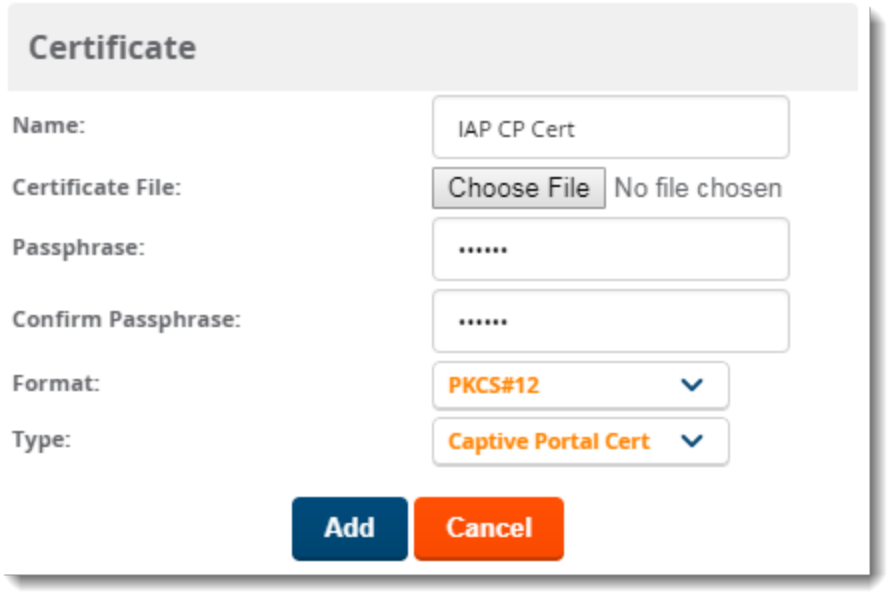
After you upload a certificate to AirWave, the certificate file becomes available on additional pages where you can select certificate files, including **AMP Setup > Authentication and Groups > Basic > Certificates**. For self-signed certificates, refer to "Installing Signed Certificates" on page 67.

For example, Figure 18 shows a certificate named IAP CP Cert being added. You can later choose this certificate for an IAP by navigating to the **Group > Basic** page for the device group that contains IAPs.

To add a certificate:

1. Go to the **Device Setup > Certificates**, then click **Add**.

Figure 18: *Adding a Captive Portal Certificate*



2. Enter a name for the certificate.
3. Click **Choose File** to find your local copy of the certificate.
4. Enter the passphrase, if any, and renter the passphrase.
5. Select the format that matches the certificate file.
6. Select the certificate type.
7. Click **Add**.

AMP CLI

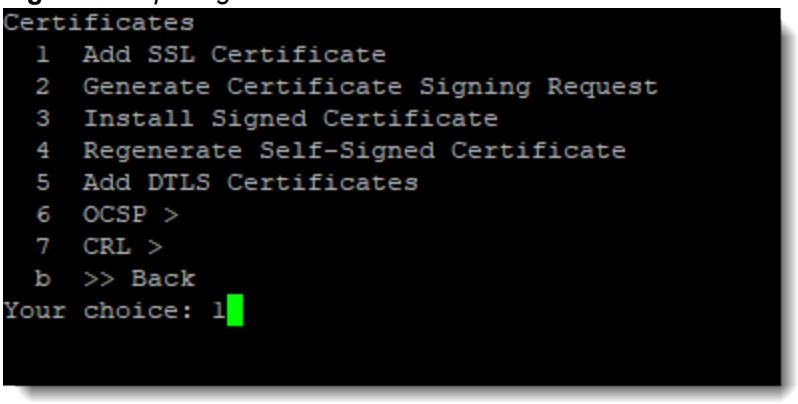
1. From the AMP CLI, enter **3-4** to open the **Configuration > Certificates** menu.

Figure 19: *Opening the Certificates Menu*

```
Certificates
  1  Add SSL Certificate
  2  Generate Certificate Signing Request
  3  Install Signed Certificate
  4  Regenerate Self-Signed Certificate
  5  Add DTLS Certificates
  6  OCSP >
  7  CRL >
  b  >> Back
Your choice:
```

2. Enter **1** to open the **Add SSL Certificate** menu.

Figure 20: *Opening the Add SSL Certificate Menu*



3. Follow the prompt to install the SSL certificate on your AirWave server. The signed certificate should be in PKCS12 format with a *.pfx or *.p12 file extension.

Changing the SSL Certificate for Aruba Instant

In order to use certificate-based authentication, you must upload a certificate issued from a supported certificate authority (CA) to the AMP server or else the SSL handshake will fail. You must also configure the AMP IP address on the Instant AP with a domain name and not an IP address. For more information about security methods for Aruba Instant, see "Aruba Instant Settings" on page 23.

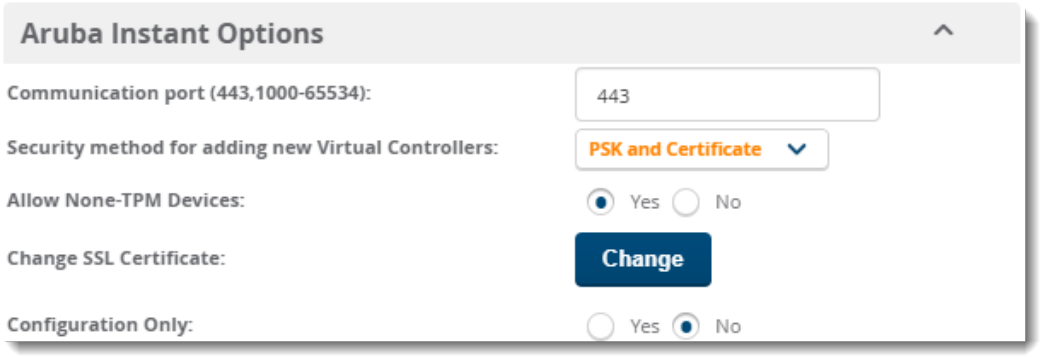
AirWave supports the following trusted CAs:

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

To change the certificate for Aruba Instant device authentication:

1. 1. Go to **AMP Setup > General**, then scroll down to **Aruba Instant Options**.
2. Select **PSK and Certificate** or **Certificate only**.

Figure 21: *Selecting a Certificate Authentication Option*



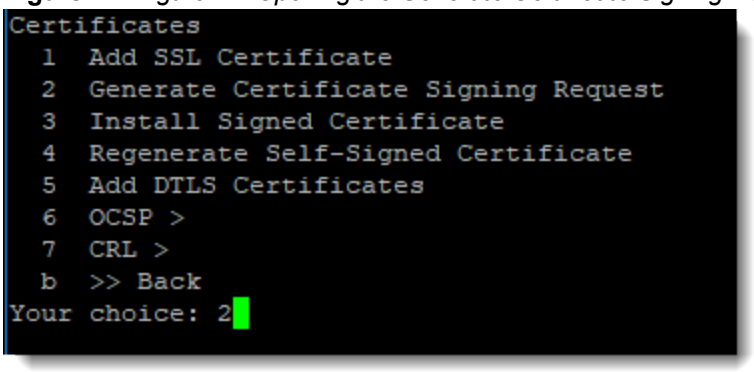
3. Click **Change** to find the certificate file on the AMP server. The certificate should be in PEM format and with a private key.
4. Click **Upload**.

Generating Certificate Signing Requests (CSRs)

To generate the CSR to request a certificate from AirWave:

1. From the AMP CLI, enter **3-4-2** to open the **Configuration > Certificates > Generate Certificate Signing Request** menu.
2. Enter **2** to generate a CSR.

Figure 22: *Figure 22: Opening the Generate Certificate Signing Request Menu*



3. Follow the prompts to enter the data associated with the organization:
   a. 2-letter country code
   b. State or province
   c. Locality or city
   d. Organization or company
   e. Organization unit or department
   f. Common name or server host name
   g. Email address
   h. Fully qualified DNS name
   i. IP addresses

Figure 23: *Entering Certificate Data*

4. Enter **a** to accept the changes and save the data.

Setting Up Certificate Authentication

On the **AMP Setup > Authentication** page, you can specify whether to use two-factor authentication. With two-factor authentication, the AirWave user name and password and a PEM-encoded certificate bundle is required. When using the Smart Card or token, AirWave will prompt you to enter the PIN.

NOTE

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

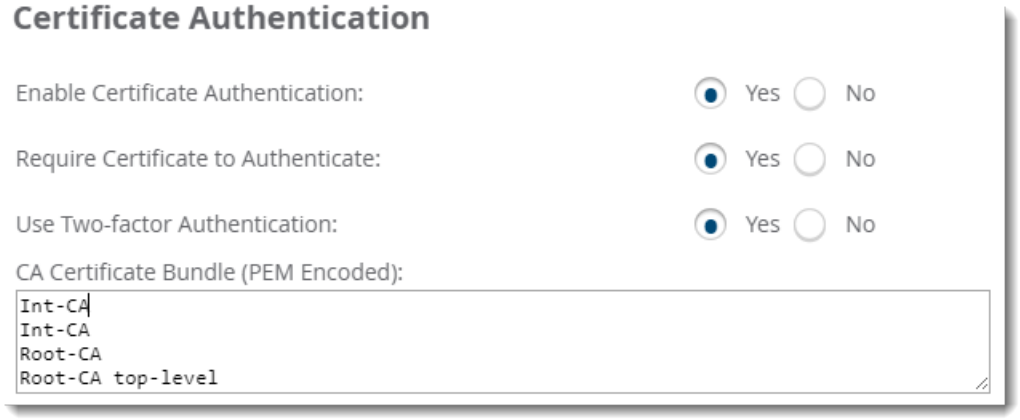
NOTE

When entering the PEM bundle, you must install every member in the certificate chain provided by the SSL vendor in order for smart card or token authentication to work.

To set up certificate authentication:

1. Go to **AMP Setup > Authentication**.
2. Select **Yes** to enable certificate authentication. Once enabled, certificate authentication options will display.
3. Select **Yes** to turn on the **Use Two-factor Authentication** option.
4. Enter your PEM certificate bundle in the text field. For example, in Figure 24, two intermediate certificates are bundled with the two root certificates, one being at the top of the chain.

Figure 24: *Two-Factor Authentication Configuration Example*



5. Scroll to the bottom of the page, then click **Save**.

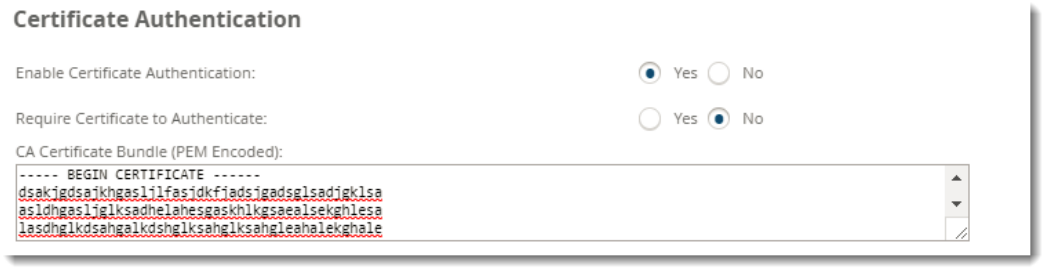
Disabling the Certificate Authentication Requirement

You might want to configure local database authentication, and in order to do so you should turn off the certificate authentication requirement and add your PEM bundle. Although certificate authentication is not required when disabled, certificate authentication, or OCSP validation, will occur for users with certificates.

To disable certificate authentication:

1. From the WebUI, go to **AMP Setup > Authentication**, select **Yes** to enable certificate authentication.
2. For the **Require Certificate Authentication** option, select **No**.
3. Enter your PEM certificate bundle in the text field.

Figure 25: *Entering the PEM Certificate Bundle*



4. Scroll down, then click **Save**.

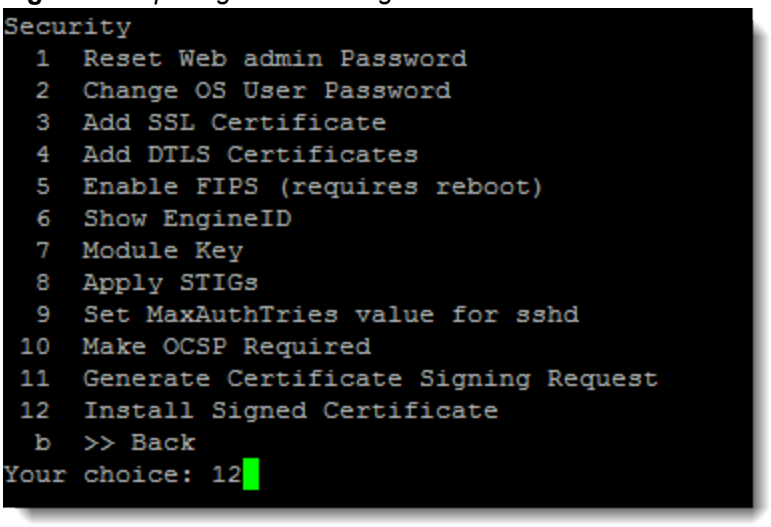
Installing Signed Certificates

Before you install the signed certificate, you must export the CSR created in "Generating Certificate Signing Requests (CSRs) " on page 65 to a third-party certificate authority (CA) and then upload the returned certificate to the AirWave server.

To install the signed certificate:

1. From the AMP CLI, enter **3-4-3** to open the **Configuration > Certificates > Install Signed Certificate** menu.

Figure 26: *Opening the Install Signed Certificate Menu*



2. Follow the prompt to select the certificate, then press **Enter**. The signed certificate should be PEM-encoded with a *.crt file extension.

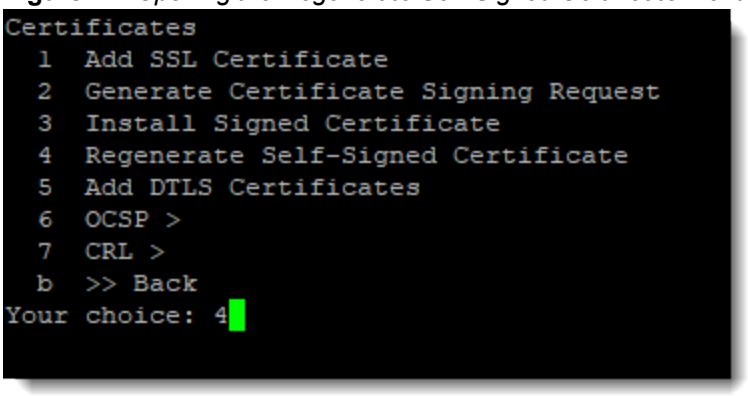
Regenerating Self-Signed Certificates

AirWave automatically generates a self-signed certificate during installation and when the host name is changed from the CLI. If you need to regenerate the self-signed certificate for any reason, you can regenerate the self-signed certificate on AMP using the CLI.

To regenerate the self-signed certificate:

1. From the AMP CLI, enter **3-4-4** to open the **Configuration > Certificates > Regenerate Self-Signed Certificate** menu.

Figure 27: *Opening the Regenerate Self-Signed Certificate Menu*



2. Enter **y** when prompted.

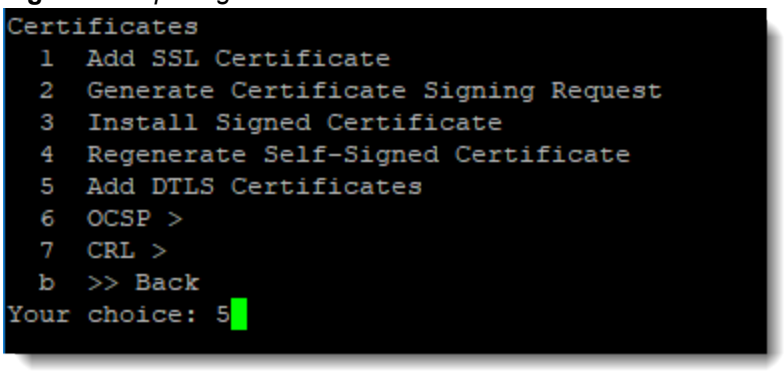
Adding DTLS Certificates

DTLS certificates can be used to encrypt secure AMON traffic on your AMP server.

To install the DTLS certificate:

1. From the AMP CLI, enter **3-4-5** to open the **Configuration > Certificates > Add DTLS Certificate** menu.

Figure 28: *Opening the Add DTLS Certificate Menu*



2. Follow the prompt to select the certificate, then press **Enter**. The signed certificate should be in PKCS12 format with a *.pfx or *.p12 file extension and contain the private key, root certificate, and intermediate certificates.

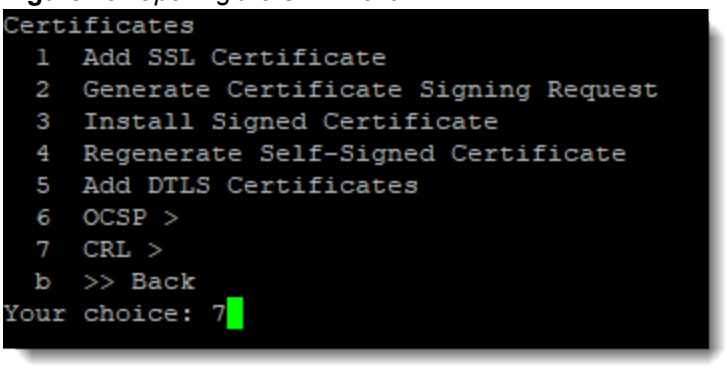
Configuring Certificate Revocation Lists (CRLs)

When you configure a CRL, AirWave checks to see if the certificate sent by the requesting device is revoked. You could also use a CRL to skip the OCSP check when an OCSP server is not accessible to perform certificate validation.

To configure the CRL:

1. From the AMP CLI, enter **3-4-7** to open the **Configuration > Certificates > CRL** menu.

Figure 29: *Opening the CRL Menu*



2. Enter **1** to make CRL required, then follow the prompts to run the function and return to the CRL menu.
3. Enter **2** to configure a CRL distribution URL, then follow the prompt to add the CRL distribution URL.
4. Enter **3** to add a CRL files and follow the prompt to add the file.
5. Enter the password for the AMP server.
6. Click **Update** to save the configuration.

Setting Up Device Types

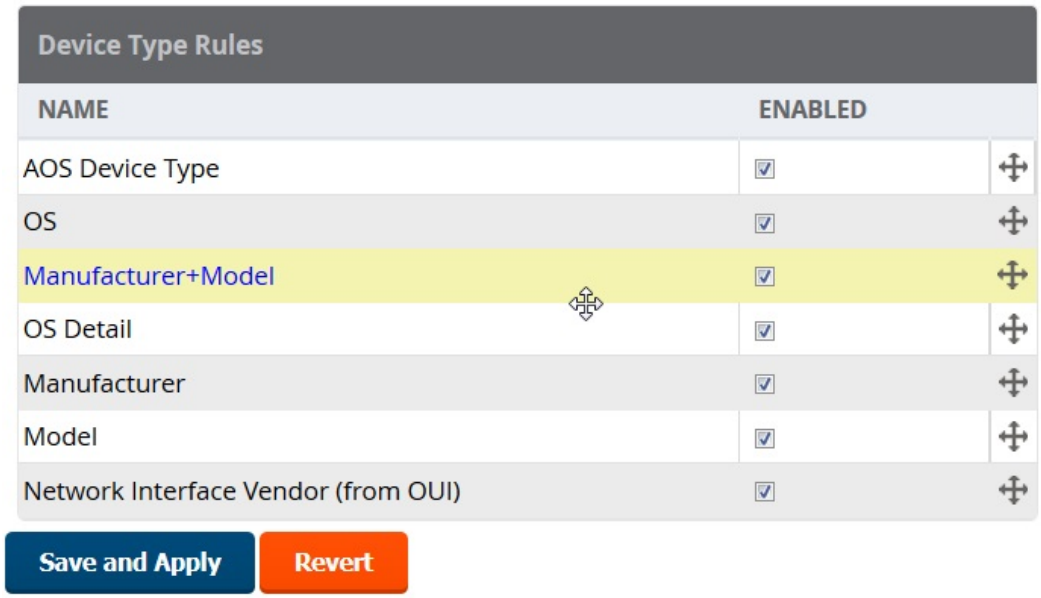
On the **AMP Setup > Device Type Setup** page, you can define how the device types displayed for users on your network is calculated from available data. The first matching property is used. These rules cannot be edited or deleted, but only reordered or enabled.

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 30.

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

Refer to "Monitoring Wired and Wireless Clients" on page 207 for more information on the **Device Type** column that appears in **Clients** list tables.

Figure 30: *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 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 70
- "Initial WLSE Configuration" on page 71
- "Configuring IOS APs for WDS Participation" on page 73
- "Configuring ACS for WDS Authentication" on page 73
- "Configuring Cisco WLSE Rogue Scanning" on page 74

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

Introduction to Cisco WLSE

Cisco WLSE functions as an integral part of the Cisco Structured Wireless-Aware Network (SWAN) architecture, which includes IOS Access Points, a Wireless Domain Service, an Access Control Server, and a WLSE. In order for AirWave to obtain Rogue AP information from the WLSE, all SWAN components must be properly configured. Table 28 describes these components.

Table 28: *Cisco SWAN Architecture Components*

SWAN Component	Requirements
WDS (Wireless Domain Services)	• WDS Name • Primary and backup IP address for WDS devices (IOS AP or WLSM) • WDS Credentials APs within WDS Group **NOTE:** WDS can be either a WLSM or an IOS AP. WLSM (WDS) can control up to 250 access points. AP (WDS) can control up to 30 access points.
WLSE (Wireless LAN Solution Engine)	• IP Address • Login
ACS (Access Control Server)	• IP Address • Login
APs	• APs within WDS Group

Initial WLSE Configuration

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

- "Adding an ACS Server for WLSE" on page 71
- "Enabling Rogue Alerts for Cisco WLSE" on page 71
- "Configuring WLSE to Communicate with APs" on page 71
- "Discovering Devices" on page 72
- "Managing Devices" on page 72
- "Inventory Reporting" on page 72
- "Defining Access" on page 72
- "Grouping" on page 72

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 74.

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.

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

Use these pages to make such configurations:

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

Inventory Reporting

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

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

Defining Access

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

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

Grouping

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

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

Configuring IOS APs for WDS Participation

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

- Primary WDS
- Backup WDS
- WDS Member

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

APs functioning as WDS Master or Primary WDS will no longer show up as Down 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 ACS Servers" on page 75.

Configuring Cisco WLSE Rogue Scanning

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

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

1. To add a Cisco WLSE server to AirWave , navigate to the **AMP Setup > WLSE** page and select **Add**. Complete the fields in this page. Table 29 describes the settings and default values.

Table 29: *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 AirWave uses to communicate with the WLSE server.
Username	None	Defines the user name 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 AirWave. The user needs permission to display faults to discover rogues and inventory API (XML API) to discover manageable APs. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow AirWave to pull the necessary XML APIs.
Password	None	Defines the password 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 AirWave. As derived from a Cisco limitation, only credentials with alphanumeric characters (that have only letters and numbers, not other symbols) allow AirWave to pull the necessary XML APIs.
Poll for AP Discovery; Poll for Rogue Discovery	Yes	Sets the method by which 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 AirWave polls WLSE to gather rogue scanning data.

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

What Next?

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

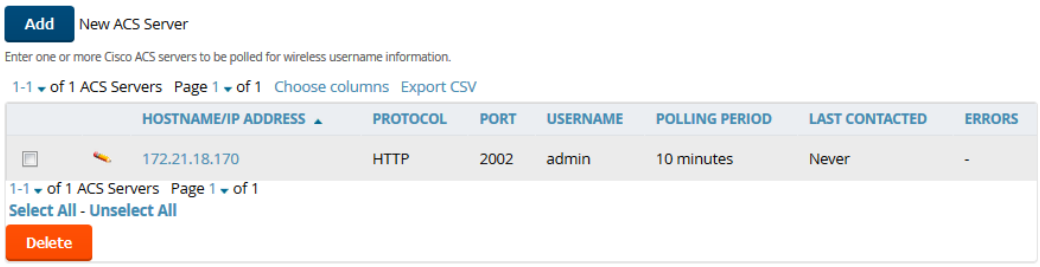
Configuring ACS Servers

This is an optional configuration. The **AMP Setup > ACS** page allows AirWave to poll one or more Cisco ACS servers for wireless user name information. When you specify an ACS server, AirWave gathers information about your wireless users. Refer to "Setting Up Device Types" on page 69 if you want to use your ACS server to manage your AirWave users.

Perform these steps to configure ACS servers:

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

Figure 31: *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 30 describes these fields:

Table 30: *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 AirWave uses when it polls the ACS server.
Port	2002	Sets the port through which AirWave communicates with the ACS. AirWave generally communicates over port 2002.
Username	None	Sets the user name of the account AirWave uses to poll the ACS server.
Password	None	Sets the password of the account AirWave uses to poll the ACS server.
Polling Period	10 min	Launches a drop-down menu that specifies how frequently 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 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. Aruba support remains available to you for any phase of AirWave installation.

Integrating NMS Servers

You can integrate AirWave with Network Management System (NMS) servers. Doing so enables 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 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.

AirWave provides integration with Netcool/OMNIbus and HP ProCurve Manager (PCM). To download the integration files, go to **AMP Setup > NMS**.

PCI Compliance Monitoring

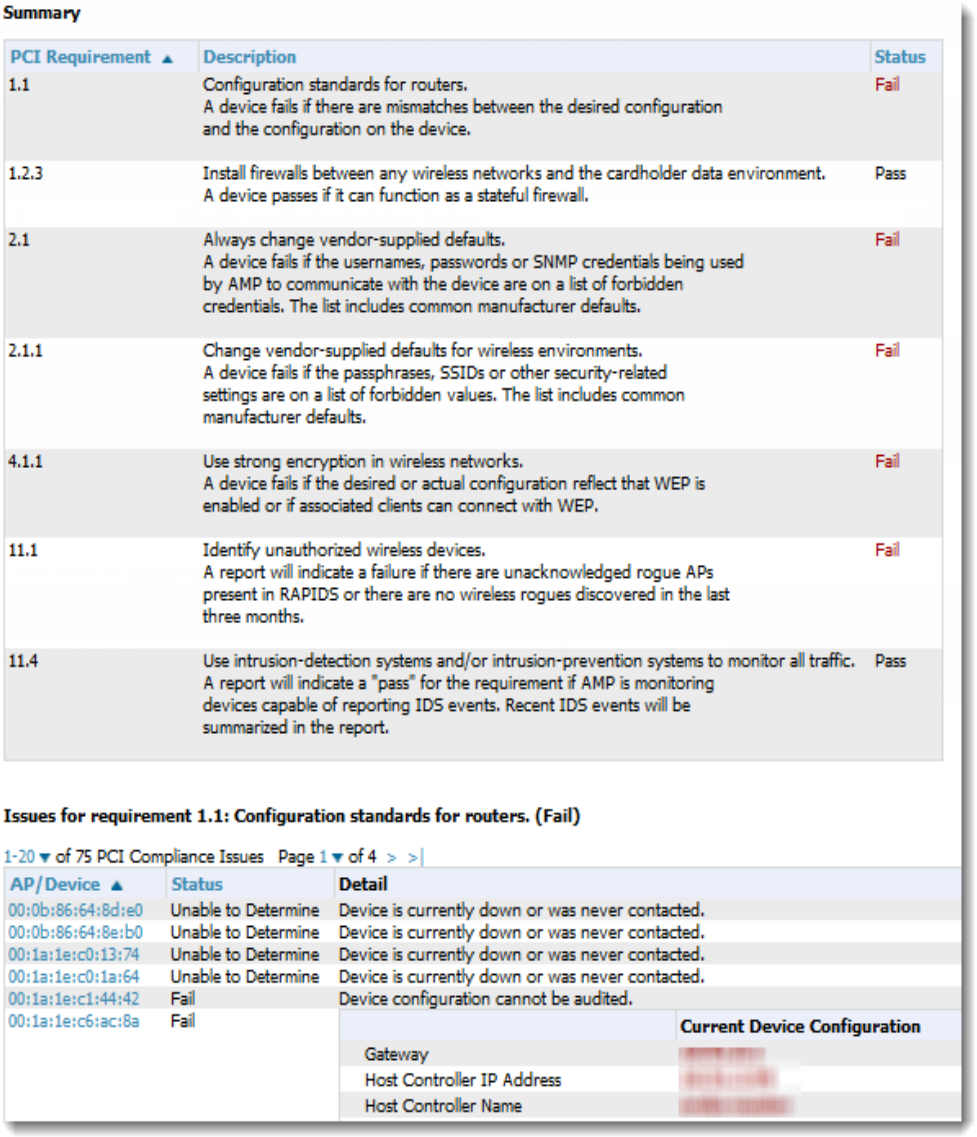
AirWave provides compliance monitoring tools that can help your organization be prepared for a PCI Data Security Standard (DSS) audit. With use of AirWave, your organization can monitor firewalls, network devices, and other services to show PCI compliance.

Check Compliance

The PCI compliance report displays which requirements 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, AirWave provides diagnostic information and recommends actions required to achieve Pass status when sufficient information is available.

You can find the PCI compliance report for a device by navigating to **Devices > List**, hovering the pointer over a device, and clicking **Compliance** from the shortcut menu. If you created a PCI compliance report from the **Reports Definition** page, AirWave displays the report on the **Generated Reports** page when it is available, as shown in Figure 32. For information, see "Viewing Generated Reports" on page 367.

Figure 32: *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 schedule, view, and re-run custom PCI compliance reports. For information about working with reports, see "Creating, Running, and Sending Reports" on page 329.

Enabling PCI Compliance Monitoring

When you enable PCI compliance monitoring, 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 78.

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 329. In addition, you can view the real-time PCI auditing of any given device online. Perform these steps:
   a. Go to the **Devices > List** page.
   b. Select a specific device. The **Monitor** page for that device displays. The **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

AirWave currently supports the PCI 3.0. requirements described in Table 31. When the requirements are disabled, AirWave does not check for PCI compliance or report on status.

AirWave users without RAPIDS visibility will not see the 11.1 PCI requirements in the PCI compliance report.

Table 31: *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 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 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.

Deploying WMS Offload

The 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.
- AirWave WebUI. This graphical user interface (GUI) provides access to the WMS offload feature.

Refer to the *Aruba and AirWave 8.2.4 Best Practices Guide* for additional information, including detailed concepts, configuration procedures, restrictions, ArubaOS infrastructure, and 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 AirWave. WMS master controllers provide this data so that 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 AirWave monitoring:
   a. Disable debugging.
   b. Ensure the AirWave server is a trap receiver host.
   c. Ensure proper traps are enabled.
2. Configure AirWave to optimally monitor the AirWave infrastructure:
   a. Enable WMS offload on the **AMP Setup > General** page.
   b. Configure SNMP communication.
   c. Create a proper policy for monitoring the 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:
   - ArubaOS
   - RF Plan
6. Use RTLS for increasing location accuracy (optional):
   a. Enable RTLS service on the AirWave server.
   b. Enable RTLS on ArubaOS infrastructure.

Integrating External Servers

When you configure AirWave to integrate with external servers, AirWave provides a hyperlink on the **Devices > Monitor** page for the device to launch the external application from a web browser.

To configure an external server:

1. Go to **AMP Setup > External server**.
2. Scroll down the page and locate the external server, then enter the following settings:
   - Juniper Network Director

        - Enter the IP address or hostname of the Juniper Network Director.
    - Brocade Network Advisor
        - Enter the IP address or hostname of the Brocade Network Advisor.
    - HPE Intelligent Management Center (IMC)
        - Enter the IP address or hostname of the IMC server.
        - (Optional) Click the **IMC Protocol** drop down list and select the **HTTPS** or **HTTP** protocol.
        - (Optional) Enter a port number in the **IMC Port** field.
        - Enter the user name for accessing the IMC server, then confirm this password.
    - Aruba NetEdit Network Advisor
        - Enter the IP address or hostname of the NetEdit Network Advisor.
3. Click **Save**.

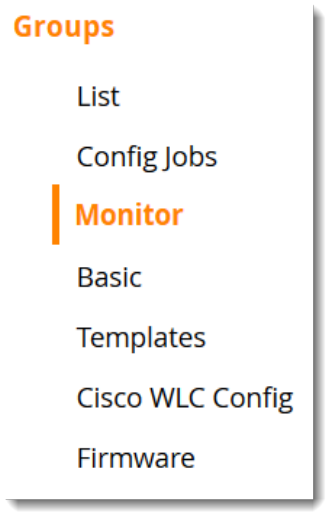
AirWave automates the processes of device configuration and compliance auditing using device groups. A *Group* can include one device to hundreds of devices that share common configuration settings, and you can define groups based on geography, usage or security policies, function, or another variable. Variables include basic settings, security settings, and radio settings.

Navigation Basics

When you select a device group from the Groups List page, the navigation sidebar varies, depending on the default group and type of devices that you added to AirWave. After you create additional device groups, you can change the default group by navigating to **AMP Setup > General** and selecting a group from the Default Group drop-down menu.

Figure 33 shows a navigation sidebar menu that is available when you select a group that contains Cisco WLCs.

Figure 33: *Navigation Sidebar*



The following WebUI pages support group monitoring and configuration:

- List. This page lists all groups configured in AirWave and provides the foundation for all group-level configurations. For more information, see "Viewing Device Groups" on page 82
- 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. The default view of the **Groups > Monitor** page is predefined and cannot be modified. However, you can create a new view, or edit and copy a view, and save the view to access information you frequently use. For more information on filtering data from your view, see "Creating Filtered Views" on page 150.
- Basic. This page becomes available when you create a new group on the **Groups > List** page. For more information, see "Configuring Basic Settings for Device Groups" on page 93.
- Templates. This page manages templates for any device group. You can use templates to manage the configuration of third-party devices in a group using a configuration file. Variables configure device-specific and group-level properties. For more information, see "Using Configuration Templates" on page 236.

- Security. This page defines general security settings for device groups, to include RADIUS, encryption, and additional security settings on devices. For more information, see "Configuring Security for Device Groups" on page 105
- 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. For more information, see "Configuring SSIDs and VLANs for Device Groups" on page 110.
- AAA Servers. This page configures authentication, authorization, and accounting settings in support of RADIUS servers for device groups. For more information, see "Configuring AAA Servers for Device Groups" on page 104.
- Radio. This page defines general 802.11 radio settings for device groups. "Configuring Group Radio Settings" on page 114
- Controller Config. This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Aruba devices on the network. Use this page as an alternative to the **Device Setup > Aruba > Configuration** page. The appearance of this page varies depending on whether AirWave is configured for global configuration or group configuration. For more information, see the *Aruba Controller Configuration Guide*.
- Switch Config. This page manages ArubaOS Device Groups, AP Overrides, and other profiles specific to Aruba switches on the network. For more information, see the *Aruba Switch Configuration Guide*.
- Instant Config. This page manages Aruba Instant devices on the network. For more information, see the *Aruba Instant in AirWave 8.2.8.2 Deployment Guide*.
- Cisco WLC Config. This page becomes available when you select a device group that contains Cisco WLC devices and consolidates controller-level settings from several pages (Group Radio, Security, SSIDs, Cisco WLC Radio and AAA Server). For more information, see "Configuring Cisco WLC Device Groups" on page 118
- PTMP. This page defines settings specific to Proxim MP devices when present and is only available when a Proxim MP device is added to this group. For more information, see "Configuring PTMP Settings for Device Groups" on page 124.
- Proxim Mesh. This page defines mesh AP settings specific to Proxim devices when present. For more information, see"Configuring Proxim Mesh Radio Settings" on page 125.
- MAC ACL. This page defines MAC-specific settings that apply to Proxim, Symbol, and ProCurve 520 devices when present. For more information, see "Configuring Group MAC ACLs for Device Groups" on page 127.
- Firmware. This page enables you to manage firmware files for many device types in one location. For more information, see "Specifying the Minimum Firmware Version for Device Groups" on page 128.
- 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**. For more information, see "Comparing Device Groups" on page 84.

Viewing Device Groups

You can view device groups by navigating to **Groups > List** . When you configure AirWave for the first time, Access Points is the only group in the list.

From the Groups List page, you can:

- Create a group by clicking Add at the top of the page. Alternatively, you could create a group by selecting group from the list and clicking to clone the group. The copied group will be added to the group list with "copy of" appended in front of the group name.
- Compare two groups. For more information, see "Comparing Device Groups" on page 84.
- Click or hover your mouse over the icon for quick access to other Groups pages. For information about the Groups pages, see "Navigation Basics" on page 81.

For example, you can select Basic from the shortcut menu to change group configurations. Refer to "Configuring Basic Settings for Device Groups" on page 93 .

- Add groups to a global group. For more information, see "Subscribing other Groups to a Global Group" on page 88.
- Delete a group. For more information, see "Deleting a Group" on page 89.

Table 32 describes the device group details available on the **Groups > List** page.

Table 32: *Groups > List Fields and Descriptions*

Field	Description
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).
SSID	The SSID assigned to supported device types within the group.
Total Devices	Total number of devices contained in the group including APs, controllers, routers, or switches.
Changes	This field is available when a group has unapplied changes.
Is Global Group	This field is available if a group is designated as global. A global group may not contain APs, but it may be used as a template for other groups. **NOTE:** This column might indicate **Yes** if this group has been pushed to AirWave from a Master Console.
Global Group	Specifies which group this Subscriber Group is using as its template.
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, 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.
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. By default, most polling intervals do not match the up/down period.
Duplicate	Creates a new group with the name **Copy of <Group Name>** with identical configuration settings. (Aruba configuration settings will have to be manually added back.)

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 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 34 illustrates this page.

Figure 34: *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.

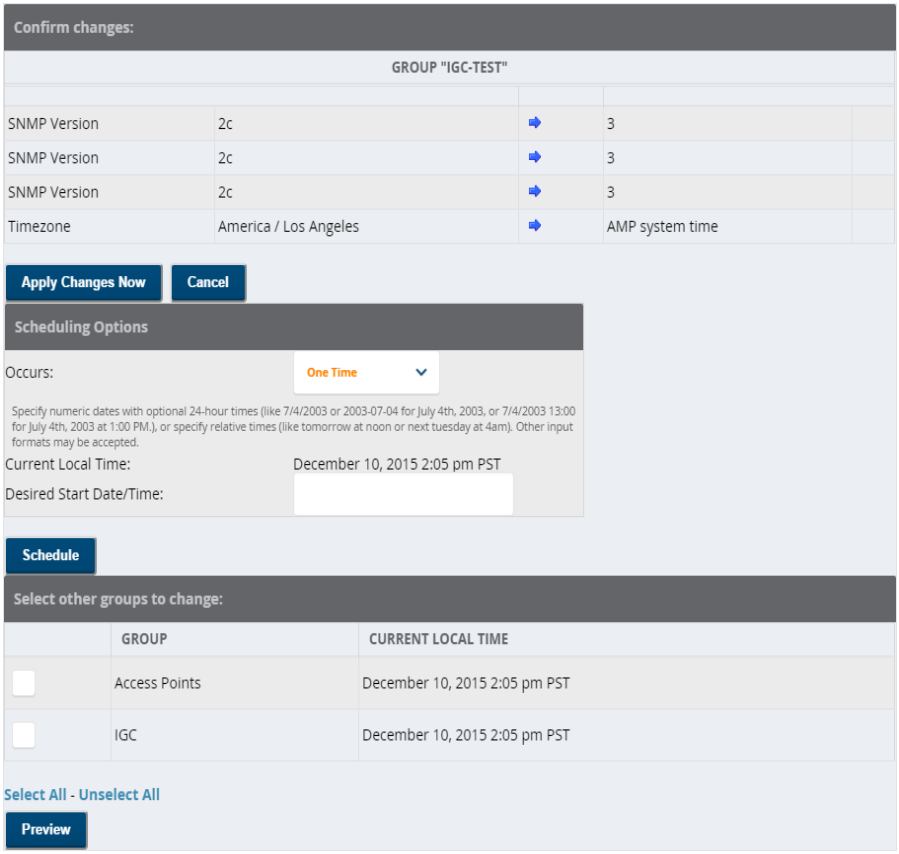
- The default setting of the **Compare** page is to highlight settings that differ between two groups.
  - To display settings that are similar or identical between two device groups, select **Show Similar Fields** at the top left of the page. The result may be a high volume of information.
  - Select **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.

Changing 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 35 illustrates the confirmation message that appears.

Figure 35: *Groups > Basic Configuration Change Confirmation Page Illustration*



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

   - **Scheduling Options** — Schedules the changes to be applied to this group in the future. Enter the desired change date in the **Start Date/Time field**. You can also specify if this is a one-time schedule or a recurring schedule. Recurring options are **Daily**, **Weekly**, **Monthly**, and **Annually**. AirWave takes the time zone into account for the group if a time zone other than 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**.

Using Global Groups for Group Configuration

The AirWave group configuration feature allows you to push configurations defined on a global group to the managed groups subscribed to that global group.

About Global Group Membership

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. illustrates the **Groups > List** page.

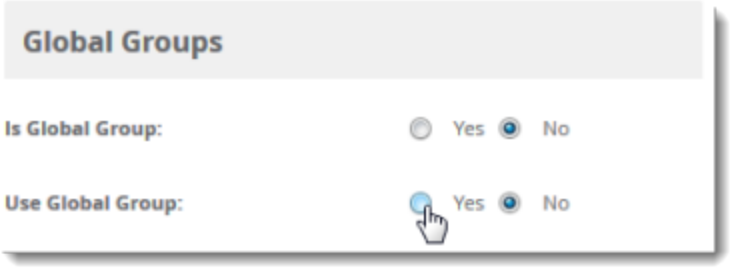
Creating a Global Group

The Use Global Group option becomes available when you have at least two groups configured in AirWave. You can configure AirWave to push a group configuration to a group when you enable this option.

To configure a global group:

1. Navigate to **Groups > List**.
2. Select a the group from the list.
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.

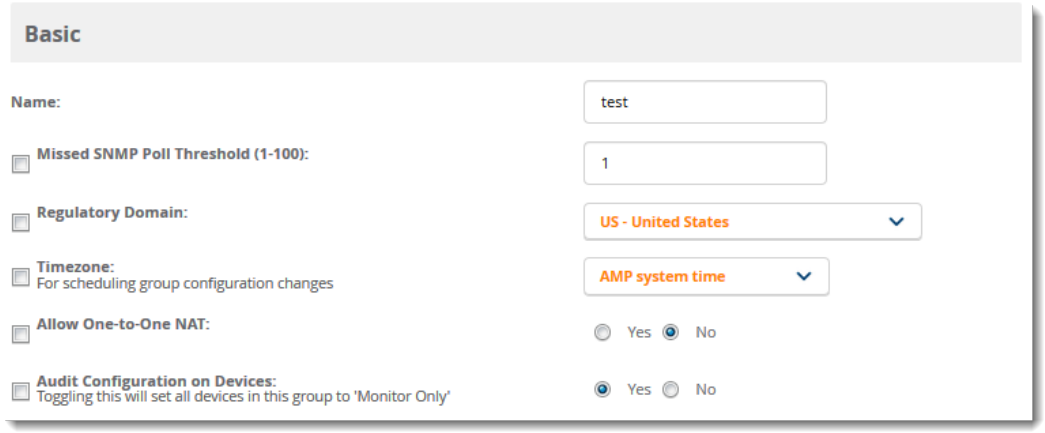
Figure 36: *Selecting the Use Global Group Option*



5. To associate the group with a global group, select the group from the Global Group drop-down menu.
6. Click **Save and Apply**.
7. Click **Apply Changes Now**.

When the Groups list is updated with the global group, you will see **Yes** in the "Is Global Group" column, and when you go to the Basic page for the global group, there will be checkboxes next to the basic settings. Figure 37 shows an example for a global group called "test".

Figure 37: *Basic Settings for the Global Group*



When AirWave pushes a global group configuration to subscriber groups, all settings are static except for those with the checkbox selected; you can change the value or setting of the checked field 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**).

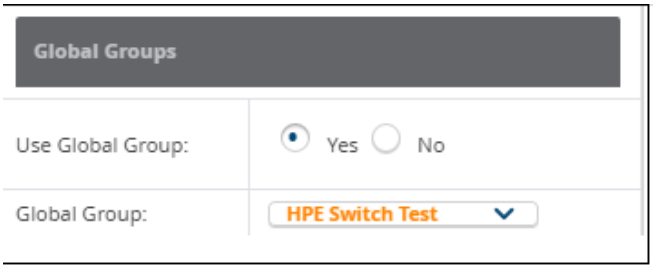
Global templates are also configurable as part of global groups; for more information, see "Using Configuration Templates" on page 236.

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 38: *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 you want to change a global group into a regular group and it has subscribers, you need to remove the subscribers first before you can change the "Is Global Group" option to **No** on the **Groups > Basic** page.

Deleting a Group

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

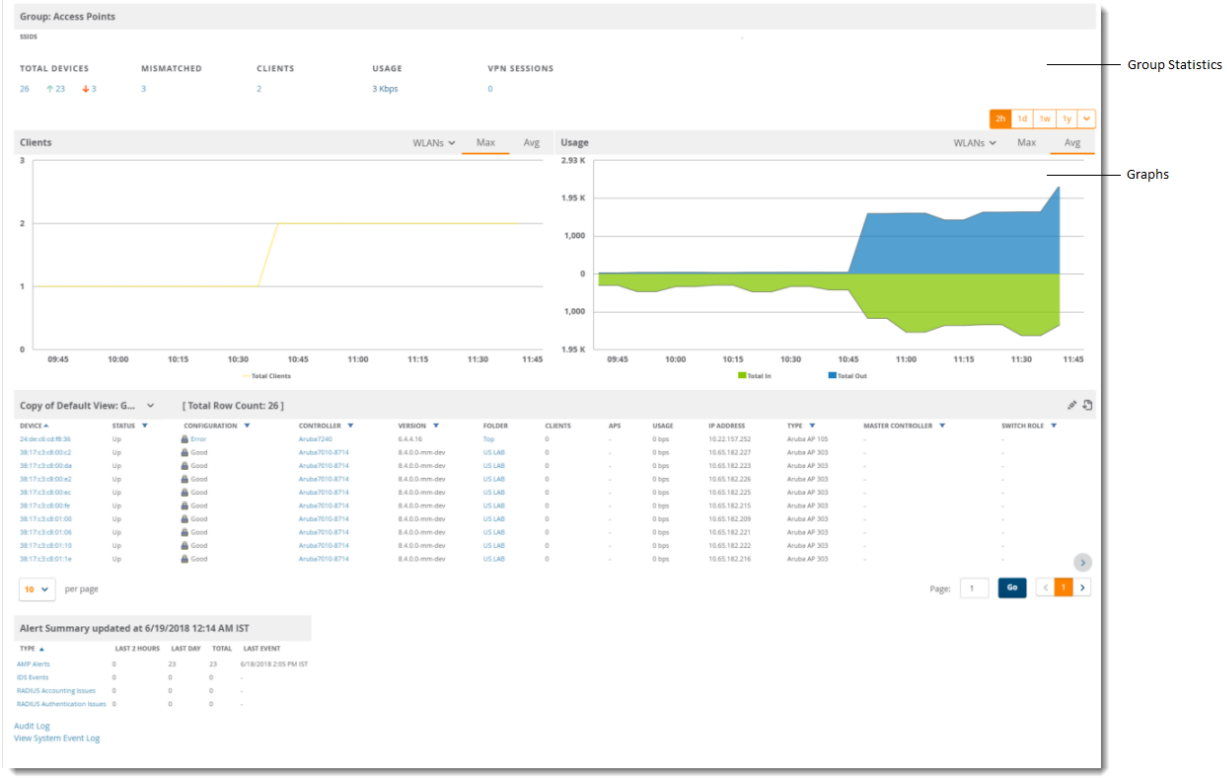
1. Browse to the **Groups > List** configuration page.
2. Ensure that the group you wish to delete is not marked as the **default** group. (See the **AMP Setup > General** page.) AirWave does not permit you to delete the current default group.
3. Ensure that there are no devices in the group that you want to delete. 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. AirWave will not delete a group in which either of those cases is true.
5. Select the checkbox, and click the **Delete** button.

Monitoring Device Groups

You can find the monitoring page by navigating to **Groups > Monitor** page and selecting a device group from the list.

Figure 39 shows the main components of the monitoring page for the default device group called Access Points.

Figure 39: *Group Monitoring Page*



Here are some of the things you can view on or from the **Groups > Monitor** page:

- Group statistics. The total number of devices contained in the group includes APs, controllers, routers, or switches. From the summary counts at the top of the page, you can click links to monitoring pages for devices and connected clients.
- Graphs. The client and usage graphs show the attached clients and average bandwidth or VPN session usage for the devices in the group. You can change the sample interval, or show the maximum or average statistics by clicking the menu options in the graph header.
- Group table. The default view of the devices group includes these columns:

- Device. This information shows the device MAC address and provides a quick link to the monitoring page for the device. Hover over the blue link to access shortcuts to other pages, such as Manage, Config, Monitor, and Compliance.
- Status. This information shows whether devices are up or down in the group.
- Configuration. This information shows whether the device configuration is good, or there is an error or mismatch. Click the blue link to access the Device Configuration page and review the device configuration.
- Controller. This information shows the name of the controller and provides a quick link to the monitoring page for the controller.
- Version. This information shows the firmware version running on the controller.
- Folder. This information shows the name of the folder the device belongs to and provides a quick link to the list of devices for the folder.
- Clients. This information shows the number of clients per device.
- APs. This information shows the number of APs per device, if applicable.
- Usage. This information shows the total speed of all clients at that moment.
- IP Address. This information shows the IP address of the device.
- Type. This information shows the device model.
- Master Controller. If the controller role is master, AirWave displays the device type and provides a quick link to the monitoring page for the device.
- Switch Role. For switches that support VSF stacking, this information shows whether the switch functions as commander, standby, member, or has been provisioned to be a member of the stack.

- Alerts. From the alert summary table at the bottom of the page, you can click links to summary pages forAMP, Intrusion Detection System (IDS), RADIUS accounting, and RADIUS authentication alerts received on the devices in the group. You can also access the audit log and system event log from this table.

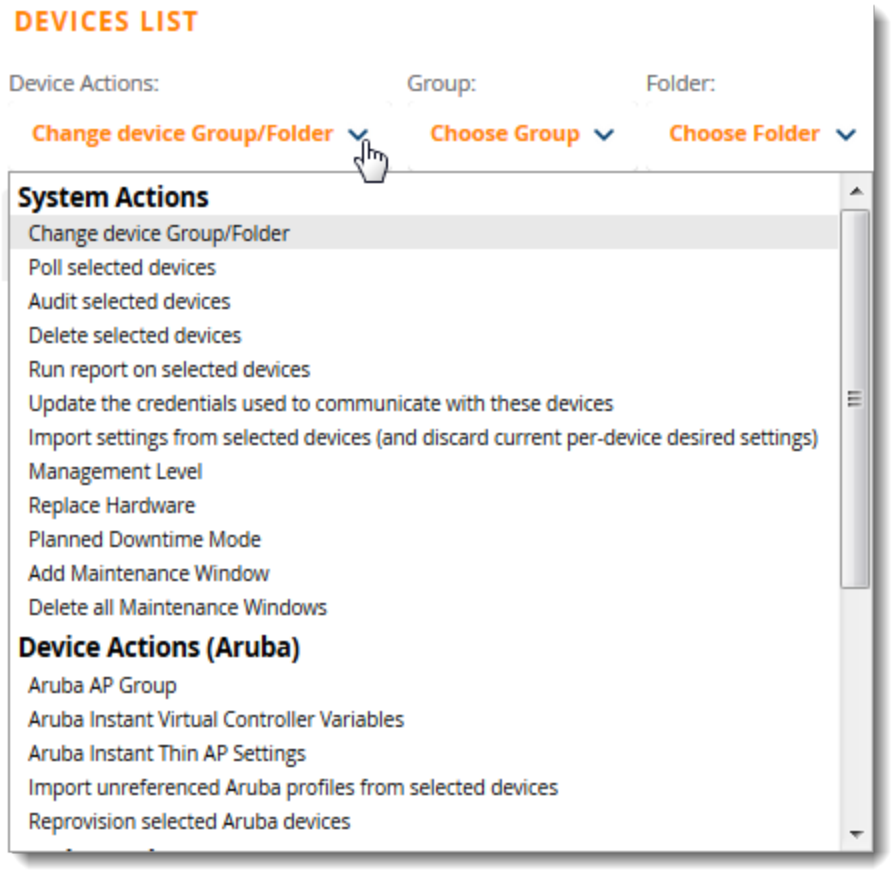
Modifying Multiple Devices

AirWave provides a Modify Devices tool that enables you to make bulk changes to devices, including controllers that have thin APS. Some of the device actions you can make include deleting multiple devices, migrating devices to another group or folder, updating credentials, and optimizing channels.

To modify multiple devices:

1. Navigate to one of the following pages that has a Device List:
   - **Devices > List**. You can also click the Up, Down, Mismatched hyperlinks on the List page to open monitoring pages for the devices with those devices states.
   - **Groups > Monitor**.
2. Click  at the top right corner of the device list, then select the devices you want to modify.
3. Select as many changes as you want from the Device Actions drop-down menu.

Figure 40: *Selecting the Device Actions*



4. Click **Apply All**.

Table 33 describes the changes you can apply to multiple devices at the same time.

Table 33: *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 device 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.
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 AirWave server.
Audit selected devices	Fetches the current configuration from the device and compares it to the desired AirWave configuration. The audit action updates the Configuration Status. **NOTE:** If a group has audit disabled for its devices, AirWave does not show the **Audit** button in the **Modify devices** list.

Table 33: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Delete selected devices	Click **Delete** to remove the selected devices from 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 "Running Reports on Selected Devices" on page 365. **NOTE:** Some reports are not device-based and can't be run with the bulk selection of devices from **Modify Devices**; these reports are New Rogue Device, Rogue Clients, Rogue Containment Audit, Traffic Analysis, and UCC.
Update the credentials used to communicate with these devices	**Update** changes the credentials 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 AirWave initially read off of the AP including channel, power, antenna settings and SSL certifications. AirWave recommends using this setting if APs have been updated outside of AirWave. Most settings on the **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 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 (Aruba)	
Aruba AP Group	When you select this option then click Update Aruba AP Group, a new window opens that allows you to assign the devices to a new AP group.

Table 33: *Modify Multiple Devices Section Fields and Default Values (Continued)*

Action	Description
Aruba Instant Virtual Controller Variables	Opens the Variable Editor page for selected Aruba Instant APs.
Import unreferenced Aruba profiles from selected devices	Select the devices that include unreferenced profiles, then click this button to import those profiles from the selected devices.
Reprovision selected Aruba devices	Configures the controller to send provisioning parameters such as radio, antenna, and IP address settings to the selected APs. Please note that APs will be rebooted as part of reprovisioning.
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 **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 **Devices > List** page. Make changes to LWAPP AP groups, including the option that was under Modify Devices.

Configuring Basic Settings for Device Groups

The first default device group set up in AirWave is the **Access Points** group, but you can configure additional device groups. After you define the basic group settings, you can save the changes without pushing these settings to the devices in the group. You might want to do this in order to push configuration changes at a later time.

To access the Basic Group Settings page:

- Add a device group from the **Groups > List page**. The **Groups > Basic** page displays and becomes available from the navigation sidebar.
- Navigate to **Groups > List**, locate the group and click  .
- Navigate to **Groups > List**, locate the group and select Basic from the shortcut menu. The shortcut menu varies depending on the group's settings.

Basic Settings

To set up the device group, you need to configure the basic settings described in Table 34.

Figure 41: *Basic Settings*

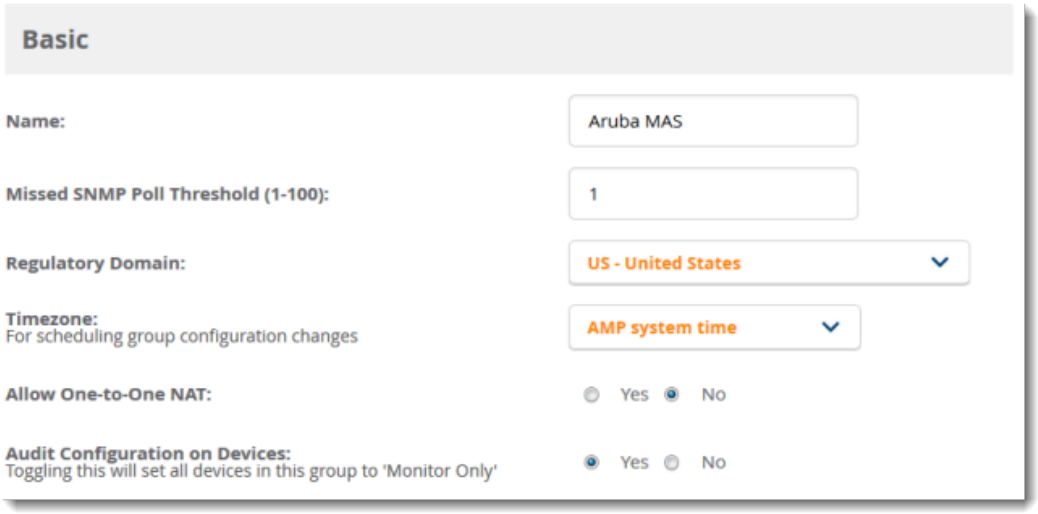


Table 34: *Basic Settings, Default Values, and Descriptions*

Setting	Default	Description
Name	Defined when first adding the group	Displays or changes the group name. Enter a name that helps to identify the group. For example, Accounting APs, Cisco devices, and Aruba controllers).
Missed SNMP Poll Threshold (1-100)	1	Sets the number of Up/Down SNMP polls that must be missed before AirWave considers a device to be down. **NOTE:** Set the number of SNMP retries and the SNMP timeout of a poll on the **Device Setup > Communication** page.
Regulatory Domain	US-United States	Sets the regulatory domain in 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.
Allow One-to-One NAT	No	Allows 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 **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. **NOTE:** Once disabled, all the devices in the groups will not be counted towards mismatched devices.

Global Groups

The global groups option becomes available on the Groups Basic page when you create a new group for the first time and it is a global group.

Table 35 describes the global group options you can define in order to push configurations to group members.

Table 35: *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 87 .
Use Global Group	No	Click this drop-down list to 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 88 . **NOTE:** This field becomes available when there are more than one groups configured in AirWave.

SNMP Polling Periods

You can override the override default SNMP polling settings with the SNMP polling period options described in Table 36.

Table 36: *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 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 36: *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

You can configure how often AirWave polls devices in the group with the routers and switches options described in Table 37. You can also disable these options.

Table 37: *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

You can configure the group display options as described in Table 38.

Table 38: *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**—AirWave displays all Group tabs and setting options. • **Only devices in this group**—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 AirWave. • **Use system defaults**—Use the default settings on **AMP Setup > General** • **Selected device types**—Allows you to specify the device types for which 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.

These options are relevant for a small number of device types and will appear when they are present.

Table 39 describes the automatic static IP address options.

Table 39: *Automatic Static IP Assignment Fields and Default Values*

Setting	Default	Description
Assign Static IP Addresses to Devices	No	Specify whether to enable AirWave to statically assign IP addresses from a specified range to all devices in the Group. **NOTE:** 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 AirWave assigns to the devices in the Group.
Number of Addresses	none	Sets the number of addresses in the pool from which 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 40 describes the settings and default values in this section.

Table 40: *Spanning Tree Protocol Fields and Default Values*

Setting	Default	Description
Spanning Tree Protocol	No	Specify whether to enable STP on Proxim APs. When you set this option to **Yes**, additional configuration fields described in this table 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, from 1 to 10 seconds, between Hello message broadcasts.
Bridge Forward Delay	15	Sets the time, from 4 to 30 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 41 describes the NTP settings and default values.

Table 41: *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 AirWave graphs and logs use the time set on the 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/HPE(OfficeConnect/FlexFabric/FlexConnect) Switch Config

AirWave automates provisioning of several models of Aruba/HPE switches. Provisioning uses template-based configuration, zero-touch provisioning (ZTP), and configuration snippets.

There are two methods of switch configuration:

- Full configuration. AirWave pushes a complete set of changes using a template to the group of devices. By default, the full configuration mode is enabled whenever you create a device group.
- Config job. AirWave pushes 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).

For help with switch configuration, refer to the *AirWave Switch Configuration Guide*.

Aruba

To configure settings specific to Aruba locate the Aruba section and adjust these settings as required.

Table 42 describes the settings and default values of this section of the **Groups > Basic** page.

Table 42: *Aruba Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by AirWave to communicate to the AP.
Offload WMS Database	No	Configures commands previously documented in the AirWave 8.2.11.1 *Best Practices Guide*. When enabled, this feature allows 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**.
Aruba GUI Config	Yes	This setting selects whether you'd like to configure your devices using the **Groups > Controller** method (either global or group) or using Templates.
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.
Archive Controller/Switch Backups	Yes	This setting enables AirWave to create config backups manually. **NOTE:** After you enable this setting, you can go to the **Device Configuration** page and click **Create Backup Now**. An archived config backup is available only Aruba controllers and Mobility Access Switches.

Aruba Instant

To specify the Aruba Instant settings to be applied to this group, locate the Aruba Instant settings section of the **Groups > Basic** page and adjust these settings as desired.

Table 43 describes the settings and default values.

Table 43: *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 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 the primary (and optionally, secondary) 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 AirWave when that device becomes active on the network.
Ignore DHCP configuration	No	When this feature is enabled, AirWave will not run a DHCP configuration audit when the device is added to AirWave. For IAP DHCP configuration, from the IAP UI, go to **DHCP Servers**.
HTTPS timeout	5 minutes	the HTTPS timeout for Instant devices is the period for which 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 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 AirWave to download a captive portal logo to your Instant APs. Upload the image (which must be 16 KB 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 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 group settings specific to Cisco IOS/Catalyst devices, as described in Table 44.

Table 44: *Cisco IOS/Catalyst Fields and Default Values*

Setting	Default	Description
SNMP Version	2c	The version of SNMP used by AirWave to communicate to the AP.
Cisco IOS CLI Communication	Telnet	The protocol 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 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 45 describes the settings and default values in this section.

Table 45: *Cisco WLC Fields and Default Values*

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

When configuring Cisco WLC controllers, refer to "Configuring Wireless Parameters for Cisco Controllers" on page 123.

Proxim/ Avaya

To configure Proxim/Avaya specific settings locate the **Proxim/Avaya** section of the **Groups > Basic** page and adjust these settings as required.

Table 46 describes the settings and default values.

Table 46: *Proxim/Avaya Settings*

Setting	Default	Description
SNMP Version	1	Sets the version of SNMP used by AMP to communicate to the AP.

Table 46: *Proxim/Avaya Settings (Continued)*

Setting	Default	Description
Enable DNS Client	No	Enables the DNS client on the AP. Enabling the DNS client allows you to set some values on the AP by hostname instead of IP address. If you select Yes for this setting, additional DNS fields display.
Primary DNS server	Blank	Sets the IP address of the Primary DNS server.
Secondary DNS server	Blank	Sets the IP address of the Secondary DNS server.
Default DNS domains	Blank	Sets the default DNS domain used by the AP.
HTTP Server Port	80	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 Table 47 describes the settings and default values.

Table 47: *HP ProCurve Settings*

Setting	Default	Description
SNMP Version	2c	Sets the version of SNMP used by AirWaveto communicate to the AP.
ProCurve XL/ZWeSM CLI Communication	Telnet	Sets the protocol 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 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.

Table 48 describes the settings and default values.

Table 48: *Symbol Settings*

Setting	Default	Description
SNMP Version	2c	Specifies the version of SNMP used by AWMS to communicate to the device.

Table 48: *Symbol Settings (Continued)*

Setting	Default	Description
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 49 describes the automatic authorization options for the device group.

Table 49: *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.
Ignore Device's Configured Folder	No	Enable this option to ignore the folder in the provisioning rule for Aruba switches configured via Activate, DHCP, or the switch comand-line interface.

Maintenance Windows

You can use maintenance windows to put multiple devices into Management mode, apply configuration changes to the devices in the group, and then reset them to Monitor-Only mode after the maintenance period is over. For more information, see "Adding a Maintenance Window for a Device" on page 230.

Configuring AAA Servers for Device Groups

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.

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

Table 50: *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 AirWave and the RADIUS server. **NOTE:** The shared secret entered in 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.

   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.

TACACS+ servers are configurable only for Cisco WLC devices. Refer to "Configuring Cisco WLC Security Parameters and Functions" on page 123.

Configuring Security for Device Groups

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 AirWave pages.

Figure 42 illustrates this page for a group of switches.

Figure 42: *Groups > Security Page*

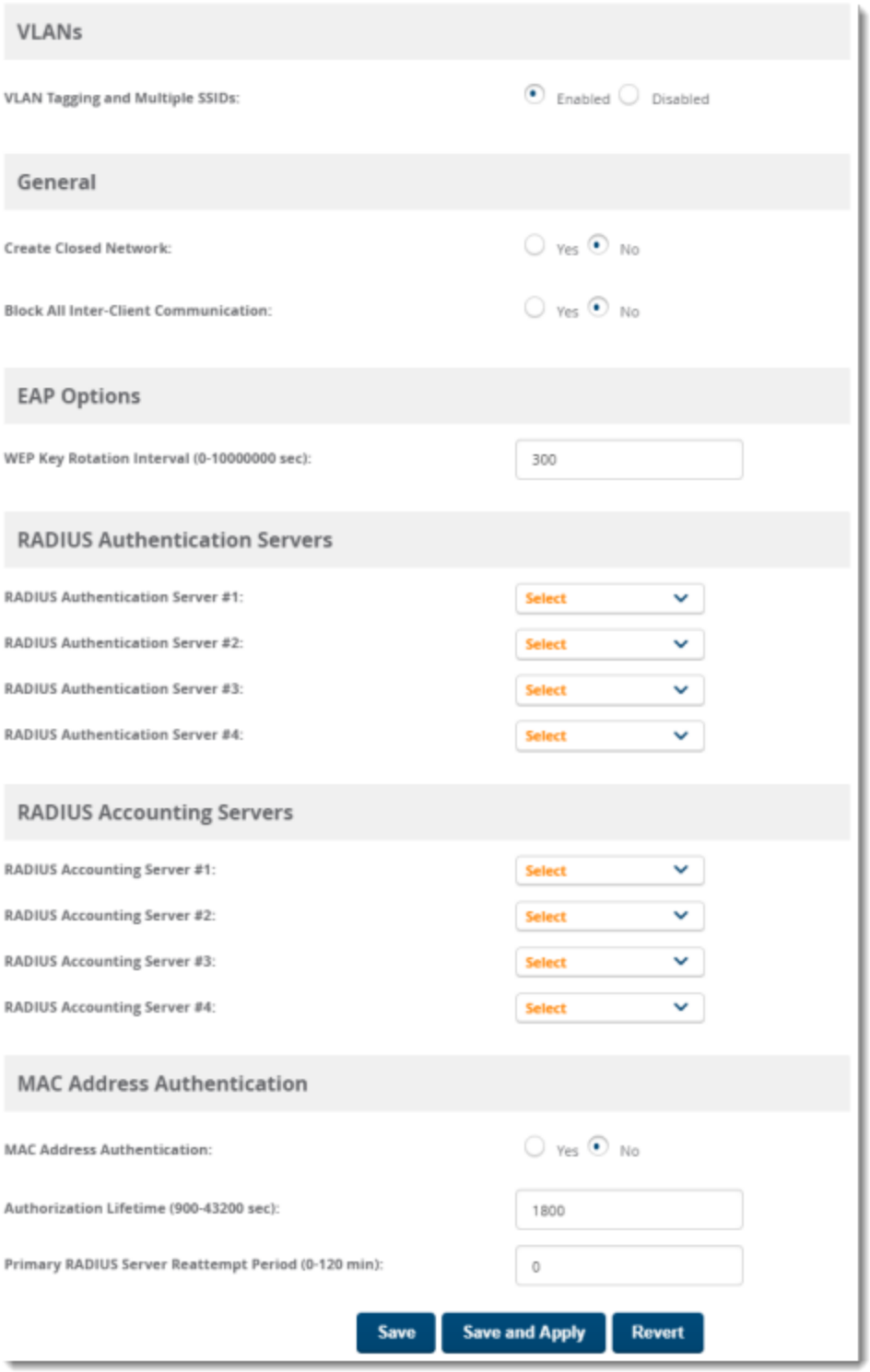


Table 51 explains the fields and default values.

Table 51: *Groups > Security Page Fields and Default Values*

Setting	Default	Description
VLANs Section		

Table 51: *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 SSIDs and VLANs for Device Groups" on page 110. 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 108 for information on configuring Encryption.
Management VLAN ID	Untagged	This setting sets the ID for the management VLAN when VLANs are enabled in 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	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.

Table 51: *Groups > Security Page Fields and Default Values (Continued)*

Setting	Default	Description
Authentication Profile Name		For Proxim devices only, this field sets the name of the accounting profile to be supported in this device group.
Authentication Profile Index	3	For Proxim devices only, this field sets the name of the accounting profile index to be supported in this device group.
MAC Address Authentication Section		
MAC Address Authentication	No	If enabled, only MAC addresses known to the RADIUS server are permitted to associate to APs in the Group.
MAC Address Format	Single Dash	Allows selection of the format for MAC addresses used in RADIUS authentication and accounting requests: • Dash Delimited: xx-xx-xx-xx-xx-xx (default) • Colon Delimited: xx:xx:xx:xx:xx:xx • Single-Dash: xxxxxx-xxxxxx • No Delimiter: xxxxxxxxxxxx This option is supported only for Proxim AP-600, AP-700, AP-2000, AP-4000, Avaya AP3/4/5/6/7/8, 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 52 for information regarding configuring encryption.

Table 52: *Groups > Security Encryption Mode settings*

Setting	Default	Description
Encryption Mode	Require 802.1X	Encryption Mode options: Require 802.1X, Optional WEP, Require WEP, Require 802.1X, Require LEAP, 802.1X + WEP, 802.1X + WEP, LEAP + WEP, Static CKIP, WPA, WPA/PSK, WPA2, WPA2/PSK, or xSec.
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	

Table 52: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
Encryption Mode Static CKIP		
CKIP Static Key (hex) and Confirm	None	Enter and confirm the Cisco Key Integrity Protocol (CKIP) static key, specified in hexadecimal digits.
CKIP Key Index	1	Select the CKIP Key Index value. This can be a value from 1 through 4.
CKIP Key Permutation	No	Specify whether to use Key Permutation.
CKIP MMH Mode	No	Specify whether to use Multi-Module Has (MMH) mode.
Encryption Mode WPA		
Unicast Cipher (Cisco only)	AES	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
Encryption Mode WPA/PSK		
Unicast Cipher (Cisco only)	AES/TKIP	Specify the Unicast Cipher. Values include AES, TKIP, and AES/TKIP.
WPA Preshared Key (Alphanumeric)	None	Enter an alphanumeric value for the preshared key.
Encryption Mode WPA2		
WPA2 WPA Compatibility Mode	Yes	Specify whether to enable WPA2 WPA Compatibility Mode.
WPA1 Cipher (Cisco WLC Only)	TKIP	Specify the WPA1 Cipher. Values include AES, TKIP, and AES/TKIP. **NOTE:** This drop down is only available if WPA2 WPA Compatibility Mode is **Yes**.
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.

Table 52: *Groups > Security Encryption Mode settings (Continued)*

Setting	Default	Description
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 SSIDs and VLANs for Device Groups

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 AirWave WebUI until *after* you configure a RADIUS server using the **Groups > AAA Servers** page, as described on "Configuring AAA Servers for Device Groups" on page 104.

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

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

To create or edit VLANs and to set SSIDs:

1. Go to **Groups > List** and select the group name for which to define SSIDs/VLANs.
2. Select the **Groups > SSIDs** configuration page. Table 53 describes the information that appears for SSIDs and VLANs that are currently configured for the device group.

Table 53: *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.

Table 53: *Groups > SSIDs Fields and Descriptions (Continued)*

Field	Description
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. 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 54.
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 54 describes the settings and default values. Note that the displayed settings can vary.

Table 54: *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.

Table 54: *SSID/VLAN Section Fields and Default Values (Continued)*

Setting	Default	Description
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 55 describes the available encryption modes. Table 52 in "Configuring Security for Device Groups" on page 105 describes configuration settings for each mode.

Table 55: *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 56 describes the settings and default values.

Table 56: *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 57 describes the settings and default values.

Table 57: *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.

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 58 describes the settings and default values.

Table 58: *Radius Accounting Servers Fields and Default Values*

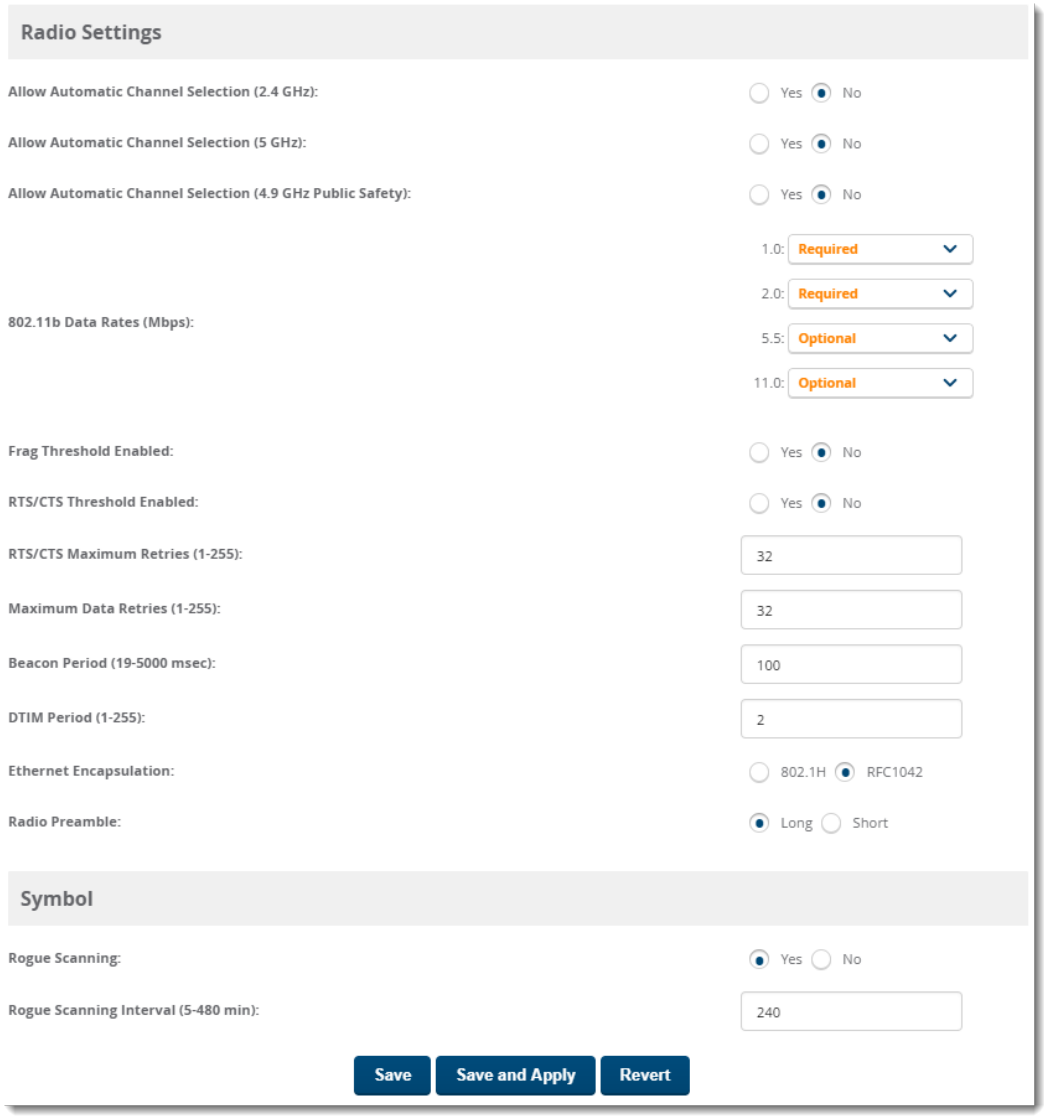
Setting	Default	Description
RADIUS Accounting Server 1-3 (Cisco WLC, Proxim Only)	None	Pull-down menu selects RADIUS Accounting servers previously entered on the **Groups > RADIUS** configuration page. These RADIUS servers dictate where the AP sends RADIUS Accounting packets for this SSID/VLAN.
Accounting 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.

Configuring Group Radio Settings

You can configure detailed RF-related radio settings for devices on the **Groups > Radio** page. If you have existing deployed devices, you might want to use the RF settings on those devices as a guide when configuring the radio settings for your default group.

Figure 43: *Groups > Radio Page*



To define RF-related radio settings for a device group:

1. Go to the **Groups > List** page, then select a group for which to define radio settings. The monitor page for the group appears.
2. Navigate to **Groups > Radio** to open the radio page for the group. Figure 43 illustrates this page.
3. Locate the **Radio Settings** area and adjust these settings as required. Table 59 describes the settings and default values.

Table 59: *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, AirWave automatically reboots the APs in the group when the change is implemented.
802.11b Data Rates (Mbps)	Required: • 1.0 • 2.0 Optional: • 5.5 • 11.0	Displays pull-down menus for various data rates for transmitting data. **NOTE:** This setting does not apply to Cisco LWAPP devices. The three values in each of the pull-down menus are as follows: • **Required**—The AP transmits only unicast packets at the specified data rate; multicast packets are sent at a higher data rate set to optional. (Corresponds to a setting of **yes** on Cisco devices.) • **Optional**—The AP transmits both unicast and multicast at the specified data rate. (Corresponds to a setting of **basic** on Cisco devices.) • **Not Used**—The AP does not transmit data at the specified data rate. (Corresponds to a setting of **no** on Cisco devices.)
Frag Threshold Enabled	No	If enabled, this setting enables packets to be sent as several pieces instead of as one block. In most cases, leave this option disabled.
Threshold Value (256-2347 bytes)	2337	If Fragmentation Threshold is enabled, this specifies the size (in bytes) at which packets are fragmented. A lower **Fragmentation Threshold** setting might be required if there is a great deal of radio interference.
RTS/CTS Threshold Enabled	No	If enabled, this setting configures the AP to issue a RTS (Request to Send) before sending a packet. In most cases, leave this option disabled.
RTS/CTS Threshold Value (0-2347 bytes)	2338	If RTS/CTS is enabled, this specifies the size of the packet (in bytes) at which the AP sends the RTS before sending the packet.
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.

Table 59: *Groups > Radio > Radio Settings Fields and Default Values (Continued)*

Setting	Default	Description
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.

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 60 describes the settings and default values.

Table 60: *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.

Table 60: *Groups > Radio > Device-Specific Fields and Default Values (Continued)*

Setting	Default	Description
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 61 describes the settings and default values.

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

Table 62: *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.

Configuring Cisco WLC Device Groups

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.

NOTE

Do not put Symbol 4131 and Proxim APs in the same group as Cisco devices. Aruba recommends setting device preferences to **Only devices in this group**.

Refer to the following topics for additional information:

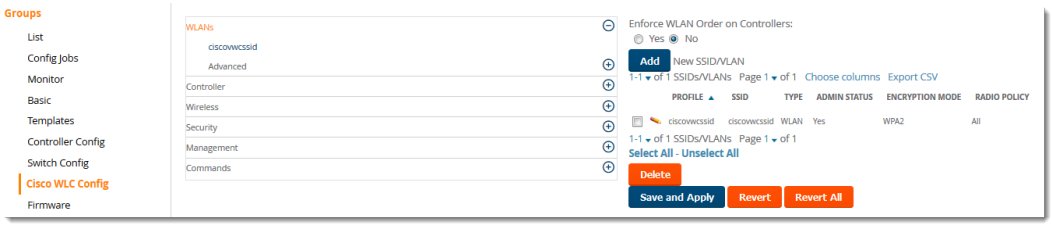
Accessing Cisco WLC Configuration

The Cisco WLC Config navigation submenu becomes available when you create a Cisco WLC device group for the first time.

To access the **Cisco WLC Config** page:

1. Navigate to **Groups > List**, then select a Cisco WLC device group.
2. Select **Groups > Cisco WLC Config** in the navigation sidebar. In the **Groups > Cisco WLC Config** page that displays, click ⊕ to expand the configurable settings.

Figure 44: *Groups > Cisco WLC Config Navigation*



NOTE

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

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**, 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 45: *Add New SSID/VLAN > General Tab Illustration*

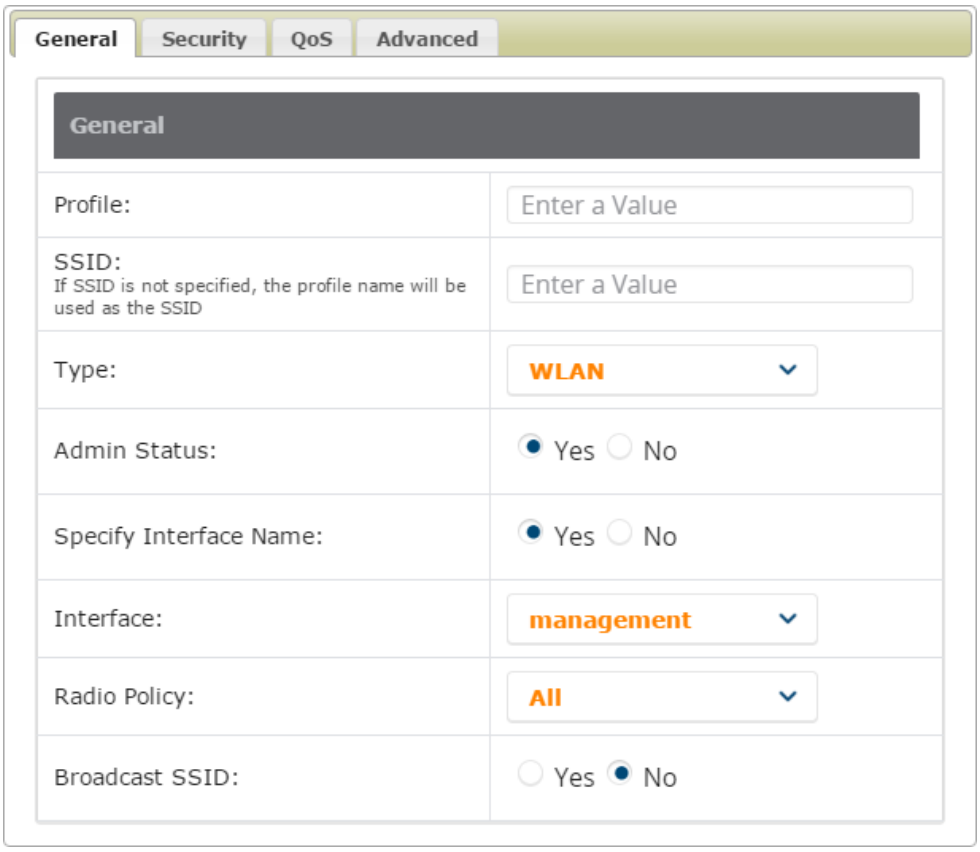


Figure 46: *Add New SSID/VLAN > Security Tab Illustration*

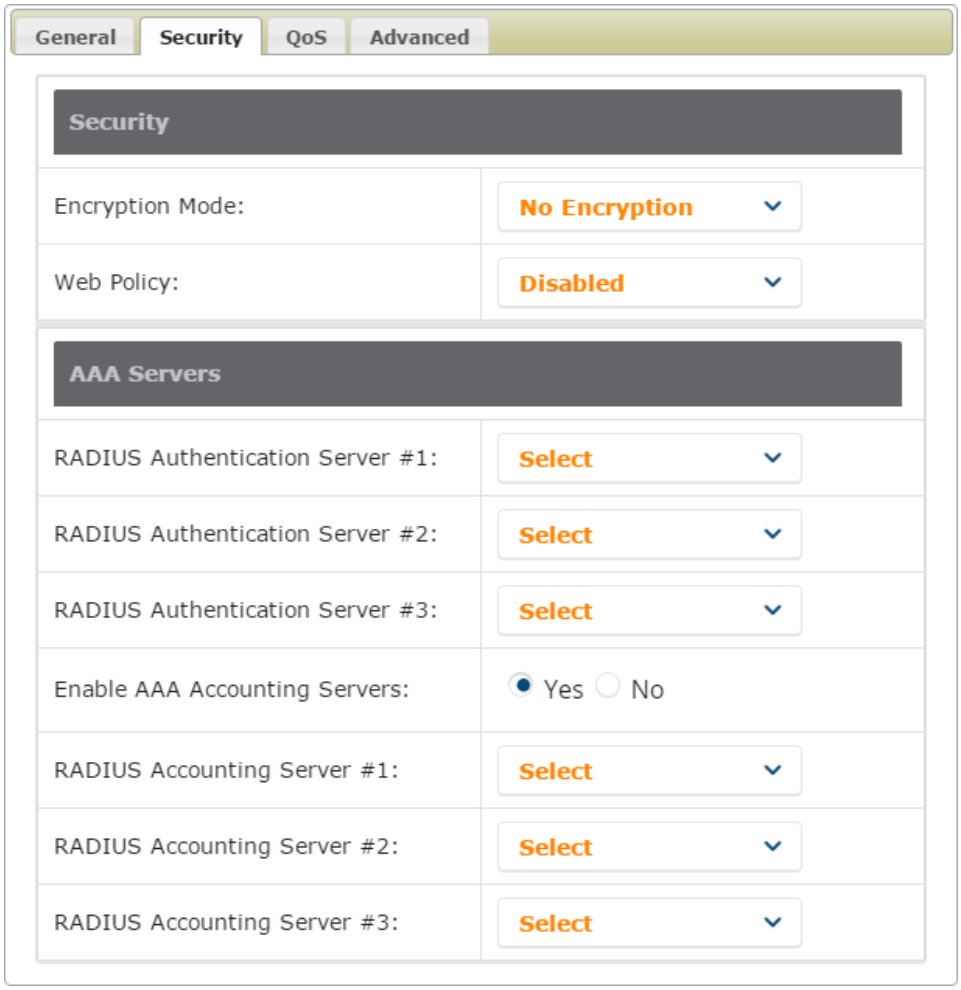


Figure 47: *Add New SSID/VLAN > QoS Tab Illustration*

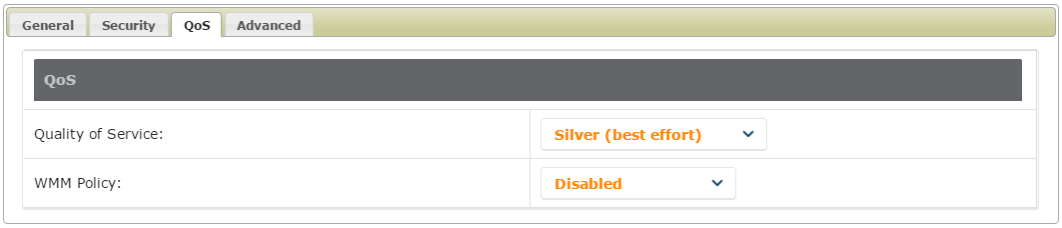
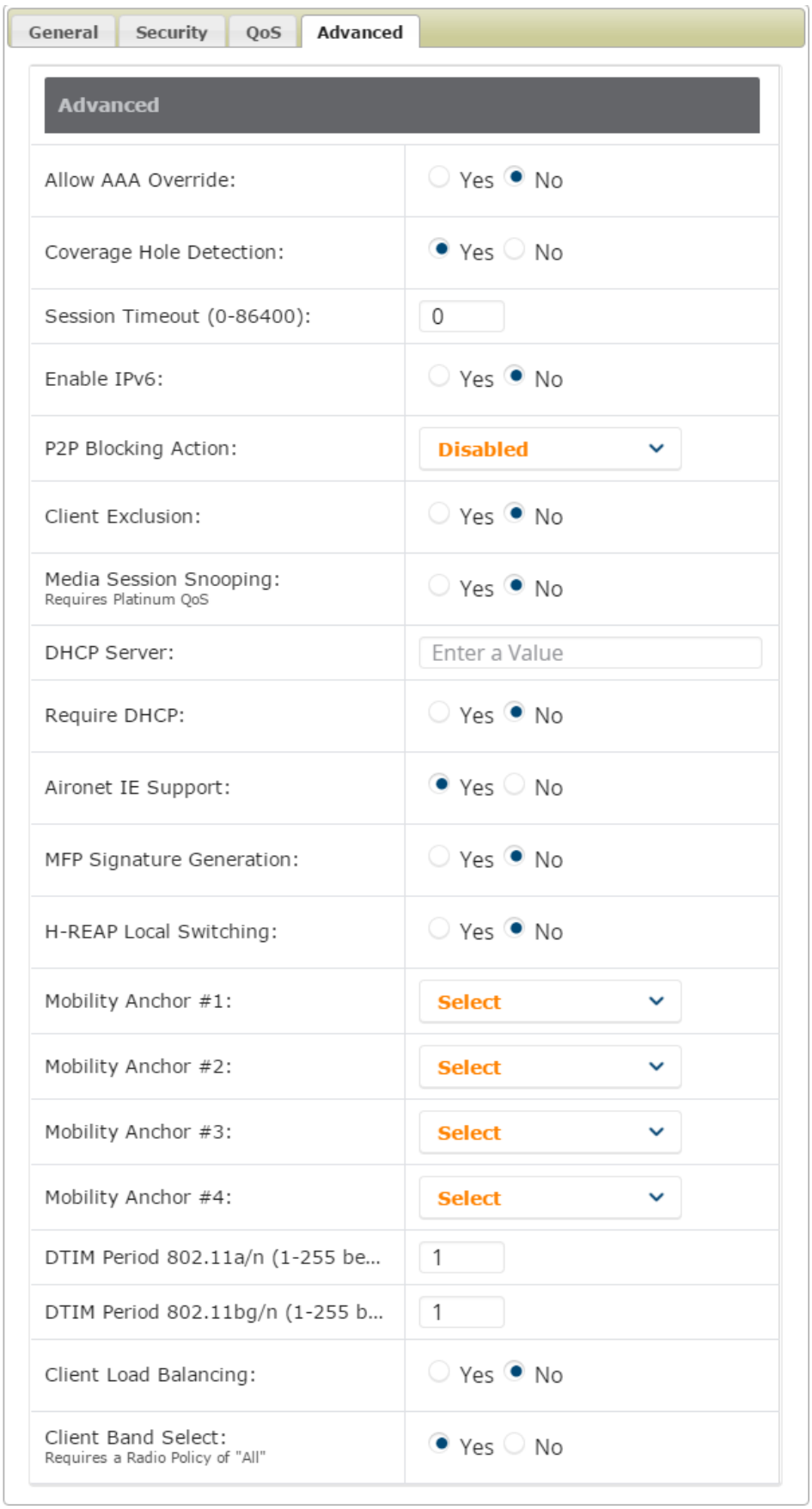


Figure 48: *Add New SSID/VLAN > Advanced Tab Illustration*



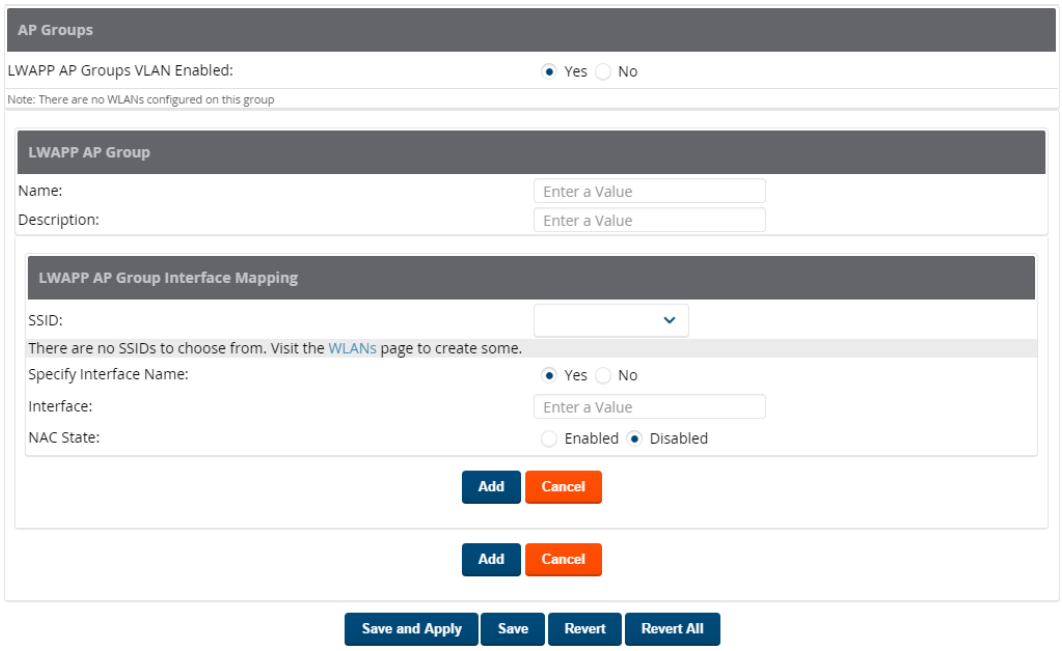
Defining and Configuring LWAPP AP Groups for Cisco Devices

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 49 illustrates this page.

Figure 49: *Groups > Cisco WLC Config > WLANS > Advanced > AP Groups Page Illustration*



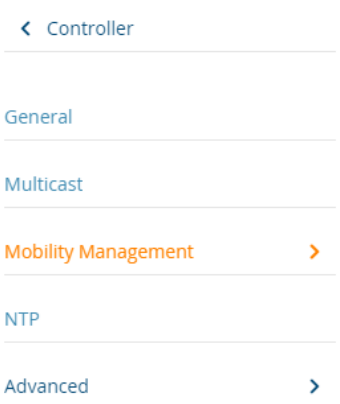
2. To add a new LWAPP AP group, select **Yes** in the **AP Groups** section. Additional controls appear.
3. Select **Add** to create a new LWAPP AP group. To edit an existing LWAPP AP group, select the pencil icon next to that group. Add one or more SSIDs and the interface/VLAN ID mapping on the **Add/Edit** 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 50.

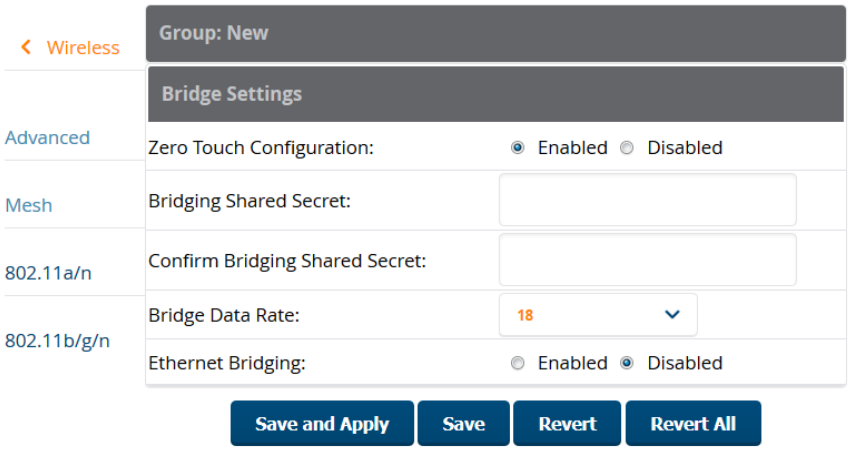
Figure 50: *Groups > Cisco WLC Config > Controller Navigation*



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 51.

Figure 51: *Groups > Cisco WLC Config > Wireless Navigation Illustration*



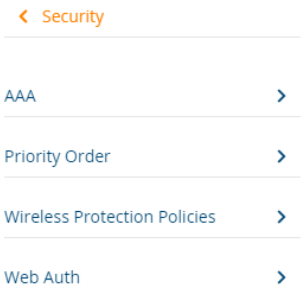
Configuring Cisco WLC Security Parameters and Functions

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**

Figure 52 illustrates these components and this navigation:

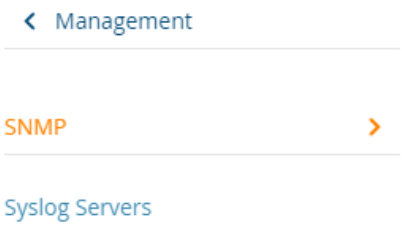
Figure 52: *Groups > Cisco WLC Config > Security Navigation Illustration*



Configuring Management Settings for Cisco WLC Controllers

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 53.

Figure 53: *Groups > Cisco WLC Config > Management Navigation Illustration*



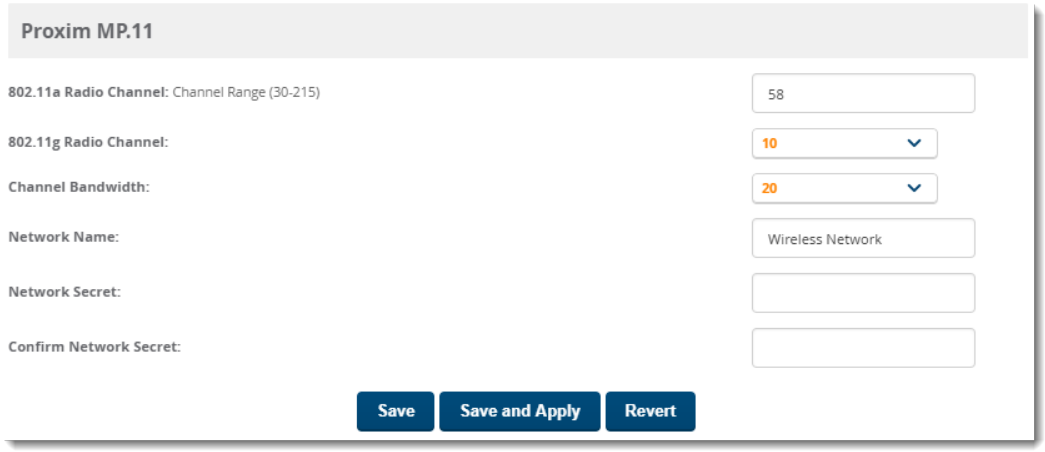
Configuring PTMP Settings for Device Groups

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.

To configure these functions:

1. Go to the **Groups > List** page and select 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** from the navigation sidebar. Figure 54 illustrates this page.

Figure 54: *Groups > PTMP Page Illustration*



3. Define the settings on this page. Table 63 describes the settings and default values.

Table 63: *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 later.

Configuring Proxim Mesh Radio Settings

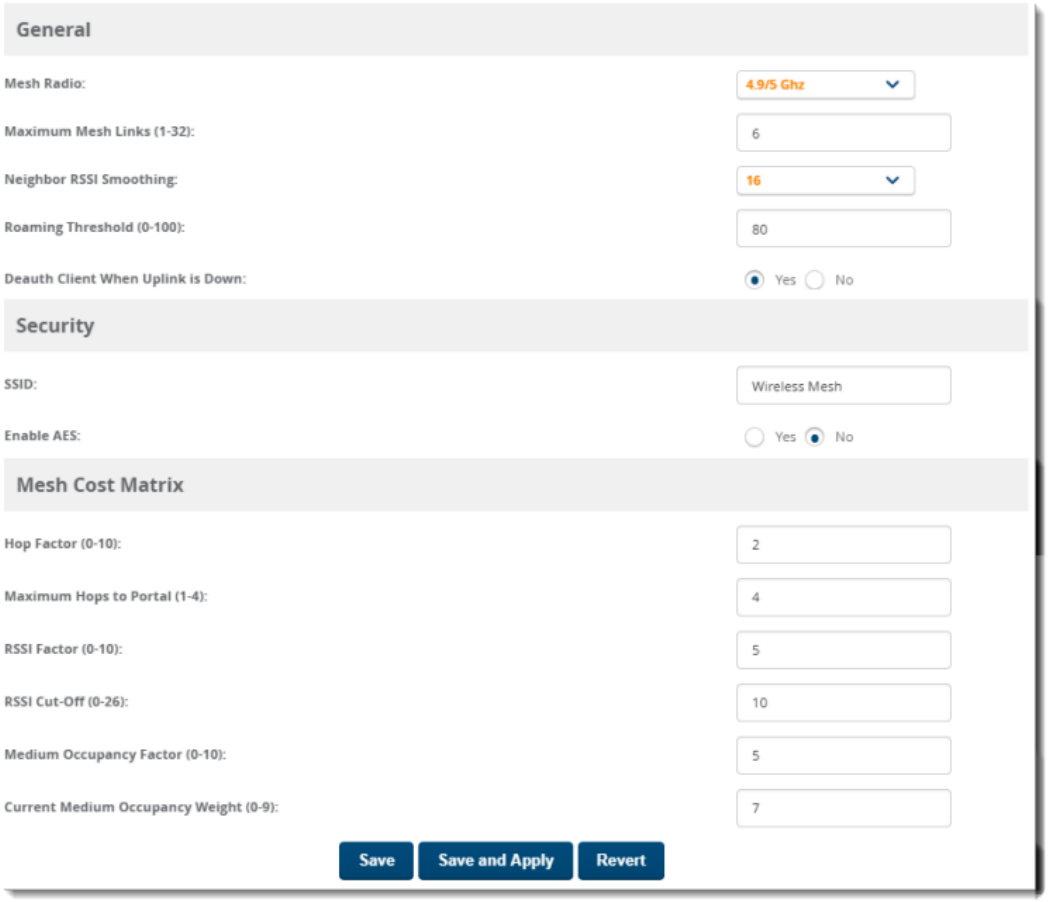
To configure mesh radio settings:

1. Go to the **Groups > Proxim Mesh** configuration page.
2. Define the settings as required for your network.
3. Do one of the following:

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

Figure 55 illustrates this page. The tables that follow describe the settings and default values.

Figure 55: *Groups > Proxim Mesh Page*



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

Table 64: *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 65: *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 66 describes these settings and default values.

Table 66: *Mesh Cost Matrix Fields and Default Values*

Setting	Default	Description
Hop Factor (1-10)	5	Sets the factor associated with each hop when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Maximum Hops to Portal (1-4)	4	Set the maximum number of hops for the AP to reach the Portal AP.
RSSI Factor (0-10)	5	Sets the factor associated with the RSSI values used when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
RSSI Cutoff (0-26)	10	Specifies the minimum RSSI needed to become a mesh neighbor.
Medium Occupancy Factor (0-10)	5	Sets the factor associated with Medium Occupancy when calculating the best path to the portal AP. Higher factors will have more impact when deciding the best uplink.
Current Medium Occupancy Weight (0-9)	7	Specifies the importance given to the most recently observed Medium Occupancy against all of the previously viewed medium occupancies. Lower values place more importance on previously observed Medium Occupancies.

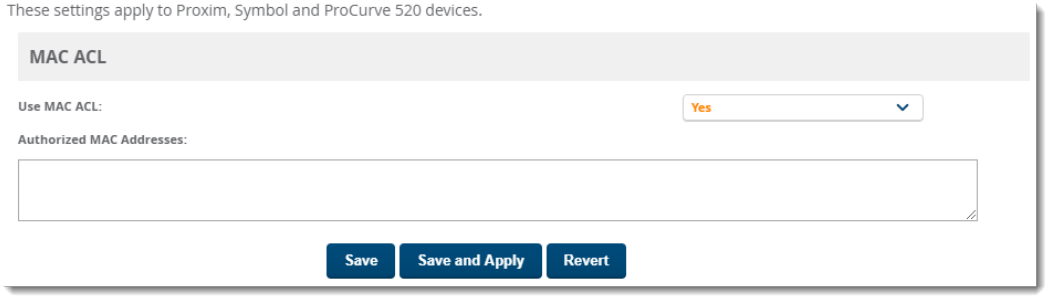
Configuring Group MAC ACLs for Device Groups

If you use Symbol, Proxim, or ProCurve 520WL wireless access points, you can 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.

To enable MAC ACL:

1. Browse to the **Groups > MAC ACL** configuration page. Figure 56 illustrates this page.

Figure 56: *Groups > MAC ACL Page*

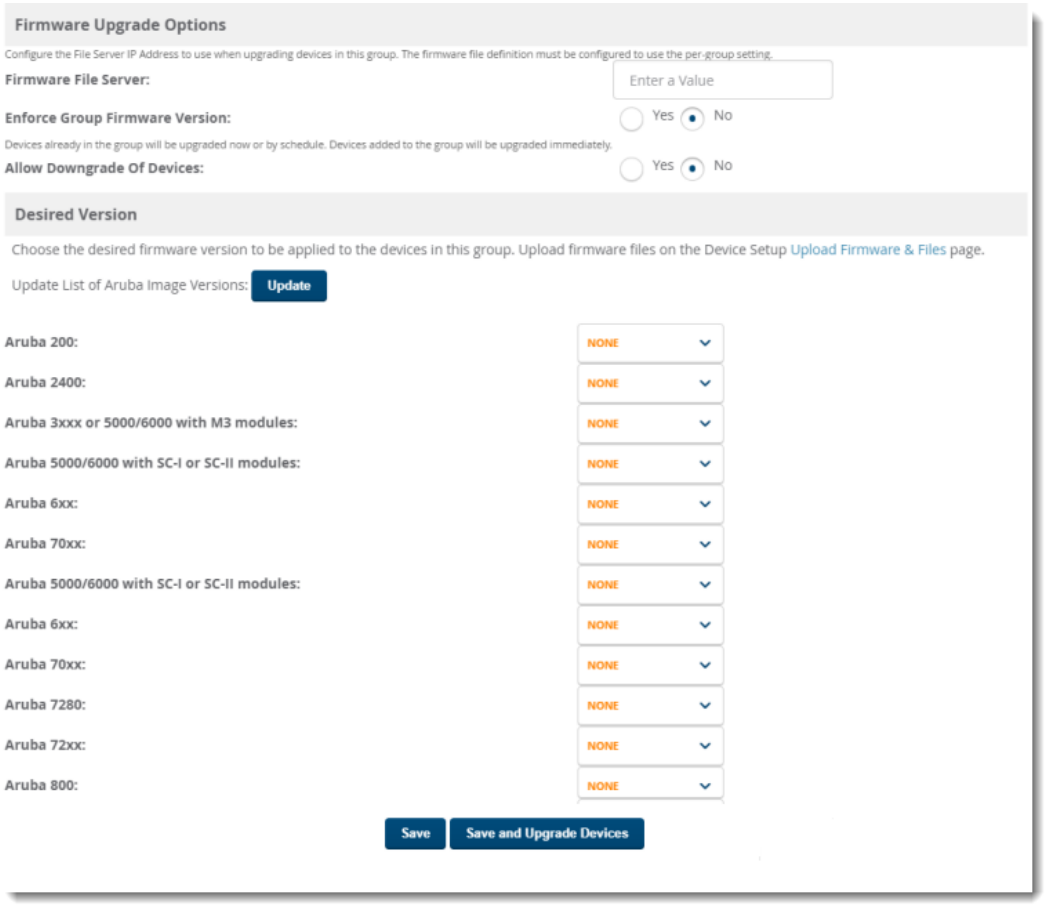


2. Select **Yes** on the **Use MAC ACL** drop-down menu.
3. Type all authorized MAC addresses, separated by white spaces.
4. Select **Save** when configurations are complete to retain these settings, or select **Save and Apply** to make the changes permanent. Alternatively, select **Revert** to cancel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

Specifying the Minimum Firmware Version for Device Groups

AirWave automatically upgrades all eligible devices in a device group when you set the minimum firmware version on the **Groups > Firmware** page. When you add devices to the device group later, you must upgrade the firmware on those devices manually.

Figure 57: *Groups > Firmware Page*



To set the minimum firmware version for a device group:

1. Navigate to **Groups > Firmware** .

2. For each device type in the group, specify the minimum acceptable firmware version. If no firmware versions are listed, go to **Device Setup > Upload Firmware & Files** to upload the firmware files to 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 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 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.

For more information about loading firmware on to an AirWave server, see "Uploading Firmware and Files" on page 57.

This chapter describes the steps you should perform after you have deployed AirWave on the network. The following sections describe:

How to Set Up Device Discovery

In order for 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.

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

This process includes:

Adding Networks for SNMP/HTTP Scanning

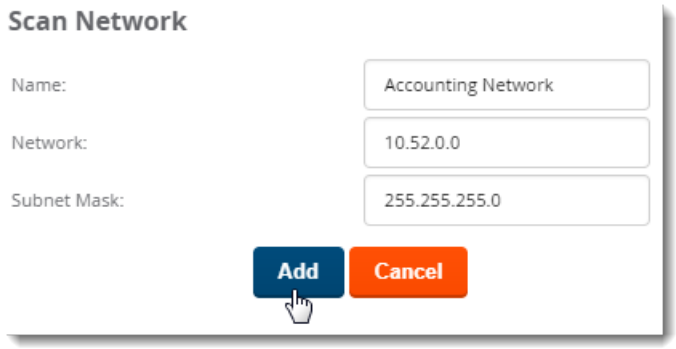
The first step when enabling SNMP/HTTP scanning for devices is to define the network segments to be scanned.

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 AirWave supports is 255.255.255.0.
6. Click **Add**.

Figure 58 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 58: *Adding a Scan Network*



AirWave displays all network segments in the **Network** section of the **Device Setup > Discover** page.

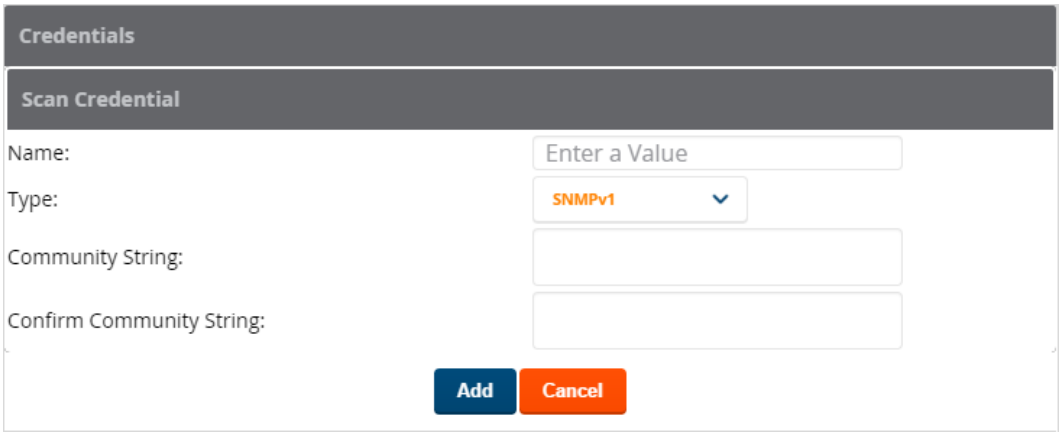
Adding Credentials for Scanning

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

Figure 59: *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 AirWave only uses it for discovering devices. To bring devices under management, 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

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" on page 132.

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. 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, "Running a Scan Set" on page 132.

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 discover these rogues without any special changes.

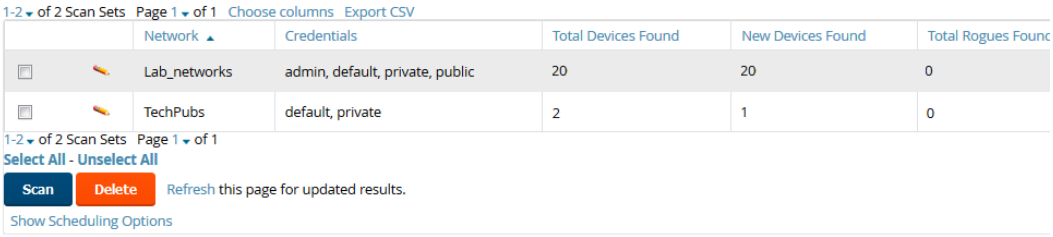
Running a Scan Set

Once a scan has been defined on the **Device Setup > Discover** page, 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 60 illustrates this page.

Figure 60: *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 67 describes the scan results and related information.

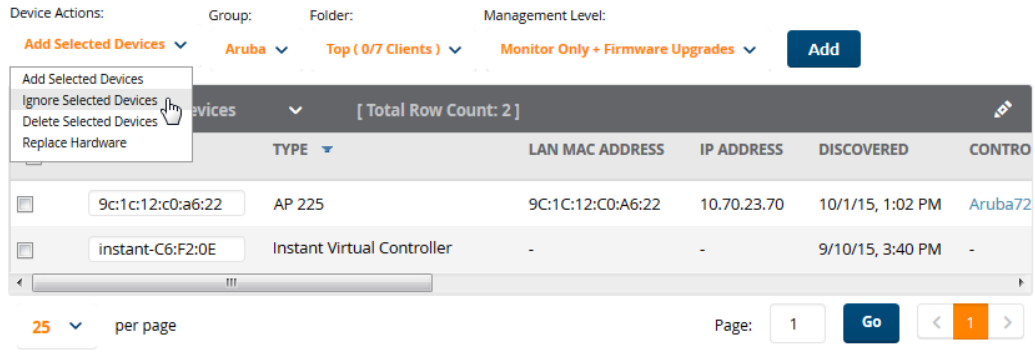
Table 67: *Device Setup > Discover > Discovery Execution Fields*

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 AirWave can configure and monitor. **Total** includes both APs that are currently being managed by 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 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 **Devices > New** page to see a full list of the newly discovered devices that the scan detected. Figure 61 illustrates this page.

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

Figure 61: *Devices > New Page Illustration*



The Cisco Discovery Protocol (CDP)

CDP uses the polling interval configured for each individual Cisco switch or router on the **Groups > List** page. 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.

Adding Devices into AirWave

If AirWave doesn't discover devices automatically, there are two methods of adding devices to AirWave. One is where you manually select your device type and model from the Add page. The other is where you bulk import devices from a CSV file.

Adding Devices Manually

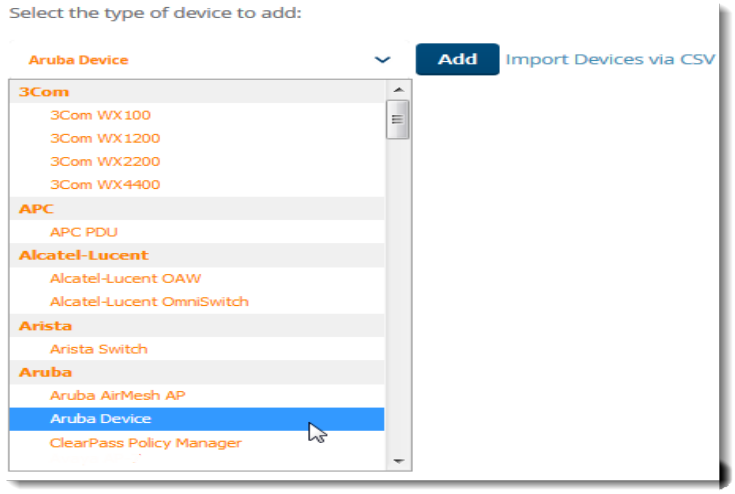
If AirWave doesn't discover devices automatically, you can manually add devices. When you add a Cisco or Aruba device, AirWave adds the make and model into its database. When you add a universal device, AirWave gets only basic monitoring information. If you don't provide SNMP credentials for the device, AirWave will monitor upstream switches, RADIUS servers, and other devices in the wired network using ICMP monitoring. Once you have added a universal device, you can view a list of its interfaces by navigating to **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. AirWave collects this information and displays it on the **Devices > Monitor** page in the **Interface** section. AirWave supports MIB-II interfaces and polls in/out byte counts for up to two interfaces. AirWave also monitors sysUptime.

To add a device into AirWave:

1. Log in to the AirWave with the following credentials:
   - Username: admin
   - Password: *admin password*.
2. Navigate to **Devices > New**, then click **Add**.
3. From the **Device Setup > Add** page, select the device from the drop-down menu.

Figure 62: *Selecting the Device*



4. Select **Add**.
5. From the Add page, enter the device communications settings and location settings. The configuration options on this page vary depending on the device. See Table 68 for information about each setting.

NOTE

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

6. At the bottom of the page, set the device management mode to **Monitor Only** or **Management read/write**.

NOTE

If you select **Manage read/write**, 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. For more information, see "Setting the Management Mode" on page 137.

7. Select **Add** to finish adding the device to the network.

Table 68 describes the settings on the Add Page.

Table 68: *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). AirWave supports IPv4 and IPv6 addresses.
SNMP Port	161	The port AirWave uses to communicate with the AP using SNMP.
SSH Port	22	For devices that support SSH, specify the SSH port number.

Table 68: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
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.
SNMPv3 Username	Taken from **Device Setup > Communication**	User name of the SNMP v3 user on the controller. 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. AirWave initially uses this user name and password combination to control the Cisco AP. 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. 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. AirWave currently only supports authentication and encryption.
SNMPv3 Auth Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 auth protocol, either MD5 or SHA-1.
SNMPv3 Privacy Protocol	Taken from **Device Setup > Communication**	Specifies the SNMPv3 Privacy protocol as either DES or AES. This option is not available for all devices.
Telnet/SSH Username	Taken from **Device Setup > Communication**	Telnet user name for existing Cisco IOS APs. 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. 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.

Table 68: *Device Communication and Location Fields and Default Values (Continued)*

Setting	Default	Description
enable Password (Confirm)	Taken from **Device Setup > Communication**	Password that allows AirWave to enter **enable** mode on the device.

Adding Devices from a CSV File

You can use a CSV file to bulk add devices to AirWave. If you specify the vendor name, AirWave automatically determines the correct type while bringing up the device. If your CSV file includes make and model information, AirWave will add the information provided in the CSV file as it did before. AirWave will not override what you have specified in this CSV file in any way.

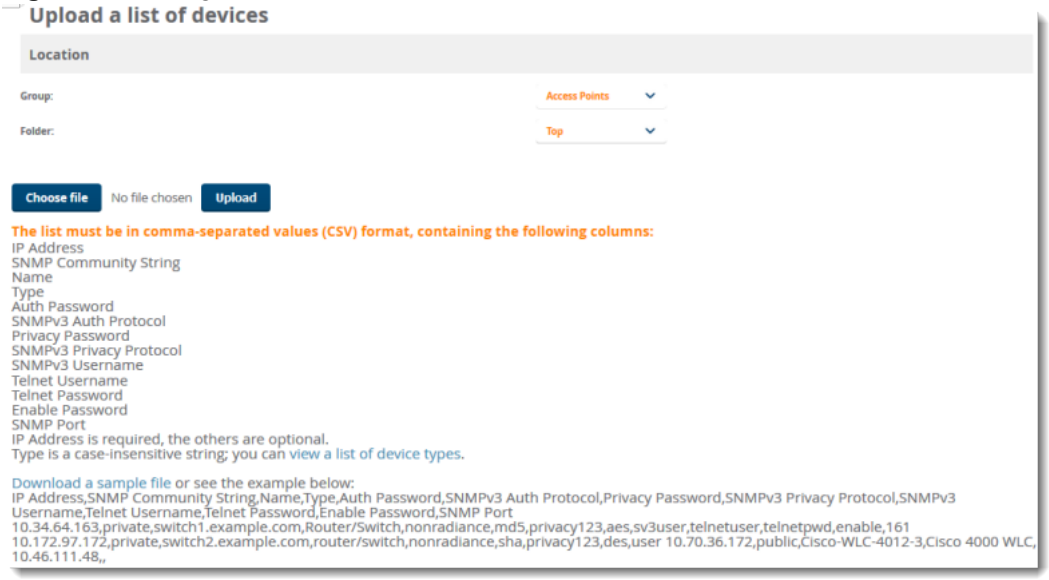
NOTE

Use the example provided on the bottom of the page, or click the blue "Download a sample CSV file" link to save the sample as a CSV file and edit the contents with an external application.

To import a CSV file:

1. From the **Device Setup > Add** page, click the blue **Import Devices via CSV** link. The **Upload a list of devices** page displays. See Figure 63.

Figure 63: *Adding Devices from CSV File*



2. Select a group and folder into which to import the list of devices.
3. Click **Choose File** to select the CSV file on your computer.
4. Click **Upload** to add the devices from the list into AirWave.

Setting the Management Mode

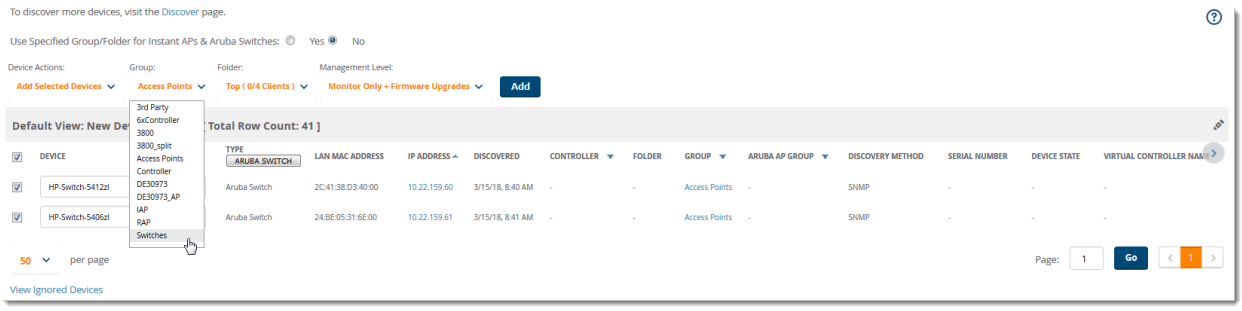
After AirWave discovers devices on your network, you need to add the devices to a group and set the management mode to **Monitor Only** to avoid overwriting important configuration settings. In this read-only mode, AirWave monitors the device, updates the firmware, compares the current configuration with the policy, and displays any discrepancies on the **Devices > Device Configuration** page. For information about device groups, refer to "Using Device Groups" on page 81.

NOTE

Placing newly discovered devices in Monitor Only mode is strongly recommended until you can confirm that all group configuration settings are appropriate for the devices. Change the management mode to **Manage Read/Write** when you are ready to push configuration changes to the devices in the group.

To put newly discovered devices into a group and set the management mode:

1. Navigate to **Devices > New**, then click to the newly discovered devices.



2. Select the group and folder to which the device will be added. You can't add devices to a global group.
3. Select **Monitor Only + FirmWare Upgrades** from the Management Level drop-down menu, then select **Add**.
4. From the **Devices > List** page, select the folder that contains one or more devices to verify that your device has been properly assigned.

Verifying the Device Configuration

When you have placed a newly discovered device in to a group and set the management mode to Monitor Only, the next step is to check the device configuration status. Determine whether AirWave will apply changes to the device if you change the management mode to **Manage Read/Write**.

AirWave uses SNMP or Telnet to read a device's configuration. SNMP is used for Cisco controllers. Aruba devices and wired routers and switches use Telnet/SSH to read device configuration. See "Individual Device Support and Firmware Upgrades" on page 233 for more details.

To verify the device configuration status:

1. Navigate to the **Devices > List**, then locate the device in the Device list.
2. Check the configuration status in the Configuration column:
   - indicates that the device is in **Monitor Only** mode. AirWave won't make any device configuration changes.
   - **Good** indicates that all of the device's current settings match the group policy settings. AirWave won't make any changes to the device configuration when the management mode changes to **Manage Read/Write**.
   - **Error** indicates that there is a problem with the device configuration. Click the blue **Error** link to access the Device Configuration page and review the error.
   - **Mismatch** indicates that at least one of the device's current configuration settings doesn't match the group policy. AirWave will push configuration changes to the device when the management mode changes to **Manage Read/Write**.
3. If there is a configuration mismatch, from the Device Configuration page, click the blue **Error** link toview the device configuration settings and it with the group configuration. When the device management mode is set to **Manage Read/Write**, the settings on the right side of the Compare Configurations page will be pushed to the device.

4. 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 move the device to another group.

Ignoring Discovered Devices

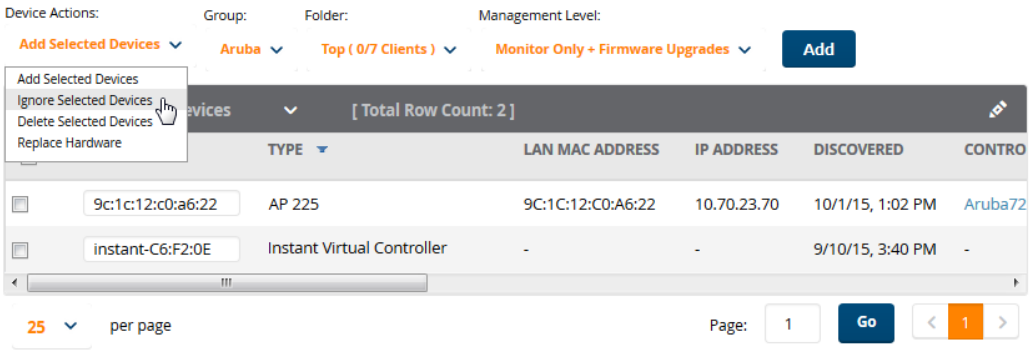
You might want to ignore a discovered device. If you know that the device will be down temporarily, you can add it to the ignore list and then remove it from the ignored list when it is online again.

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

To ignore a device:

1. Go to the **Devices > New** page.
2. Select the checkbox beside the device, and then select **Ignore Selected Devices** from the drop-down menu (see Figure 64. You can select more than one at a time.

Figure 64: *Devices > New Page Illustration*

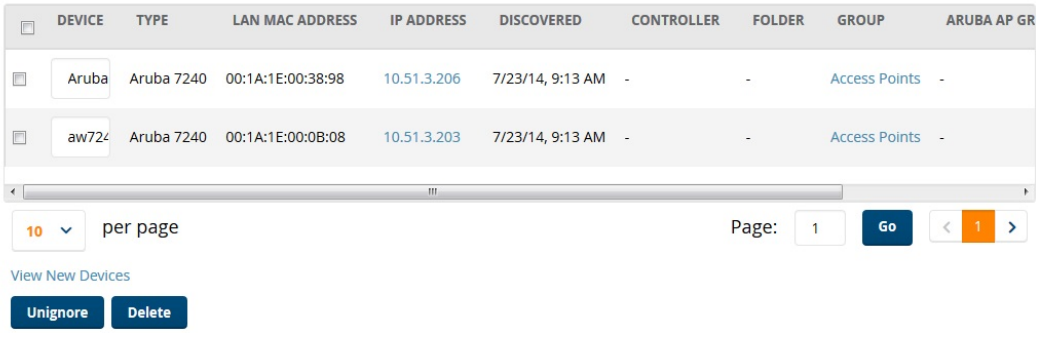


Unignoring a Device

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

1. To view all devices that are ignored, go to the **Devices > Ignored** page, illustrated in Figure 65.

Figure 65: *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 AirWave so that it appears on the **Devices > New** list.
4. The **Unignore** button will either return the device to its regular folder or group or send it to the **Devices > New** page.

Troubleshooting a Newly Discovered Down Device

If the device status on the **Devices > List** page remains **Down** after being discovered and added to a group, there is usually an error in the SNMP community string used to manage the device.

To troubleshoot a down device:

1. Go to the **Devices > List** or the **Devices > Down** page, then click the **Name** of the down device to access the device monitoring page.
2. Locate the **Status** field in the **Device Info** section. When the device is down, the status includes a description of the problem.

A device might be down for any of the discovery issues described in Table 69.

Table 69: *System Messages for Discovered, Down Devices*

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 AirWave server). Either the AP was removed from the controller, or it has roamed to another controller that AirWave does not have visibility to, or it is offline.
Controller is Down	When a controller goes down, AirWave automatically marks all associated thin APs down. This is because communication to thin APs are via the controller, and AirWave assumes that if the Controller has gone offline, then all associated APs are down as well until they are re-associated with another Controller.
Downloading	The AP is in the process of downloading firmware or configuration. **NOTE:** Applicable to Cisco WLC thin APs and some Symbol APs.
Error fetching existing configuration	AirWave could not fetch a configuration for the device. Usually this is because 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 AirWave.
SNMP Trap	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.

Table 69: *System Messages for Discovered, Down Devices (Continued)*

Message	Meaning
Unexpected LAN MAC Address found at this device's IP address	If 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 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 **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.

To view the detailed status of all your down devices at once, navigate to **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 **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 **Devices > Manage** page. Enter the appropriate credentials, and select **Apply**.
5. Return to the **Devices > List** page to see if the device appears with a Status of **Up**.

With ZTP Orchestrator, you can configure your network settings without having to log in to each Aruba device. After completing the initial configuration, you can begin to discover and deploy Aruba access devices.

Before You Begin

The following information helps you prepare to use ZTP Orchestrator for the first time:

- **Credentials required for ClearPass**. Gather network information, such as the ClearPass Policy Manager API client, RADIUS shared secret, and Downloadable User Role (DUR) credentials. The API Client and dynamic segmentation policies need to be created on ClearPass server beforehand. For instructions, refer to the *ClearPass Guest User Guide* and the *ClearPass Policy Manager User Guide*.
- **Path required for Mobility Master node configuration**. Determine the path for creating the Mobility Master node hierarchies.
- **Mobility Master and ArubaOS-CX switch configuration**. Configure Mobility Master and Aruba OS-CX Switches before you work with ZTP Orchestrator.

Minimum Requirements

In order to use ZTP Orchestrator, your access components must meet the following requirements:

- ArubaOS-CX Switches must be running firmware version 10.02.0031 or later.
- ArubaOS-S Switches must be running firmware version 16.08.002 or later.
- Aruba Mobility Master appliances must be running ArubaOS 8.5.0.0 or later.
- ClearPass appliances must be running ClearPass Policy Manager 6.7 or later.

Create ZTP Groups and Add Access Components

Use ZTP Orchestrator to integrate all the access components in your network.

1. "Create Groups for ZTP" on page 142
2. "Add ClearPass Policy Manager" on page 143
3. "Add Mobility Master" on page 144
4. "Add the ArubaOS-CX Switch" on page 144

Create Groups for ZTP

Group same device types together to simplify how you navigate ZTP Orchestrator, select devices, and access information. For smaller campus networks, you create a group of mixed device types.

To create a ZTP group:

1. Log in to the AirWave WebUI as an administrator, then go to **Device Setup > ZTP Orchestrator**.
2. From the **Network Setup** tab, click **Add/Edit Group**.
3. In the **Groups** window, enter the following settings:
   - **Name**. The name of the ZTP group.
   - **Community String/Confirm Community String**. The password that allows device access. You can use upper case letters, lower case letters, numbers, and special characters. You can't include spaces.
   - **SSH Username**. The username used to securely log in to the device.

- **SSH Password**. The password used to authenticate a secure connection to the device.

4. Select the type of device that ZTP Orchestrator will add to the group: Mobility Controllers, ArubaOS-S Switches, or both.

   For Mobility Controllers, enter the following information:

   - **MM node path**. ZTP Orchestrator creates this node path for up to three levels after **/md** (for example, **/md/sjc/sc/floor1**). You can't create multiple groups within the same hierarchy.
   - **User VLAN range**. Defines the range of VLANs, from 2 to 4092.
   - **Management VLAN ID**. The management VLAN used to manage your devices. The default is **1**.

Figure 66:

   For ArubaOS-S Switches, enter the following information:

   - **AP VLAN ID**. The ID number assigned to all access points in a VLAN.
   - **Syslog Server**. The IP address of the syslog server.
   - **NTP**. The IP address or hostname of the NTP server.
   - **Management VLAN ID**. The ID number of the management VLAN.
   - **DNS Name.** The DNS domain name.
   - **DNS IP**. The IP address of the DNS server.

5. Click **Save**.

Add ClearPass Policy Manager

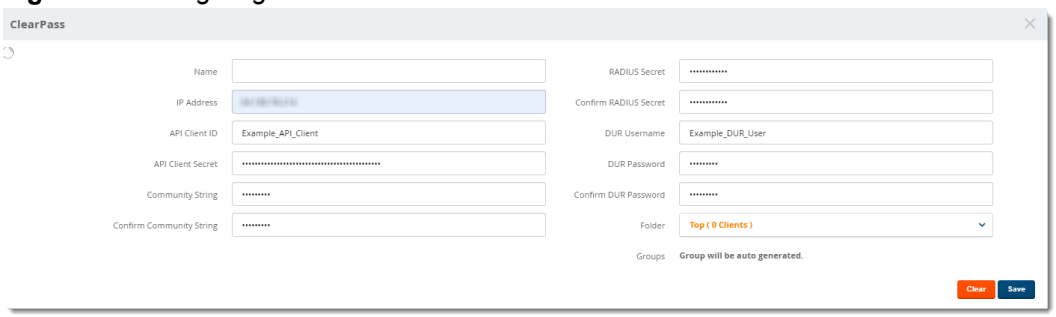
In this step, add Clear Pass Policy Manager (CPPM) as a RADIUS server to authenticate devices. CPPM will also push policies for dynamically segmented clients to access the devices.

ZTP Orchestrator works with standalone CPPM servers. ZTP Orchestrator does not support CPPM clusters.

To add CPPM :

1. In the **Network Setup** tab, click **Add ClearPass**.
2. In the **ClearPass** window, enter the following information:
   - **IP address**. The IP address of the ClearPass server.
   - **API Client ID**. The client ID used to log in to the ClearPass API Client.
   - **API Client Secret**. The client password used to access the ClearPass API Client.
   - **Community string/Confirm Community String**. The password used by CPPM to allow access to the ClearPass server.
   - **RADIUS Secret/Confirm RADIUS Secret**. The password used by CPPM to connect devices to the RADIUS server.
   - **Downloadable User Role (DUR) credentials**. The credentials used to access device attributes in DURs.
3. Click the Folder drop-down menu to add the group to an AirWave folder.
4. Click **Save**.

Figure 67: *Configuring CPPM*



Add Mobility Master

In this step, add the Mobility Master that maintains and manages the configurations for a Mobility Controller to AirWave.

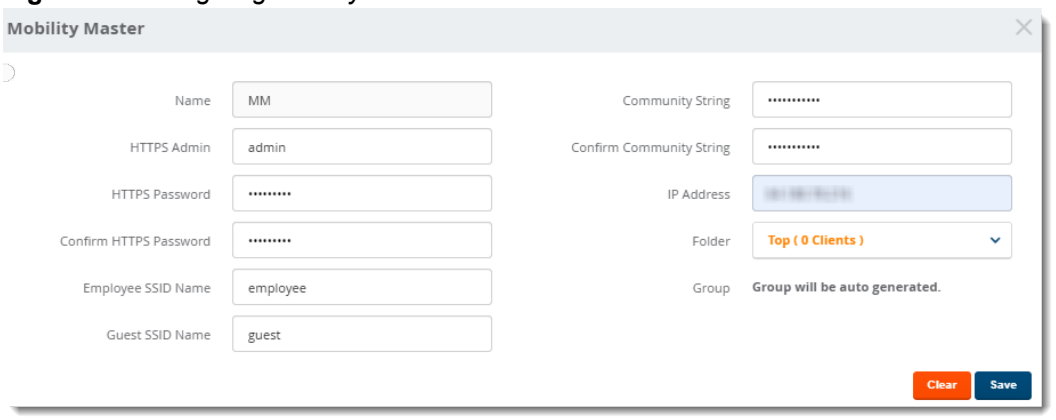
NOTE

You must add each Mobility Master server using ZTP Orchestrator. The Mobility Master servers will be added to an auto-generated group named "ZTP Orch. Mobility Master".

To add the Mobility Master server:

1. In the **Network Setup** tab, click **Add Mobility Master**. The Mobility Master window displays with required fields outlined in red.
2. Enter the following information, as shown in Figure 68:
   - **HTTPS Admin**. The user name for admin login.
   - **HTTPS Password**. The password for admin login.
   - **Community string**. The SNMP community string used to authenticate access to the Mobility Master.
   - **IP Address**. Static IP address assigned to the Mobility Master.
3. Click the **Folder** drop-down menu to add the group to an AirWave folder.

Figure 68: *Configuring Mobility Master*



4. Click **Save**.

Add the ArubaOS-CX Switch

In this step, add the ArubaOS-CX switches, which are the core and aggregation switches in the network, to AirWave.

NOTE

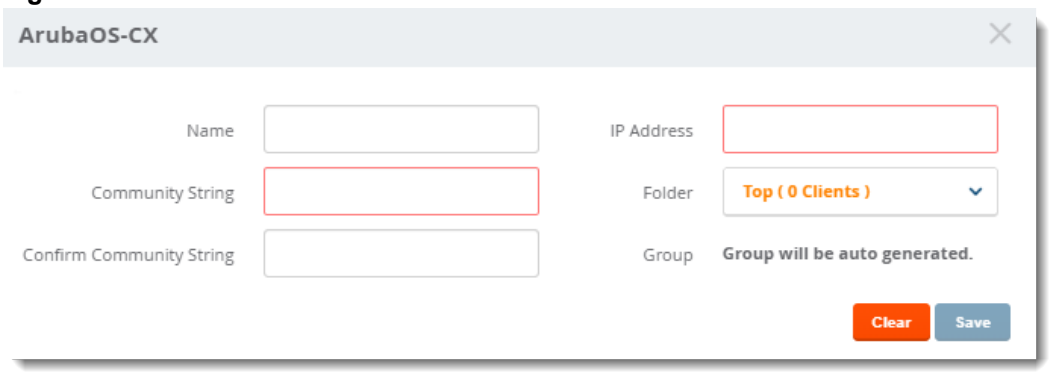
If you add two ArubaOS-CX Switches individually and they are an aggregation pair, AirWave will later show them

as a pair on the **Discover/Deploy** tab. The ArubaOS-CX Switches will be added to an auto-generated group named "ZTP Orch. ArubaOS-CX".

To add the ArubaOS-CX switches:

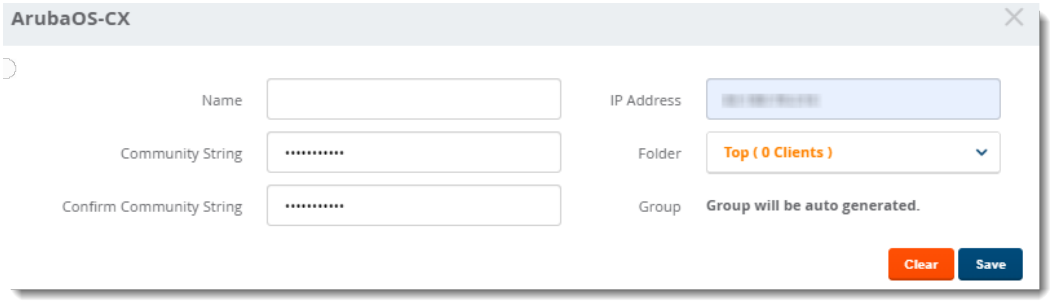
1. In the **Network Setup** tab, click **Add Mobility Master**. The ArubaOS-CX window displays with required fields outlined in red.

Figure 69: *ArubaOS-CX Window*



2. Enter the following information:
   - **Community string**. The SNMP community string used to authenticate access to the ArubaOS-CX switch.
   - **IP address**. The IP address assigned to the ArubaOS-CX switch.
3. Click the **Folder** drop-down menu to add the group to an AirWave folder.

Figure 70: *Adding ArubaOS-CX*



4. Click **Save**.

Deployment Workflow

After setting up the network, click the **Discover/Deploy** tab at the top of the page to begin on-boarding the access devices. First, you discover the access devices and then make bulk changes that include assigning the access devices to groups, folders, and, in the case of access switches, Mobility Controllers.

1. "Deploying Mobility Controllers" on page 145
2. "Deploying ArubaOS-S Switches" on page 146

Deploying Mobility Controllers

In this step, discover and then deploy Mobility Controllers. You must on-board Mobility Controllers first in order for you to connect access switches to deployed Mobility Controllers in "Deploying ArubaOS-S Switches" on page 146.

Follow these steps to discover and deploy Mobility Controllers:

1. Select **Mobility Controller** for the **Choose Device Type** option.
2. Click **Discover**. AirWave discovers Mobility Controllers using LLDP and learns which ports on the Mobility Controllers are connected to the ArubaOS-CX Switch.
3. Click to edit parameters for each Mobility Controller that you will deploy. Ensure that the IP address is correct and a static IP address. Other parameters include the name, MAC address, netmask, gateway address, folder, group, and MM node path.
4. If you changed any parameters in the **Mobility Controller** window, click **Save**. After all the Mobility Controllers are configured with a static IP address, proceed to the next step.
5. Click the check box at the top left corner of the device list to select all, or manually select the devices, then click **Deploy**.

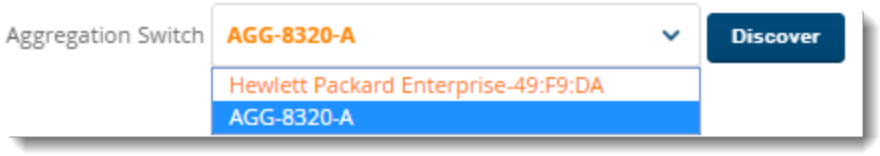
Deploying ArubaOS-S Switches

In this step, you discover and deploy ArubaOS-S Switches. When deployed, AirWave sets the management mode for the access switches to **Manage/Read-Write**.

To deploy ArubaOS-S Switches:

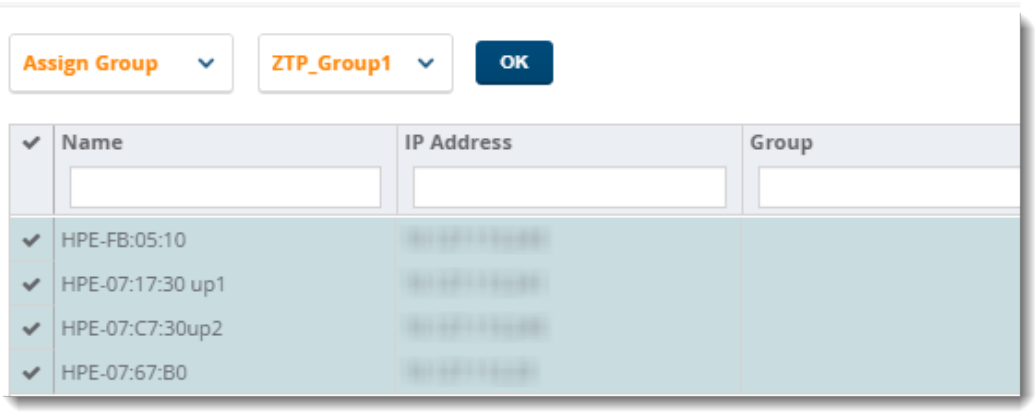
1. At the top of the page, select **ArubaOS-S Switch** for the **Choose Device Type** option.
2. Select the switch from the **Aggregation Switch** drop-down menu.

Figure 71: *Aggregation Switch Selection*



3. Click **Discover**. In this step, AirWave discovers the access switches using LLDP and learns which ports on the access switches are connected to the ArubaOS-CX Switch.
4. You can click to edit parameters for each access switch that you will deploy, including:
   - **Name**. The name of the ArubaOS-S Switch.
   - **Mobility Controller**. The Mobility Controller that provides the user-based tunneling.
   - **Folder**. The name of the device folder the switch is organized in.
   - **Group**. The name of the ZTP group the switch belongs to for configuration management.
5. If you changed any parameters in the **ArubaOS-S Switch** window, click **Save**.
6. Click the check box at the top left corner of the device list to select all, or manually select the devices; then do the following steps:
   a. Assign the access switches to a ZTP group by selecting **Assign Group** and the ZTP group from the drop-down menus, and then click **OK**.

Figure 72: *Adding Access Switches to a ZTP Group*



b. Assign the access switches to a folder by selecting **Assign Folder** and the folder from the drop-down menus, and then click **OK**.
c. Connect the access switches to the Mobility Controller by selecting **Connect to MC** and the Mobility Controller from the drop-down menus, and then click **OK**.
d. Click **Deploy**, then click **OK**.

Automated Workflow

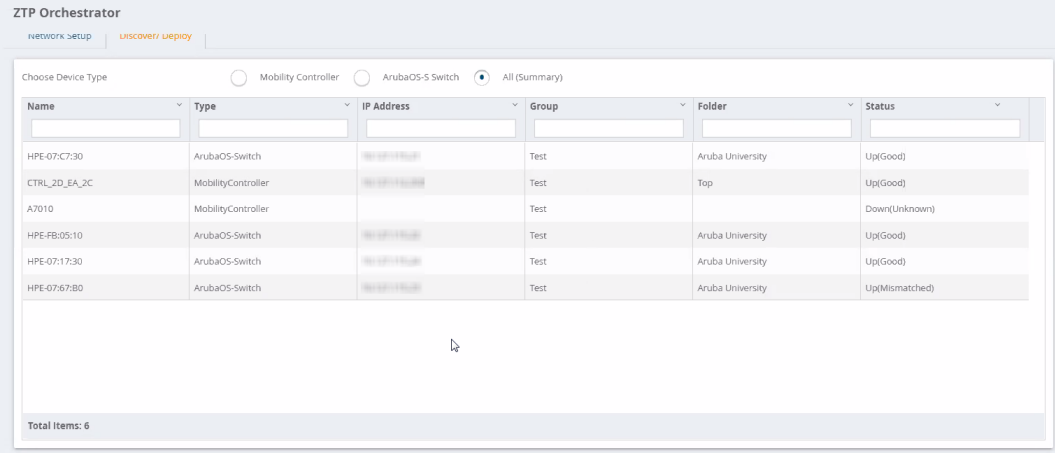
Now that you've launched the deployment, AirWave performs the following tasks:

- Push Mobility Controller details to Mobility Master so that Mobility Master can push configurations to the Mobility Controller using ZTP
- Whitelist the access switch in ClearPass after Mobility Controller configurations synch successfully with Mobility Master
- Connect factory-default access switch to LAG configured Aruba OS-CX aggregation switch. Aruba OS-CX switch uses LLDP to gather information about the access switch and sends the details to AirWave
- Generate the configuration template with LAG and user-based tunneling (UBT) configurations for the access switch
- Whitelist the access switch in ClearPass after the access switch configuration synchs successfully with AirWave

Deployment Verification

You can view deployment status updates in real-time on the **Discover/Deploy** tab by clicking **All (Summary)**. The information displayed clears after 24 hours.

Figure 73: *Deployment Summary*



NOTE

Groups displayed on the **Network Setup** tab include groups added from the **Groups > List** page.

Post Deployment

After ZTP Orchestrator on-boards a device, AirWave updates the device count in the header statistics at the top of the WebUI, as well as the **Device > List** page. New devices can be managed and monitored using AirWave and will be visible in the topology map.

Clients can start connecting to the newly deployed access switches, and all the devices will be dynamically segmented. You can monitor segmented traffic from the **Home > Traffic Analysis** page.

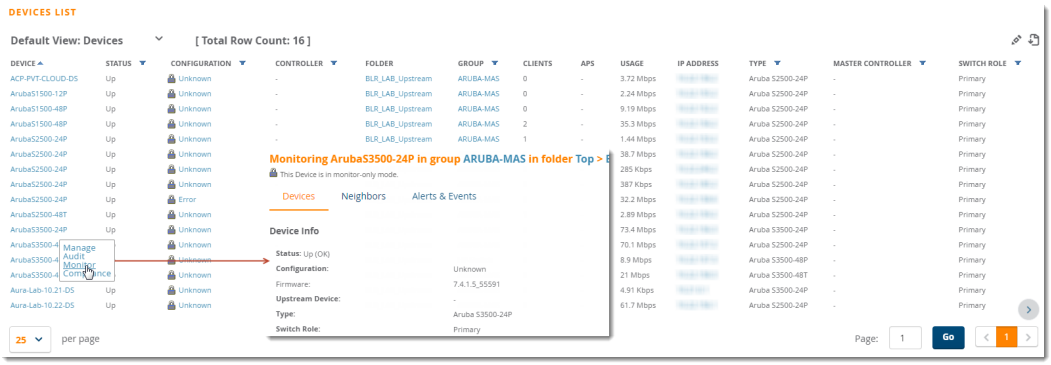
AirWave provides an easy-to-use interface that lets you monitor your entire access infrastructure. When you click a device link from the device list, you can view the monitoring page for the device.

The following sections discuss various monitoring options in AirWave:

Monitoring Basics

You can find the monitoring page by navigating to **Devices > List** and selecting a device from the list. Or, you can hover the pointer over a device and click Monitor from the shortcut menu, as shown in Figure 74.

Figure 74: *Opening the Monitoring Page for a Device*



Here are some of the things you can view on or from the **Devices > Monitor** page:

- Device Information. The information displayed varies depending on the device type. See "Device Information for Access Points, Mesh Devices, and Controllers" on page 154 or "Device Information" on page 173. The graphs on the **Devices** tab show historical data and help you identify trends and anomalies. When you hover the pointer over a graph, a detailed pop up view displays. See "Graphs for Access Points, Mesh Devices, and Controllers" on page 158 and "Graphs" on page 174.
- Detailed summary tables. Click the **Neighbors** tab to access the summary tables for neighbor devices. You can also click the **RF Neighbors** tab to monitor the nearest RF neighbors of an access point and the physical and virtual interfaces on a switch. For information, see "Monitoring Access Points, Mesh Devices, and Controllers" on page 154 and "Detailed Summary Tables" on page 174, respectively.
- Alerts and events. Click the **Alerts & Events** tab to access the alert tables about AirWave, Intrusion Detection System (IDS), RADIUS accounting, and RADIUS authentication issues. For information about alert summaries, see "About Alerts" on page 320. The **Alerts & Events** tab also displays the event tables for device events and recent AMP device events. These tables also appear on the **System > Event Log** page. To learn more about these events, see "Using the Event Log" on page 308.

From the **Devices > Monitor** page, you can:

- Use Quick Links. Open the WebUI for a controller in a pop up window, or run a command on a device. For example, use the **show stacking members** command to verify the switches in a stack or the **AP LED Blinking Enable** command to flash the LEDs on an AP.
- Locate a device. Search by typing the IP address, name, version, or other information. Results include hypertext links to additional pages.
- Poll the device. Override the preset polling interval by clicking Poll Now in the top right corner of the page. AirWave refreshes all but rogue data. For information about polling multiple devices, see "Poll selected devices" on page 91.
- Authenticate rogue devices found on wired networks. Look for unauthenticated devices in the **Connected Devices** tables, then acknowledge them by modifying editable fields. Learn how to do this in "Monitoring ArubaOS-CX and Mobility Access Switches" on page 173.
- Diagnose issues. Go to the **Clients > Diagnostics** page, where you can check for network status, location, trends, and alerts. Find more information about "" on page 215.
- Monitor a network interface for a wired device. Find more information about "Interfaces" on page 177.
- Go to Topology by clicking  in the upper-right corner of the monitoring page to monitor or troubleshoot a device or switch interface from the topology map. For more information, see "Using Topology" on page 286.

Customizing the Monitoring Page

You can adjust how much information displays in your tables, then filter the results. You can also categorize information using groups.

First 25 Results

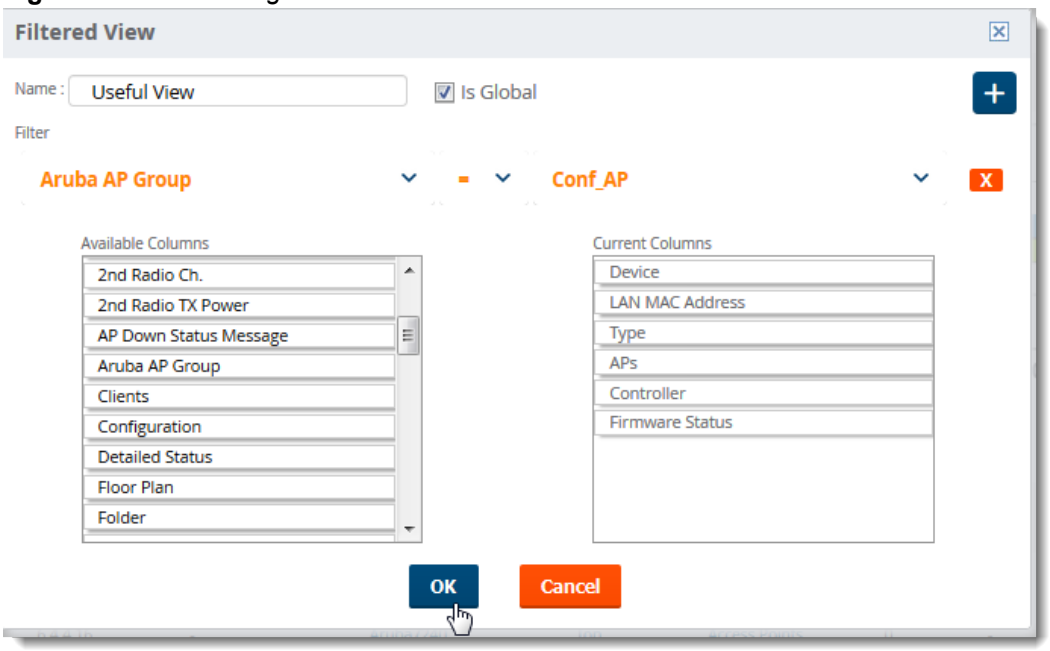
AirWave displays only 25 rows of information. To display a different number of entries per page, click and select 10, 25, 50, 100, 250, or 500. Longer page lengths require more time for the page to load.

Creating Filtered Views

To create a new filtered view:

1. Navigate to a page that contains a default view list, such as **Devices > List** or **RAPIDS > List**.
2. In the Devices List, select **New View** from the Default View drop-down menu to create a filtered view.
3. In the **Name** field, type the name for the filtered view.
4. If you want to give all users access to the filtered view, select **Is Global**. Only Administrators can edit global filtered views.
5. Click  to add device groups to the filtered view, or  to remove them.
   a. Scroll the list of parameters and select a **Device** or **Radio** parameter.
   b. If required, enter search parameters such as "=" to refine the filter parameters.
   c. To create a filtered view with multiple filter parameters, click **Add Filter** again and define any additional filter parameters. For example, to create a view that displays APs with more than zero clients but less than five clients, you would need to create one filter with the parameters **Clients > 0**, and a second filter with the parameters **Clients < 5**.
6. Drag and drop data columns from the **Available Columns** list to the **Current Columns** list to select which columns display in the view. You can reorder the columns in the **Current Columns** list by dragging and dropping the data column to a different place in the list.

Figure 75: *Customizing the View*

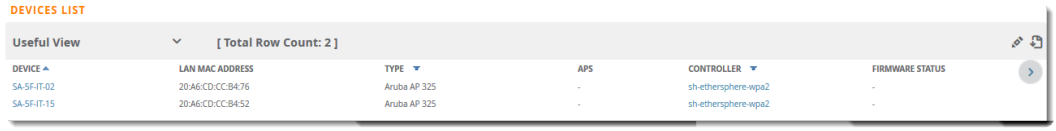


7. Click **OK**.

Figure 76: *Creating a Filtered View*

The Devices List displays the new filtered view.

Figure 77: *New Filtered View*



Editing Filtered Views

You can edit a custom filtered view at any time, by selecting the view in the view list, then selecting the ⚙ icon and modifying filter parameters and column displays.

Table 70: *Filter icons*

Icon	Description
+	Click this icon to create a custom filtered view.
⚙	Click this icon to edit an existing custom filtered view.
⧉	Click this icon to clone a filtered view.
🗑	Click this icon to delete a custom filtered view.

Showing Filters, Clearing Filters, Resetting Grouping

To change how AirWave displays data, 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 Show Filters to add parameters to the table view.
- Click Clear Filters to remove filters and return to the default table view.
- Click Reset Grouping if you no longer want to group capabilities in the table view.

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 devices AirWave users can see, or the devices that AirWave loads in Topology.

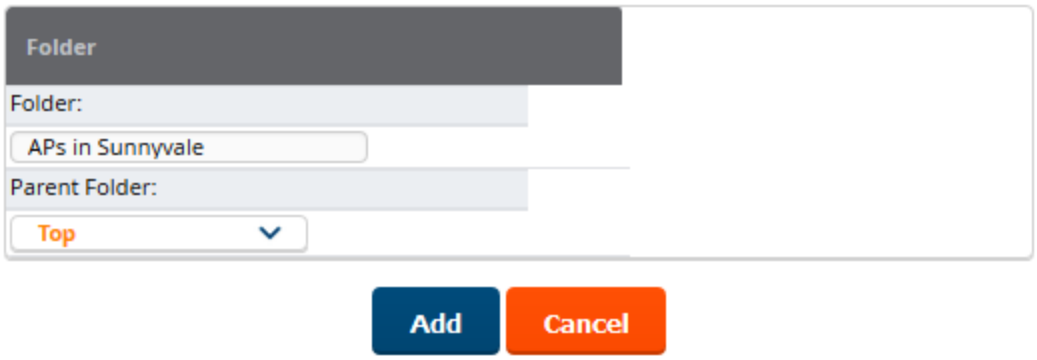
Adding Device Folders

To add a device folder:

1. Go to **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 78 shows how to create the *APs in Sunnyvale* folder.

Figure 78: *Adding a New Folder*



Moving Folders

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

To move folders:

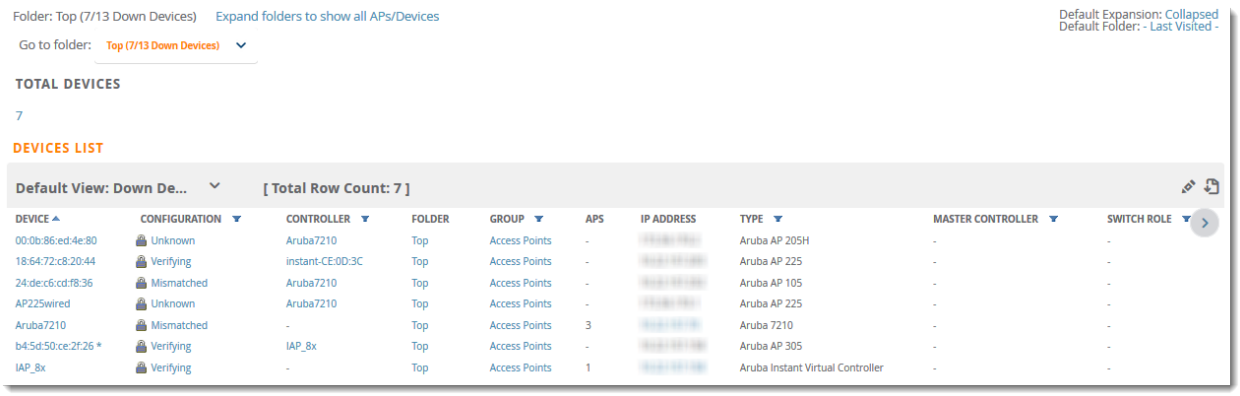
1. Select the folder you want to move from **Go to folder** at the upper left of the **Devices** page.
2. Scroll to bottom of the page and click .
3. Select the new parent folder and click **Save**.

Expanding Folders

You can change the information displayed on the **Devices > List** and **Clients > Connected** pages by selecting a folder at the top left corner of the page.

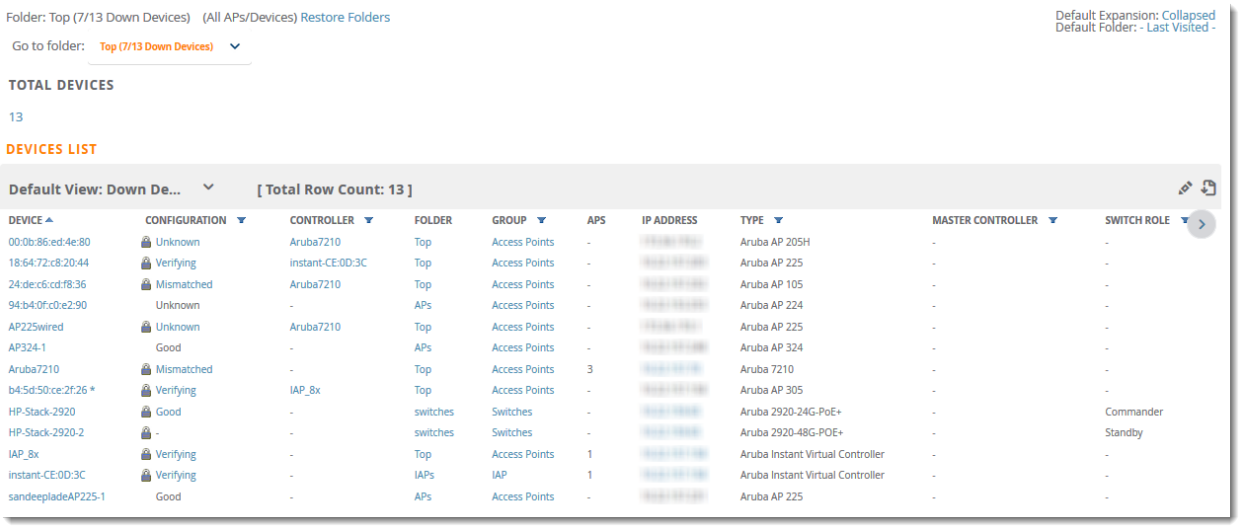
For example, if you select the **Top** folder and then click **Down** in the navigation bar, AirWave displays the 7 down devices in the Top folder.

Figure 79: *Collapsed View of the Down Devices in the Top Folder*



When you select **Expand folders to show all devices**, AirWave displays an expanded view of all 13 down devices in the Top folder and its subfolders.

Figure 80: *Expanded View of Down Devices in the Top Folder and Subfolders*



Changing Default Views

You can change the way AirWave displays default views in the **Devices > List** and **Clients > Connected** pages. To change the default view, click the **Default Expansion** or **Default Folder** drop-down menus at the top right corner of the page to change your view, as shown in Figure 81.

Figure 81: *Default Expansion and Default Folder Options*

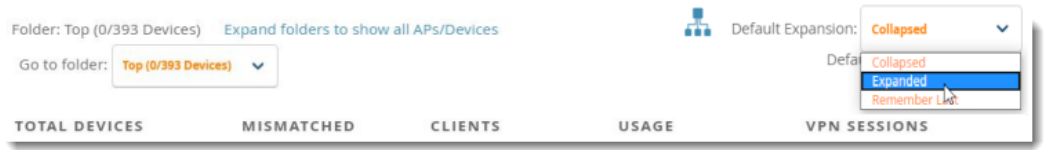


Table 71: *Ways to View Devices and Clients in Folders*

Default View Options	Description
Default Expansion	• **Collapsed**: AirWave shows details from the current folder. This view doesn't show details from the subfolders. • **Expanded**: AirWave shows details of the current folder and its subfolders. • **Remember Last**: AirWave stores your last view and displays it for you again. **NOTE:** The default expansion view affects the way AirWave displays the network on the topology map. For more information about topology maps, see "Using Topology" on page 286.
Default Folder	• **Last Visited**: AirWave displays the last folder you accessed. • **Folder**: When you select a folder, AirWave limits the information displayed to devices or clients in a specific folder.

Monitoring Access Points, Mesh Devices, and Controllers

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

For information about switch monitoring, see "Monitoring ArubaOS-CX and Mobility Access Switches" on page 173 and "Monitoring ArubaOS Switches" on page 179.

Device Information for Access Points, Mesh Devices, and Controllers

By default, the **Devices > Monitor** page displays the **Devices** tab. Table 72 describes the fields and information displayed in the **Device Info** section of this tab for different models and types of wireless devices.

Table 72: *Device Information for Wireless Devices*

Field	Description
Status	Displays the connection status between AirWave and the device: • **Up**. Everything is working as it should. • **Down**. Either AirWave can reach the device but can't speak with it using SNMP, or AirWave is unable to reach the device or connect to it using SNMP. **NOTE:** Verify that SNMP is enabled on the device. Many APs ship with SNMP disabled. This usually means 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 AirWave wants them to have. • **Mismatched** means there is a configuration mismatch between what is on the AP and what AirWave wants to push to the AP. The **Mismatched** link directs you to this specific **Devices > Device Configuration** 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. AirWave helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Licenses (Appears for Aruba controllers)	Selecting this link opens a pop-up window that lists the built-in licenses as well as other installed licenses for this controller. This also shows whether any license has expired.
Controller (Appears for APs)	Displays the controller for the associated AP device as a link. Select the link to display the **Devices > Monitor** page for that controller.
Aruba AP Group	Name of the AP group to which the device belongs.
Upstream Device	Name of the upstream device, if available.
Upstream Port	Number of the port used to connect to the upstream device.
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 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 device has been rebooted. This is the amount of time the device reports and is not based on any connectivity with 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 AirWave uses to communicate to the device. 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 Arubacontrollers, if Single Sign-On is enabled for your role in this AirWave and you have access to this controller, you will not have to enter the credentials for this controller again after selecting this link.

Field	Description
Outer IP	Public IP address for a RAP device.
Remote LAN IP	LAN IP address for a RAP. This address is useful for troubleshooting from the local network.
Quick Links	**Open controller UI :** A drop-down menu that allows you to jump to the controller's WebUI in a new window. For Arubacontrollers, if Single Sign-On is enabled for your role in 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 **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.
Power Supply	Displays the PoE type for the AP.
Power Consumption	Displays the power usage on the AP.
Notes	Displays notes entered for the device.

*****These fields are only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Mesh Devices" on page 168.

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 **Devices > Monitor** page of the AirWave WebUI, and selecting a supported show command. For a list of devices that support show commands via the AirWave **Devices > Monitor** page, refer to the AirWave*Supported Infrastructure Devices* document. For complete information about the output of each command, refer to the documentation for that switch.

Radios

Table 73 describes the information in the **Radio** table for APs.

Table 73: *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.

Table 73: *Devices > Monitor > Radio Fields and Descriptions (Continued)*

Field	Description
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 only, devices that support the 802.11n standard can use both 20 MHz and 40 MHz channels, and devices that support 802.11ac can use 20MHz, 40 MHz, 80MHz and 160 MHz channels to increase throughput.
Mesh Links *	The total number of mesh links to the device including uplinks and downlinks.
Role	Whether the radio acts as a Mesh Node or Access
Active SSIDs	The SSID(s) of the radio.

***This field is only available for mesh APs. To see an example of mesh monitoring, see "Monitoring Mesh Devices" on page 168.

Wired Interfaces

Devices with wired interfaces (other than Aruba Instant APs) will display the **Wired Interfaces** table, which is described in Table 74:

Table 74: *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 AirWave is able to ping it and fetch SNMP information. If the AP is listed as **Down**, then 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.
Aruba Port Mode	Either Active Standby (which provides redundancy so that when an active interface fails, the user traffic can failover to the standby interface) or one of the forwarding modes (Split, Bridge).
Input Capacity	The input capacity of the interface.
Output Capacity	The output capacity of the interface.

Graphs for Access Points, Mesh Devices, and Controllers

Figure 82 illustrates the interactive graphs available on this page. Use the drop down button next to the graph title to select a different graph.

Figure 82: *Interactive graphs for an Aruba controller*

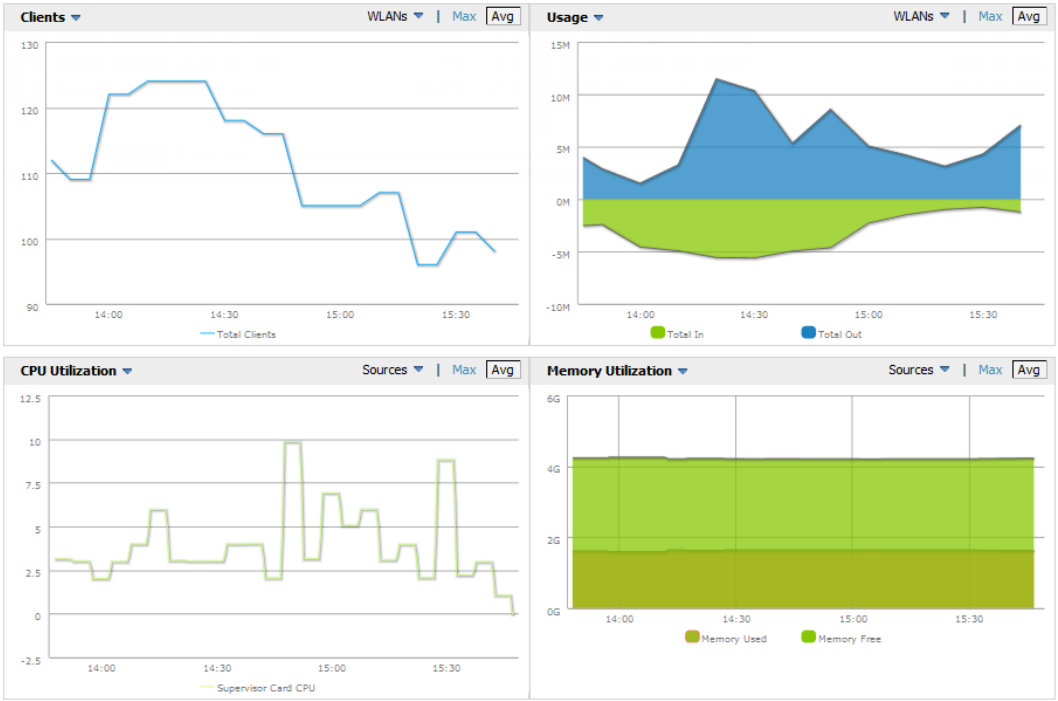


Table 75 describes the graphs on this page.

Table 75: *Devices > Monitor > Devices Graphical Data*

Graph	Description
Clients	Formerly Users. Shows the max and average client count reported by the device radios for a configurable period of time. User count for controllers are the sum of the user count on the associated APs. Check boxes below the graph can be used to limit the data displayed.
Usage	Formerly Bandwidth. Shows the bandwidth in and out reported by the device for a configurable period of time. Bandwidth for controllers is the sum of the associated APs. Check boxes below the graph can be used to limit the data displayed.
CPU Utilization (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only)	Reports overall CPU utilization (not on a per-CPU basis) of the device.
Memory Utilization (controllers, Aruba AirMesh, or the Aruba Mobility Access Switch only	Reports average used and free memory and average max memory for the device.

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.

Clients

Click the **Clients** tab on the Devices > Monitor page to view information about connected clients. Table 76 describes the fields and information displayed in the **Connected Clients** table.

Table 76: *Devices > Monitor > Clients > Connected Clients Fields and Default Values*

Field	Description
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 AirWave.
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.
VLAN	The number of the VLAN.
SSID	SSID to which the client is connected.
Usage	Displays the average bandwidth consumed by the MAC address.
LAN IP Addresses	Displays the IP assigned to the user MAC. This information is not always available. AirWave can gather it from the ARP cache of switches discovered by AirWave. This column can accommodate multiple IP addresses for a client if it has both IPv4 and IPv6.
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 AirWave provide the RADIUS Accounting Auth type • **WPA2**—Wi-Fi Protected Access 2 encryption • No Encryption AirWave considers all other types as not authenticated. The information 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 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**.
Username	Provides the name of the User associated to the AP. AirWave gathers this data in a variety of ways. It can be taken from RADIUS accounting data or traps.
Role	The role of the connected client such as employee, perforce, or logon (captive portal).

Table 76: *Devices > Monitor > Clients > Connected Clients Fields and Default Values (Continued)*

Field	Description
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.
Association Time	Displays the first time AirWave recorded the MAC address as being associated.
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 69.
Signal Quality	Displays the average signal quality the user experienced.

AirMesh Links

If you are viewing an Aruba AirMesh device's monitoring page, the **Mesh Links** table displays information about each mesh device linked to this device, as shown in Figure 83:

Figure 83: *Mesh Links Table on Devices > Monitor Illustration*

Neighbors

AirWave uses the source protocol (SNMP/HTTP or CDP/LLDP) to discover devices on the network and goes a step further and discovers neighbors directly connected to a monitored device.

You can view information about all neighbors on the **Neighbors** table of the monitoring page, as shown in Figure 84.

Figure 84: *Neighbors Table*

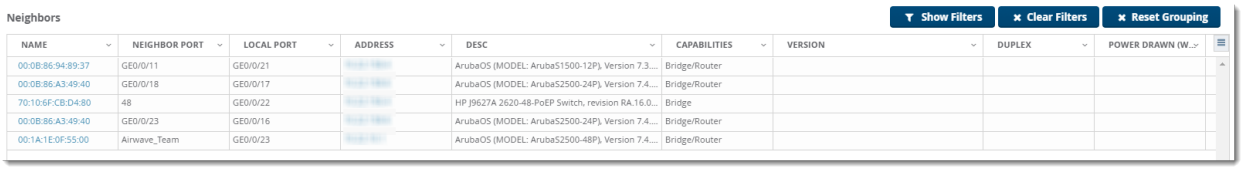


Table 77 describes the **Neighbors** table fields. This table displays all columns by default. To customize the data fields displayed in the **Neighbors** table, click the (☰) icon at the end of the table and select only those fields you wish to view.

Table 77: *Neighbors Table Fields and Descriptions*

Field	Description
Name	Displays the name of the neighbor device. For example, a MAC address, hostname, or make and model. If an IP address is known for the device, a link provides access to the monitoring page.
Neighbor Port	Displays the port ID of the neighbor device.

Field	Description
Local Port	Displays the port ID of the local device.
Address Type	Displays the type of address of the neighbor device.
Address	Displays the network address associated with the neighbor. This link provides access to the web management interface. Hover your pointer over the to open a management window to the device using HTTP, HTTPs, telnet or SSH.
Desc	Specify a description that provides additional information about the neighbor device (recommended).
Capabilities	Displays the device type: router, switch, or none (information is not available)
Version	Displays the software version running on the neighbor device.
CDP Version	Indicates the software version running on the neighbor device.
Duplex	Indicates the mode of operation of the connection: simplex, duplex, or half-duplex.
Power Drawn (Watts)	Displays the amount of power used on the interface of the neighbor device.
VTP Mgmt Domain	Displays the name of the group of VLANs associated with the neighbor device.
Sysname	Displays the system name of the neighbor device.
Primary Mgmt Address Type	Displays the type of address of the primary management interface.
Primary Mgmt Address	Displays the network address of the primary management interface.
Secondary Mgmt Address Type	Displays the type of address of the secondary management interface.
Secondary Mgmt Address	Displays the network address of the secondary management interface.
Physical Location	Displays the location of the neighbor device.
Native VLAN	Displays the ID number of the VLAN on the neighbor device.
Appliance ID	Displays the ID number of the appliance.
VLAN ID	Displays the ID number of the management VLAN on the neighboring device.
Last Change	Indicates when the device was last seen.
MTU	Specifies the largest packet size which can be received on the neighbor device.
Source	Displays the protocol used for device discovery: CDP.

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

Wireless controllers also include interface-specific data for wired interfaces on the **Devices > Interfaces** page. For more information, see "Monitoring ArubaOS-CX and Mobility Access Switches" on page 173

RF Neighbors

If you are monitoring a wireless device, the **Devices > Monitor** page displays the **RF Neighbors** tab. This table displays information about other devices in the AP's RF neighborhood, including the name of the AP or device, the radio channel(s) and radio signal RSSI (in dBm) detected by the AP, and the RAPIDs classification type for that device.

Alerts & Events

Click the **Alerts & Events** tab to access the alert tables about AirWave, Intrusion Detection System (IDS), RADIUS accounting, and RADIUS authentication issues. For information about alert summaries, see "About Alerts" on page 320. The **Alerts & Events** tab also displays the event tables for device events and recent AMP device events. These tables also appear on the **System > Event Log** page. To learn more about these events, see "Using the Event Log" on page 308.

Advanced Monitoring

This tab appears at the top of the **Devices > Monitor** page for controllers only. For information on advanced monitoring, see "Monitoring 7000 Controllers " on page 198.

Viewing the Radio Statistics Page

The Radio Statistics page contains statistics for pinpointing network issues for Aruba APs and Cisco WLC thin APs running firmware 4.2 or later.

Depending on the AP, assigned group profiles, and recent activity on a radio, you can evaluate:

- Recent and historical changes in the network
- Real-time statistics from the AP's controller
- Actively interfering devices (requires that you set Aruba to Spectrum mode)
- Summary of major issues

To open the Radio Statistics page, navigate to the **Devices > List** page, then select the AP from the **Devices** list to open the **Devices > Monitor** page for that AP. Locate the radio in the **Radios** table and click the hyperlink to open the **Radio Statistics** page, as shown in Figure 85.

Figure 85: *Accessing Radio Statistics from an AP Monitoring Page*

Radios

INDEX ▲	NAME	MAC ADDRESS	CLIENTS	USAGE (Kbps)	CHANNEL	TX POWER	ANTENNA TYPE	CHANNEL WIDTH	SSID
1	802.11bgn	F0:7F:06:4E:1F:30	0	0.00	11	1 (22 dBm)	Internal	20 MHz	cis8510 (cis8510)...
2	802.11ac	F0:7F:06:4E:1F:30	0	0.00	36	1 (15 dBm)	Internal	20 MHz	cis8510 (cis8510)...

Running Commands from the Radio Statistics Page

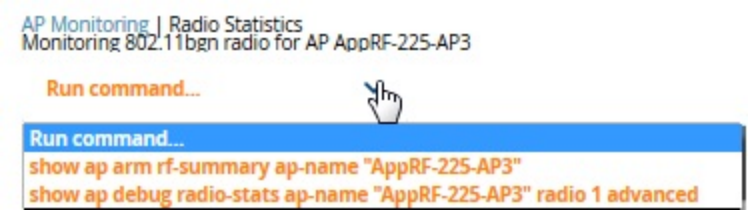
Adaptive Radio Management (ARM) provides automated channel optimization, transmit power adjustment and channel width tuning for an individual AP or group of APs.

Starting with ArubaOS 8.0, only standalone controllers support the Adaptive Radio Management (ARM) feature.

To run a show command:

1. Navigate to the **Devices > Monitor** page, then select the AP from the Devices List.
2. In the monitoring page for the AP, locate the radio in the **Radios** table and click the hyperlink to open the **Radio Statistics** page.
3. Click **Run command** and choose a command, as illustrated in Figure 86.

Figure 86: *Running a show command*



When this command is selected, a new browser window launches with the statistics in plain text. Other ARM- and AirMatch-tracked metrics are visible in the **Radio Statistics** page for Aruba APs.

Issues Summary section

The **Issues Summary** section only displays when noise, client count, non-802.11 interfering devices, channel utilization, usage, and MAC and PHY errors reach a certain threshold of concern, as described in Table 78 and illustrated in Figure 87:

Table 78: *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 87: *Issues Summary Section Illustration*

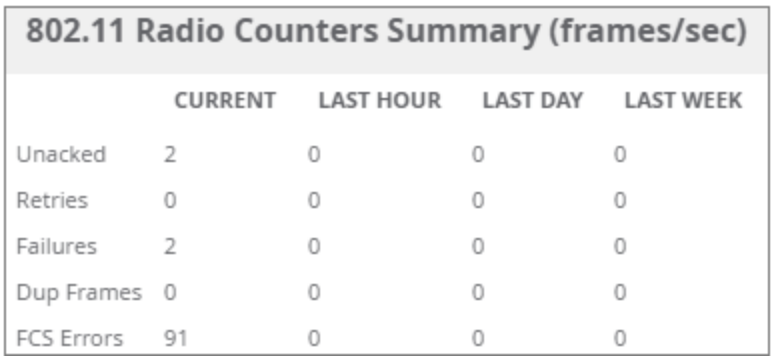
These issues highlighted in this section can be examined in detail using the corresponding interactive graphs on the same page. See the "Radio Statistics Interactive Graphs" on page 164 section of this chapter for details.

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 88.

Figure 88: *802.11 Radio Counters Summary table*



802.11 Radio Counters Summary (frames/sec)

	CURRENT	LAST HOUR	LAST DAY	LAST WEEK
Unacked	2	0	0	0
Retries	0	0	0	0
Failures	2	0	0	0
Dup Frames	0	0	0	0
FCS Errors	91	0	0	0

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**.

Radio Noise and Radio Errors graphs are not supported for Autonomous Cisco Aironet APs.

The two graph panes enable simultaneous display of two different information sets, as detailed in the following table:

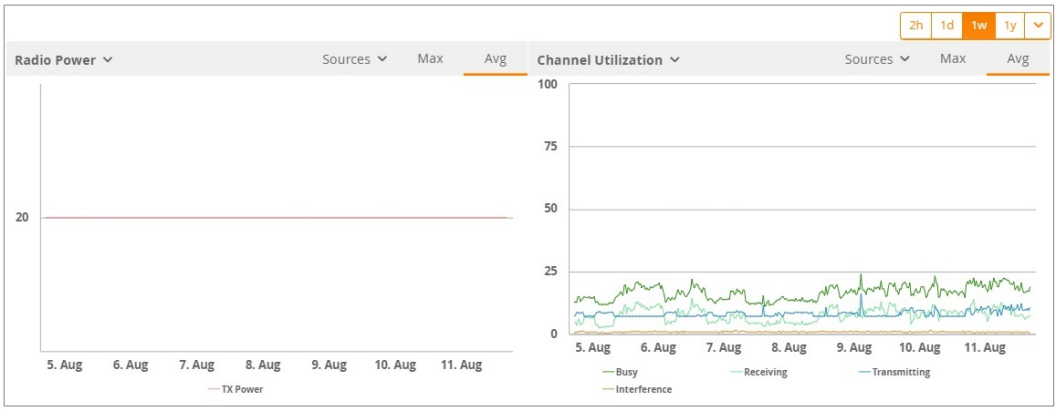
Table 79: *Radio Statistics Interactive Graphs Descriptions*

Graph Title	Description
Clients	A line graph that displays the maximum users associated to the corresponding radio at polling intervals over the time range set in the slider. Select **Show All** for other metrics such as average users and max users for various individual devices.
Usage	An area graph displaying the average bandwidth in each direction for the radio. Select **Show All** for other metrics such as max bandwidth in and out, average and max mesh/overhead or overhead bandwidth, and average/max Enet0.
Radio Channel	An area graph that displays the channel changes (if any) of the radio over time. Frequent, regular channel changes on an Aruba or Cisco WLC AP radio usually indicate that the Adaptive Radio Management feature (ARM) in ArubaOS is compensating for high noise levels from interfering devices.
Radio Noise	An area graph that displays signal interference (noise floor) levels in units of dBm. Noise from interfering devices above your AP's noise threshold can result in dropped packets. For ARM-enabled Aruba APs, crossing the noise threshold triggers an automatic channel change.

Table 79: *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 **Devices > Manage** page for this radio's AP, or enable ARM on Aruba APs to dynamically adjust the power toward your acceptable Coverage Index as needed. For more information, see the Adaptive Radio Management chapter of the *ArubaOS User Guide*.
Radio Errors	A line graph displaying the frame reception rate, physical layer error rate (resulting from poor signal reception or broken antennas), and the data link (MAC) layer (corrupt frames, driver decoding issues) for the radio.
802.11 Counters	A line graph that displays statistics such as frame rate, fragment rate, retry rate, duplicate frame rate, and other metrics tracked by 802.11 counters.
Channel Utilization	Displays max and average percentages on this radio for busy, interfering receiving and transmitting signals. This graph can display historical information for up to six months only, even if a longer time range is selected using the calendar tool above the graph, or longer historical data retention settings defined on the **AMP Setup > General > Historical Data** fields. Special configuration on the controller is required to enable this data. Consult the *Aruba and AirWave Best Practices Guide* in **Home > Documentation** for details. **NOTE:** (Aruba and Cisco WLC thin APs on supported firmware versions only)
Channel Width	A line graph that indicates the channel widths used by the AP radio (20MHz, 40Mhz, 80Mhz or 160Mhz) over the selected time frame. c
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 89: *Radio Statistics Interactive Graphs Illustration – Radio Power and Channel Utilization displayed*

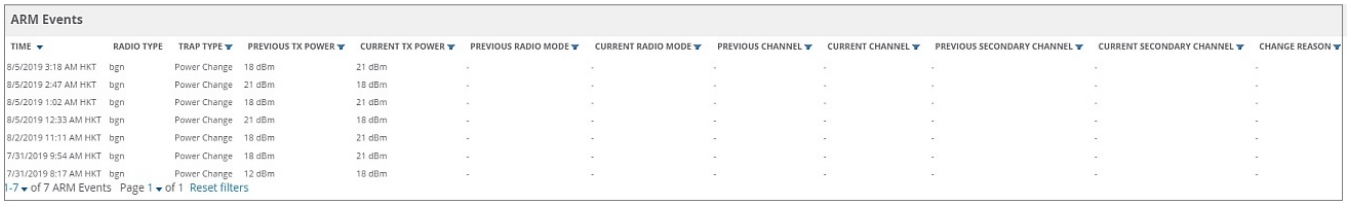


Recent ARM Events Log

If a radio references an active and enabled ARM profile and AirWave is enabled as a trap host, ARM-initiated events are displayed in the ARM Events table with the original and modified values.

You can filter the results and export the table in CSV format. The columns and values are illustrated in Figure 90.

Figure 90: *ARM Events Table*



The columns and values are described in Table 80.

Table 80: *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 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.

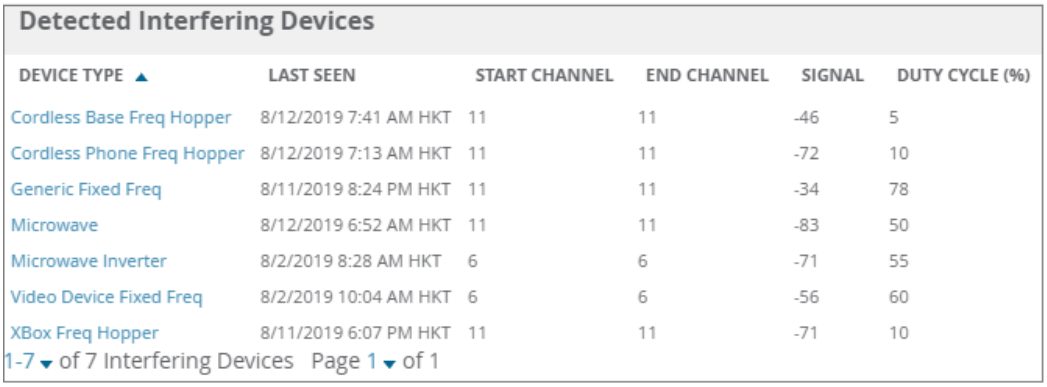
For information about configuring AirWave as a trap host, see the *Aruba and AirWave Best Practices Guide* in **Home > Documentation**.

Detected Interfering Devices Table

For Aruba APs running in Spectrum mode, the same non-802.11 interfering devices identified in the **Issues Summary** section are classified in the **Detected Interfering Devices** table along with the timestamp of its last detection, the start and end channels of the interference, the signal to noise ratio, and the percentage of time

the interference takes place (duty cycle), as illustrated in Figure 91. This table can be exported to CSV format, and the displayed columns can be moved or hidden as needed.

Figure 91: *Detected Interfering Devices Table Illustration*



Detected Interfering Devices

DEVICE TYPE ▲	LAST SEEN	START CHANNEL	END CHANNEL	SIGNAL	DUTY CYCLE (%)
Cordless Base Freq Hopper	8/12/2019 7:41 AM HKT	11	11	-46	5
Cordless Phone Freq Hopper	8/12/2019 7:13 AM HKT	11	11	-72	10
Generic Fixed Freq	8/11/2019 8:24 PM HKT	11	11	-34	78
Microwave	8/12/2019 6:52 AM HKT	11	11	-83	50
Microwave Inverter	8/2/2019 8:28 AM HKT	6	6	-71	55
Video Device Fixed Freq	8/2/2019 10:04 AM HKT	6	6	-56	60
XBox Freq Hopper	8/11/2019 6:07 PM HKT	11	11	-71	10

1-7 ▾ of 7 Interfering Devices Page 1 ▾ of 1

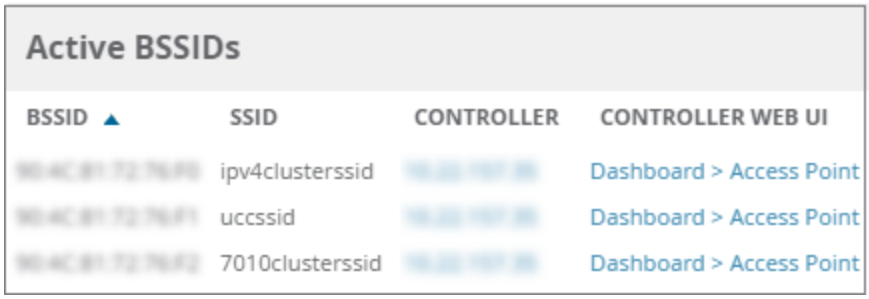
Possible device types for the **Detected Interfering Devices** table include:

- Audio Device Fixed Freq
- Bluetooth
- Cordless Base Freq Hopper
- Cordless Phone Fixed Freq
- Cordless Phone Freq Hopper
- Generic Fixed Freq
- Generic Freq Hopper
- Microwave
- Microwave Inverter
- Unknown
- Video Device Fixed Freq
- Wi-Fi
- XBox Freq Hopper

Active BSSIDs Table

The Active BSSIDs table maps the BSSIDs on a radio with the SSID it broadcasts to the network, as illustrated in Figure 92. This table appears only for Aruba AP radios.

Figure 92: ***Active BSSIDs*** *Table Illustration*



AirMatch Statistics for Mobility Master

AirMatch enhances ARM by analyzing the past 24 hours of RF network statistics and proactively optimizing the network for the next day.

NOTE

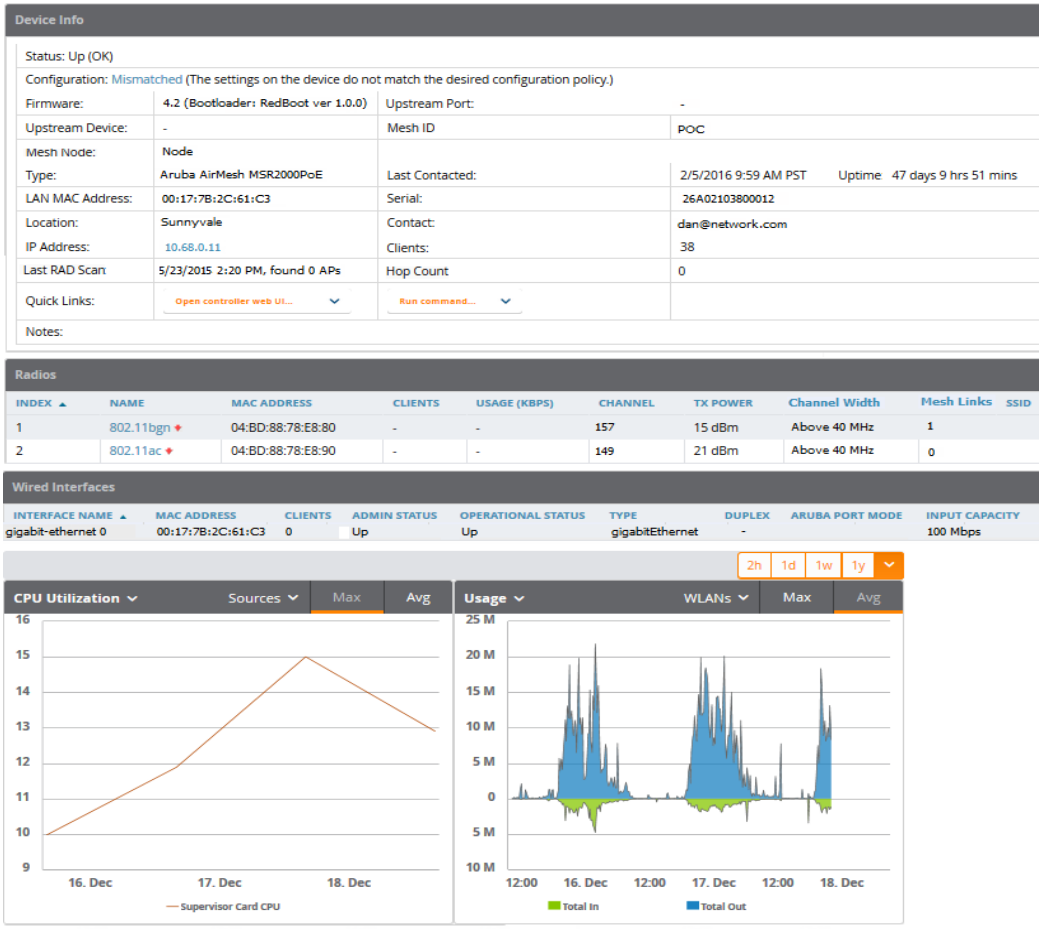
You can enable AirMatch on managed devices associated to Mobility Master running ArubaOS 8.0 or later. AirMatch dashboard will be populated for ARM-enabled AOS 6.x controllers. Configure the AMP server as a trap host to populate the "Channel Change Reasons" graph and "Channel Changes" in the AirMatch dashboard.

For more information on AirMatch, refer to the RF Planning and Channel Management chapter in the *ArubaOS User Guide*.

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 93: *Devices > Monitor page for a Mesh Device*



These fields are described in detail in "Device Information for Access Points, Mesh Devices, and Controllers" on page 154.

Setting up Spectrum Analysis

The spectrum analysis software modules available on many Aruba 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 Aruba's Adaptive Radio Management (ARM) technology. While the spectrum analyzer identifies and classifies Wi-Fi and non-Wi-Fi sources of interference, ARM automatically ensures that APs serving clients will stay clear of interference.

Individual APs or groups of APs can be converted to dedicated spectrum monitors through the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile.

Each 802.11a and 802.11g radio profile references a spectrum profile, which identifies the spectrum band the radio will monitor and analyze, and defines the default ageout times for each monitored device type. By default, an 802.11a radio profile references a spectrum profile named **default-a** (which configures the radio to monitor the upper channels of the 5 GHz radio band), and an 802.11g radio profile references a spectrum profile named **default-g** (which configures the radio to monitor all channels the 2.4 GHz radio band).

Most interference will occur in the 2.4 GHz radio band.

For more information about Spectrum analysis and ARM technology, including a list of APs that support spectrum analysis refer to the *ArubaOS User Guide*.

Spectrum Configurations and Prerequisites

The following prerequisites must be in place to configure an AP to run in Spectrum mode in 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.
- Aruba GUI Config must be enabled for that AP's group in the **Groups > Basic** page.

There are three main situations in which you would set one or more devices to Spectrum mode in AirWave:

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

Setting up a Permanent Spectrum Aruba AP Group

If you have multiple supported Aruba APs in multiple controllers that you want to run in Spectrum mode over the long run, you create a special Aruba AP group and set up a profile that is set to **spectrum-mode** and references the default **Spectrum** profile. Set up more than one profile if you want to utilize both radio bands in Spectrum mode.

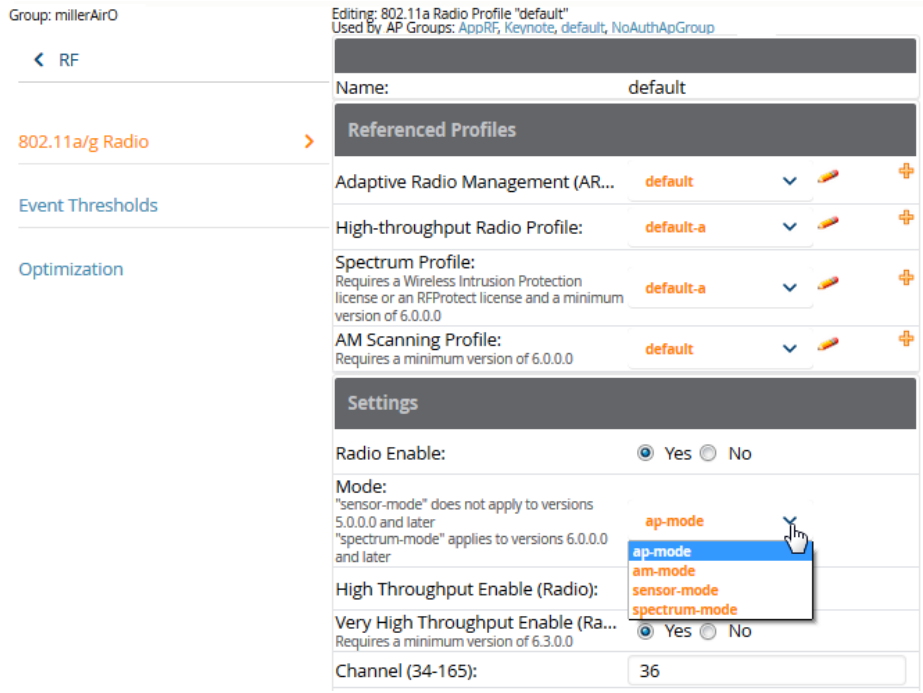
If you use an 802.11a or 802.11g radio profile to create a group of spectrum monitors, all APs in any AP group referencing that radio profile will be set to spectrum mode. Therefore, best practices are to create a new 802.11a or 802.11g radio profile just for spectrum monitors.

If **Use Global Aruba Configuration** is enabled in **AMP Setup > General**, create the configuration below, then go to the controller group's **Controller Config** page and select the newly created Aruba AP Group.

Perform these steps to set the AP group to use the default Spectrum profile settings:

1. On the **Groups > Controller Config** page, click the **Add New Aruba Group** button.
2. Give the new Group a name (such as Spectrum APs), and select the plus sign next to the **802.11a Radio Profile** field to create a new radio profile.
3. Enter a name under the General Settings section of **Profiles > RF > 802.11a/g Radio**.
4. In the **Other Settings** section, change the **Mode** field from **ap-mode** to **spectrum-mode**, as illustrated in Figure 94, and then select **Save**.

Figure 94: *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 Aruba AP Group are managed by the same controller and you want to temporarily override one or more profile settings in your spectrum-mode APs, you can set up a controller override.

To disable spectrum mode in this group, change the referenced radio profile back to **default**.

Configuring an Individual AP to run in Spectrum Mode

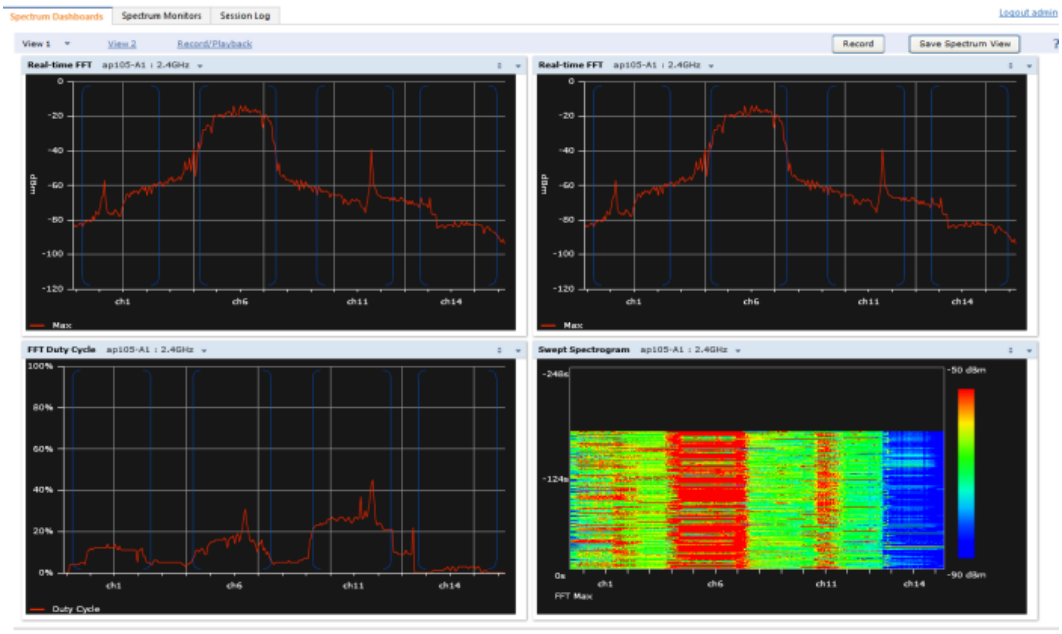
If you want to temporarily set an individual radio in an AP to run in Spectrum mode without creating or changing Aruba AP Groups or radio profiles, perform these steps to set up a Spectrum Override on a supported Aruba AP:

1. Navigate to **Devices > List**, right-click the Spectrum-supported AP in the Devices List, and then select **Audit** from the shortcut menu. Or you can navigate to **Devices > Config** to access the Device Configuration page.
2. After reviewing the device configuration, 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 **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 95.

Figure 95: *Spectrum Analysis on Controller Dashboard*

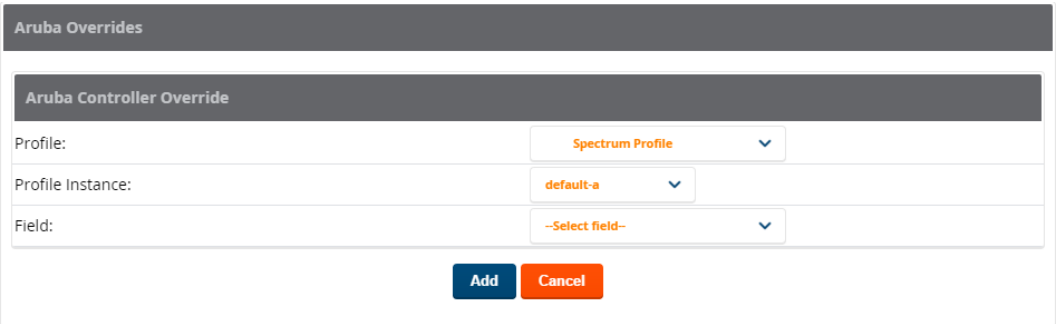


To disable Spectrum mode on this individual AP after it has collected data, return to the **Devices > Manage** page for this AP and set the **Spectrum Override** field back to **No**.

Configuring a Controller to use the Spectrum Profile

You can use AirWave to customize individual fields in the profile instance used by a particular controller without having to create new Aruba AP groups and new radio profiles. To do this, you can set a controller-level override for its referenced Spectrum profile on the **Devices > Manage page**, as illustrated in Figure 96. This will affect all Spectrum-supported APs managed by this controller.

Figure 96: *Override Section of a Supported Controller's Manage Page*



Perform these steps to override individual profile settings for an Aruba controller that is part of a spectrum-mode Aruba AP group:

1. Select a Spectrum-supported Aruba controller that is referencing a Spectrum profile, and go to its **Devices > Manage** page. Set it to **Manage Read/Write** mode.
2. Under the Aruba Overrides section, click the **Add New Aruba Controller Override** button.
3. In the **Profile** drop-down menu, select the **Spectrum Profile** type.
4. In the **Profile Instance** drop-down menu, select the instance of the Spectrum profile used by the controller.

5. In the **Field** drop-down menu, select the setting you would like to change (such as an Age-Out setting or a Spectrum Band), and enter the overriding value below it.
6. Select **Add** to save your changes.
7. Repeat this process to create additional overrides for this controller.
8. When you have finished, select **Save and Apply**.

You can also use the above procedure to turn on Spectrum mode for radio profiles on one particular controller, or use the overrides to point your radio profile to a non-default Spectrum profile for just this controller.

Monitoring ArubaOS-CX and Mobility Access Switches

AirWave displays the detailed information and tools to help you monitor ArubaOS-CX and Mobility Access Switches.

For information about these features, see the following sections:

- "Device Information" on page 173
- "Graphs" on page 174
- "Detailed Summary Tables" on page 174

For information on the general monitoring data that appears on the **Devices > Monitor** page for all device types, see "Monitoring Basics" on page 149.

Device Information

Table 81 describes the device information that you see in the switch monitoring page for the ArubaOS-CX Switches and Mobility Access Switches.

Table 81: *Device Information for the ArubaOS-CX Switches and Mobility Access Switches*

Field	Description
Status	Displays the connection status between AirWave and the wired device: • **Up**. Everything is working as it should. • **Down**. Either AirWave can reach the device but can't speak with it using SNMP, or AirWave is unable to reach the device or connect to it using SNMP. **NOTE:** When the device is down due to an `SNMP get failed` error, verify that SNMP is enabled on the device and check the SNMP credentials that AirWave is using on the **Devices > Manage** page. An `ICMP ping failed` error indicates that AirWave can't connect to the device, or the device needs to be rebooted or reset. **NOTE:** The monitoring page for ArubaOS-CX Switches includes a hypertext link next to the device status to launch **NetEdit Network Advisor**.
Configuration	• **Good**. All the settings on the device agree with the settings AirWave wants them to have. • **Mismatched**. There is a configuration mismatch between what is on the device and what AirWave wants to push to the device. The **Mismatched** link directs you to this specific **Devices > Device Configuration** page where each mismatch is highlighted. • **Unknown**. The device configuration has not yet been fetched, and there might be an issue with credentials. • **Verifying**. 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.

Table 81: *Device Information for the ArubaOS-CX Switches and Mobility Access Switches (Continued)*

Field	Description
Firmware	The firmware version running on the AP. **NOTE:** Newer AirMesh APs include the new bootloader APBoot. AirWave helps to identify the new AirMesh APs from the old SKUs by displaying the bootloader information here.
Upstream Device	The upstream device (also called the CDP neighbor) that AirWave discovers using CDP, or, for non-Cisco devices that AirWave supports, using bridge forwarding tables.
Upstream Port	The upstream port on the device.
Type	The make of the device.
Model	The model of the device.
Last Contacted	The most recent time AirWave has polled the device (see "Configuring Basic Settings for Device Groups" on page 93 for information about the poll interval).
Switch Role	The role of the device, which might, for example, be primary or secondary.
LAN MAC Address	The MAC address of the Ethernet interface on the device.
Serial	The serial number of the device.
Location	The SNMP location of the device.
Contact	The person to contact.
IP Address	The IP address that AirWave uses to communicate with the device. This link provides access to the web management interface. Hover your mouse to access the device using HTTP, HTTPs, telnet or SSH.
Usage	The combined bandwidth through the device at time of polling.

Graphs

The following interactive graphs are available:

- Clients. This graph shows the maximum and average client count reported by the device.
- Usage. This graph shows the bandwidth in and out reported by the device.
- CPU utilization. This graph shows the overall CPU utilization (not on a per-CPU basis) of the device.
- Memory utilization. This graph shows the average used, free memory, and average max memory for the device.

If you click a graph, a full size view opens. Click  to choose which graph to display on the monitoring page.

Detailed Summary Tables

AirWave can help you monitor the wired infrastructure, providing detailed summary tables about your wired network on the **Devices > Monitor** page. From this page, you can drill down into diagnostics, client details, and interface monitoring pages from links found in these tables.

Neighbors

AirWave uses the source protocol (SNMP/HTTP or CDP/LLDP) to discover devices on the network and goes a step further and discovers neighbors directly connected to a wired device.

You can view information about all neighbors on the **Neighbors** table of the monitoring page, as shown in Figure 97.

Figure 97: *Neighbors Table*

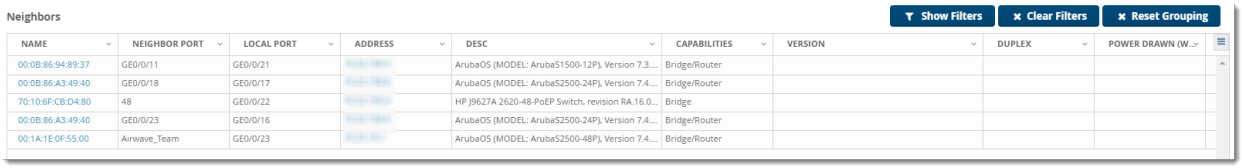


Table 82 describes the **Neighbors** table fields. This table displays all columns by default. To customize the data fields displayed in the **Neighbors** table, click the (☰) icon at the end of the table and select only those fields you wish to view.

Table 82: *Neighbors Table Fields and Descriptions*

Field	Description
Name	Displays the name of the neighbor device. For example, a MAC address, hostname, or make and model. If an IP address is known for the device, a link provides access to the monitoring page.
Neighbor Port	Displays the port ID of the neighbor device.
Local Port	Displays the port ID of the local device.
Address Type	Displays the type of address of the neighbor device.
Address	Displays the network address associated with the neighbor. This link provides access to the web management interface. Hover your pointer over the to open a management window to the device using HTTP, HTTPs, telnet or SSH.
Desc	Specify a description that provides additional information about the neighbor device (recommended).
Capabilities	Displays the device type: router, switch, or none (information is not available)
Version	Displays the software version running on the neighbor device.
CDP Version	Indicates the software version running on the neighbor device.
Duplex	Indicates the mode of operation of the connection: simplex, duplex, or half-duplex.
Power Drawn (Watts)	Displays the amount of power used on the interface of the neighbor device.
VTP Mgmt Domain	Displays the name of the group of VLANs associated with the neighbor device.
Sysname	Displays the system name of the neighbor device.
Primary Mgmt Address Type	Displays the type of address of the primary management interface.

Field	Description
Primary Mgmt Address	Displays the network address of the primary management interface.
Secondary Mgmt Address Type	Displays the type of address of the secondary management interface.
Secondary Mgmt Address	Displays the network address of the secondary management interface.
Physical Location	Displays the location of the neighbor device.
Native VLAN	Displays the ID number of the VLAN on the neighbor device.
Appliance ID	Displays the ID number of the appliance.
VLAN ID	Displays the ID number of the management VLAN on the neighboring device.
Last Change	Indicates when the device was last seen.
MTU	Specifies the largest packet size which can be received on the neighbor device.
Source	Displays the protocol used for device discovery: CDP.

Connected Devices

AirWave detects authenticated and rogue devices and reports them in the **Connected Devices** table (see Figure 98). AirWave also uses upstream data to calculate possible neighbors and reports these devices in the **Connected Devices** table.

Most information will not be available for rogue devices. If you click and add a name, device type, location, contact, or notes to a rogue device, the device will move to the client table and be considered an unauthenticated client. The device category will change from device to client.

NOTE

When AirWave discovers more than one MAC address from one port and none of the MAC addresses have LLDP/CDP information, AirWave will list only one unknown device without a MAC address.

NOTE

When AirWave discovers a switch that doesn't have a MAC address, it classifies the device as an unknown client. You cannot authenticate the client by modifying the device because it doesn't have a MAC address associated with it.

Figure 98: *Connected Devices Table*

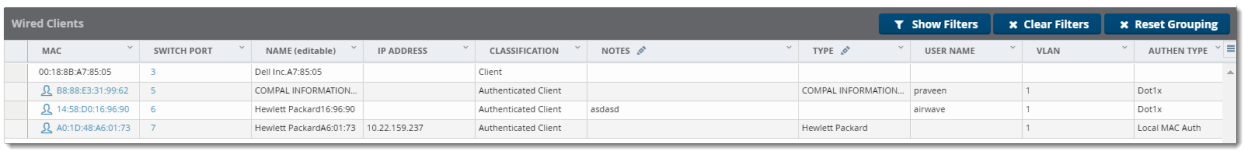


Table 83: *Connected Devices Fields and Descriptions*

Field	Description
MAC	MAC address for the device. This link provides access to the diagnostics page for the client. Find more information about "" on page 215.
Switch Port	Port number associated with the device. This link provides access to the monitoring page for the interface.
Name	Name of the device. You can enter any name.
IP Address	If the gateway is managed by AirWave, the IP address is shown here.
Classification	Displays the classification of the device after AirWave detects the device: • Authenticated Client. This link provides access to the Connected Client page. • Client. This link provides access to the Rogue table, where you can identify the device.
Notes	Notes to help you identify the client. You can enter anything.
Type	Type of device. You can enter anything.
User Name	Name that is used on the device for authentication.
User Role	Identifies the role-based operations that can be performed on the device.
VLAN	The number of the VLAN.
Stack Role	In a stack of switches, the role can be: master.
Bandwidth	The bandwidth used by the device. If the device supports bandwidth per MAC address, the bandwidth shown is the total bandwith used by all attached devices.
Host Name	The hostname of the neighbor device, which is retrieved from the DNS lookup.
Authen Type	The authentication server type: • Dot1x • Captive Portal • Local MAC Auth • WPA-PSK

Interfaces

The **Devices > Interfaces** page for managed switches and routers displays interface-specific data, graphs, and detailed summary tables for any connected clients and wired clients. For stacked switches, the master switch displays information for the interfaces of all the members, including its own.

From the **Physical Interfaces** and **Virtual Interfaces** tables, click any interface link to open the **Interface Monitoring** page for that interface, as shown in Figure 99

Figure 99: *Opening the Monitoring Interface Page*

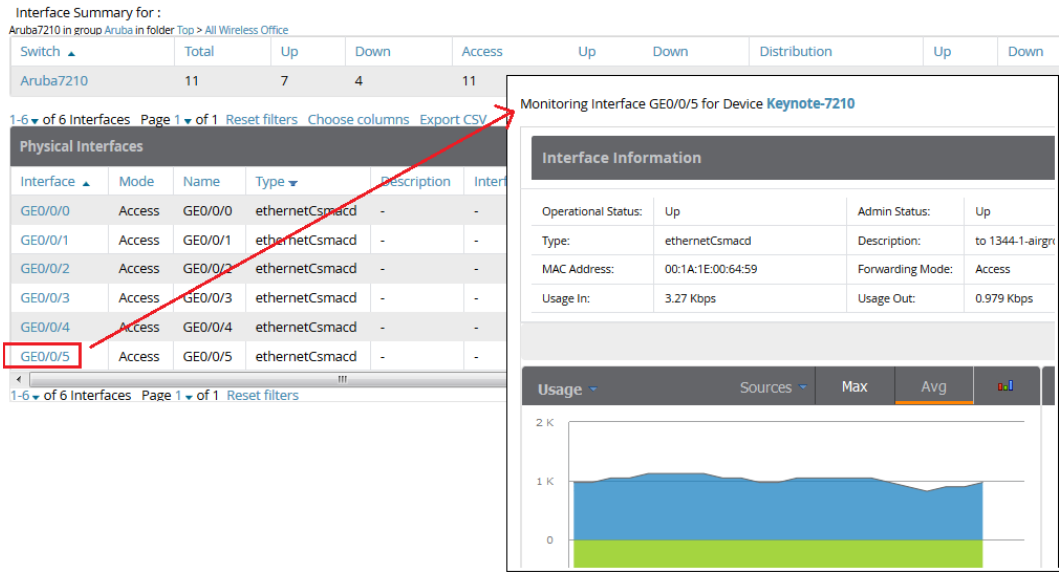


Figure 100 shows an example of interface information for an Ethernet CSMA/CD interface.

Figure 100: *Interface Information*

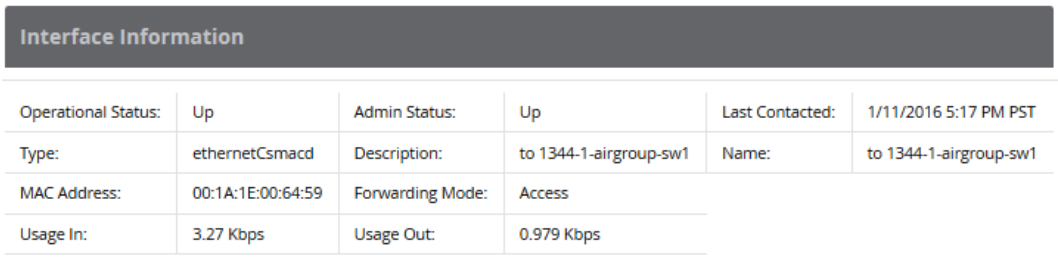


Table 84 describes fields that you see in **Interface Information** for switches and routers.

Table 84: *Interface Information Fields and Descriptions*

Field	Description
Operational Status	Displays the operational state of the interface: Up or Down.
Type	Type of interface.
MAC Address	Displays the MAC address assigned to the interface.
Usage In	Displays the incoming interface load in Kbps.
Admin Status	Displays the configuration on the port: Up or Down.
Description	Information about the interface.
Forwarding Mode	Indicates whether the interface is configured as an access port with one VLAN or a trunk interface with two or more VLANs.

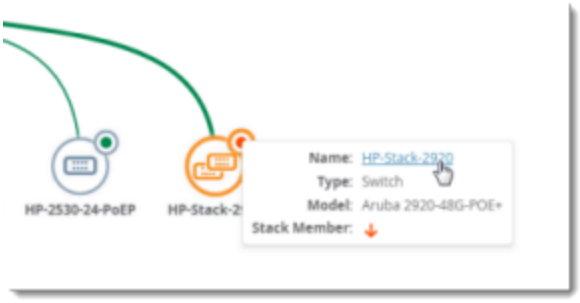
Table 84: *Interface Information Fields and Descriptions (Continued)*

Field	Description
Usage Out	Displays the outgoing interface load in Kbps.
Last Contacted	The most recent time AirWave has polled the interface.
Name	Name of the interface. You can enter any name.

Monitoring ArubaOS Switches

Available for ArubaOS-Switches, AirWave puts all your switch monitoring information into a single page. There are horizontal tabs across the top of the page, so you don't have to scroll down to view the data. You can open the switch monitoring page by navigating to **Devices > List** and selecting a switch from the list. Or, from a topology map, hover over the device to access the quick link in the tooltip (see Figure 101).

Figure 101: *Accessing a Monitoring Page from Topology*



NOTE

New switch monitoring pages aren't available for the Aruba CX 6300 or 6400 switches.

Getting Started

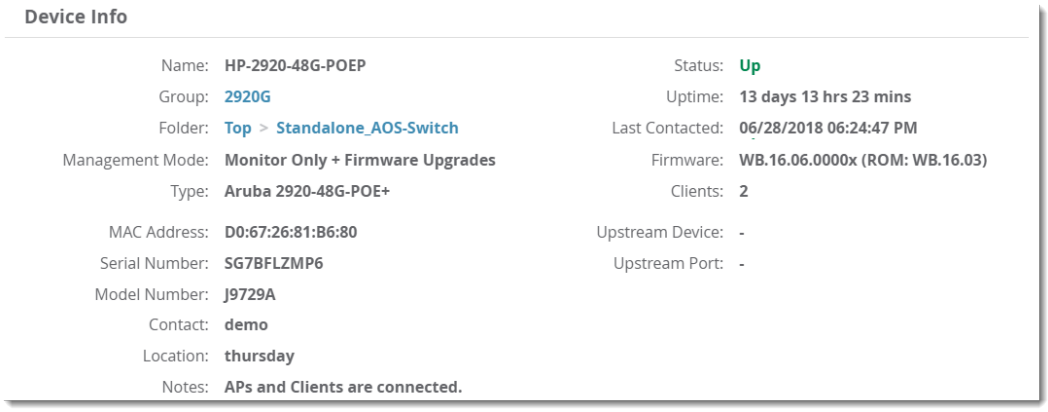
From the monitoring page for a switch or switch stack, you can view color-coded status, navigate using quick links, and get details from tooltips.

Color-Coded Status

Color-coded thresholds and icons help you visualize status and hardware-related alerts. For information on the threshold values that each color represents, see "Hardware Tab" on page 194.

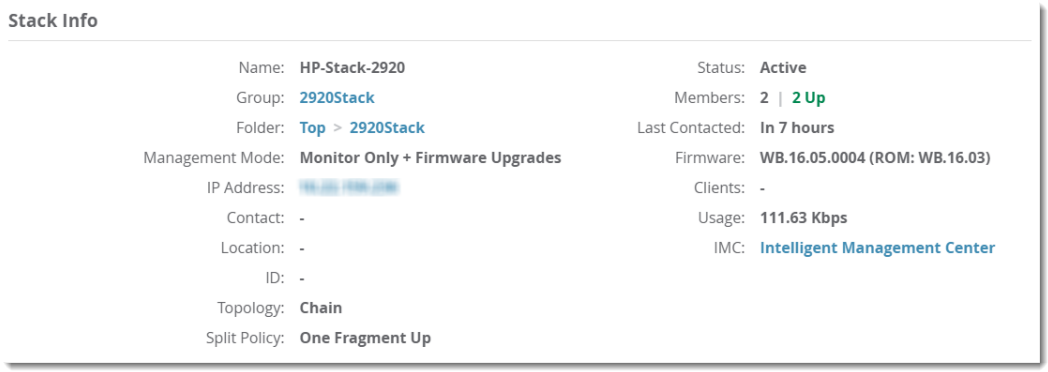
For current device status, green text indicates whether the device is up (Figure 102).

Figure 102: *Device Information*



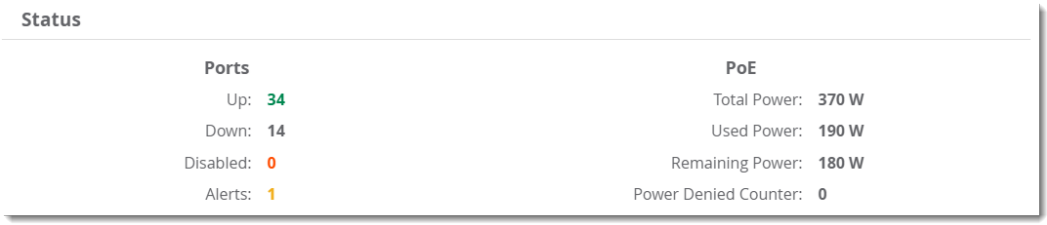
Gray text indicates that the switch is disabled, or the stack is active (Figure 103).

Figure 103: *Stack Information*



Color-coded port status shows you the health of your ports (Figure 104).

Figure 104: *Ports and Power over Ethernet (PoE) Status*

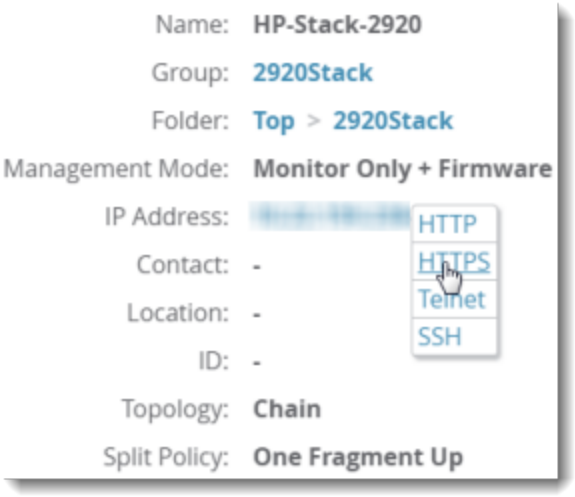


Navigate Using Quick Links

Blue links let you navigate to group and folder monitoring pages; open a WebUI, CLI session, or the Intelligent Management Center (see Figure 103). These quick links also let you switch between stack and stack member monitoring pages .

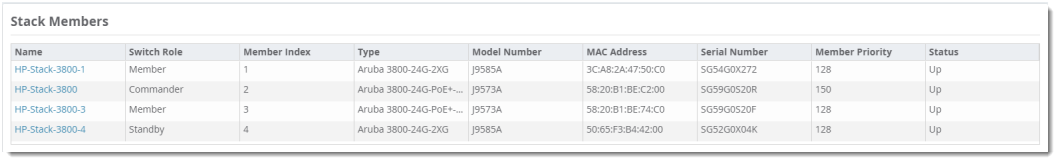
In Figure 105, clicking the IP address link and selecting HTTPS will open a secure HTTP session with the stack commander.

Figure 105: *Accessing the WebUI from the Stack Information*



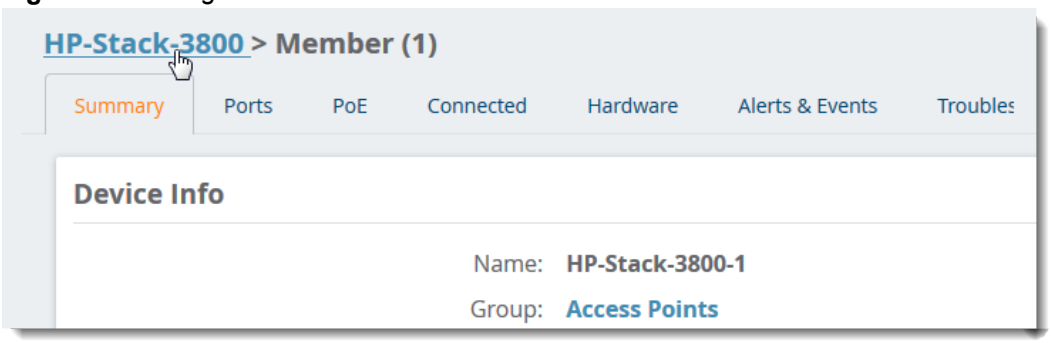
When looking at a stack, AirWave will display information about each stack member in the Stack Member table at the bottom of the Summary tab. You can easily go from one switch member to another in the stack by clicking the blue stack member link to open the monitoring page for the stack member (see Figure 106).

Figure 106: *Accessing the Monitoring Page for a Stack Member*



If you navigate away from the monitoring page for the stack, you will see the stack name link in the upper-left corner of the WebUI (see Figure 107). Click this link to return to the monitoring page.

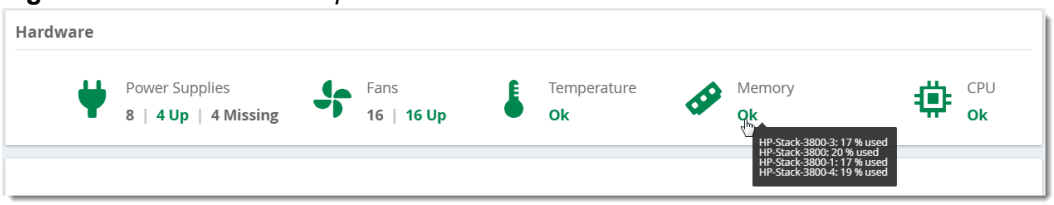
Figure 107: *Navigate Backwards from the Member to the Stack*



Get Details from Tooltips

Find out details about power supplies, environmental information, memory and CPU consumption by pointing your mouse over the statistics. When looking at the hardware status for the stack, icons and color-coded thresholds are the same as for stand-alone switches, but AirWave displays the details for stack members (see Figure 108). For more information about monitoring your hardware, see "Hardware Tab" on page 194.

Figure 108: *Hardware Tooltips*



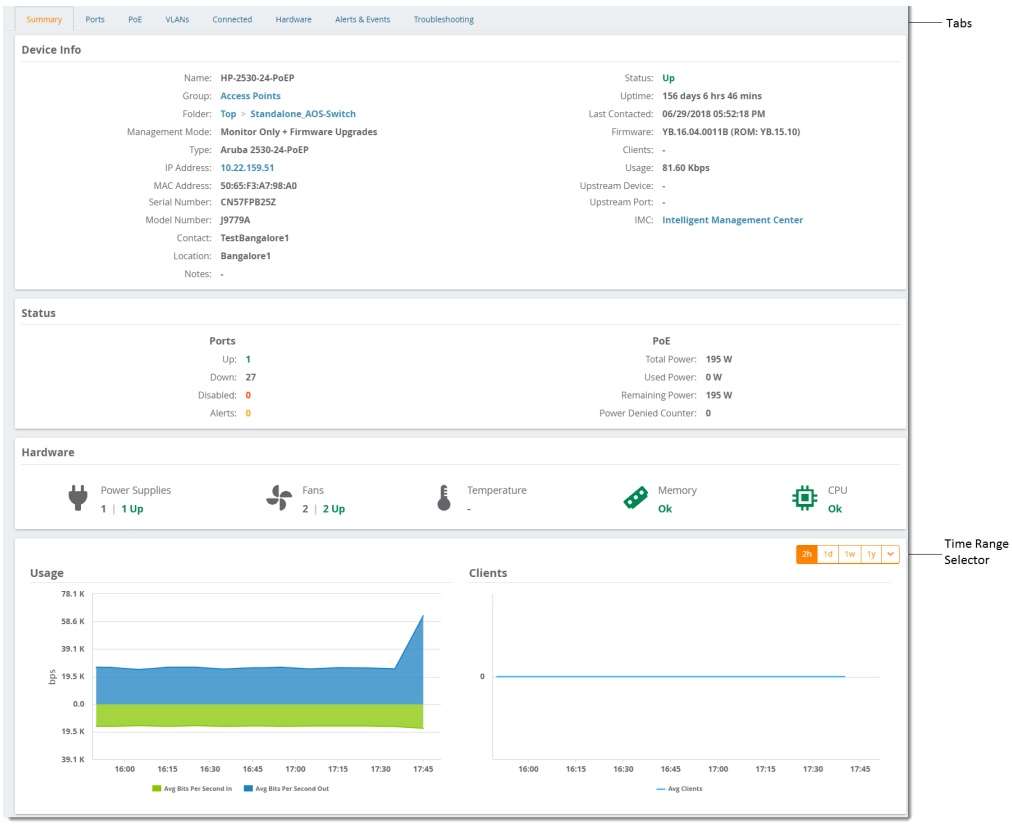
Get details about usage and connected clients by pointing your mouse over the graphs. For more information about monitoring connected clients, see "Viewing the Connected Device Port" on page 191.

Figure 109: *Viewing Graph Tooltips*

Back to the Top

Summary Tab

The Summary tab is the central point for monitoring your switches and switch stacks. Track status like device uptime, trunk and uplink connectivity, available power, number of fans present, environmental information, CPU and memory usage. For stacks, you can see important information like member status, stack topology, and split stacking policy.

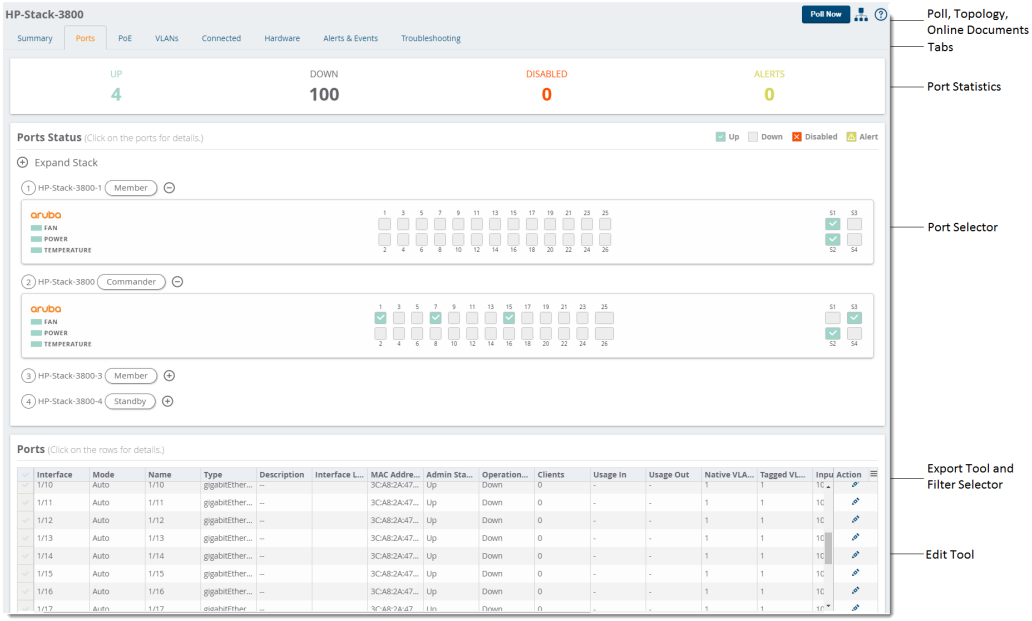


Back to the Top

Ports Tab

With the Ports tab, AirWave displays the front panel of the switch, letting you visualize port status, hardware status, and other properties. Select **Ports** at the top of the Switch Monitoring page to open the Ports tab.

Figure 110: *Ports Tab for a Switch Stack*



See Port Counts

You can see from the colored numbers how many ports are up, down, disabled, or how many alerts are red and require action.

You can also identify SFP ports on a Gigabit switch by their rectangular shape, and stack ports by their number. For example, if there are Stack Ports 1, 2, 3, and 4, you'll see them labeled as S1, S2, S3, and S4 on the switch faceplate, as shown in Figure 111.

Figure 111: *Example of Stack Ports*

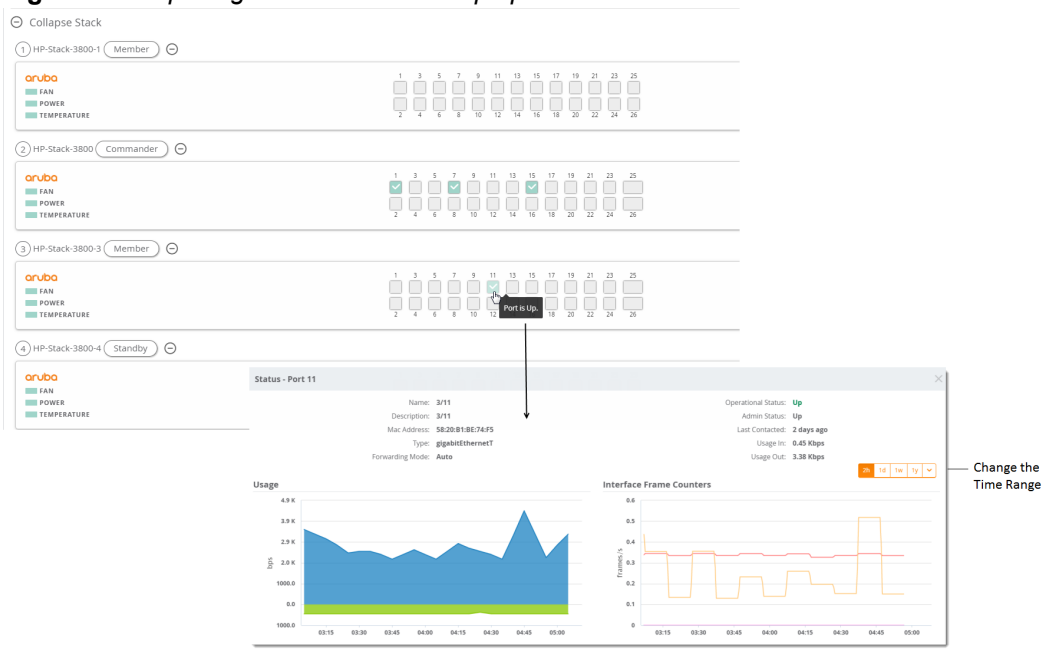
NOTE

Port status isn't available for stack ports.

Open a Port Status Pop-Up

You can point your mouse over the interactive faceplate to view port status, or click the port to view details and graphs in a pop-up window, as shown in Figure 112. If you manage a large number of devices and you want to collapse the view, click ⊖ at the stack or member level.

Figure 112: *Opening the Ports Status Pop-up*

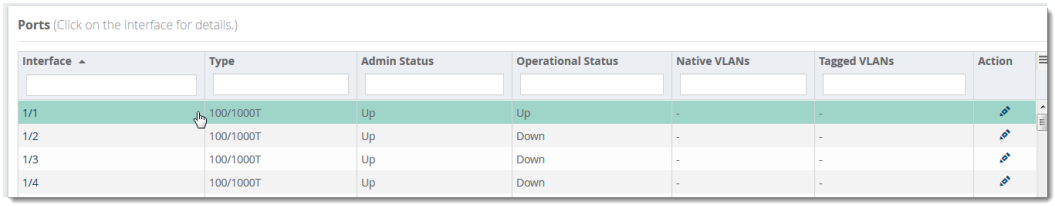


Edit a Physical Interface

You can configure the port interface and add optional details using the Edit tool.

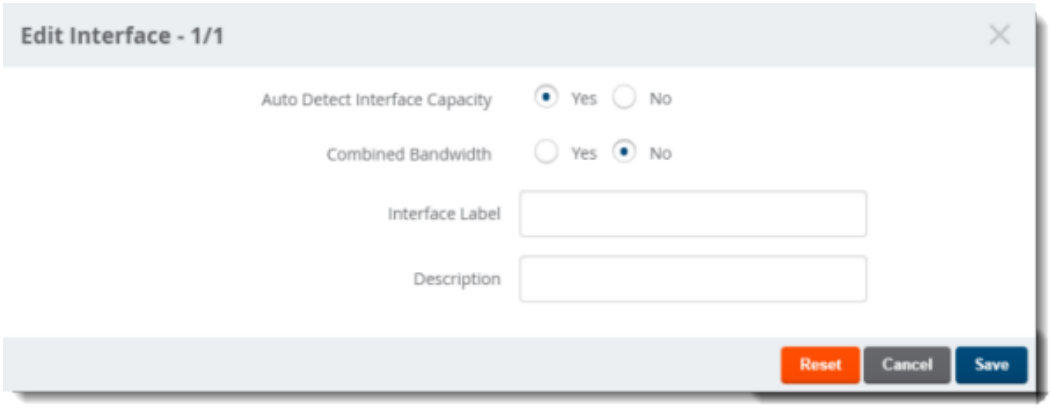
1. From the Ports tab, locate the interface in the Port table.

Figure 113: *Selecting the Interface*



2. Click to open the Edit Interface pop-up window.
3. Type a descriptive label to identify the port interface.
4. Type a port description that could be helpful for anyone tracing the port.

Figure 114: *Edit Interface for a Port*



5. Click **Save**.

Get Interface Details

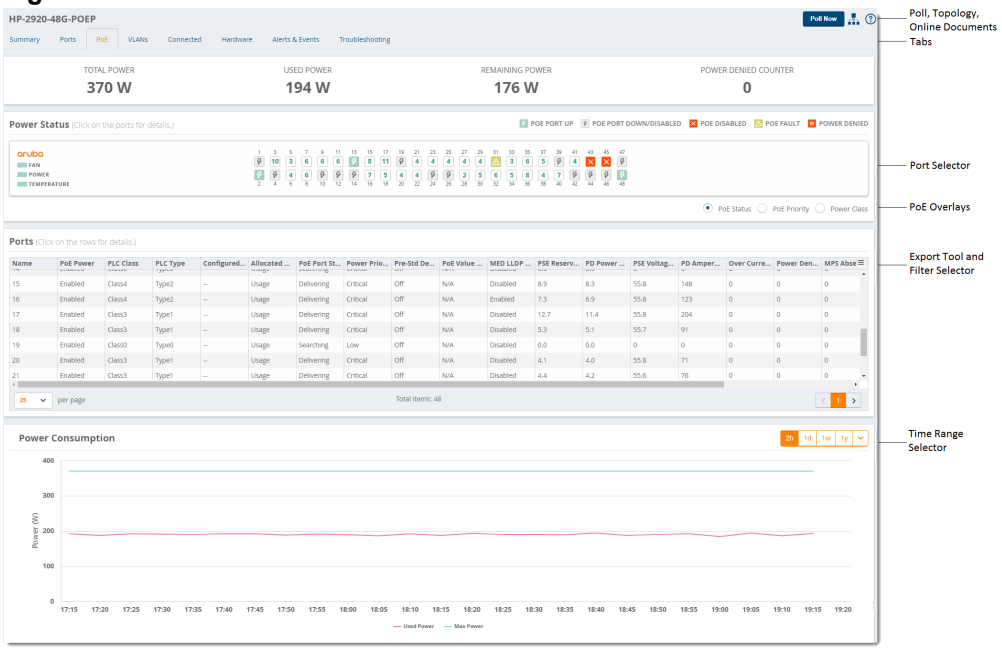
From the Ports table, you can see:

- Interface identified by the interface number.
- Port speed and duplex (data transfer operation), or mode.
- If available, the name of the interface entered on the Edit Interface pop-up.
- Type of port, such as gigabit Ethernet (gigabitEthernetT) and 10 gigabit Ethernet (tenGbE-T).
- If available, information about the interface entered on the Edit Interface pop-up.
- If available, the interface label.
- MAC Address assigned to the interface.
- Admin Status: up or down.
- Operational status of the interface: up or down.
- How many clients are connected to the device.
- If available, the incoming interface load in Kbps.
- If available, the outgoing interface load in Kbps.
- ID number of the native VLAN on the neighbor device.
- Ports that are part of the specific tagged VLAN.
- Input capacity of the interface in Mbps.
- Output capacity of the interface in Mbps.
- Maximum transaction unit (MTU) which can be received on the neighbor device.
- Port duplex mode, which can be set to auto-negotiate the duplex mode when the device makes a network connection, or manually set to full or half-duplex mode.
- If the port is part of a trunk.
- If the port is part of a group of trunks.

PoE Tab

If the switch supports PoE, AirWave provides detailed information on the configuration, power usage, and statistics of a selected port. Select **PoE** at the top of the monitoring page for the switch or stack to open the PoE tab.

Figure 115: *PoE Tab*



See PoE Statistics

High-level counts tell you the total power available, used, and remaining. When more power is required than allowed for a device or port, AirWave will display a powered denied count.

Change the Faceplate Using Overlays

You can change the information you see in the faceplate by selecting the PoE status, PoE priority, or Power Class overlays at the lower right corner of the faceplate.

In Figure 116, Ports B23 and B24 are online and not using power.

Figure 116: *Power Status Overlay*

In Figure 117, the power priority for all the PoE ports is low. If there is a power demand higher than the power budget on the switch, Port B1 has priority over Port B24.

Figure 117: *Power Priority Overlay*

In Figure 118, all the PoE ports are designated as PoE Power Class 0 and must be allocated up to 12.95 W.

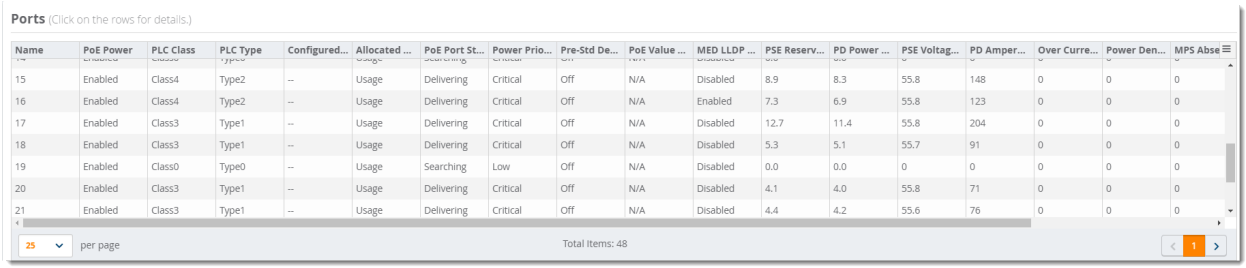
Figure 118: *Power Class Overlay*

Get Port Details

From the Ports table (Figure 119), you can see :

- PoE configuration, including the PoE power, PLC class/type, power allocation method, current PoE port status, power priority, pre-standard detection, and the maximum power draw allocated to a PD on a port.
- LLDP information, including whether the switch supports PoE negotiation over LLDP.
- Statistics like PSE reserved power, actual power drawn from the PD, over current count, power denied count, PSE voltage, PD power draw, MPS absent count, short count, PSE TLV configured, and PSE TLV configured.

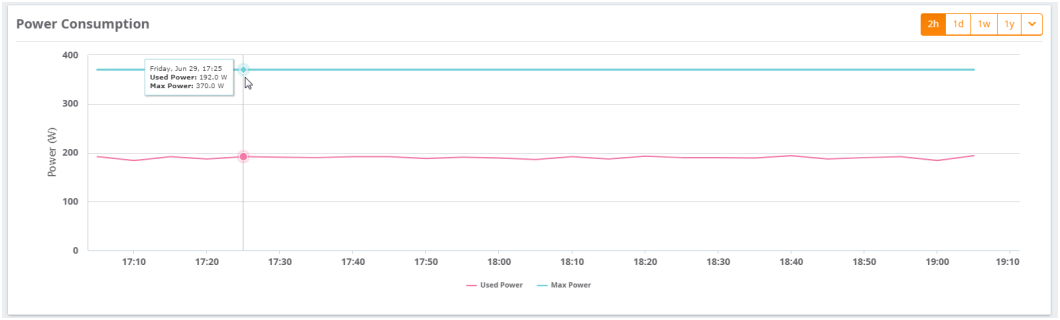
Figure 119: *Ports Table*



View Power Consumption

The Power Consumption graph shows you the maximum power and power in use on the PoE slot, as shown in Figure 120.

Figure 120: *Power Consumption Graph*



Back to the Top

VLANs Tab

The VLANs tab shows all the details about the switch, including the configured VLANs and the port mappings for both tagged and untagged VLANs. Selecting **VLANs** at the top of the monitoring page for the switch or stack opens the VLANs tab.

NOTE

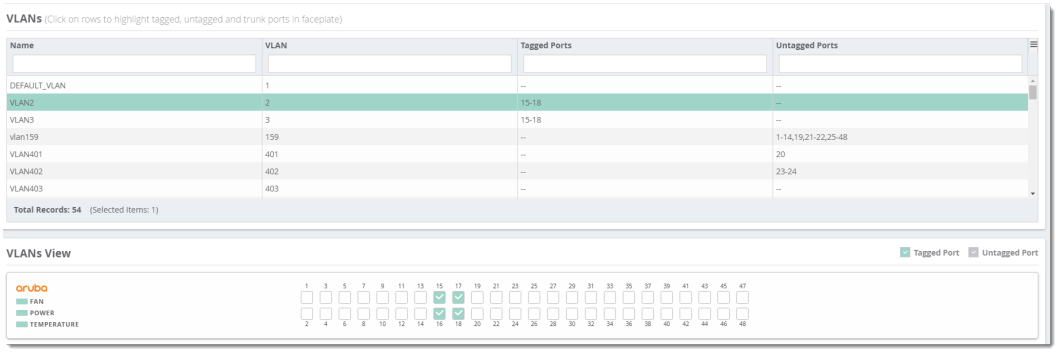
The VLANs tab isn't available for members in the stack, and it is only available from the stack view.

Change the VLANs View in the Faceplate

You can change the VLANs view by select a VLAN from the VLANs table. AirWave highlights the tagged or untagged ports in the faceplate.

In Figure 121, AirWave highlights tagged Ports 15 to 18 when you select VLAN 2.

Figure 121: *Highlighting the Tagged Ports in the Faceplate*



Get Trunk Details

If VLAN trunking information is available, AirWave displays a list of active trunks on the device or the configured trunk groups. Active trunks are trunk groups that have ports assigned to them.

Get Virtual Interface Details

From the Virtual Interface table, you can see:

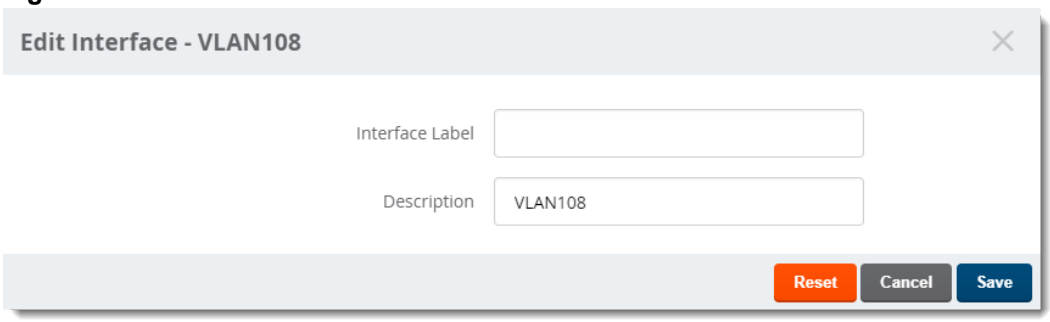
- Interface configuration, including the name, type of interface, MAC address, IP address and an alias, and the IPv6 global unicast address.
- Status on the port and interface.
- If any, interface labels entered on the Edit Interface pop-up. For more information, see "Edit a Virtual Interface" on page 189.

Edit a Virtual Interface

You can configure the virtual interface and add optional details using the Edit tool.

1. Navigate to the monitoring page of a switch that has a configured VLAN.
2. Select the VLANs tab, then scroll down the page to locate the interface in the Virtual Interfaces table.
3. Click  to open the Edit Interface pop-up window.

Figure 122: *Edit Interface*



4. Type a descriptive label to identify the port interface.

5. Type details in the Description field that could be helpful for anyone working with the device.
6. Click **Save**.

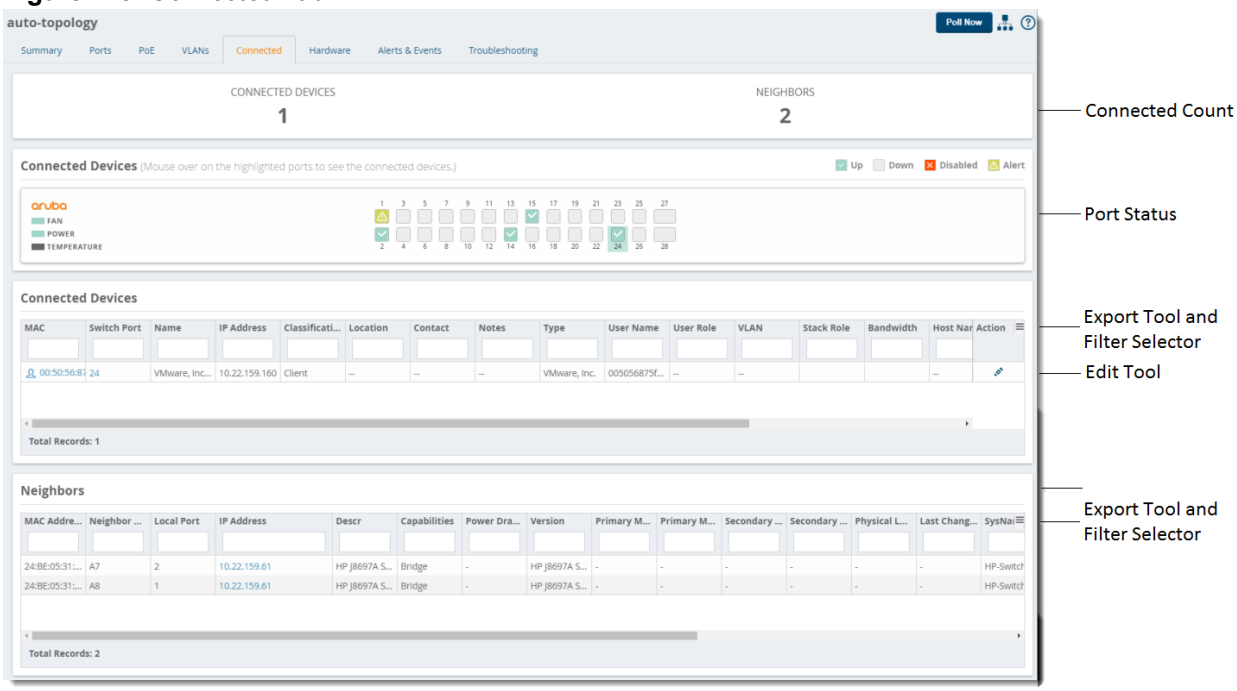
Connected Tab

When AirWave detects client devices connected to the switch and neighbors that are up or down stream, you can access information about them from the Connected tab.

To view connected devices and neighbors:

1. From the navigation sidebar, go to **Devices > List** and select a switch from the list.
2. Select Connected at the top of the Switch Monitoring page.

Figure 123: *Connected Tab*



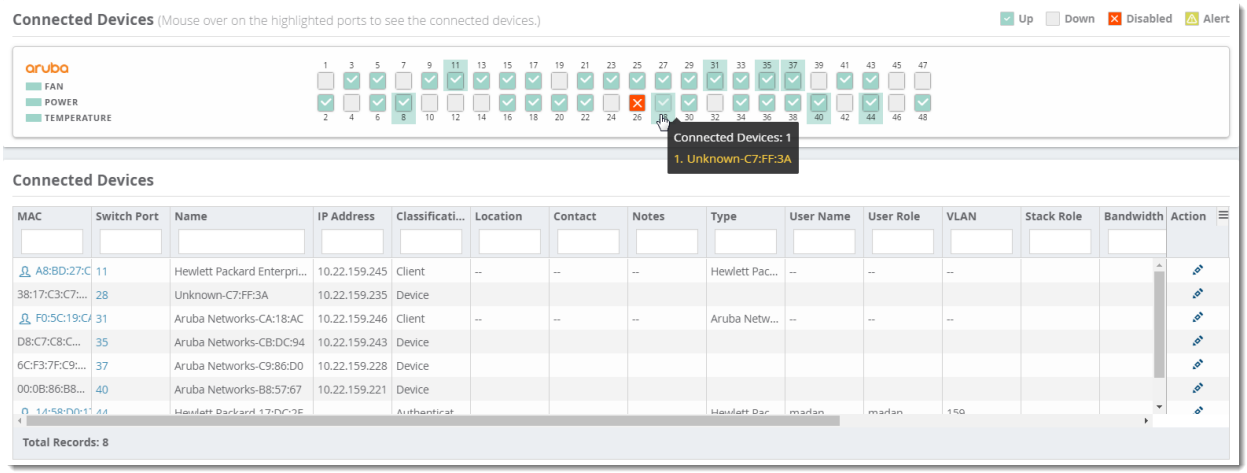
See Connected Device and Neighbor Counts

AirWave detects authenticated and rogue devices and reports them in the Connected Devices table. AirWave also uses upstream data to calculate possible neighbors and reports these devices in the Neighbors table (see Figure 123).

Determine Which Device Is Connected to a Port

Mouse-over the port number to view status and connected devices. In Figure 124, you can see from the tooltip information about the rogue and get the MAC address of the device from the Connected Devices table beneath the faceplate.

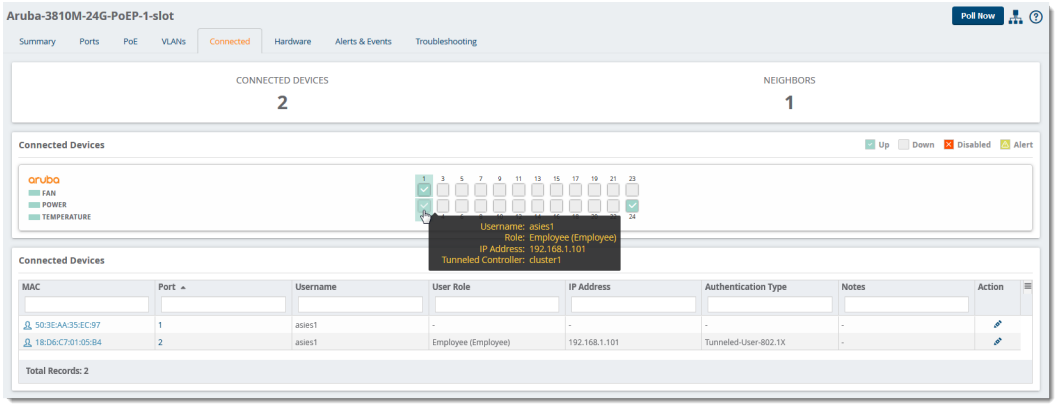
Figure 124: *Viewing Connected Device Details from the Tooltip*



View Dynamic Segmentation Information

In the switch plate view, you can see the pieces of the dynamic segmentation, and when you mouse over the port, how many users are tunneled, user names, user roles, and IP address of the tunneled controller. Figure 125 shows an example where two users are tunneled through Ports 1 and 2 (indicated by the green shaded area which extends over the port number). Beneath the faceplate in the Connected Devices table, AirWave provides the authentication type and MAC address links to the device.

Figure 125: *Viewing the Connected Device Port*



Get Connected Devices Details

Table 85 describes fields that you see in the Connected Devices table.

Table 85: *Connected Devices Fields and Descriptions*

Field	Description
MAC	MAC address for the device. This link provides access to the diagnostics page for the client (see "" on page 215.
Switch Port	Port number associated with the device. This link provides access to the monitoring page for the interface.
Name	Name of the device. You can enter any name.
IP Address	If the gateway is managed by AirWave, the IP address is shown here.

Field	Description
Classification	Displays the classification of the device after AirWave detects the device: • Authenticated Client. This link provides access to the Connected Client page. • Client. This link provides access to the Rogue table, where you can identify the device.
Notes	Notes to help you identify the client. You can enter anything.
Type	Type of device. You can enter anything.
User Name	Name that is used on the device for authentication.
User Role	Identifies the role-based operations that can be performed on the device.
VLAN	The number of the VLAN.
Stack Role	In a stack of switches, the role can be: master.
Bandwidth	The bandwidth used by the device. If the device supports bandwidth per MAC address, the bandwidth shown is the total bandwith used by all attached devices.
Host Name	The hostname of the neighbor device, which is retrieved from the DNS lookup.
Authen Type	The authentication server type: • Dot1x • Captive Portal • Local MAC Auth • WPA-PSK

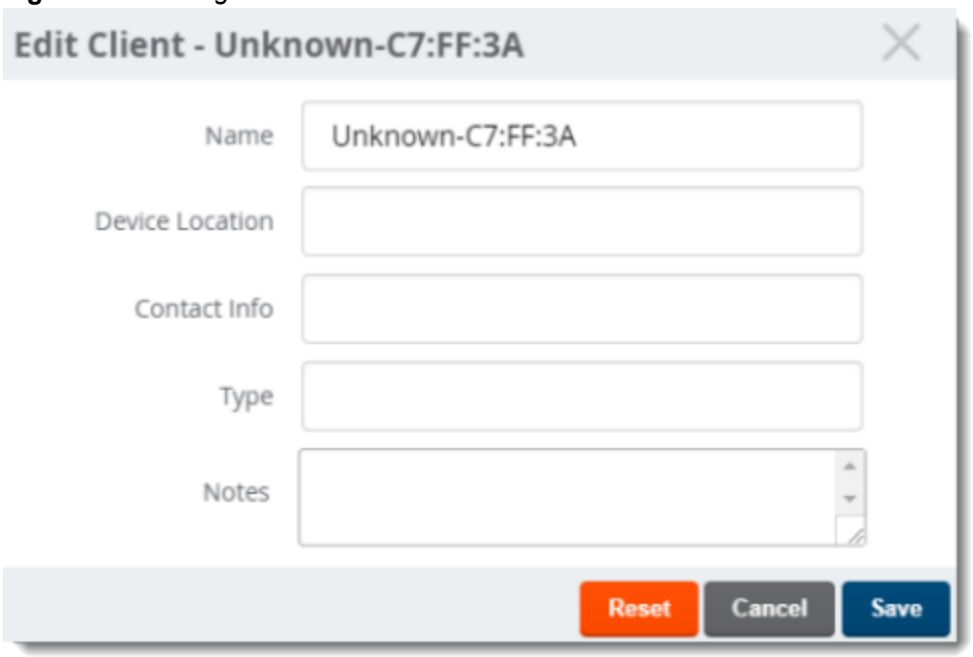
Edit a Connected Device

AirWave doesn't gather much information about connected devices. If you edit a connected device, AirWave reclassifies the devices as an unauthenticated client.

To edit a connected device:

1. Navigate to the monitoring page of a switch that has a connected device.
2. From the Connected tab, locate the device in the Connected Devices table.
3. Click  to open the Edit Client pop-up.

Figure 126: *Editing the Connected Device*



4. Add a name, device type, location, contact, or notes to the unknown device.
5. Click **Save**.

Get Neighbor Details

AirWave uses SNMP/HTTP or CDP/LLDP to discover devices on the network and goes a step further, discovering neighbors directly connected to the switch. You can filter the Neighbors table to display neighbors connected to the port.

Table 86 describes the Neighbors Table fields and descriptions.

Table 86: *Neighbors Table Fields and Descriptions*

Field	Description
Name	Displays the name of the neighbor device. For example, a MAC address, hostname, or make and model. If an IP address is known for the device, a link provides access to the monitoring page for the device.
Neighbor Port	Displays the port ID of the neighbor device.
Local Port	Displays the port ID of the local device device.
Address Type	Displays the type of address of the neighbor device.
Address	Displays the network address associated with the neighbor. This link provides access to the web management interface. Hover your pointer over the to open a management window to the device using HTTP, HTTPs, telnet or SSH.
Desc	Specify a description that provides additional information about the neighbor device (recommended).
Capabilities	Displays the device type: router, switch, or none (information is not available)

Field	Description
Version	Displays the software version running on the neighbor device.
CDP Version	Indicates the software version running on the neighbor device.
Duplex	Indicates the mode of operation of the connection: simplex, duplex, or half-duplex.
Power Drawn (Watts)	Displays the amount of power used on the interface of the neighbor device.
VTP Mgmt Domain	Displays the name of the group of VLANs associated with the neighbor device.
Sysname	Displays the system name of the neighbor device.
Primary Mgmt Address Type	Displays the type of address of the primary management interface.
Primary Mgmt Address	Displays the network address of the primary management interface.
Secondary Mgmt Address Type	Displays the type of address of the secondary management interface.
Secondary Mgmt Address	Displays the network address of the secondary management interface.
Physical Location	Displays the location of the neighbor device.
Native VLAN	Displays the ID number of the VLAN on the neighbor device.
Appliance ID	Displays the ID number of the appliance.
VLAN ID	Displays the ID number of the management VLAN on the neighboring device.
Last Change	Indicates when the device was last seen.
MTU	Specifies the largest packet size which can be received on the neighbor device.
Source	Displays the protocol used for device discovery: CDP.

Hardware Tab

Color-coded thresholds show power status for power supplies, fans, and temperature on the Hardware tab, and graphs show you overall CPU and memory usage (see Figure 127).

You can't customize hardware thresholds.

Figure 127: *Hardware Tab*

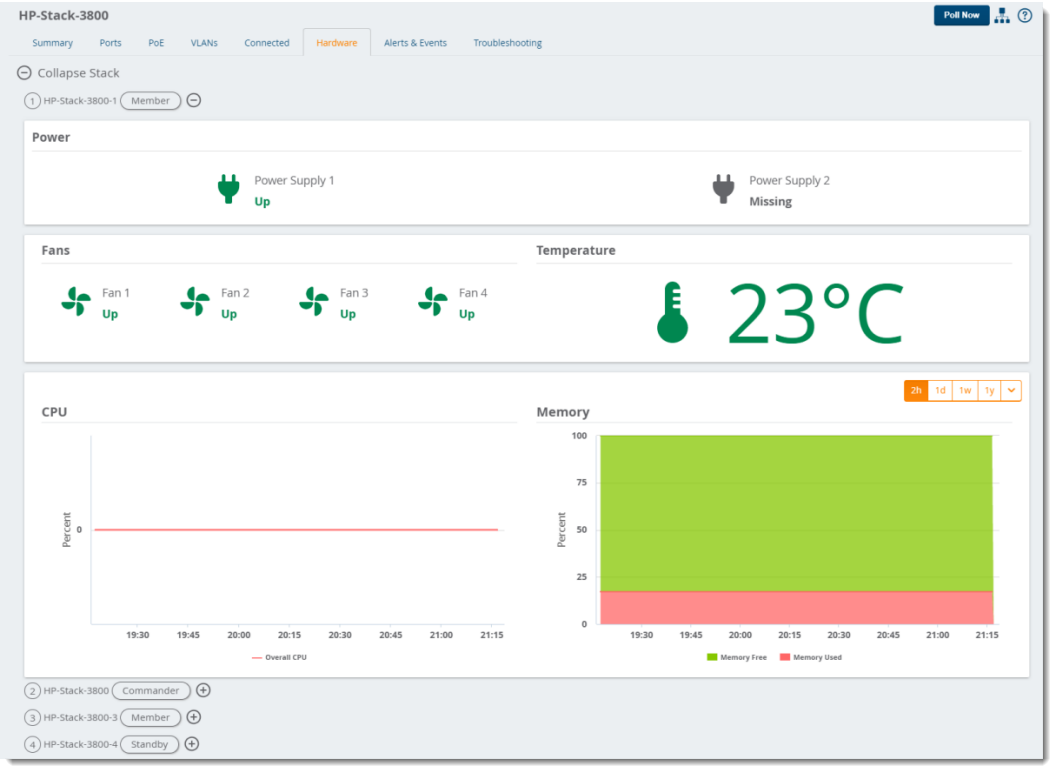


Table 87 describes the color-coded thresholds and icons on the Hardware tab.

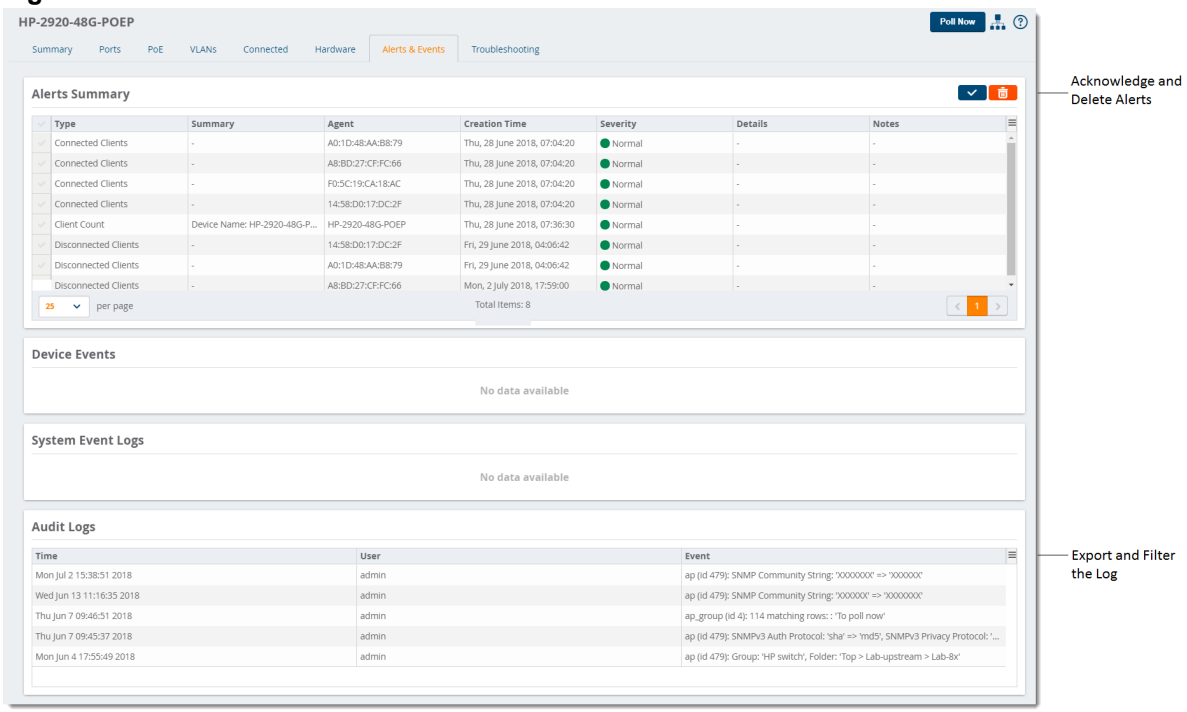
Table 87: *Hardware Status and Thresholds*

Status	Power Supply	Fan	Memory	CPU	Temperature
Good	All power supplies are up. **NOTE:** The status is OK even if there are missing power supplies.	All fans are up. **NOTE:** The status is OK even if there are missing fans.	Usage is < 75%.	Usage is < 75%.	The temperature is in the range of 0° C to 55 ° C.
Fair	NA	NA	Usage is between 75% to 90%.	Usage is between 75% to 90%.	NA
Poor	NA	At least 1 fan is down	Usage is > 90%.	Usage is > 90%.	The temperature is <0° C or > 55° C.
Info	Missing power supplies.	Missing or removed fans.	NA	NA	Information is unavailable.

Alerts & Events Tab

The Alerts & Events Tab provides monitoring information for the device (see Figure 128). AirWave can you alert you to redundant power supply or 802.3bt failures and power consumption or interface outputs reaching capacity.

Figure 128: *Alerts & Events Tab*

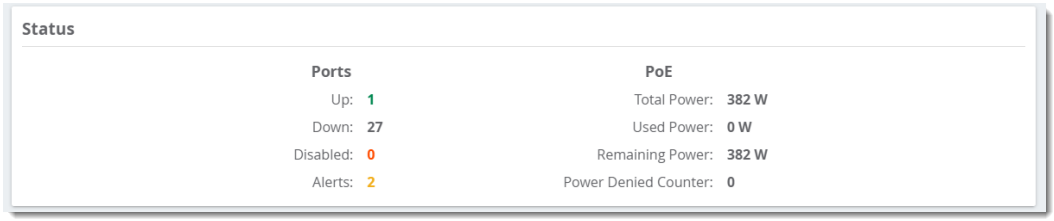


Acknowledge an Alert

To acknowledge an alert:

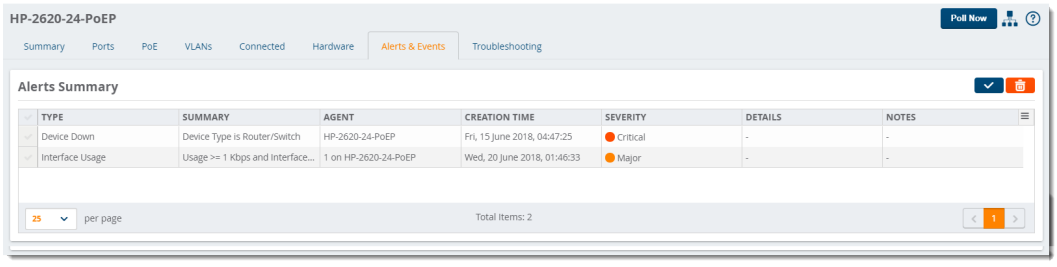
1. Go to **Devices > List**, then select a switch from the list. For example, the status in Figure 129 shows 2 alerts on the switch.

Figure 129: *Viewing Alerts on the Summary Tab*



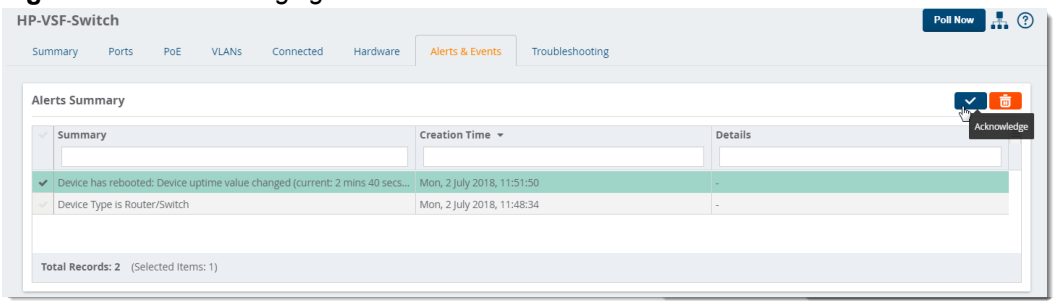
2. Select the **Alerts & Events** tab near the top of the page. Information about the alerts are at the top of the page, as shown in Figure 130.

Figure 130: *Alerts Summary on the Alerts & Events Tab*



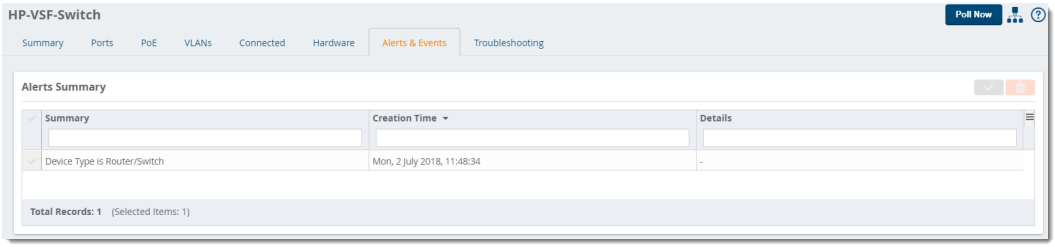
3. Select the alert and click ✓ to acknowledge the alert (Figure 131).

Figure 131: *Acknowledging the Alert*



4. Check the Alerts Summary table to confirm that AirWave cleared the alert (see Figure 132).

Figure 132: *Confirming That the Alert Cleared*



Troubleshooting Tab

Schedule commands to run automatically from the CLI, run commands on a device or a stack, and run cable tests in the Troubleshooting tab.

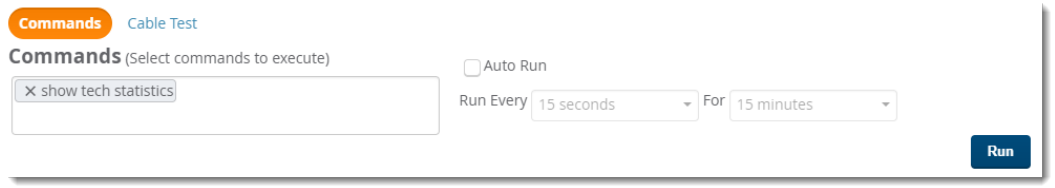
Run a Command

AirWave put all the useful commands into a drop-down menu on the Troubleshooting tab.

To run a command:

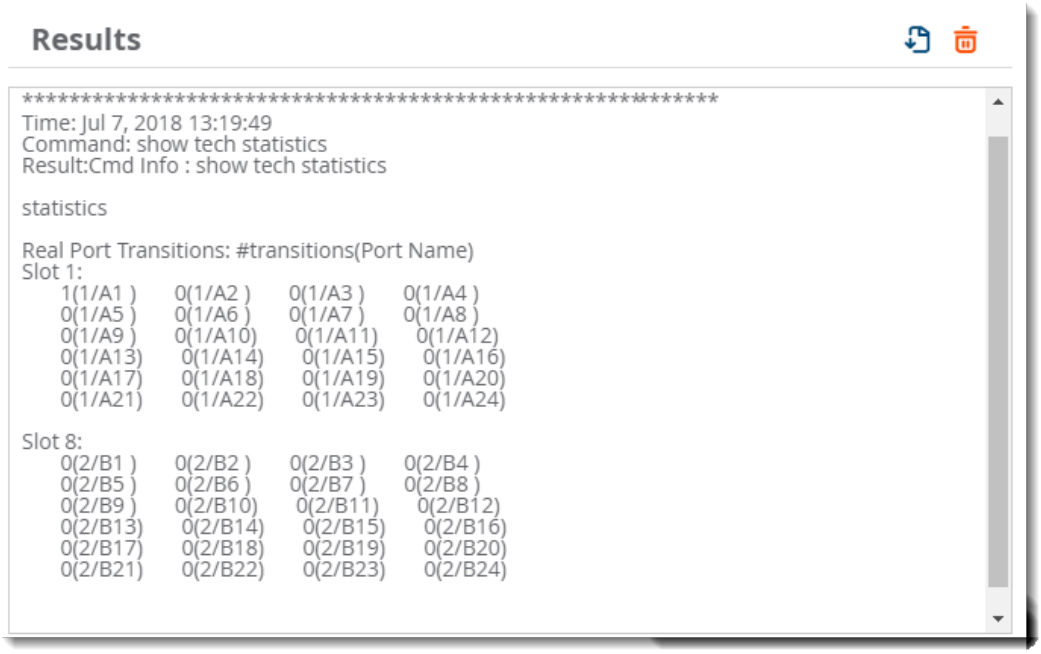
1. Go to **Devices > List**, then select a switch from the list to monitor.
2. In the Troubleshooting tab, click the Command field and select one or more commands from the drop-down.

Figure 133: *Selecting a Command*



3. If you want to schedule a set of commands to run automatically at a specific time, select **Auto Run** and enter a time interval.
4. Click **Run**. The output of the show tech statistics command in Figure 134 shows only 1 port transition in Port A1.

Figure 134: *Viewing the CLI Output*



5. Click to export the results to a text file, or click to clear the results.

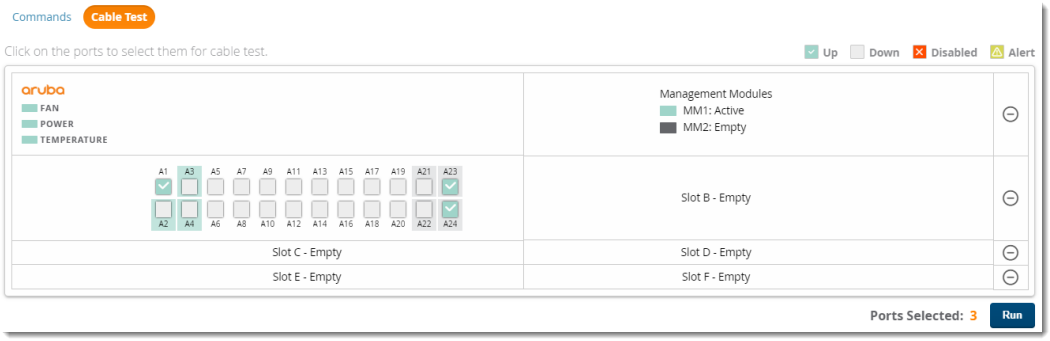
Test a Cable

You can identify a faulty or miswired cable by running a cable test against one or more ports. The cable test might stop or delay the network. AirWave will notify you if this happens.

To run a cable test:

1. Go to Devices > List, then select a switch from the list to monitor.
2. In the Troubleshooting tab, click **Cable Test**.
3. Select the ports from the faceplate. In Figure 135 shows that Ports A2, A3, and A4 will be tested.

Figure 135: *Selecting Ports*



4. Click **Run**.

Monitoring 7000 Controllers

AirWave provides WAN monitoring tools to help you monitor your remote branch network.

In order to use this feature, ensure that you have AMON enabled on the mobility controller. After you add the controller as an Aruba device, you can begin monitoring the managed device. For more information, see "Additional AMP Services" on page 32 and "Adding Devices into AirWave" on page 134.

To open the WAN monitoring page:

1. Navigate to **Devices > List** and select a controller from the list.
2. Click the **Advanced Monitoring** tab at the top of the monitoring page. Clicking the blue **Go Back** link at the top left corner of the WAN Monitoring page will return you to the device monitoring page.

Figure 136: *Accessing the WAN Monitoring Page*

WAN monitoring is described in the following sections:

- "Summary Tab" on page 199
- "WAN Tab" on page 200
- "Tunnel Tab" on page 202

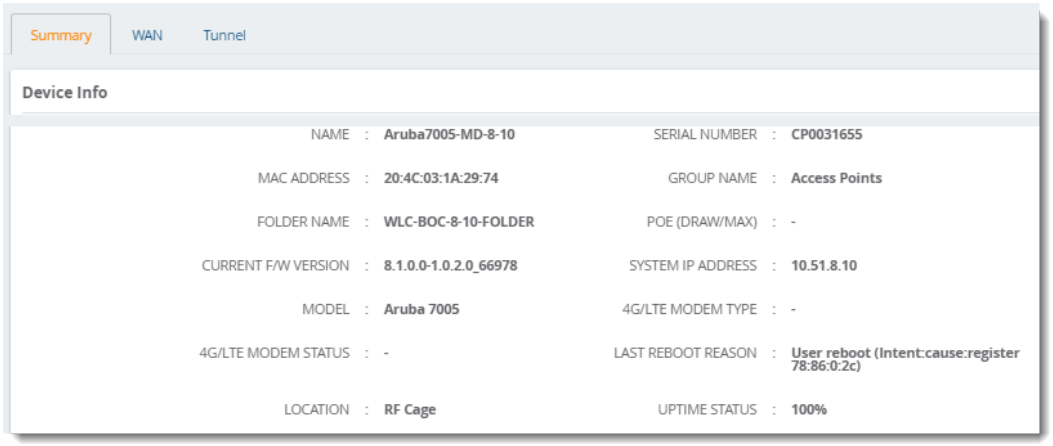
NOTE

Port status isn't available for stack ports.

Summary Tab

The Summary tab is the central point for monitoring your Aruba 7000 Series Mobility Controllers. In addition to device information, such as folder and group membership, firmware version, POE status, and modem status, you can track uplink connectivity.

Figure 137: *Device Information for an Aruba 7005 Mobility Controller*



The following graphs are available on the Summary tab:

- WAN Availability. This graph shows the branch gateway's WAN uplink availability for the selected time range. Availability is determined by default gateway, monitored IP, and data VPN Concentrator reachability.

- VPN Hub Availability. This graph shows the VPN concentrator's tunnel availability. Availability is determined by the probe settings configured using the Health Check option.
- Aggr. WAN Usage. This graph shows the branch gateway's aggregate inbound and outbound traffic usage by WAN interface. You can select "All Traffic" or "Internet vs VPN".
- Aggr. WAN Compression. This graph shows aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage.

Figure 138: *WAN Monitoring Graphs*

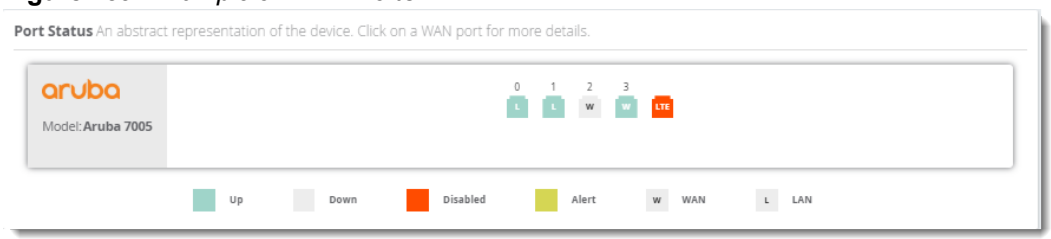
WAN Tab

If the gateway is provisioned as a branch gateway, the WAN tab displays port status, summary information about the WAN interfaces, and details further down the page.

See WAN Ports

You can see from the colored numbers how many ports are up, down, disabled, or how many alerts are red and require action (see Figure 139).

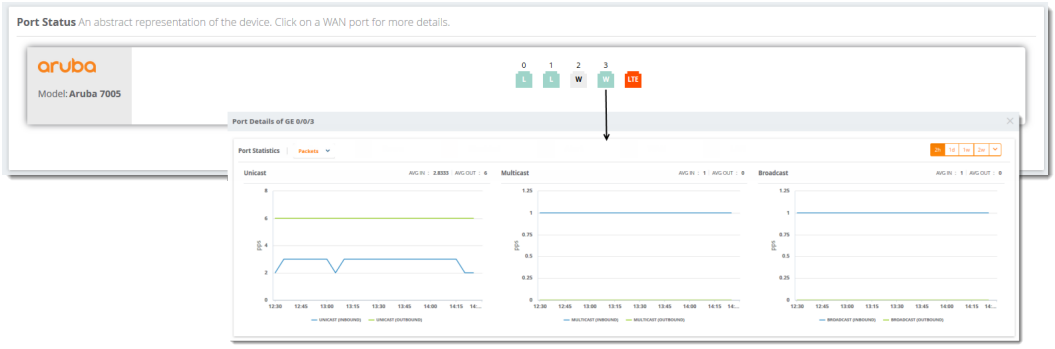
Figure 139: *Example of WAN Ports*



Open the Port Details Pop-Up

You can point your mouse over the interactive faceplate to view port status, or click the port to view details and graphs in a pop-up window (see Figure 140). You can also access the Port Details from the WAN Interface Summary table at the bottom of the page.

Figure 140: *Opening the Port Details Pop-Up*



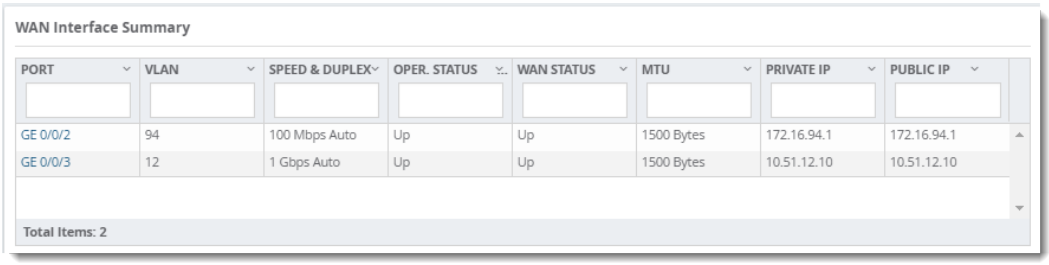
To change the Port Details graphs, from the Port Statistics drop-down list:

- Select "Packets" to view the inbound and outbound packets for unicast, multicast, and broadcast traffic.
- Select "Errors" to view CRC errors, error frames, and collisions.

WAN Interface Summary

The WAN Interface Summary table lists port interfaces and provides the total number of WAN interfaces (see Figure 141).

Figure 141: *WAN Interface Table*



The WAN interface summary table displays the following information:

- Port. Displays the port number as a hyperlink to the Port Details pop-up window.
- VLAN. Displays the VLAN ID.
- WAN Status. Displays the WAN port status.
- Speed & Duplex. Displays the uplink speed and duplex type.
- Oper. Status. Displays the operational status.
- MTU. Displays the MTU size on the port.
- Private IP. Displays the private IP address.
- Public IP. Displays the public IP address.

Get WAN Interface Details

You can select a port from the WAN Interface Details drop down to view the WAN interface details (see Figure 142).

Figure 142: *Selecting a Port*

The following graphs are available on the WAN tab:

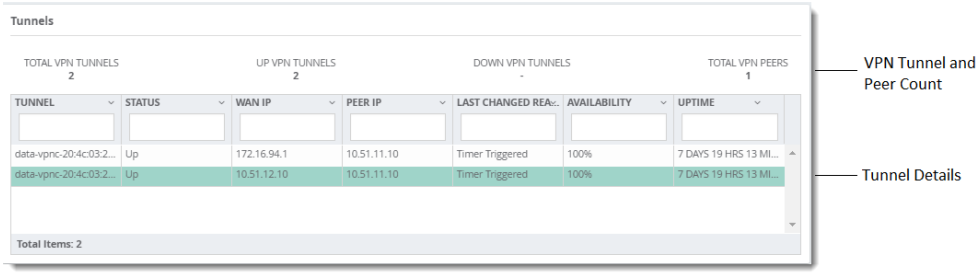
- Availability. Provides a graphical representation of the selected WAN interface's availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway, monitored IP, and VPN Concentrator.
- Throughput. Shows the throughput for the WAN interface in megabits per second.
- Usage. Shows the inbound and outbound traffic usage.
- WAN Compression. Shows the average bandwidth savings from data compression as a percentage.
- Latency. Shows the round-trip time of ping responses in microseconds.
- Jitter. Shows the variation in the delay times of received packets in microseconds.
- Packet Loss. Shows packet loss as a percentage.
- MOS Score. Shows the transport health score, ranging from 1 to 5.

Tunnel Tab

The Tunnel tab displays tunnel counts at the top of the page and details in a table (see Figure 143). For information about the graphs on the page, see "Tunnel Details" on page 202.

See Tunnel Counts and Details

Figure 143: *Tunnels Table*



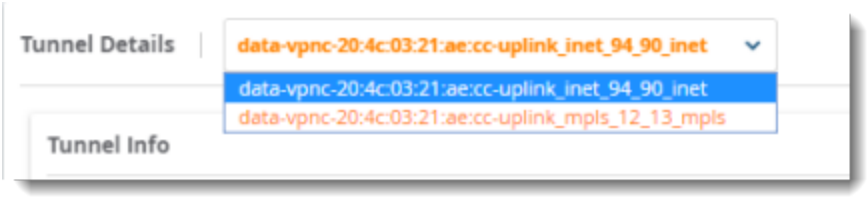
The Tunnels table lists the total number of tunnels and the following details:

- Tunnel. Displays the tunnel number.
- Status. Displays the status of the tunnel.
- WAN IP. Displays the WAN IP address.
- Peer IP. Displays the peer IP address.
- Last Changed Reason. Displays the reason for the last status change of the tunnel.
- Availability. Displays the percentage of time the tunnel was up.
- Uptime. Displays how long the tunnel was up.

Tunnel Details

You can select a tunnel from the drop down at the top left of the Tunnel Details section to view the tunnel interface details (see Figure 144).

Figure 144: *Selecting a Tunnel*



In addition to tunnel information, such as status, IP address, uplink port details, VLAN ID, availability, and uptime, you can view the following graphs on the Tunnels tab:

- Throughput. Displays the inbound and outbound traffic rates for the tunnel.
- Latency. Displays the latency in microseconds.
- Jitter. Displays the jitter in microseconds.
- Packet Loss. Displays the packet loss as a percentage.
- MOS Score. Displays the transport health score, ranging from 1 to 5.

Monitoring Controller Clusters

After adding controller clusters to AirWave, you can get a quick cluster status on the Controller Clusters dashboard. You will find a count of the controllers, APs and clients are associated with these clusters at the top of the page and cluster information, including fault tolerance in the table beneath the counters.

You can access the Controller Clusters dashboard by navigating to **Devices> Controller Clusters**.

Figure 145: *Controller Cluster Dashboard*

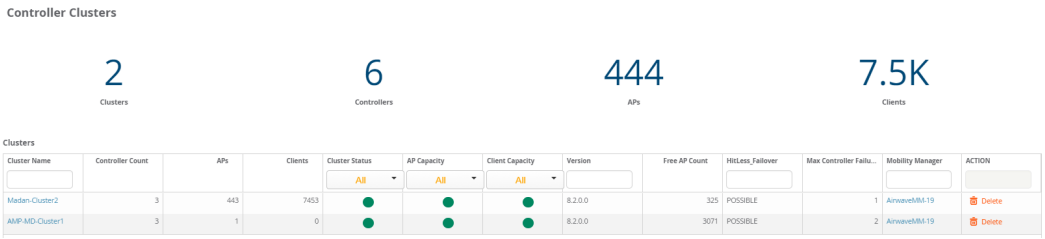


Table 88 describes the fields in the Cluster table. You can select any column heading to sort the data, or enter a text into the column search fields to filter the results.

Table 88: *Clusters Table*

Field	Description
Cluster Name	Name of the controller cluster.
Controller Count	Number of controller in the cluster.
APs	Number of APs associated to controller in the cluster.
Clients	Number of clients connected to controller in the cluster.
Cluster Status	An orange circle indicates that 1 or more cluster controllers is down. A green circle indicates that all controllers are active

Table 88: *Clusters Table (Continued)*

Field	Description
AP Capacity	A green circle indicates that the cluster is below 60% AP capacity. A yellow circle indicates that the cluster is between 60% and 80% AP capacity. An orange circle indicates that the cluster is at greater than 80% AP capacity.
Client Capacity	A green circle indicates that the cluster is below 60% client capacity. A yellow circle indicates that the cluster is between 60% and 80% client capacity. An orange circle indicates that the cluster is at greater than 80% client capacity.
Version	Displays the ArubaOS version running on all the controllers in the cluster.
Free AP Count	Indicates how many APs you can add to a controller before you must add another controller to the cluster.
Hitless Failover	Indicates whether the cluster can handle a hit less failover. The cluster must be L2-connected.
Max Controller Failover	Indicates how many controllers can survive a failover.
Mobility Manager	Displays the host name of the Mobility Master managing the cluster.
Action	Let's you delete the cluster the cluster from AirWave.

Viewing Details about the Controller Cluster

From the Clusters table, you can click on the cluster name to open the **Cluster Detail** page, which displays graphs, controller information, and cluster events.

Capacity Graphs

The graphs show:

- AP Capacity. This graph shows the percentage of a cluster's total AP capacity being used and the percentage of AP capacity being used on each controller in the cluster.
- Client Capacity. This graph shows the percentage of a cluster's total client capacity being used and the percentage of client capacity being used on each 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 at the top right corner of the page.

Controller Statistics

Table 89 describes the fields in the Controllers table. 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 89: *Controllers Table*

Field	Description
Name	Name of the controller in the cluster.

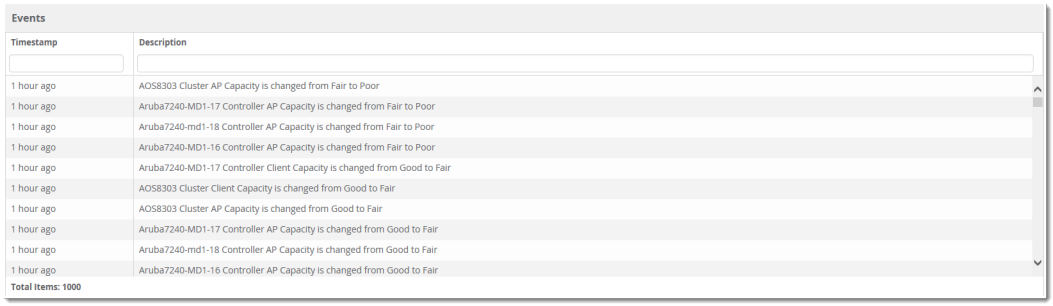
Table 89: *Controllers Table (Continued)*

Field	Description
IP	IP address of the controller in the cluster.
Status	An orange circle indicates that the controller is down. A green circle indicates that the controller is active.
AP Capacity	A green circle indicates that the controller is below 60% AP capacity. A yellow circle indicates that the controller is between 60% and 80% AP capacity. An orange circle indicates that the controller is at more than 80% AP capacity.
Client Capacity	A green circle indicates that the controller is below 60% client capacity. A yellow circle indicates that the controller is between 60% and 80% client capacity. An orange circle indicates that the controller is at greater than 80% client capacity.
Role	Displays the controller's role within the cluster, either **Leader**, **Member**, or **Isolated Leader**.
Type	Displays the controller model type.
Version	Displays the version of ArubaOS running on the controller.

Monitoring Cluster Events

The Events table displays a description and timestamp for each cluster event. In Figure 146, you can see events when a cluster member is deleted, crosses a capacity threshold, or changes its role within the cluster. For information about creating a controller cluster trigger, see "Device Triggers " on page 310.

Figure 146: *Cluster Events*

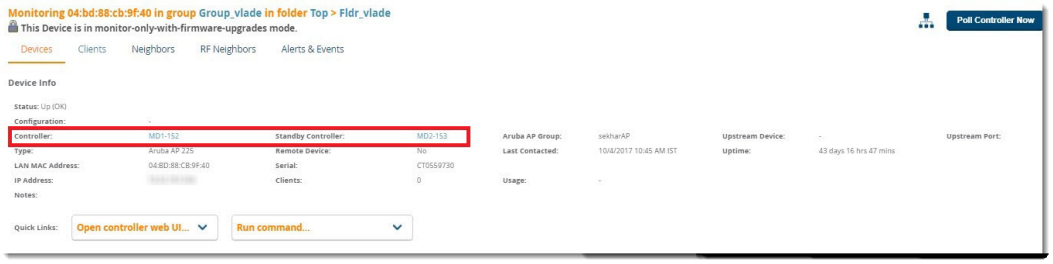


Where to Find Additional Cluster Information

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

- The **Device Info** section of the **Devices > Monitor** page for a cluster controller includes the name of the cluster to which that controller belongs.
- The **Device Info** section of the **Devices > Monitor** page for an AP associated to a cluster controller displays information about its active controller and its standby controller . Figure 147 shows the **Devices > Monitor** page for an AP associated to a cluster member.

Figure 147: *Devices > Monitor page for an AP in a Controller Cluster*



Monitoring Clients

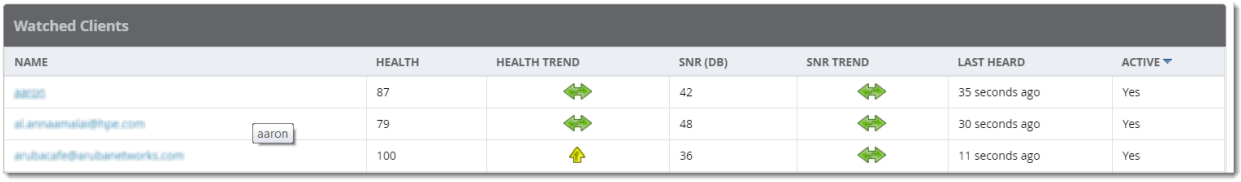
Clients are the end-user devices that access the network through other devices monitored or managed by AirWave. You can view summarized information about all the wired and wireless clients in a dashboard on the **Clients > Overview** page.

Here are some of the things you can view on the dashboard:

- Graphs. The graphs show usage trends for all clients on your network. By default, these graphs show data over the last two hours. You can click in the graph to view details in a popup window, or click 

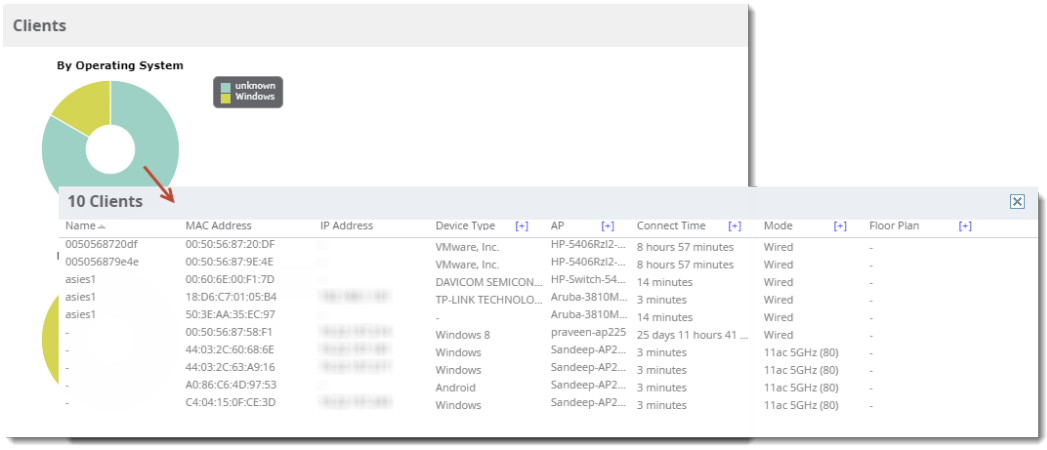
in the top right corner, to change the reported time interval.
- Watched Clients. If any clients are on the watched list, then a Watched Clients table displays on the Overview page, as shown in Figure 148. You can click the client name link to go to the **Clients > Diagnostics** page. Find more information about "" on page 215.

Figure 148: *Watched Clients Table*



- Pie charts. The categories include operating system, device type, SSID, and WLAN vendor. You can click on the chart or the interactive keys to view client details in a popup window, as shown in Figure 149. In the popup window, hyperlinks enable you to drill down further into diagnostic pages, floor plans, and dashboards for UCC, Traffic Analysis, and Clarity. For information about using UCC and Traffic Analysis, see "Using the UCC Dashboard" on page 269 and "Monitoring Application Traffic" on page 267.

Figure 149: *Drilling Down to Client Details*



AirWave also provides several pages from the Clients menu which allow you to perform the following tasks:

- "Monitoring Wired and Wireless Clients" on page 207
- "Monitoring Rogue Clients" on page 208
- "Supporting Wireless Guest Users" on page 209
- "Supporting VPN Users" on page 211
- "Monitoring RFID Tags" on page 212

For information about creating AirWave users and AirWave user roles, refer to:

- "Creating AirWave Users" on page 39
- "Creating AirWave User Roles" on page 41

Monitoring Wired and Wireless Clients

The **Clients > All** page shows all clients that AirWave monitors, including down clients.

The **Clients > Connected** page contains the following information:

- The Folder field shows the current folder of Connected Clients you are viewing. You can view users under a particular folder from the Go to folder drop down menu.
- Links under the Folder fields showing the **Total Devices**, **Mismatched**, **Clients**, and **Usage** (a static, unlinked statistic) summarize the device information for this folder. Select these links to open detail pages for each:
  - **Total Devices** redirects to the **Devices > List** for that folder,
  - **Mismatched** redirects to the list in **Devices > Mismatched** for that folder.
  - **Clients** refreshes the page but expands to include users in the subfolders.
- Interactive graphs display average and max **Clients** over time, and **Usage** in and out for the selected folder over time.
  - Select a time range option from the upper-right corner of the graphs.
  - Select the WLANs drop down to view up to six clients, or select Total Clients.
  - Click in a graph to view a pop-up of the graph.
- Below the Clients and Usage graphs is the list of connected users.

The number of clients in AirWave can differ from the number of clients that you see on the controller. This is because AirWave and the controller count clients differently. The controller counts connections to the network as clients, while AirWave counts devices as clients. For example, in the case where a single device connects to the network multiple times, the controller will count one client for each connection that the device makes to the network. AirWave will only recognize the device as a single client, though, regardless of the number of connections.

The columns in the default view of the **Clients > Connected** and **Clients > All** pages are defined in AirWave and cannot be modified. However, you can create a new view in each of these pages that returns custom information based on the filter parameters and data columns you selected when creating that new view. For more information, see "Creating Filtered Views" on page 150.

The information on this page can also be adjusted in the following ways:

- The **Alert Summary** section displays custom configured alerts that were defined in the **System > Alerts** page.
- Use the **Filter** icon ( ) next to certain columns (**AP/Device**, **Role**, **VLAN**, **Connection Mode**, and others) to filter the results by one of the values under that column. You can filter the list by substring match under the **Username** column.

The **Clients > Connected** page includes SSID information for users, and can display wired users using remote Access Point (RAP) devices in tunnel and split-tunnel mode.

Figure 150: *Default View: Connected Clients Table*

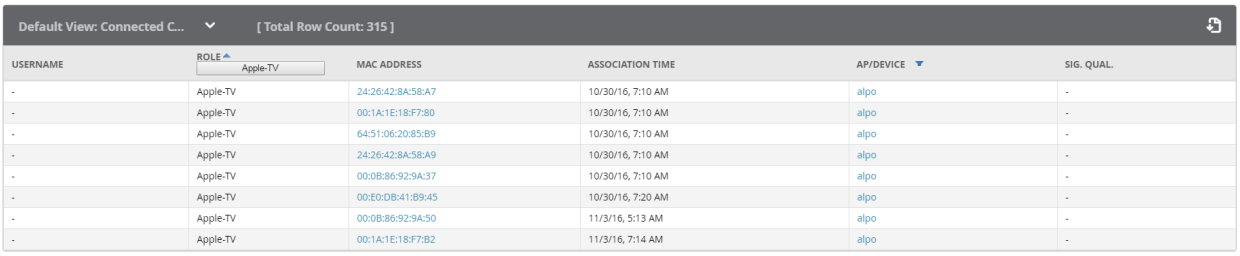


Table 90: *Default View: Connected Clients Table Fields and Descriptions*

Field	Description
AP/Device	Displays the name of the AP to which the MAC address is associated as a link to this AP's **Devices > Monitor** page.
Association Time	The first time AirWave recorded the user for this association.
MAC Address	The radio MAC address of the user associated to APs as a link to the **Users > Detail** page for this user.
Role	Specifies the role that the Aruba controller assigned to the connected user, such as employee.
Username	Displays the name of the user associated to the AP. AirWave gathers this data from device traps, SNMP polling, or RADIUS accounting. User names appear in italics when a user name for that MAC address has been stored in the database from a previous association, but AirWave is not getting a user name for the current association. This may indicate that the user has not yet been authenticated for this session or AirWave may not be getting a user name from an external source.

Monitoring Rogue Clients

You can view connected rogue clients in AirWave by navigating to **Clients > Rogue Clients**, as shown in Figure 151.

From the Rogue Clients page, you can:

- Click the MAC address of a rogue to classify the device on the **Client > Client Details** page.
- Click the Rogue AP link to review the AP Details, rogue associations, and discovery events on the **RAPIDS > Details** page for the AP.

Figure 151: *Clients > Rogue Clients Page*

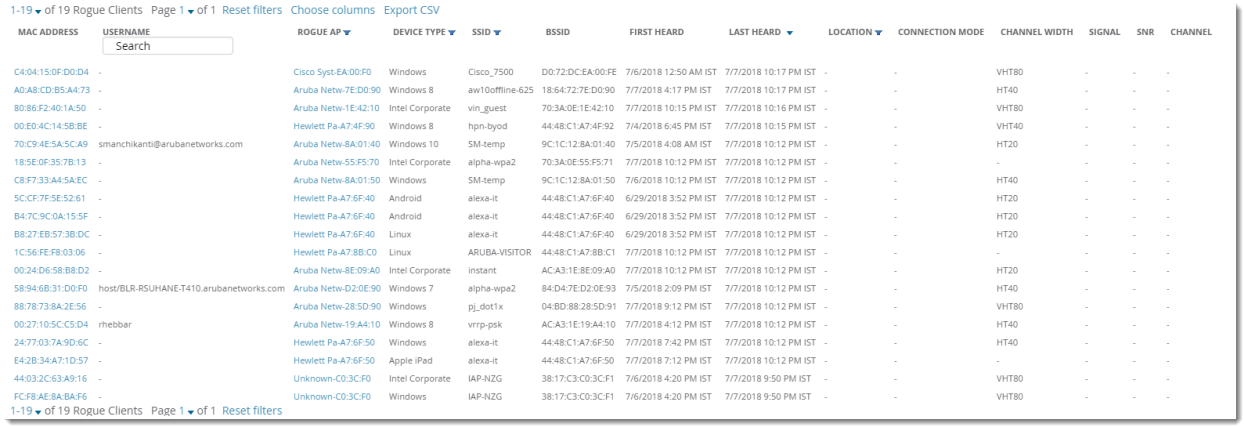


Table 91 describes the fields on this page.

Table 91: *Clients > Rogue Clients Fields*

Field	Description
MAC Address	Displays the MAC address of the rogue client. Click on this to jump to the **Clients > Client Detail** page for this rogue.
Username	The user name associated with this client.
Rogue AP	The name of the Rogue AP. Click on this to jump to the **RAPIDS > Detail** page for this AP.
Device Type	The type of device, such as iPhone, Windows 7, etc.
SSID	The SSID of this client.
BSSID	The BSSID of this client.
First Heard	The date and time when this rogue client was first noticed.
Last Heard	The date and time when this rogue client was last noticed.
Location	If a location is available, you can click on this link to open the VisualRF floor plan and location on which this client resides.
Connection Mode	Shows the type of connection, such as 802.11n, 802.11b, etc.
Ch BW	Shows the channel bandwidth for this rogue client.
Signal	Shows the signal value for this rogue client.
SNR	Shows the signal-to-noise ratio.
Channel	Shows the channel on which this rogue client is broadcasting.

Supporting Wireless Guest Users

AirWave supports guest user provisioning for Aruba Networks, Dell Networking W-Series, Alcatel-Lucent, and Cisco WLC devices. This feature allows employees to create user accounts that allow guests to access a wireless

network.

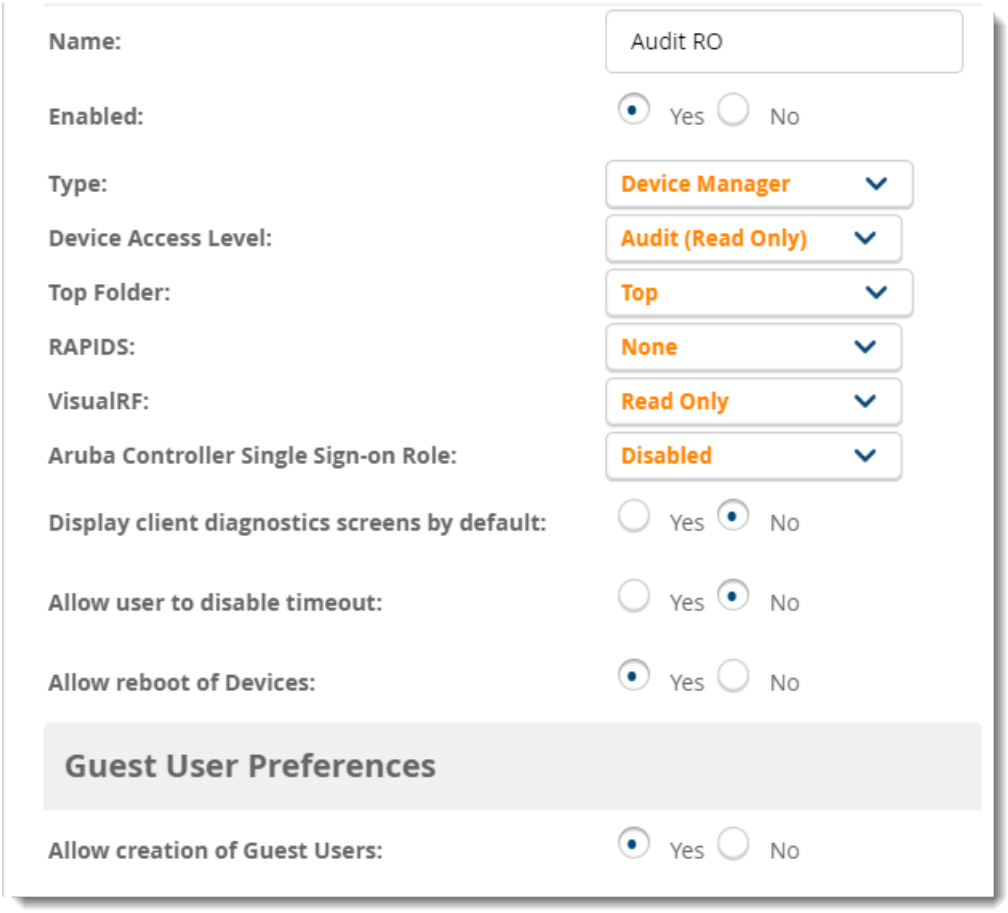
NOTE

In order to configure these settings in the **Guest User Preferences** section on **AMP Setup > Roles > Add** page and the **Clients > Guest Users** subtab, you must enable the **Guest User Configuration** option on the **AMP Setup > General > Device Configuration** page.

Configure the Audit Role

1. Navigate to the **AMP Setup > Roles** page, then click **Add** to create a new role.
2. Enter a name for the role, then select **Device Manager** type and **Audit (Read Only)** device access level.
3. In the **Guest User Preferences** section, click **Yes** to enable the **Allow creation of Guest Users** option.

Figure 152: *Creating an Audit Role*



4. Click **Add** to save the role.

Create the Audit User

1. Go to **AMP Setup > Users**, then click **Add** to create a new audit user.
2. Enter the following information:
   - **Username**. Name for the user.
   - **Role**. This is the role you created in Step 3.
   - **Password**. Password used to authenticate the user.
   - Optionally, enter a **Name**, **Email**, **Phone**, or **Notes**.

   This user information should be given to employees who will create guest user accounts.
3. Click **Add** to save the audit user.

Create a Guest User

1. Go to **Clients > Guest Users**, then click **Add** to create guest users. Or, you can edit existing users and repair guest user errors from the page.
2. To add a new guest user, select **Add**, and enter the following information:
   - **Username**. Click **Generate** to get a random name which will appear on the **Guest User** detail page.
   - **Password**. Click **Generate** to get a random password which will appear on the **Guest User** detail page.
   - **Name**. Enter a name for the guest user.
   - Optionally, enter a **Company Name**, **Sponsor Name**, **Expiration**, **WLAN Profile** (applies to only Cisco WLCs), or **Description**. If you want to send the guest user credentials to email recipients, click **Yes** and enter the email addresses.
3. Click **Add** to save the guest user.

After you create the wireless guest user, the **Clients > Guest Users** page displays guest users and information, such as the expiration date and the SSID for Cisco WLC.

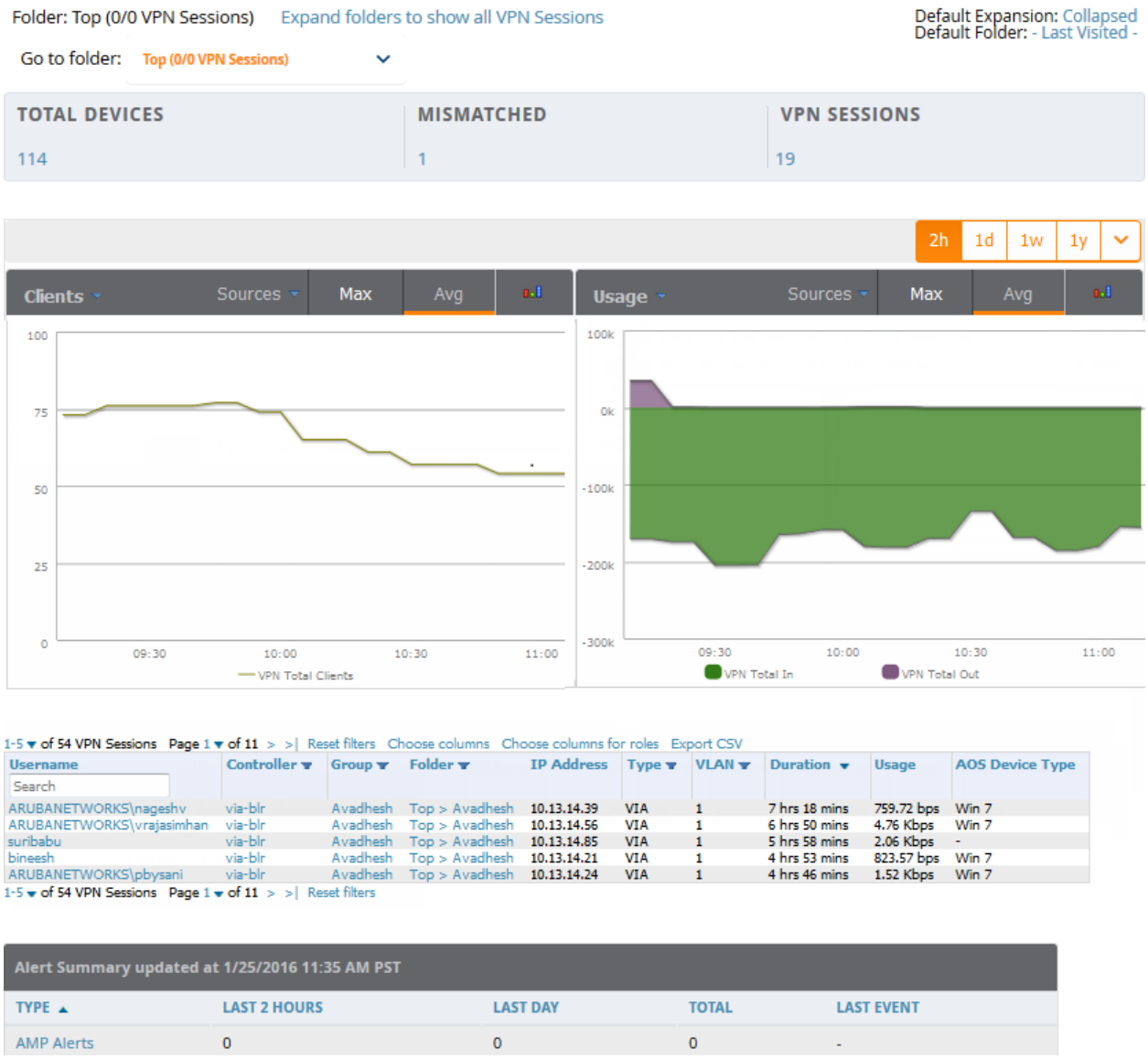
Repair Guest User Errors

The **Clients > Guest Users** page reports current status by the controller. If error messages appear in the **Status** column, select the guest user and click **Repair guest user errors**.

Supporting VPN Users

The **Clients > VPN Sessions** page shows active VPN Sessions along with device type and HTTP fingerprinting information.

Figure 153: *Clients > VPN Sessions Page Illustration*



When a VPN user name is selected, a **Clients > VPN User Detail** page displays with current VPN sessions, a user and bandwidth interactive graph, and a historical VPN sessions list table.

Monitoring RFID Tags

Radio Frequency Identification (RFID) uses radio wave tags to identify and wireless devices with radio waves. Active tags have a battery and transmit signals autonomously while passive tags have no battery. RFID tags often support additional and proprietary improvements to network integration, battery life, and other functions.

Supported RFID tag vendors include: Aeroscout, Ekahau, Innerwireless-PanGo, Vestac, and Newbury.

The **Clients > Tags** page displays the RFID tags that are heard by thin APs and reported back to a controller that AirWave monitors. Figure 154 shows an example of the list of tags.

To identify lost or stolen inventory, you can use the **Inactive Tag** trigger to generate an alert if a tag is not reported to AirWave after an interval. For information about enabling this trigger, refer to "Client Triggers" on page 314.

Figure 154: *Tags Table*

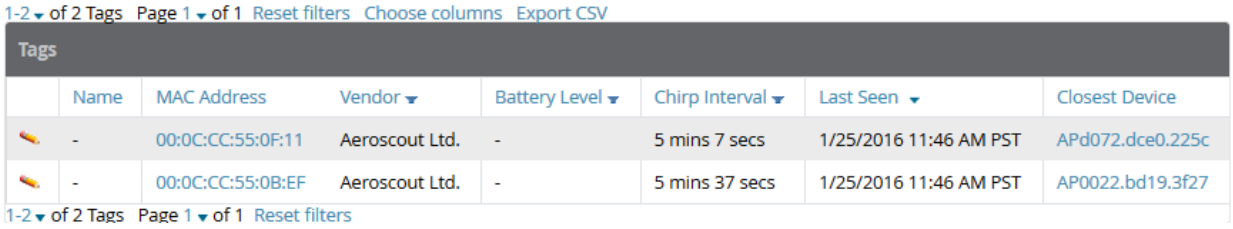


Table 92 describes the **Tags** table fields.

Table 92: *Tags Table Information*

Field	Description
Name	User-editable name associated with the tag. Click the **pencil** icon to edit the name, or add notes to the tag.
MAC Address	MAC address of the AP that reported the tag.
Vendor	Vendor of the tag. You can display all or filter by vendor.
Battery Level	Displays battery information—filterable in drop-down menu at the top of the column; is not displayed for Aeroscout tags.
Chirp Interval	Displays the tag chirp frequency or interval, filterable from the drop-down menu at the top of the column. Note that the chirp interval from the RFID tag influences the battery life of active tags as well as search times. If a tag chirps with very long chirp interval, it may take longer time for the location engine to accurately measure x and y coordinates.
Last Seen	Date and time the tag was last reported to AirWave.
Closest Device	The device that last reported the tag to the controller (linked to the AP monitoring page in AirWave).

Managing Mobile Devices with SOTI MobiControl and AirWave

Overview of SOTI MobiControl

SOTI MobiControl, the mobile device management platform for Windows Mobile, Apple, and Android devices, has been integrated into AirWave to provide direct access to the MobiControl Web Console.

MobiControl runs on your Mobile Device Manager (MDM) server. This server provisions mobile devices to configure connectivity settings, enforce security policies, restore lost data, and other administrative services. Information gathered from mobile devices can include policy breaches, data consumption, and existing configuration settings.

Refer to the following for additional information:

- "Prerequisites for Using MobiControl with AirWave" on page 214
- "Adding a Mobile Device Management Server for MobiControl" on page 214
- "Accessing MobiControl from the Clients > Client Detail Page " on page 215

Prerequisites for Using MobiControl with AirWave

In order to use the MobiControl integration in AirWave, the following is required:

- An 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 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 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 AirWave, navigate to **AMP Setup > MDM Server** and click **Add**. Complete the fields on this page. Table 93 describes the settings and default values:

Table 93: *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, AirWave will connect to port 80 of the SOTI server; with HTTPS, 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 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 AirWave polls the MDM server. The default is 5 minutes.

2. When finished, select **Add.**

The list page for the MDM server also displays:

- **Last Contacted –** The last time AirWave was able to contact the MDM server.
- **Errors** – Issues, if any, encountered during the last contact.

During each polling period, 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 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.

Troubleshooting Client Issues

AirWave enables you to monitor and diagnose end-user issues from the **Clients > Client Detail** and **Clients > Diagnostics** pages. The following sections describe typical tasks you can do.

- "Evaluating User Status" on page 215
- "" on page 215

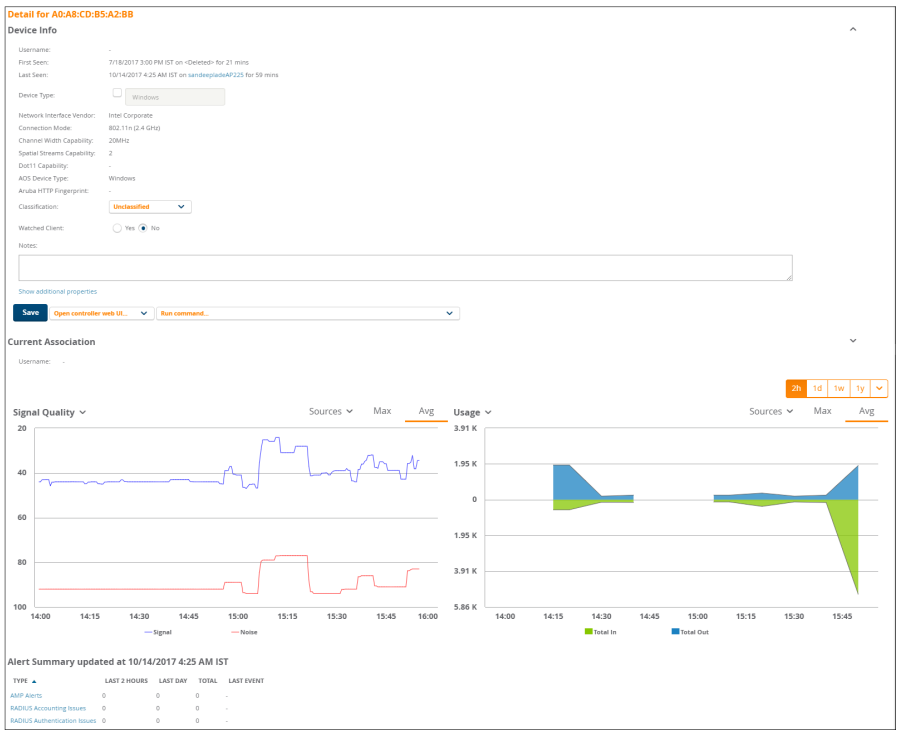
Evaluating User Status

From the **Clients > Client Detail** page, you can review device information for wired and wireless devices, evaluate signal quality and usage graphs, and respond to alerts.

You can access this page by doing one of the following:

- Search for a user. In the resulting window, click the MAC address link.
- Click the MAC address link in the **Devices > Monitor** page, the **Clients > Connected** page, or the **Clients > All** page.

illustrates a partial view of the **Client Detail** page.



Here are some additional things you can do from the **Clients > Client Detail** page:

- View the location of a device . If VisualRF is enabled, you can view a map of the user location and facility information.
- Add a client to a watched List. You can enable the **Watched Client** option on this page to add a client to the **Watched Clients** list on the **Clients > Overview** page, allowing you to track performance metrics for selected clients. For example, you might have a user who repeatedly reports connectivity issues when moving from one room to another. Adding this client to a watched list allows you to track client issues.
- View client neighbors. You can monitor neighbors that AirWave discovers on the **Client Neighbors** table.
- View UCC Information. View call details for a client on the **UCC Calls** table
- View Clarity data. You can view a timeline of all phases of the client connecting to a network on the **Clarity** graphs.
- View association history. View the **Association History** table to see a list of devices to which the client has associated. more information, see "Viewing the Client Association History" on page 218.
- View rogue association history. View the **Rogue Association History** table to see a list of devices to which the client has associated.For more information, see "Viewing the Rogue Association History" on page 218.

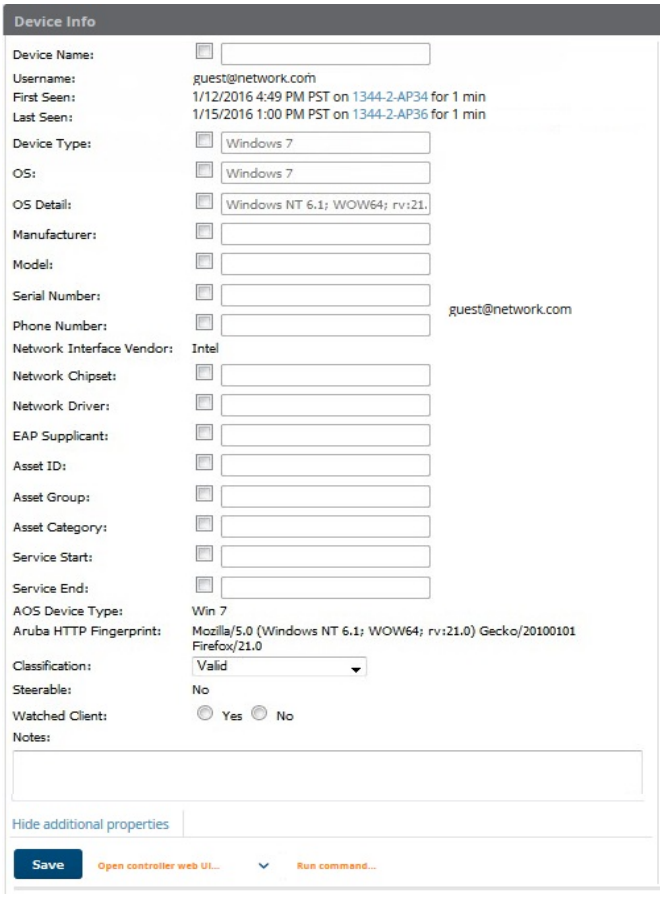
Enabling Mobile Device Access Controls

Mobile Device Access Control (MDAC) secures, provisions, and manages network access for Apple® iOS and other employee-owned mobile devices by enabling device fingerprinting, device registration, and increased device visibility. For more information on MDAC, refer to http://www.arubanetworks.com/technology/mobile-device-access-control/.

To display these options:

1. select the **Show additional properties** link at the bottom of the **Device Info** section of the C**lients > Client Detail page**.
2. Enable these additional settings them by selecting the check box next to the Device Type, OS , OS Detail , and Manufacturer fields.
3. Enter a value for each field, then click **Save**.

Figure 155: *Showing Additional Properties*



Classifying Aruba Devices

If you have deployed Arubacontrollers and have WMS Offload enabled on the network, the **Classification** setting in the **Device Info** section of the **Clients > Client Detail** page allows you to classify the device, and to push this configuration to the controllers that govern the devices. The classifications options are as follows:

- **Unclassified**—Devices are unclassified by default.
- **Valid**—If the **Protect Valid Stations** option is enabled, this setting designates the device as a legitimate network device. When this **Valid** setting is pushed, this setting prevents valid stations from connecting to a non-valid AP.
- **Contained**—When this status is pushed to the device, Aruba will attempt to keep it contained from the network.

You can classify the user regardless of whether WMS Offload is enabled. If WMS Offload is enabled, the classification will get pushed to the controller.

Accessing Quick Links to Aruba Devices

The Device Info section of the **Clients > Client Detail** page includes the following drop-down menus to support quick access to Aruba devices

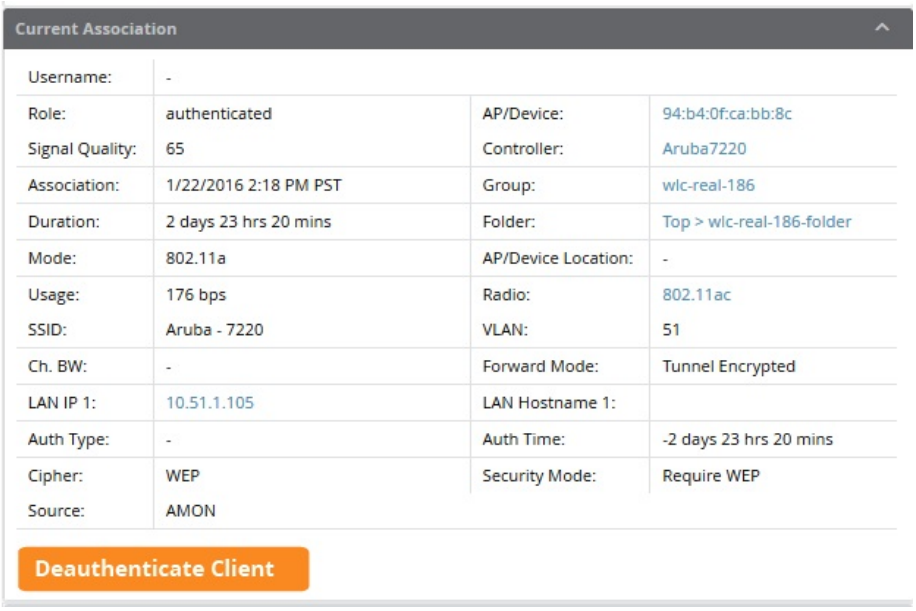
- **Open controller web UI:** A drop-down menu that allows you to jump to the controller's WebUI in a new window.
- **Run command:** A drop-down menu with a list of CLI commands you can run directly from the **Devices > Monitor** page.

Figure 156: *Open Controller Web UI and Run Command Menus*

Deauthenticating a Client

Aruba controllers and Cisco WLC running firmware version v4.0.0.0 or later support the **Deauthenticate Client** feature. To use this feature, expand the **Current Association** section of the **Clients > Client Detail** page, then click **Deauthenticate Client**. (see Figure 157).

Figure 157: *Deauthenticating the Client*

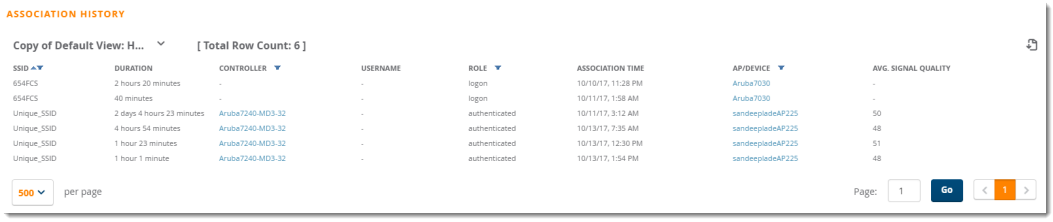


Viewing the Client Association History

Past association details of a client are tracked in the **Association History** table, which is located under the VisualRF illustration (if available) and the **Alert Summary** in the **Client Detail** page.

The columns in this table, shown in Figure 158, are the same as the fields in the **Current Association** section for this user.

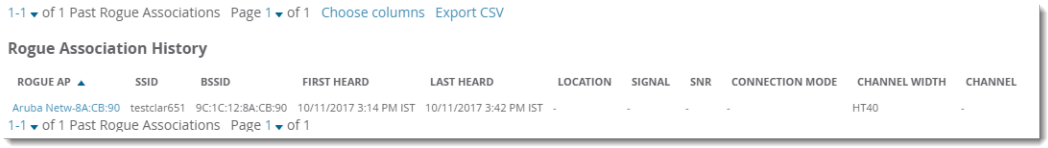
Figure 158: *Client Association History Table*



Viewing the Rogue Association History

Past association details of a rogue client are tracked in the **Rogue Association History** table, which is located at the bottom of the **Clients > Client Detail** page.

Figure 159: *Rogue Association History Table*



Diagnosing Status and Connectivity

AirWave looks at the client status and network connectivity and then puts them in interactive dashboards on the **Clients > Diagnostics** pages. Devices in the network can include clients, access points, switches, wireless controllers, and routers.

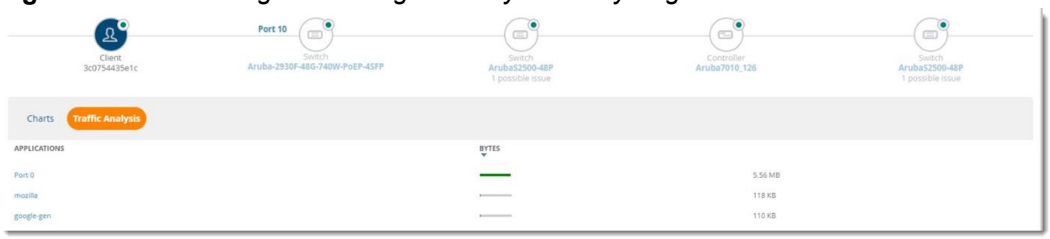
To view client diagnostics, select a client from the search results window or the **Clients > Connected** page, then select **Clients >Diagnostics**. Figure 160 shows an example Client Diagnostics page.

Figure 160: *Accessing Client Trend Charts from the Dashboard*

The information displayed on the **Clients > Diagnostics** page depends on the type of device you are viewing, and which display tab you select at the top of the dashboard.

This page includes the **Charts**, **UCC**, **Clarity**, **Traffic Analysis** and **AirSlice** tabs when displaying information wireless clients. However, if you are monitoring a dynamically segmented wired tunnel client, AirWave displays only **Charts** and **Traffic Analysis** tabs, as shown in Figure 161, and APs and controllers display only single page with no tabs.

Figure 161: *Client Diagnostics Page for a Dynamically Segmented Wired Tunnel Client*



The **Clients > Diagnostics** page can display the following information, depending upon the type of device selected:

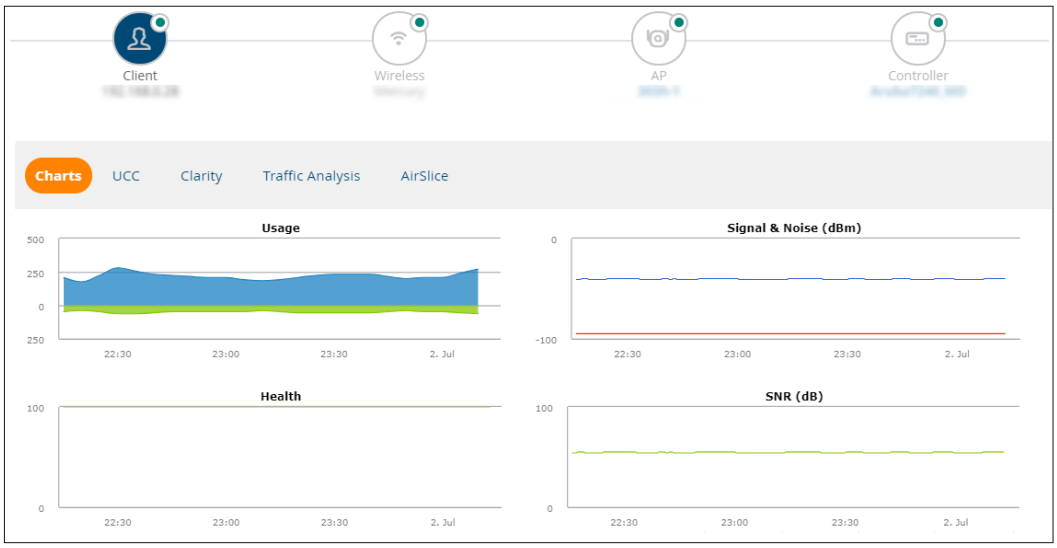
- Trends for APs including data about associated clients, and network usage.
- Trends for controllers, including data about associated clients, network usage, CPU utilization and Memory Utilization information.
- Quality metrics, including possible issues
- Match events
- Device information, including device name, type, MAC address and user role
- Current association information for a client
- Radio information for a wireless network
- Switch information

- Performance information, including number of clients and usage data
- Floorplan location, if VisualRF is enabled.

Charts

If you are viewing data for a wired or wireless client, select the **Charts** tab at the top of the **Clients >Diagnostic** page to view charts for data usage, Signal &Noise information, device health and Signal-to-Noise (SNR) ratios.

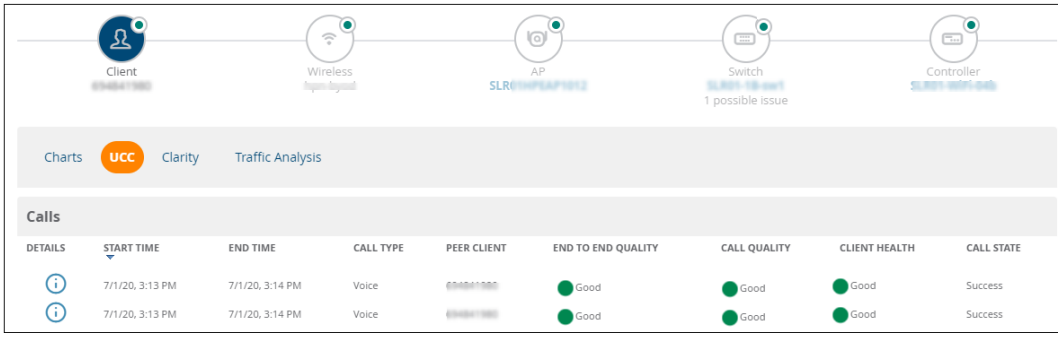
Figure 162: *Charts on the Clients >Diagnostics page*



UCC

Select the **UCC** tab at the top of the **Clients >Diagnostic** page to view call details for a client on the **UCC Calls** table, as well as status indicators showing call quality and client health as good, fair, poor or unknown.

Figure 163: *UCC Call Details*



Clarity

You can view a timeline of all phases of the client connecting to a network on the **Clarity** graphs.

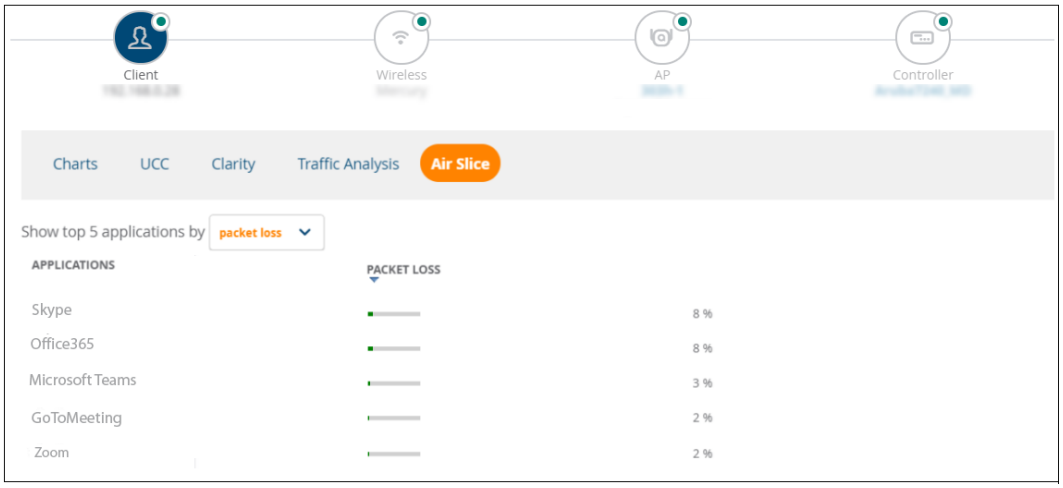
Figure 164: *Clarity Information*

Air Slice

Aruba Air Slice guarantees performance for latency-sensitive, high-bandwidth, and IoT services at the radio level, using the Policy Enforcement Firewall (PEF) for deep packet inspection. This feature is supported in AirWave for controllers or Mobility Master/managed devices running ArubaOS 8.7 or later.

Click the **Air Slice** tab on the **Clients>Diagnostics** page to view graphs showing the five applications experiencing the greatest amount of packet loss, latency, or jitter.

Figure 165: *Air Slice Graph Showing Packet Loss Data*



This section contains the following topics describing individual device configuration within device groups:

While most device configuration settings can be efficiently managed by 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.

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

AirWave automatically saves the last 10 device configurations for reference and compliance purposes. Archived device configurations are linked on the **Devices > Device Configuration** 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 **Devices > Device Configuration** page. This applies to startup or running configuration files.

Compare two configurations to highlight the specific lines that are mismatched. The Device Configuration page provides links to AirWave pages where any mismatched settings can be configured.

Moving a Device from Monitor Only to Manage Read/Write Mode

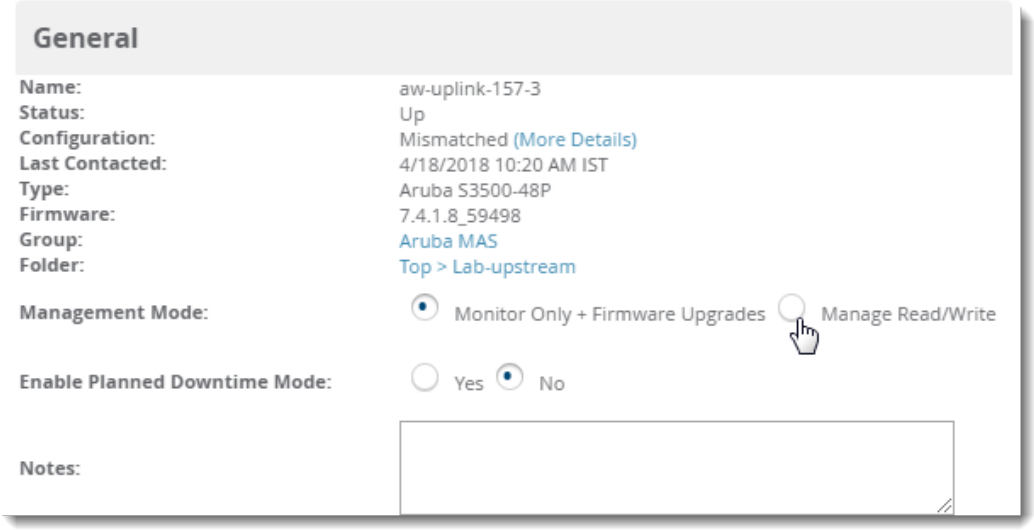
You can move the device to **Manage Read/Write** mode after you have verified any configuration mismatches on the **Devices > Device Configuration** page, or you have confirmed that the device configuration status is **Good** on the **Devices > List** page.

You can set multiple devices into Planned Maintenance Mode in the **Modify Devices** link on an AP list page. For more information, refer to "Modifying Multiple Devices" on page 90.

To move a device to **Manage Read/Write** mode:

1. Go to the **Devices > List** page, then right-click on the device and select **Manage** to open the Manage page.
2. From the the **General** area, select **Manage Read/Write**, as shown in Figure 166.

Figure 166: *Selecting the Management Mode*



3. Scroll down, then select **Save and Apply**.
4. Click **Confirm Edit** on the confirmation page to retain these settings and push the 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.

NOTE

Use the **Enable Planned Maintenance Mode** field in **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. For more information, refer to "Modifying Multiple Devices" on page 90.

Configuring Device Settings

The device settings on the Management page vary depending on the device vendor and model. If any changes are scheduled for a device, you can view them in a **Scheduled Changes** section at the top of the page and click the Job link to access to the **System > Configuration Change Job Detail** page.

NOTE

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

NOTE

Devices running Instant 8.5.0.0 or later display the "Sesimagotag Channel" option which configures the communication channel used in electronic shelf labelling.

To configure device settings:

1. Go to **Devices > List** , then right click the device and select **Manage** from the shortcut menu to access the **Device Management** page.
2. View the current status of the device in the **General** section.

Table 94 describes the device settings on the **Device Management** page.

3. To update the device status, go to **Devices > Device Config** then click **Audit**.

Table 94: *General Device Configuration Settings*

Field	Description
Name	Displays the name currently set on the device.
Status	Displays the current status of a device. If a device is **Up**, then AirWave is able to ping it and fetch SNMP information from the device. If the device is listed **Down** then AirWave is either unable to ping the device or unable to read the necessary SNMP information from the device.
Configuration	Displays the current configuration status of the device.
Last Contacted	Displays the last time AirWave successfully contacted the device.
Type	Displays the device type. **NOTE:** This information displayed on this page depends on the device type.
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 device.
Template	Displays the name of the group template currently configuring the device. 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 device. Also displays a link to the **Devices > List** page for the folder.
Management Mode	Displays the current management mode of the device. No changes are made to the device when it is in **Monitor Only** mode. AirWave pushes configurations and makes changes to a device when it is in **Manage Read/Write** mode.
Enable Planned Maintenance Mode	Put this device into planned maintenance. During the maintenance mode, no device 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 a device list page.
Notes	Provides a free-form text field to describe device information.

4. Review and provide the following information in the **Settings** area.

Table 95 describes field settings, default values, and information for the **Settings** section of this page.

Table 95: *Devices > Manage > Settings Fields and Default Values*

Setting	Default	Device Type	Description
Name	None	All	User-configurable name for the device (max. 20 characters)
Domain Name	None	IOS	Field populated upon initial device discovery or upon refreshing settings. Enable this option from **AMP Setup > Network** page to display this field on the **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.

Table 95: *Devices > Manage > Settings Fields and Default Values (Continued)*

Setting	Default	Device Type	Description
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 provided if the device goes down.
Organization	Read from Device	Instant	The Organization string of the IAP.
Aruba AP Group	default	All	Specifies the Aruba AP Group in which this devices resides.
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

5. Complete additional settings on the **Devices > Manage** page, to include H-REAP, certificates, radio settings, and network settings. Table 96 describes many of the possible fields.

For complete listing and discussion of settings applicable only to *Aruba* devices, see the Aruba *Device Configuration Guide.*

Table 96: *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.

Table 96: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
Mesh Mobility	Static	Mesh Devices	Select **Static** if the AP is static, as in the case of a device mounted on a light pole or in the ceiling. Select **Roaming** if the AP is mobile. Two examples would be an AP mounted in a police car or utility truck.
Receive Antenna	Diversity	Cisco	Drop-down menu for the receive antenna provides three options: **Diversity** —Device will use the antenna that receives the best signal. If the device has two fixed (non-removable) antennas, the **Diversity** setting should be used for both receive and transmit antennas. **Right** —If your device has removable antennas and you install a high-gain antenna on the device's right connector (the connector on the right side when viewing the back panel of the device), use this setting for receive and transmit. **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 device receives information on the antenna with the best signal strength and quality. The device transmits on the antenna from which it last received information. **Primary Only**—The device transmits and receives on the primary antenna only. Secondary Only: The device transmits and receives on the secondary antenna only. **Rx Diversity**—The device receives information on the antenna with the best signal strength and quality. The device transmits information on the primary antenna only.
Transmit Power Reduction	0	Proxim	Transmit Power Reduction determines the device's transmit power. The max transmit power is reduced by the number of decibels specified.

Table 96: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
Channel	6	All	Represents the device's current RF channel setting. The number relates to the center frequency output by the device's RF synthesizer. Contiguous devices should be set to different channels to minimize 'crosstalk,' which occurs when the signals from APs overlap and interfere with each other. This RF interference negatively influences WLAN performance. 802.11b's 2.4-GHz range has a total bandwidth of 80-MHz, separated into 11 center channels. Of these channels, only 3 are non-overlapping (1, 6, and 11). In the United States, most organizations use only these non-overlapping channels.
Transmit Power Level	Highest power level supported by the radio in the regulatory domain (country)	Cisco, Symbol, Proxim AP-600, AP-700, AP-2000 (802.11g)	Determines the power level of radio transmission. Government regulations define the highest allowable power level for radio devices. This setting must conform to established standards for the country in which you use the device. You can increase the coverage radius of the access point by increasing the Transmit Power Level. However, while this increases the zone of coverage, it also makes it more likely that the device will interfere with neighboring devices. 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. AirWave will still monitor the Ethernet page and ensure the device stays online. Customers typically use this option to temporarily disable wireless access in particular locations. This setting can be scheduled at a device level or Group level. **NOTE:** You cannot disable radios unless rogue scanning is disabled in **Groups > Radio**.
Use DHCP	Yes	All	If enabled, the device will be assigned a new IP address using DHCP. If disabled, the device will use a static IP address. For improved security and manageability, disable DHCP and using static IP addresses.

Table 96: *Additional Settings (Continued)*

Setting	Default	Device Type	Description
LAN IP	None	All	The IP Address of the device Ethernet interface. If One-to-One NAT is enabled, AirWave will communicate with the device 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.

6. Locate the **Template Options** area on the **Devices > Manage** page.

This section only appears for IOS APs, Symbol devices, and Aruba controllers in groups with Aruba GUI Config disabled.

Table 97 describes field settings, default values, and additional information for this page.

Table 97: *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 device. 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	AirWave will read the SSL Certificate off of the device when it comes UP in 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 device 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.

7. For Cisco WLC devices, go to the interfaces section of the **Devices > Manage** page. Select **Add new Interface** to add another controller interface, or select the **pencil** icon to edit an existing controller interface. Table 98 describes the settings and default values. For detailed descriptions of Cisco WLC devices supported by AirWave, refer to the Cisco WLC product documentation.

Table 98: *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.

Adding a Maintenance Window for a Device

When you add a maintenance window for a device, AirWave changes the management mode to **Manage Read/Write** and stops polling or monitoring the device.

AirWave will push the last saved configuration to the device, regardless of any pending changes to the group it belongs to or its device settings. Ensure all device configurations stored in AirWave are saved before you proceed.

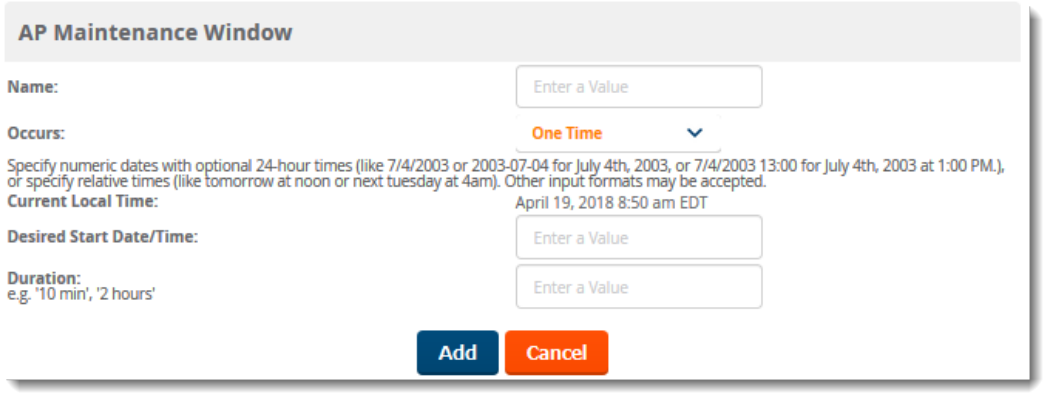
It is recommended you change the management mode to **Planned Downtime** before you change the maintenance window to prevent the device from entering **Manage Read/Write** mode. AirWave continues monitoring these device while you configure the maintenance window.

You can also use the **Modify Devices** link to add or delete maintenance windows on multiple devices at once. This feature can also be used from the Master Console to set maintenance windows for multiple AirWave servers.

To add a maintenance window:

1. Navigate to **Devices > List** , then right click the device and select **Manage** from the shortcut menu to access the Management page.
2. Scroll down the Management page to the **Maintenance Windows** section.
3. Click **Add**.

Figure 167: *Adding a Maintenance Window for a Device*



4. Enter a name for the maintenance window.
5. Select the frequency of the maintenance window.
6. Enter the start time and the duration of the maintenance window.
7. Click **Add**.

Creating Dynamic Variables

When you apply a configuration template that has dynamic variables, AirWave inserts the variable definitions to the device configuration. AirWave displays both group-level and device-level variables on the **Device > Manage** page.

NOTE

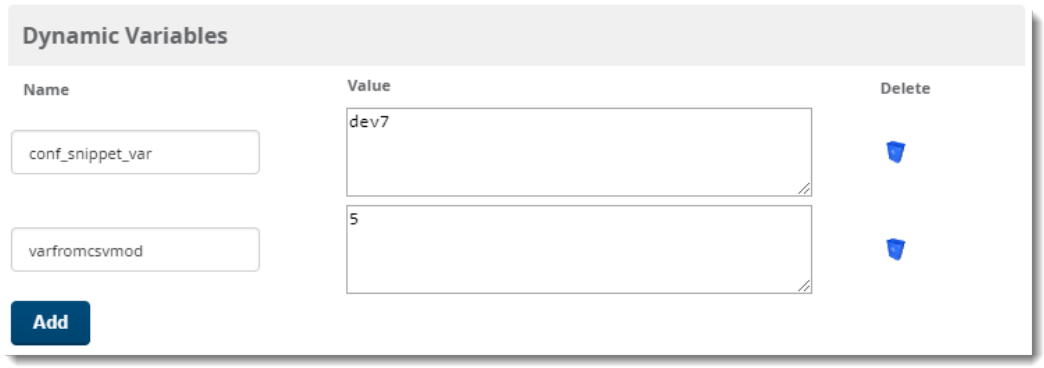
If a dynamic variable with the same name was created on the **Groups > Template** page, AirWave gives precedence to the dynamic variable created on the **Device > Manage** page.

To create a dynamic variable:

1. Go to the **Device > List**, and select a device.
2. From the navigation bar, click **Manage**, then scroll down the **Devices Manage** page to the **Dynamic Variables** section.
3. Click **Add**, then enter the variable name and default value. The variable value can include more than one line of text. You can't use spaces, periods, or non-alphanumeric characters. . If you want to create additional variables, repeat this step for each variable.

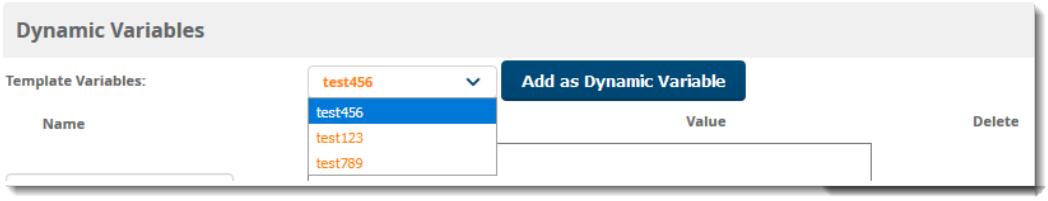
Figure 168 shows two dynamic variables, called "conf_snippet_var" and "varfromcvsmod".

Figure 168: *Adding Dynamic Variables*



4. To use a variable from a configuration template, select the variable from the **Template Variables** drop-down menu, then click **Add as Dynamic Variable**.

Figure 169: *Dynamic Variables from a Group Configuration Template*



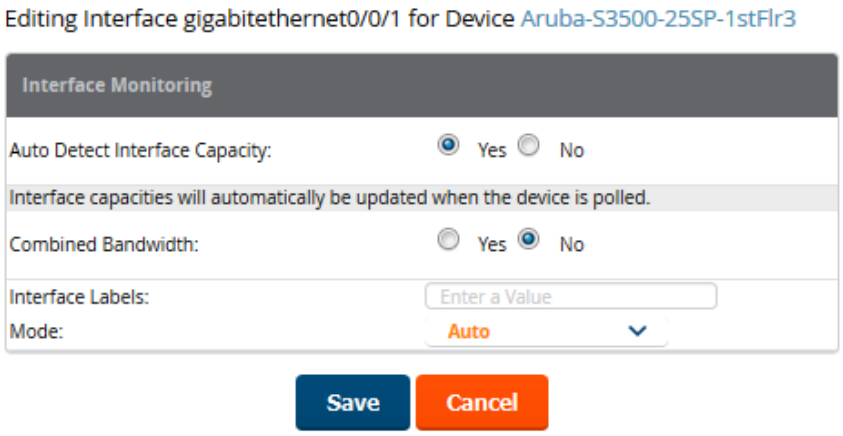
5. Scroll down to the bottom of the **Devices Manage** page, then click **Save and Apply**.

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.

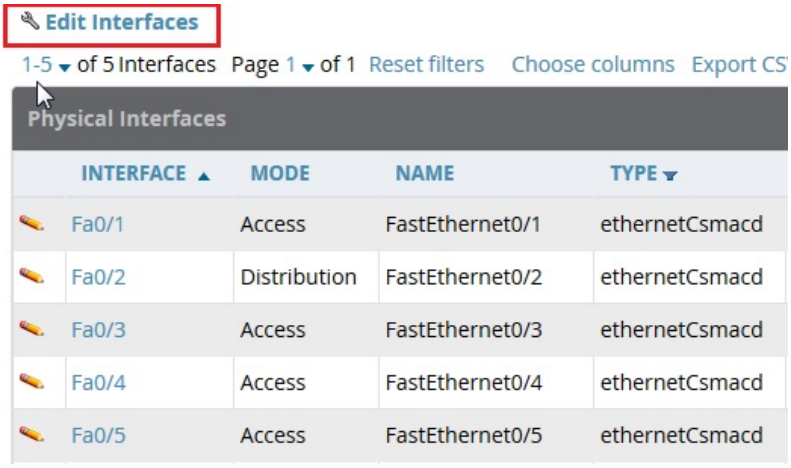
You can configure interface settings individually or in groups. For individual settings, select the pencil icon next the interface name in **AP/Devices > Interfaces**. This takes you to the **Interface Monitoring** window which may a slightly different appearance than Figure 170, depending on the device type, and whether you are configuring a physical or virtual interface.

Figure 170: *Editing a Switch Interface*



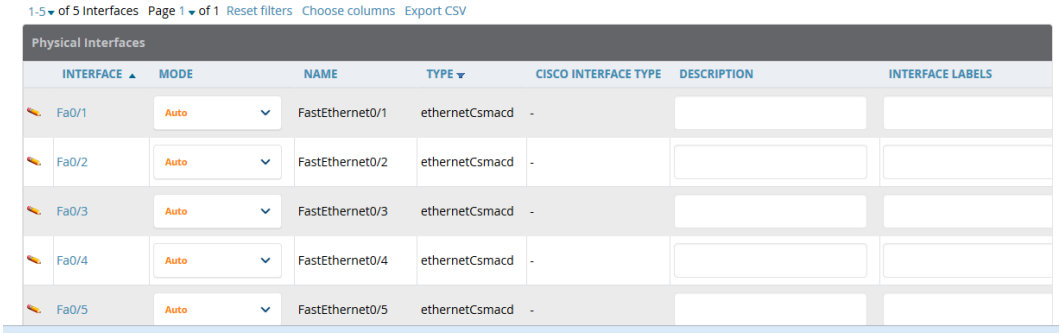
To configure interfaces as a group, select **Edit Interfaces** above the Physical or Virtual Interfaces table as shown in Figure 171.

Figure 171: *Edit Multiple Interfaces*



You will remain on the same page, but will have the option to make changes to the most commonly edited settings in batch mode, as shown in Figure 172.

Figure 172: *Multiple Interface Editing Page Illustration*



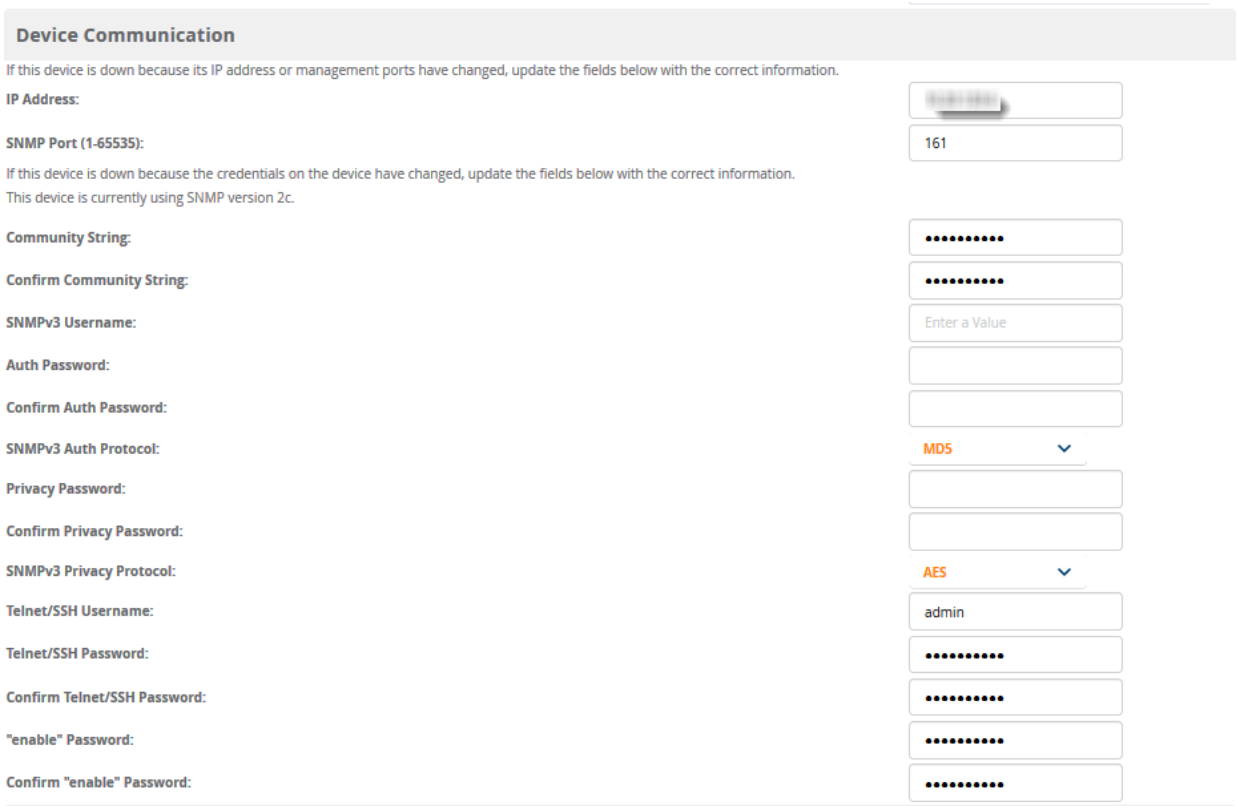
AirWave assembles the entire running configuration using templates and your modifications to these pages. For a more detailed discussion on templates, see "Using Configuration Templates" on page 236.

Individual Device Support and Firmware Upgrades

Perform the following steps to configure device-level communication settings. The available device communication fields will vary, depending on the device brand and model.

1. Locate the **Device Communication** area on the **Devices > Manage** page.
2. Enter the credentials to be used to manage the device. Figure 173 illustrates this page.

Figure 173: *Devices > Manage > Device Communication*



3. Enter and confirm the appropriate **Auth Password** and **Privacy Password**.
4. 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 now.

NOTE

Some device configuration changes might require a system reboot, in which case you might schedule these changes to occur when users will not be affected.

Click **Update Firmware** 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 AirWave Administrator has enabled **Allow firmware upgrades in monitor-only mode** on the **AMP Setup > General** page, *and* you are looking at an **Devices > Manage** page for a controller or autonomous AP that supports firmware upgrades in AirWave. See the Supported Infrastructure Devices document on the **Home > Documentation** page for a list of the AirWave-supported devices that can perform firmware upgrades. In most cases, you cannot upgrade firmware directly on thin APs.

Figure 174 illustrates the page that opens and Table 99 describes the settings and default values.

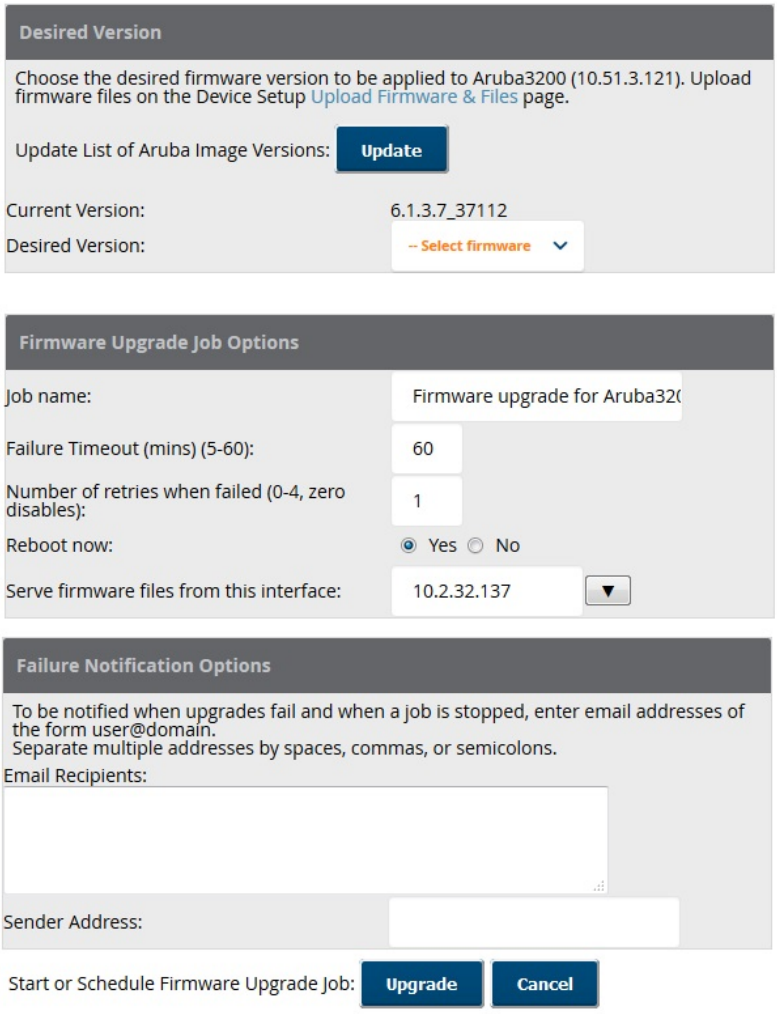
Table 99: *Update Firmware Fields and Default Values*

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.

Table 99: *Update Firmware Fields and Default Values (Continued)*

Setting	Default	Description
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 174: *Devices > Manage Firmware Upgrades*



Initiating a firmware upgrade will change the **Firmware Status** column for the device to Pending in **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 AirWave, and contains the following topics:

Group Templates

Templates are helpful configuration tools that allow AirWave to manage virtually all device settings. A template uses variables to adjust for minor configuration differences between devices.

Supported Devices

You can create group templates on the **Groups > Templates** page for the following types of devices:

- 3Com
- Alcatel-Lucent
- Aruba
- Cisco Aironet IOS
- Cisco Catalyst switches
- Dell
- Enterasys
- HPE
- Motorola
- Nortel
- Siemens
- Trapeze

You can also create local templates in a subscriber group—using global groups does not mean that global templates are mandatory

Use the graphical Aruba config feature in support of Aruba devices, particularly for ArubaOS 3.3.2.x and later. Refer to the *AirWave 8.2.6 Controller Configuration Guide* for additional information.

Template Variables

A template uses variables to adjust for minor configuration differences between devices. You can use variables to configure device-specific properties, such as name, IP address and channel, or group-level properties, such as

SSID and RADIUS server.

The AirWave template understands these variables:

- %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 **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, Adding and Editing Templates

AirWave displays the Information about the group template, such as the name, type of device, status, fetch date, and version restriction.

The device type field 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.

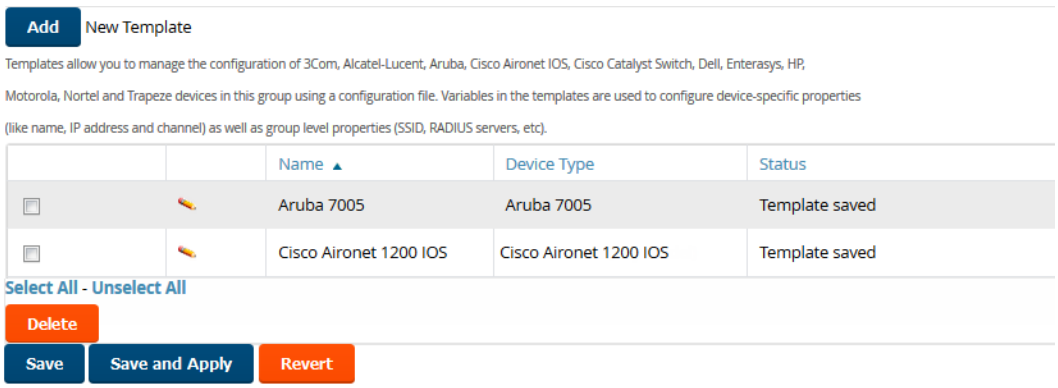
Version restriction designates that the template only applies to APs running the version of firmware specified. If the restriction is **None**, then the template applies to all the devices of the specified type in the group. If there are two templates that might apply to a device the template with the 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.

When applicable, there is a notes section that 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.

To view, add, and edit templates:

1. Go to the **Groups > List** page, then select a group.
2. Navigate to **Groups > Templates**.
3. From the **Templates** page (see Figure 175) do one of the following:
   - Click **Add** to create a group template.
   - Click to edit a group template.

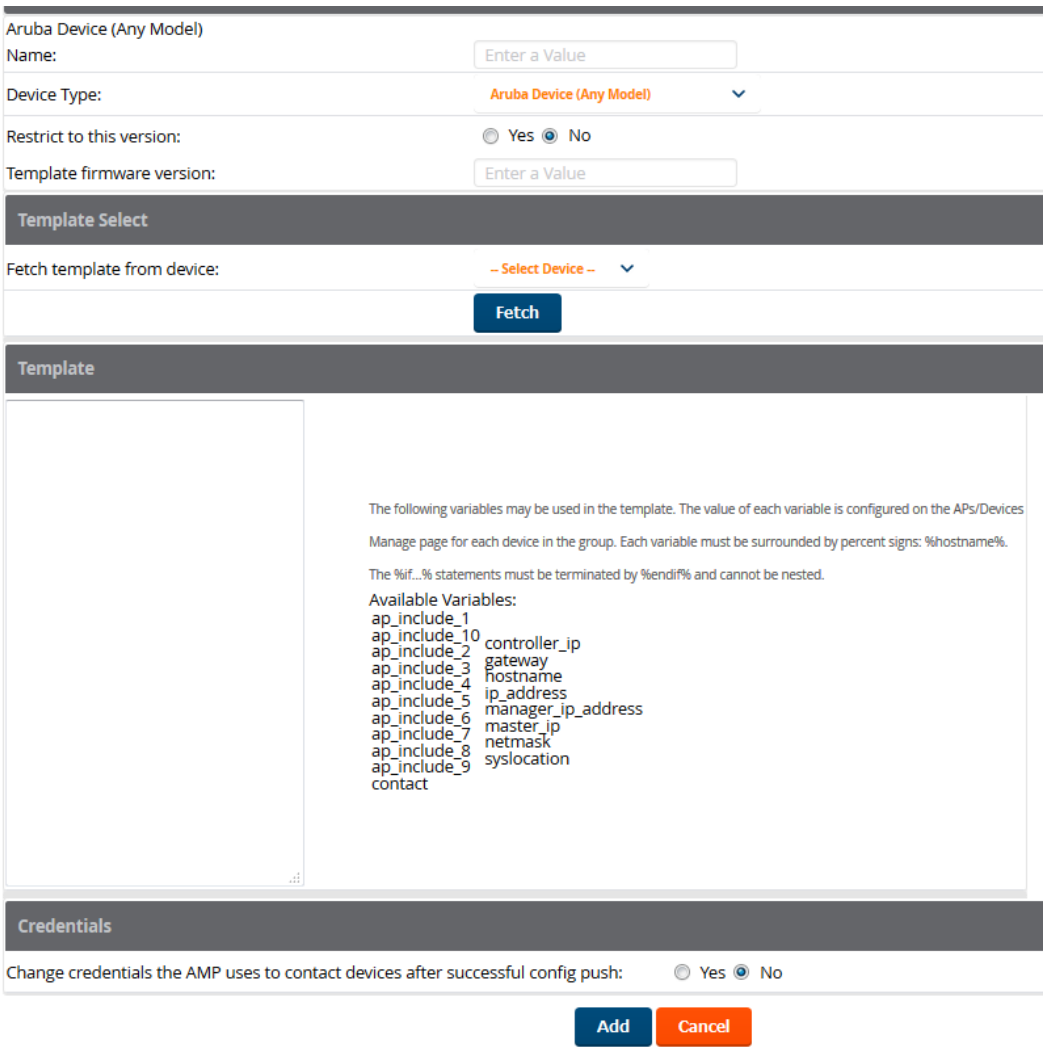
Figure 175: *Group Template Page*



4. Refer to for help configuring the template and default values.

5. Click **Add** to save the new template, or click **Save** if you made changes to an existing template.
6. To create a new template and add it to the AirWave template inventory, go to the **Groups > List** page, and select the group name. The **Details** page appears.
7. Select **Templates**, and then **Add**.
8. Complete the configurations illustrated in Figure 176.

Figure 176: *Groups > Templates > Add Template Page Illustration*



The settings for the **Add a Template** page are described in Table 100. Note that the fields can vary based on the Group.

Table 100: *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 252.
Name	None	Defines the template display name.
AP Type	Cisco IOS (Any Model)	Determines that the template applies to APs or devices of the specified type. If **Cisco IOS (Any Model)** is selected, the template applies to all IOS APs that do not have a version specific template specified.
Reboot APs After Configuration Changes	No	Determines reboot when AirWave applies the template, copied from the new configuration file to the startup configuration file on the AP. If **No** is selected, 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 **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 241 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.

Table 100: *Groups > Templates > Add Template Fields and Default Values (Continued)*

Setting	Default	Description
Change credentials the AMP uses to contact devices after successful config push:	No	Specify whether to change the credentials that AirWave uses to contact devices after the configuration has been pushed. If this option is enabled, then new credential information fields display. **NOTE:** Starting with AirWave 8.2.11.1, If this setting is not enabled, AirWave will push the username: **manager** and password **<device-serial-number>** to factory-default switches running firmware version 16.10.008 or later releases during the Zero-Touch Provisioning (ZTP) process.
Community String	None	If the template is updating the community strings on the AP, enter the new community string AirWave should use here. 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 AirWave should use here. 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 AirWave should use here. AirWave updates the credentials it is using to communicate to the device after the device has been managed.
enable Password	None	If the template is updating the enable password on the AP, enter the new enable password AirWave should use here. 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. 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. 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. 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

To prevent configuration changes from being applied to APs until you are sure you have the correct configuration, work with a small group of access points that are in Monitor Only mode until you are familiar with the template configuration process.

To configure templates within a group:

1. Select a group to configure, then select an AP from the group to serve as a *model* AP for the others in the group. Your selection should be configured with all the desired settings. If any APs in the group have two radios, select a model AP that has two radios and that both are configured properly.
2. Go to **Groups > Templates**, then select **Add** to add a new template.
3. Select the type of device that will be configured by this template.
4. Select the model AP from the drop-down list, and select **Fetch**.
5. 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 "Template Syntax" on page 243.

   These variables are always encapsulated between % signs. On the right side of the configuration page is the **Additional Variables** section. This section lists all available variables for your template. Variables that are in use in a template are green, while variables that are not yet in use are black. Verify these substitutions to ensure that all of the settings that you believe should be managed on an AP-by-AP basis are labeled as variables in this fashion. If you believe that any AP-level settings are not marked correctly, please contact Aruba customer support before proceeding.
6. Specify the device types for the template. The templates only apply to devices of the specified type.
   - Specify whether AirWave should reboot the devices after a configuration push. If the **Reboot Devices after Configuration Changes** option is selected, then AirWave instructs the AP to copy the configuration from 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 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.
7. 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.
8. 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 AirWave will audit the devices and compare their current configuration to the one defined in the template.

If you set the reboot flag to **No**, then some changes could result in configuration mismatches until the AP is

rebooted.

For example, changing the SSID on Cisco IOS APs requires the AP to be rebooted. Two other settings that require the AP to be rebooted for configuration change are Logging and NTP. A configuration mismatch results if the AP is not rebooted.

If logging and NTP service are not required according to the Group configuration, but are enabled on the AP, you would see a configuration file mismatch as follows if the AP is not rebooted:

IOS Configuration File Template

```
…
(no logging queue-limit)
…
```

Device Configuration File on Devices > Device 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
…
```

9. Once the template is correct and all mismatches are verified on the **Devices > Device Configuration** page, navigate to **Groups > Monitor** and click  at the right corner of the device list to select the devices to change the management mode to Manage Read/Write. The AP pulls the new startup configuration file from AirWave. For more information, see "Setting the Management Mode" on page 137.

You can set the management mode for individual devices from the **Devices > Manage** configuration page. For more information, see "Moving a Device from Monitor Only to Manage Read/Write Mode" on page 222.

Template Syntax

Template syntax is comprised of the following components, described in this section:

Using AP-Specific Variables

When a template is applied to an AP, all variables are replaced with the corresponding settings from the **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 AirWave.

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

Using Directives to Eliminate Reporting of Configuration Mismatches

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, 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 AirWave from reporting mismatches for this type of variance.

AirWave provides two types of directives that can be used within a template to control how 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 AirWave ignores them when verifying configurations. Lines enclosed in `<ignore_and_do_not_push>` cause 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 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 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 101:

```
%if variable=value%
…
%endif%
```

Table 101: *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 **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 102 are substituted with values specified on each access point's **Devices > Manage** configuration page within the 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. AirWave would typically detect and flag this variance between the running-config file and startup-config file as a configuration mismatch. To prevent AirWave from reporting a configuration mismatch between the desired startup-config file and the running-config file on the AP, AirWave suppresses the lines in the desired configuration when auditing the AP configuration (similar to the way 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 102.

Table 102: *Substitution Variables in Templates*

Variable	Meaning	Command	Suppressed Default
hostname	Name	hostname %hostname%	-
channel	Channel	channel %channel%	-
ip_address netmask	IP address Subnet mask	ip address %ip_address% %netmask% or ip address dhcp ...	-
gateway	Gateway	ip default-gateway %gateway%	-
antenna_ receive	Receive antenna	antenna receive %antenna_ receive%	diversity
antenna_transmit	Transmit antenna	antenna transmit %antenna_ transmit%	diversity
cck_power	802.11g radio module CCK power level	power local cck %cck_power%	maximum
ofdm_power	802.11g radio module OFDM power level	power local ofdm %ofdm_ power%	maximum
power	802.11a and 802.11b radio module power level	power local %power%	maximum
location	The location of the SNMP server.	snmp-server location %location%	-
contact	The SNMP server contact.	snmp-server contact %contact%	-
certificate	The SSL Certificate used by the AP	%certificate%	-
ap include	The AP include fields allow for configurable variables. Any lines placed in the AP Include field on the **Devices > Manage** configuration page replace this variable.	%ap_include_1% through %ap_include_10%	-
chassis id	serial number of the device	%chassis_id%	-
domain	dns-domain of the device	%domain%	-
interfaces	Interfaces of the device	%interfaces%	-

Configuring Templates for Aruba Instant

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

Be sure that the default configuration is validated and has been pre-tested in a non-production environment prior to applying it to a production network. Any changes that are made to this configuration will follow the same process each time and will be applied to other Instant networks as described in this document.

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 AirWave. 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%
```

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. 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 AirWave normal **Group** configuration pages. 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 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

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

- If the **Reboot Devices after Configuration Changes** option is selected, then AirWave instructs the AP to copy the configuration from 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 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.

Changes made on the standard 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 **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 AirWave to login to the AP must have level 15 privileges. Without them, 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 "Configuring Device Interfaces for Switches" on page 232. You can import interface information as described in this section or by fetching a template from that device, as described in "Configuring General Templates" on page 242.

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 AirWave using templates. 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 "Configuring Cisco IOS Templates" on page 248. 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 AirWave users to define a single template in a global group that can be used to manage member devices. They turn settings like group RADIUS servers and encryption keys into variables that can be configured on a per-group basis.

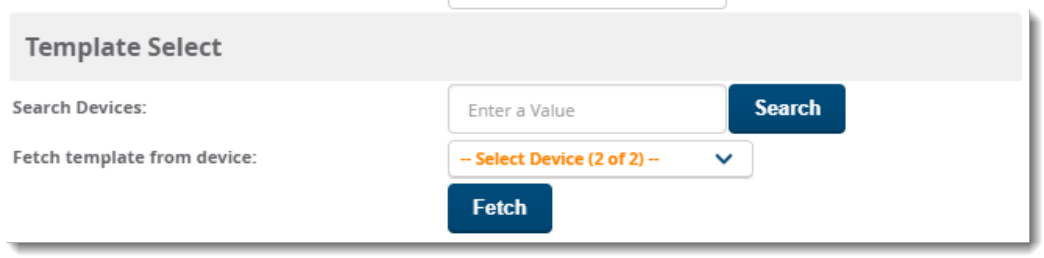
NOTE

If a variable with the same name exists at the template level and at the device level , AirWave gives precedence to the dynamic variable created at the device level.

To create global templates, or edit global templates:

1. Go to the **Groups > List**, and select a device group.
2. From the AirWave navigation pane, select **Templates**.
3. In the Templates page, click **Add**. Or, click to edit a template.
4. Select a device as a model for the global template

Figure 177: *Selecting the Device*



5. Click **Fetch**. The fetched configuration populates the template field.

Figure 178: *Fetching the Device Configuration*

6. If you want to use a template variable with the configuration template, click **Add** at the bottom left of the Template Variables section. You can also populate global template variables by uploading a CSV file (see step 10 on page 254).
7. Enter the variable value and default value. The variable value can include a multiline string. You can't use spaces, periods, or non-alphanumeric characters. You can change the default value later for the group template.

Figure 179: *Adding a Template Variable*

8. Once you have configured your global template, select **Add**. Or click **Save** if you made changes to an existing template. You are redirected to a confirmation configuration page where you can review your changes.
9. Click **Apply Changes Now**.

10. After you created the 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
    ```
11. 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.
12. 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.
13. 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.

The Home Overview page provides access to live monitoring of network components and other functions. AirWave includes the following live monitoring features:

This chapter also provides the following information:

Customizing the Dashboard

You can customize the dashboard so you see only what you want in your reports with widgets.

To customize the dashboard:

1. Navigate to **Home > Overview**, then click at the upper-right corner of the page.
2. Drag and drop widgets from the **Available Widgets** list and an open space on the dashboard within gridlines. The widget label turns orange if you place it over occupied space.
3. Click **Save**.

Available Widgets

When a widget is enabled, the information that displays can vary based on the user's permission level. Certain roles can limit the top folder that a user sees.

Table 103 describes all the widgets.

Table 103: *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 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 AirWave is aware of from polling the device. The information in these graphs is color coded to match the selected check boxes.
Monitoring and Configuration Pie Charts	The **Monitoring Status** pie chart 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 **Devices > Down** page. The **Configuration Compliance** pie chart 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 **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 AirWave alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last AirWave server reboot. • Click on **AMPAlerts** 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 103: *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 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 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 AirWave server reboot. This is the same table that displays on the **RAPIDS > Overview** page.
RAPIDS: OS Pie	The **RAPIDS: OSPie** 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.

Table 103: *Available Widgets (Continued)*

Widget	Description
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.
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 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 AirWave over the last 24 hours based on the device type (such as a specific operating system or smart phone type).

Table 103: *Available Widgets (Continued)*

Widget	Description
Clients By Device Mfgr	This pie chart shows the percentage of clients that have attached to 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 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 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 AirWave over the last 24 hours based on the device operating system (such as Windows or Android).
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to 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 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.

Adding Widgets

You can change the widgets on this page by clicking in the upper-right corner of the **Home > Overview** page.

To add a widget:

1. Select a widget from the **Available Widgets** list, then drag the widget across to the right side of the page.
2. Place the widget in an open space within the gridlines. The widget label turns orange if you place it over occupied space.
3. Click **Save**.

Available Widgets

Table 104 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 104: *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 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 AirWave is aware of from polling the device. The information in these graphs is color coded to match the selected check boxes.
Monitoring and Configuration Pie Charts	The **Monitoring Status** pie chart 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 **Devices > Down** page. The **Configuration Compliance** pie chart 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 **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 AirWave alerts, IDS events, and RADIUS authentication issues over the last 2 hours, the last 24 hours, and the total since the last AirWave server reboot. • Click on **AMP Alerts** to drill down to more detailed alert information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link. • Click on **IDS Events** to drill to more detailed event information. This link takes you to the **RAPIDS > IDS Events** page. • Click on **RADIUS Authentication Issues** to drill to more detailed RADIUS authentication information. This information displays in the current page. You can return to the **Alert Summary** graph by selecting the **Home Overview** link.
Quick Links	The **Quick Links** section is enabled by default. This section provides the user with easy navigation to a specific folder, group, report, or common task.
RAPIDS: Acknowledged	The **Acknowledged RAPIDS Devices** pie chart shows the percentage of acknowledged and unacknowledged RAPIDS that the user has visibility into. The RAPIDS information appears from the moment a rogue is discovered until it is deleted. Ignored rogues, however, are not included in this chart. This chart also displays on the **RAPIDS > Overview** page.

Table 104: *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 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 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 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.

Table 104: *Available Widgets (Continued)*

Widget	Description
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.
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 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 AirWave over the last 24 hours based on the device type (such as a specific operating system or smart phone type).

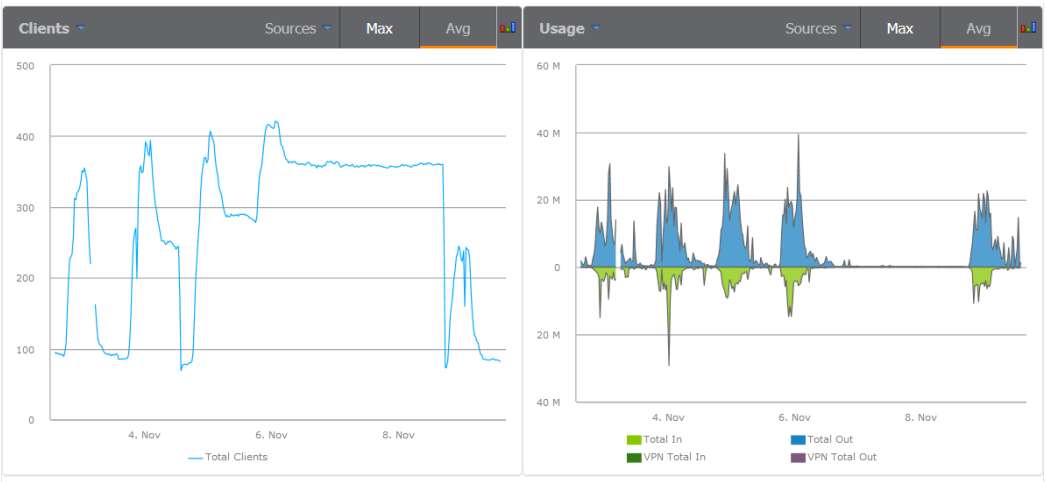
Table 104: *Available Widgets (Continued)*

Widget	Description
Clients By Device Mfgr	This pie chart shows the percentage of clients that have attached to 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 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 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 AirWave over the last 24 hours based on the device operating system (such as Windows or Android).
Clients By Device OS Detail	This pie chart shows the percentage of clients that have attached to 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 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.

Defining Graph Display Preferences

Many of the graphs in AirWave are Highcharts, which allow you to adjust the graph settings attributes as shown in Figure 180.

Figure 180: *Interactive Graphs on the **Home > Overview** Page*



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

These charts can be used and customized as follows.

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

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

Monitoring Your Network Health

To view your overall network health, navigate to **Home > Overview**. The top header of the page displays the status of your network, while the navigation pane on the left side of the page allows you to navigate through the AirWave WebUI.

Figure 181 illustrates this Overview page. The information that displays varies depending on your role.

Figure 181: *Home > Overview Page*

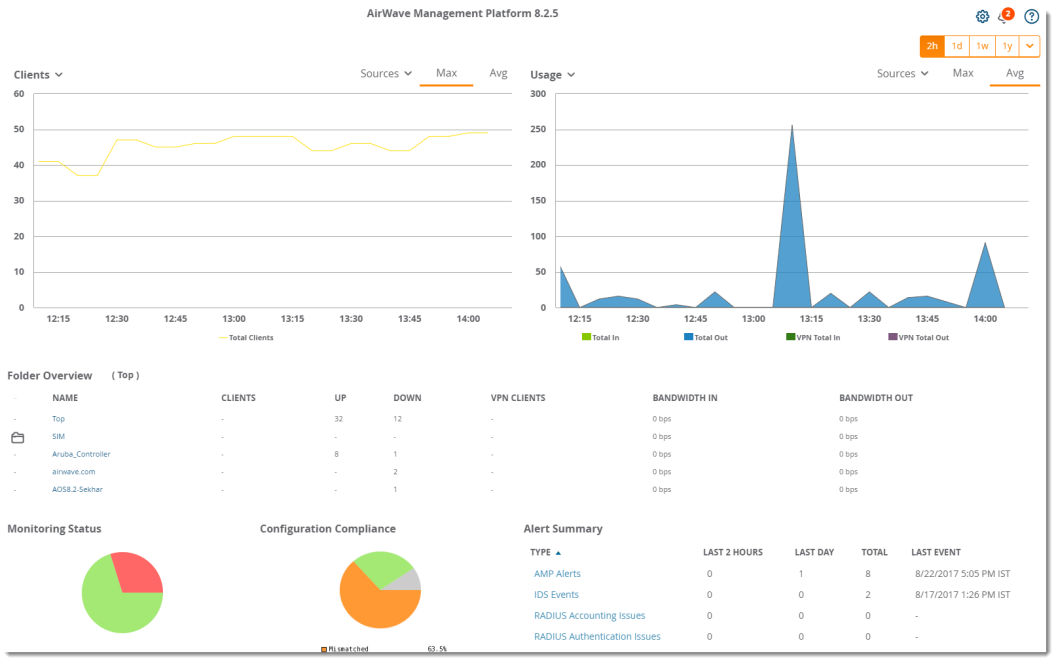


Table 105 describes the sections and graphs that appear in the Overview page.

Table 105: *Home > Overview Sections and Charts*

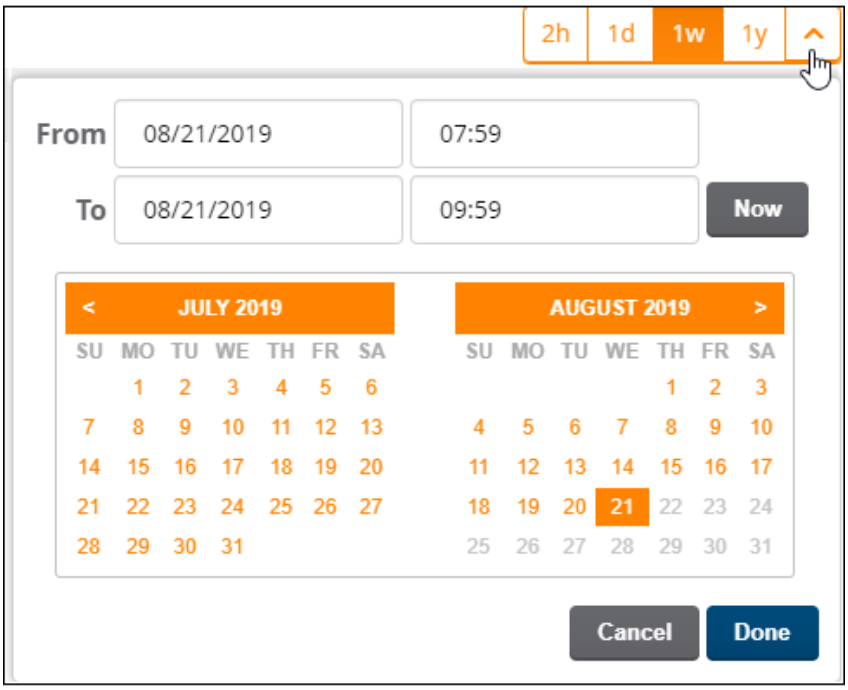
Section	Description
Graphs	You can select the following graphs to display: • Clients. This graph shows a summary of the number of users on the network during a specified period of time. By default, AirWave displays the maximum number of users. To display a list of data series that this graph can display, such as the user count by SSID, select **Show All** . Or, clear the **Max Clients** or **Avg Clients** check boxes to change the display. • Client Health. This graph shows the percentage of clients with good, fair, and poor health. The client health metric displayed in these charts is the efficiency at which that AP transmits downstream traffic to a particular client. AirWave compares 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, with no data retries) to calculate this metric. To view the new graph from the Home page, select **Client Health** from the **Clients** menu. • 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 SecondIn** 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.
Folder Overview	This table displays statistics for device folders and provides shortcuts to monitoring pages for the device folders.
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 **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 **Devices > Mismatched** page.
Alert Summary	This section displays all known and current alerts configured and enabled in the **System > Alerts** page (refer to "Creating New Triggers" on page 308). Alerts can be sorted using the column headers (**Type**, **Last 2 Hours**, **Last Day**, **Total**, or **Last Event**). The **Alert Summary** field displays the following alerts: • AMP Alerts • IDS Events • RADIUS Accounting Issues • RADIUS Authentication Issues

Table 105: *Home > Overview Sections and Charts (Continued)*

Section	Description
Quick Links	The following hyperlinks take you to frequently used pages in AirWave: • Go to folder. This link displays the device folders and opens the **Devices > List** page for the folder you select. See "Using Device Folders" on page 152. • Go to group. This link displays the groups and opens the **Groups > Monitor** page for the group you select. See "Using Device Groups" on page 81. • View Latest Reports. This link displays the most recent reports generated and opens the **Reports > Details** page for the report you select, or the **Reports > Generated** page for the list of all generated reports. See "Creating, Running, and Sending Reports" on page 329. • Common Taks. These links takes you to pages where you can perform the following tasks: ▪ Configure Threshold Alerts—This link opens the **System > Triggers** page. See "Viewing Triggers" on page 318. ▪ Configure Default Credentials—This link opens the **Device Setup > Communication** page. See "Configuring Communication Settings for Newly Discovered Devices" on page 56. ▪ Discover New Devices on Your Network—This link opens the **Device Setup > Discover** page. See "Discovering, Adding, and Auditing Devices " on page 130. ▪ Supported Devices and Features—When you click this link, you will download *AirWave 8.2.11.1 Supported Infrastructure Devices*. ▪ Upload Device Firmware—This link displays the **Device Setup > Upload Firmware & Files & Files Upload** page. See "Uploading Firmware and Files" on page 57. ▪ View Event Log—This link displays the **System > Event Log** page. See "Using the Event Log" on page 308.

Use the calendar tool at the top of these graphs to view historical data for the previous two hours, day, month or year. You can also click the down arrow and select a start date and end date to view data for a custom time period. Historical data is only available for the time periods selected in the **AMP Setup > General > Historical Data Retention** settings.

Figure 182: *Using the Calendar Tool to Select a Custom Time Range*



Monitoring Application Traffic

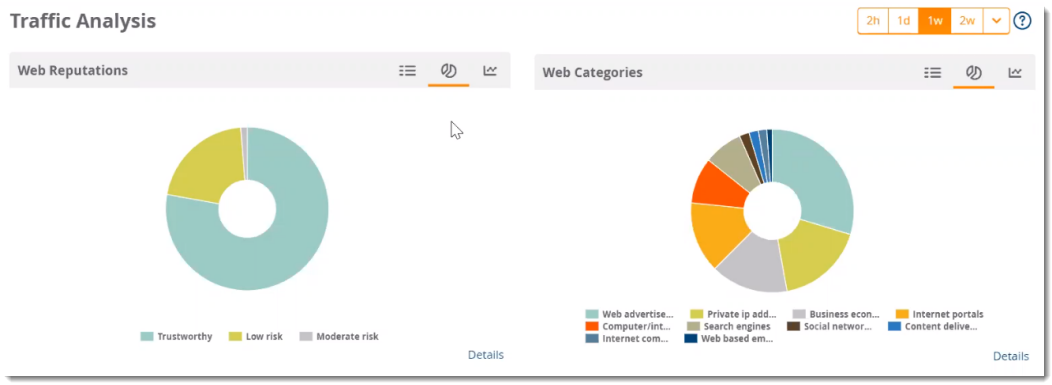
The **Home > Traffic Analysis** page displays the following mobile app usage and network performance statistics in the dashboard:

- Web reputations
- Web categories
- Applications
- Destinations
- WLANs
- Roles
- Device types
- Users

User roles determine your access to device-level or folder-level information.

Figure 183 shows charts of the Web Reputations and Web Categories trends over a one-week period.

Figure 183: *Traffic Analysis Dashboard*



Change Your Views

From the dashboard, you can change your views from the default chart views to tables and graphs as follows:

- Click to view usage data in a table.
- Click to view the percent usage of each category in a chart. Hover your mouse above each section of the chart to view the category name and usage, in KB and percentage (%).
- Click to view a graph of usage in MB over time.

Click the **Details** hyperlink, to see the following information:

- **Category**: The name of the user.
- **Bytes**: The total usage in bytes (MB).
- **Packets**: The total number of packets transmitted or received.
- **Web Reputation**: The web reputation, which indicates the safety of the site.
- **Web Category**: The type of website.
- **Application**: The number of users connected to applications detected in your network per level of web reputation.
- **Destination**: The number of destinations reached through the given category.
- **User Role**: The number of roles assigned to the user.
- **Devices**: The number of devices connected to the given category.
- **User Name**: The name of the user.
- **Device MAC**: The MAC address of the user.
- **WLANs**: The number of WLANs to which the user is connected.

Search and Filter

You can apply filters to your views for all categories, except for **Web Reputations**.

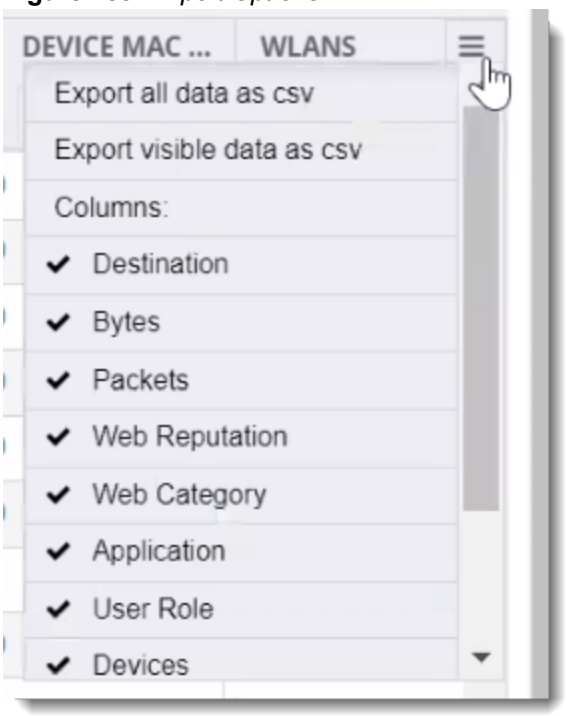
1. Go to Home > Traffic Analysis, then click on the **Details** hyperlink of any category you want to view.
2. Enter text into the **Search** field.
3. Click Filter to apply the filter. AirWave displays matching results in the **Details** table. Figure 184 shows web categories whose information contains the text string **web**.

Figure 184: *Search Results Showing Filters*

Export the Data

You can export all data or filtered data, as shown in Figure 185, Export Options .

Figure 185: *Export Options*



Using the UCC Dashboard

The UCC dashboard in 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. In support of AOS 6.5 and 8.2, you can also see who provides the UCC service for WiFi calls.

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.

If Heuristics is enabled in AirWave and there is no end-to-end call quality information, AirWave will display information based on UCC call quality (see "Additional AMP Services" on page 32).

Viewing UCC Charts, Graphs, and Tables

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. AirWave obtains these metrics from RTCP messages sent from the client (if the client is capable of sending them). For audio calls, AirWave obtains these metrics from the Aruba AP that inspects the RTP flows.

The following table describes the UCC scores and quality indications.

Table 106: *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. 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 271).
- 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 270 for information about the UCC score).

Client information, such as a description of the client device, 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.

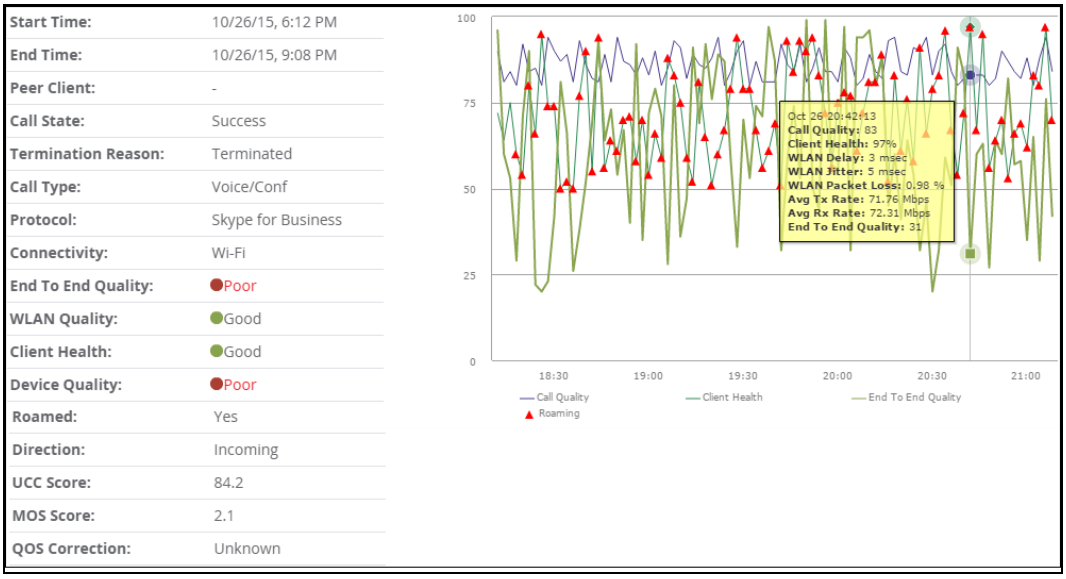
Table 107: *AP Details*

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.
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 186: *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.

You can filter UCC reports by SSIDs as shown in Figure 187. To create a UCC report go to **Reports > Definitions**, then click **Add**.

Figure 187: *SSID Restrictions*

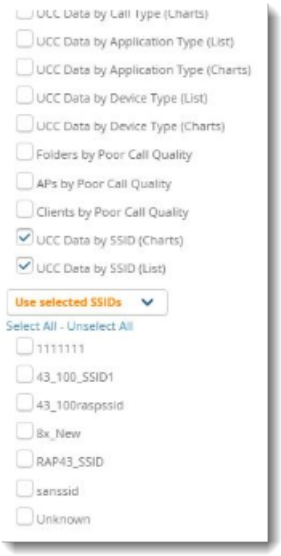


Table 108: *UCC Report Fields*

Field	Description
Quality Metric	The metric used to determine the quality of calls.
Connectivity Type	The type of connection used to complete VoIP calls: • Wi-Fi to Conference. Conference call connectivity between wireless, wired, and desktop-shared devices. • Wi-Fi to External. Call connectivity between wireless devices to other devices on an external network. • Wi-Fi to Wi-Fi. Call connectivity between wireless devices within the same network. • Wired to Wi-Fi. Call connectivity between wired and wireless devices within the same network. • Wired to External. Call connectivity between wired devices to other devices on an external network. • Wired to Wired. Call connectivity between wired devices on the same network.
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.

Table 108: *UCC Report Fields (Continued)*

Field	Description
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.

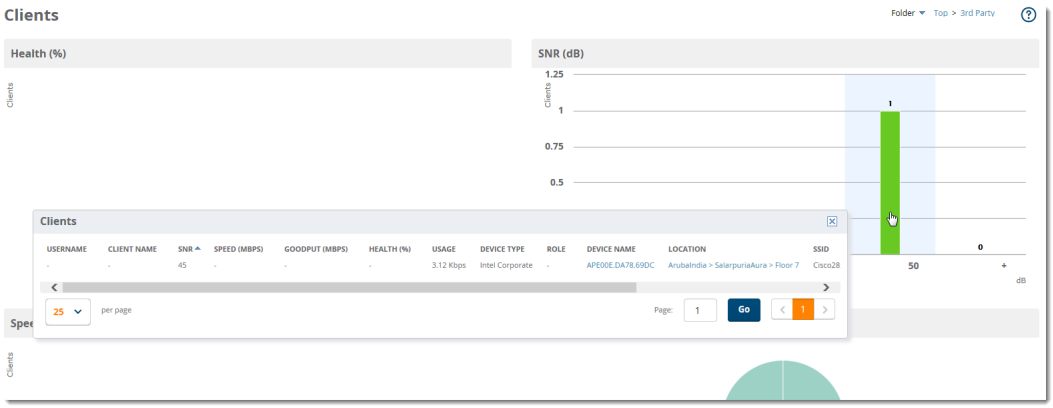
Viewing RF Performance

AirWave helps you identify clients with low SNR rates, health, speed, and goodput, putting the data in interactive RF performance graphs on the Clients page. You can find these graphs by navigating to **Home > RF Performance**.

From the Clients page , you can do the following:

- In the upper-right corner of the page, select a folder from the drop-down menu to narrow down the results. Keep in mind that folder-level permissions are assigned to user roles. Find more information about "Creating AirWave User Roles" on page 41 and "Using Device Folders" on page 152.
- In any graph, click on a value is to view the Clients table, or click the hyperlinks in the Clients table to access shortcuts to monitoring pages and, if available, VisualRF floor plans (Figure 188).
- In the Client page, you can click the client name link to go to the **Clients > Diagnostics** page. Find more information about "" on page 215.

Figure 188: *Accessing the Clients Table*



NOTE

Speed and goodput graphs are available for Aruba devices that support AMON, and health graphs are available for controllers running ArubaOS 6.3 or later.

Viewing RF Capacity

AirWave summarizes radio and channel utilization information for network traffic in the last week and puts the data in interactive RF capacity graphs on the Radios page. You can find these graphs by navigating to **Home > RF Capacity**. These graphs refresh after nightly maintenance completes. The process goes over all the radios and determines the maximum client count and maximum channel utilization for each radio.

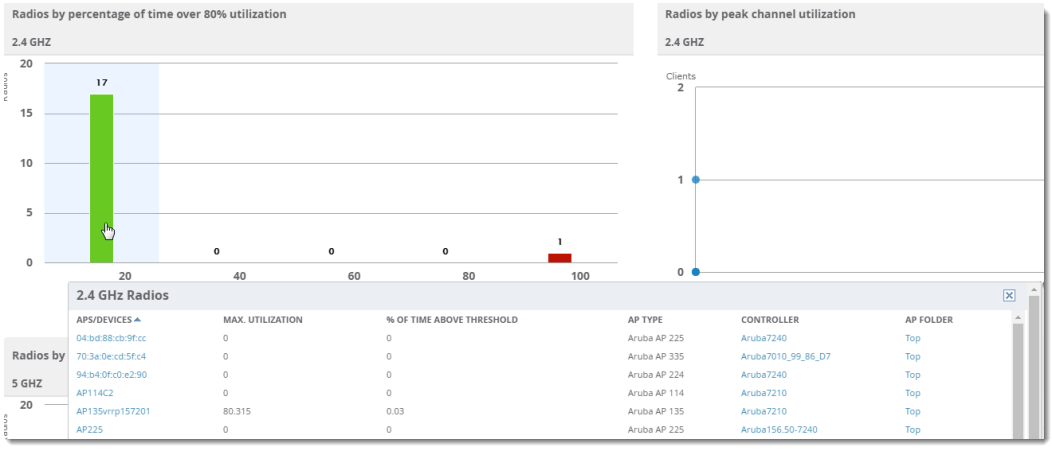
NOTE

The Radios page is available to only Admin users.

AirWave displays two sets of data for 2.4 GHz and 5 GHz channels:

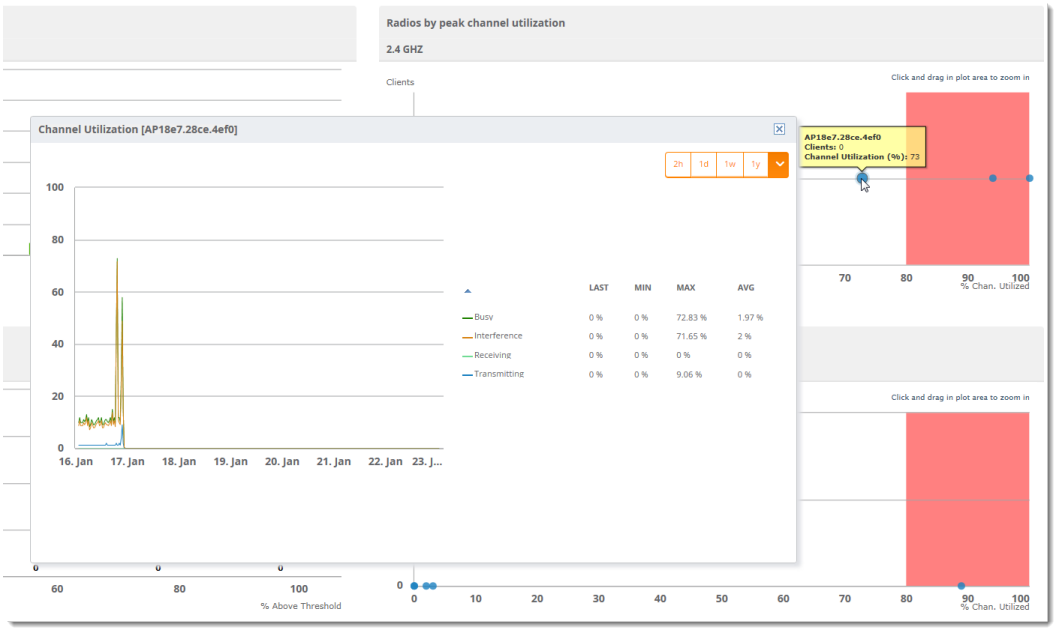
- Radios by percentage of time over 80% utilization. These graphs show the percent of the time that the radios are above the threshold during the day when in use. AirWave determines the normal usage time based on stored utilization samples. Values in red indicate that these radios are above the threshold 75 to 100% of the time. You might want to investigate these radios to see if you need to upgrade them or add additional APs to this location. The information on this graph is collected every 24 hours, after nightly maintenance, and includes data from the last week. You can click on a bar in this graph to view details in a pop-up window (see Figure 189).

Figure 189: *Accessing Device Details for Radios*



- Radios by peak channel utilization. This graph shows the total number of clients connected to radios and corresponding radios connected during peak channel utilization. Data collection occurs every 24 hours, after nightly maintenance, and AirWave includes utilization data from the last week in this graph. You can click plot points, which represent radios, to view historical utilization information for the last two hours, day, week, year, or view a custom time range in a pop-up window (see Figure 190).

Figure 190: *Accessing the Channel Utilization Details for a Radio*



Using the AirMatch Dashboard

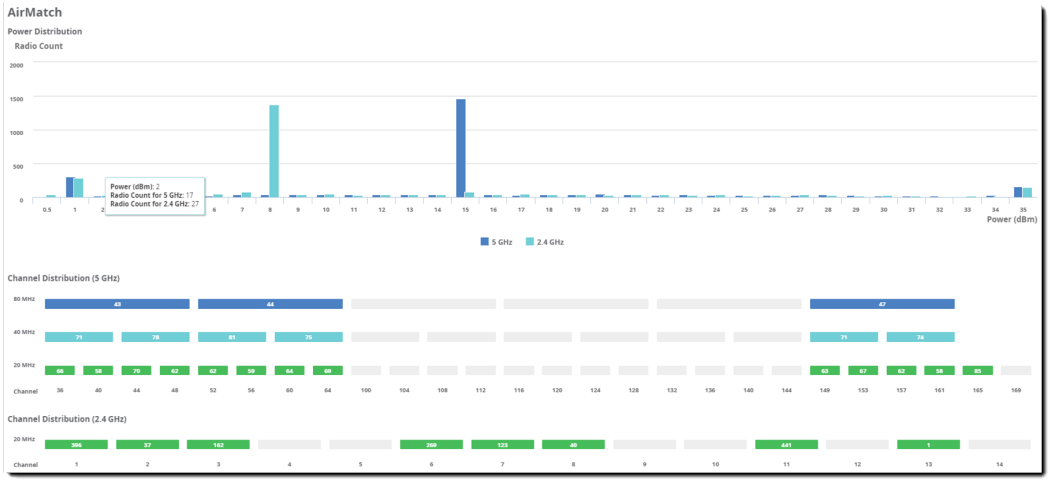
Available for AOS 6.x (ARM) and AOS 8.x (AirMatch), the AirMatch dashboard gives insight into the entire WLAN network. To open the dashboard, go to **Home > AirMatch**.

From the dashboard, you can view the following charts:

- Power distribution. Shows the transmit power for 5 GHz and 2.4 GHz channels.
- Channel distribution (5 GHz). Shows the radio count in the 5 GHz channels and the distribution of channel bandwidth in the 20 GHz, 40 GHz, and 80 GHz ranges.
- Channel distribution (2 GHz). Shows the radios in the 2.4 GHz channels and the distribution of channel bandwidth in the 20 GHz, 40 GHz, and 80 GHz ranges.
- Channel change reasons. Shows channel change reasons if AirMatch can determine the cause of the noise and interference.
- Channel changes (by band and folder). Shows channel changes across multiples APs in a given folder.

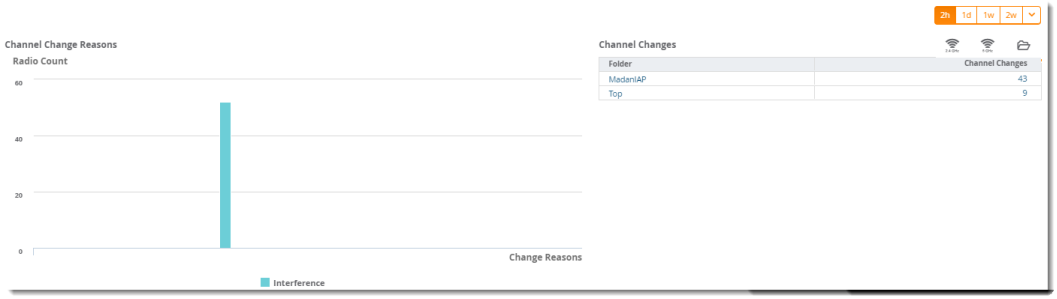
Power and channel distribution charts use color to display separate statistics for clients connecting to the network using 2.4 GHz or 5 GHz channels, as shown in Figure 191.

Figure 191: *Power and Channel Distributions*



You can toggle between statistics for 2.4 GHz or 5 GHz channels when viewing change reasons, by clicking the 2.4 GHz or 5 GHz option links beneath the time slider, as shown in Figure 192. You can also choose the folder view option.

Figure 192: *Change Reasons*



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 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.

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 AirWave.

Figure 193: *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. 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. AirWave will remember the new setting the next time that the page is launched.

The **Thresholds** button is disabled while the page is loading. The **Folder** drop down is disabled until the first plot points display.

Figure 194: *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.

Using Clarity

The Clarity Dashboard enables you to monitor wireless clients as they connect to the wireless network and determine the cause of network connectivity and performance issues.

NOTE

AirWave receives Clarity Live data through AMON messages sent from controllers on the network. The controllers must be running ArubaOS 6.4.3 or later.

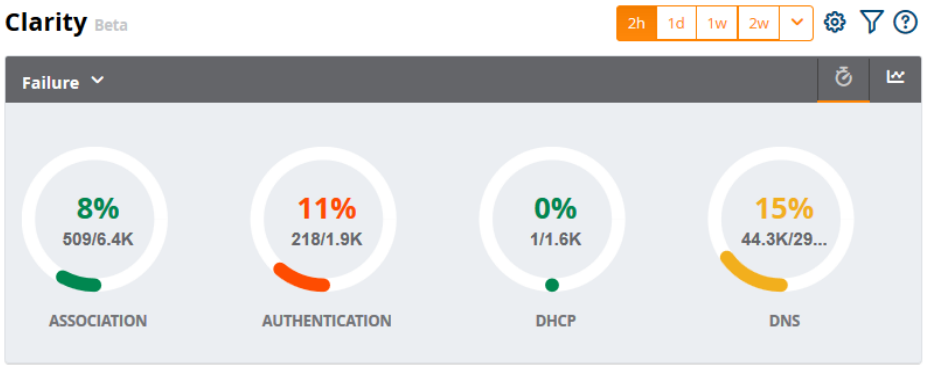
View Clarity Charts

From the dashboard, you can drill down and view real-time data for devices in a specific sub-folder, or view data for a different time interval.

Failures Rates

Figure 195 shows statistics for a 2-hour period, including the percentage of failures for each process, number of failures, and total number of attempts.

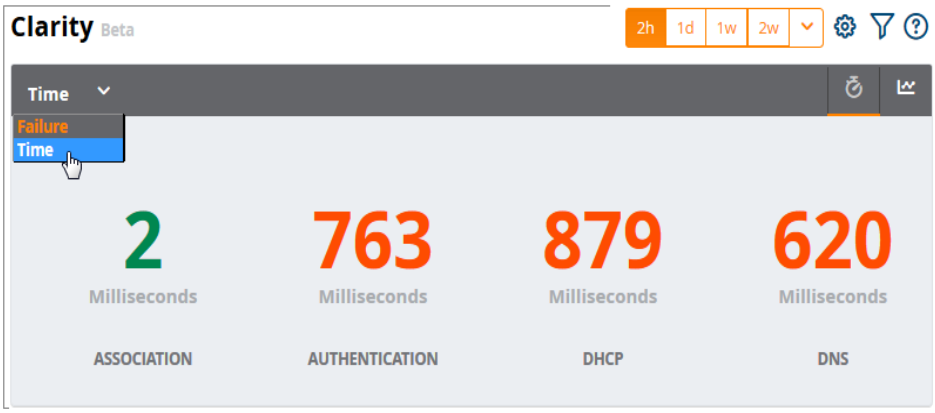
Figure 195: *Failure Rates*



Process Times

To display the average process times over the selected time interval, click the **Failure** drop-down menu in the upper left corner of the dashboard and click **Time**.

Figure 196: *Average Process Times*



Clarity Thresholds

Each icon in the **Summary** table represents quality thresholds for the number failures *and* the average amount of time it takes the process to complete.

For example, if a process has a high failure rate but a good process time, the icon will be red, indicating the most severe threshold crossed in either category. Hover your mouse over an icon to display the number of authentication process failures and successes for clients associating to individual APs or folders of APs, as well as the average time it took for each process to complete.

Refer to Table 109 for descriptions of what each icon color represents and the thresholds for process times and failure rates.

Table 109: *Icon Color Codes and Thresholds*

Icon Color	Description	Process Time Thresholds	Failure Rate Threshold
	Good failure rate *and* process time	• Good Association time: <10 ms • Good Authentication time: <500ms • Good DHCP time: <100 ms • Good DNS time: <100 ms	< 10% failures
	Fair failure rate *or* process time	• Fair Association time: 10 -20 ms • Fair Authentication time: 500-1000ms • Fair DHCP time: 100 - 200ms • Fair DNS time: 100 -200ms	>10% to 20% failures
	Poor failure rate *or* process time.	• Poor Association time: >20 ms • Poor Authentication time: >1000 ms • Poor DHCP time: >200 ms • Poor DNS time: >200ms	>20% failures

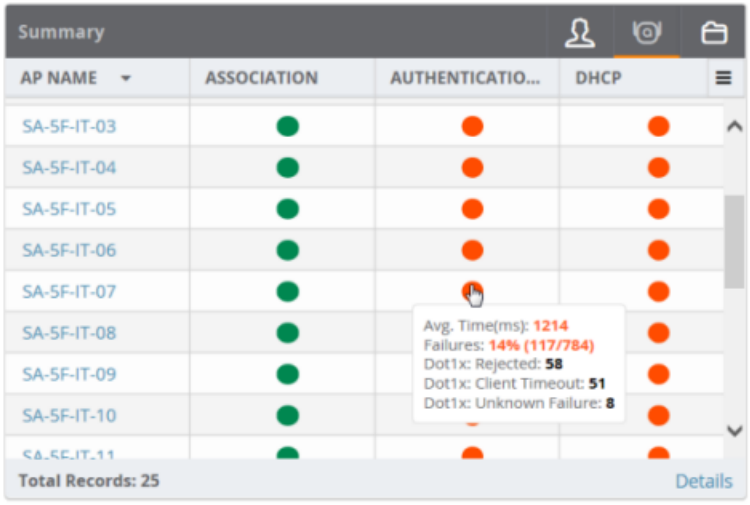
View User Details from the Summary Table

Clarity Live allows you to use the **Summary** table to navigate directly to user details. For example, you can narrow your results to list users that have used a specific server to authenticate, and you can click the **Client MAC address** link to open the User Detail page for the client.

To view user details for a client:

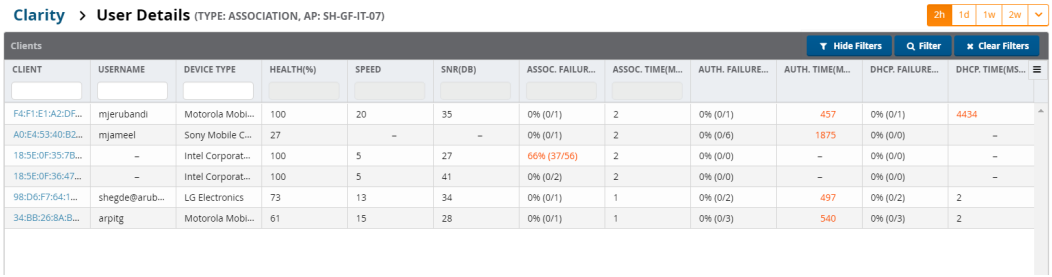
1. In the **Summary** table on the **Home >Clarity** page, locate a client and click in the Authentication column (see Figure 197). Or, you can open the **User Details** page by clicking Association or DHCP.

Figure 197: *Opening the User Details Page for a Client*



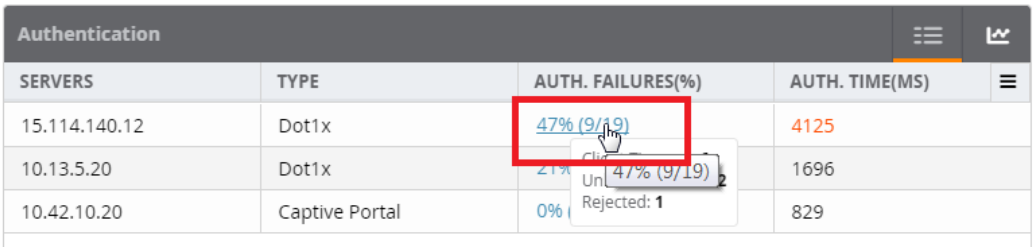
The **User Details** page opens (see Figure 198).

Figure 198: *Clarity User Details*



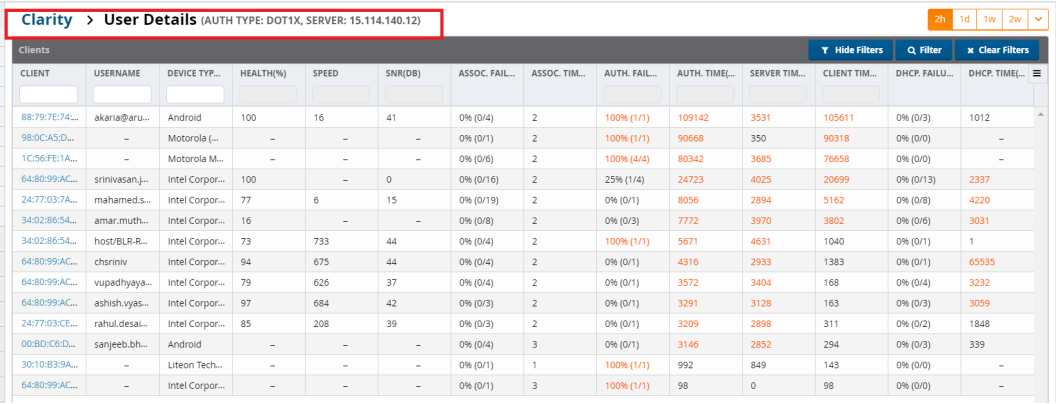
2. Narrow the scope of your analysis, by selecting a link from the **User Details** page. For example, to see authentication failures for all users who have used a specific Dot1x server, click **Auth. Failures (%)** for the server (see Figure 199).

Figure 199: *Filtering Your Results*



The **User Details** page displays filtered results (see Figure 200).

Figure 200: *Filtered User Details for Authentication Failures for Users on a Dot1x Server*



View Authentication Failure Data

The **Authentication** table provides information for the client authentication processes on the network.

Table 110: *Authentication Table fields*

Column	Description
Servers	IP address of an authentication server.
Type	Indicates the authentication server type: • Dot1x: 802.1x • Captive Portal: Captive portal authentication • MAC Auth:MAC authentication • WPA-PSK: WPA encryption with pre-shared key (PSK) authentication
Failures (%)	This column shows the percentage of authentication failures for that server, followed by the total number of failures and the total number of authentication attempts over the selected time interval.
Avg. Time (ms)	The average time it took to successfully complete the authentication process over the selected time interval. Times for both failed and successful attempts are calculated in this average.

Click in the table heading to display of graph of average authentication times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the authentication times during that portion of the time interval, or click to return to the table view.

View DHCP Failure Data

The **DHCP** table on the **Home>Clarity** page provides information about authentication on the network.

Table 111: *DHCP Table fields*

Column	Description
Servers	IP address of a DHCP server.
Avg. Time (ms)	The average time it took to successfully complete the DHCP provisioning process over the selected time interval. Times for both failed and successful attempts are calculated in this average.

Click the in the table heading to display of graph of DHCP times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the DHCP provisioning times during that portion of the time interval, or click to return to the table view.

View DNS Failure Data

The **DNS** table displays the information for DNS resolution attempts.

Table 112: *DNS Table fields*

Column	Description
Servers	IP address of a DNS server.
Failures (%)	This column shows the percentage of DNS resolution failures for that server, followed by the total number of failures and the total number of DNS resolution attempts over the selected time interval.
Avg. Time (ms)	The average time it took to successfully complete the DNS resolution process over the selected time interval. Times for both failed and successful attempts are calculated in this average.

Click  in the table heading to display of graph of DNS resolution times for each server during the selected time interval. Hover your mouse over any section of the graph to view details about the resolution times during that portion of the time interval, or click  to return to the table view.

View Association Data

The **Association** table on the **Home>Clarity** page displays the following information for association times and failures on the network.

Table 113: *Association Table fields*

Column	Description
APs	Name of an AP.
Failures (%)	This column shows the percentage of failed association attempts failures for that AP, followed by the total number of failures and the total number of association attempts over the selected time interval.
Avg. Time (ms)	The average time it took to for a client to associated to the AP over the selected time interval. Times for both failed and successful attempts are calculated in this average.

Click  in the table heading to display of graph of association times for each AP during the selected time interval. Hover your mouse over any section of the graph to view details about the association times during that portion of the time interval, or click  to return to the table view.

Working with Clarity Data

First 25 Results

Clarity Live displays only 25 subfolders and APs with the lowest performance levels. If you have more than 25 subfolders or APs in the folder view, you can increase the number of results returned per page.

To see more than 25 results:

1. Click the **Details** link at the bottom right corner of a Clarity table. A **Details** pop up window appears.
2. Click the **per page** drop down list in the lower left corner of the window and select the number of results.

Click  to view information about APs, or click  to return to the default folder view. To see the top 25 users by Clarity issue, click  at the top right of the Summary table.

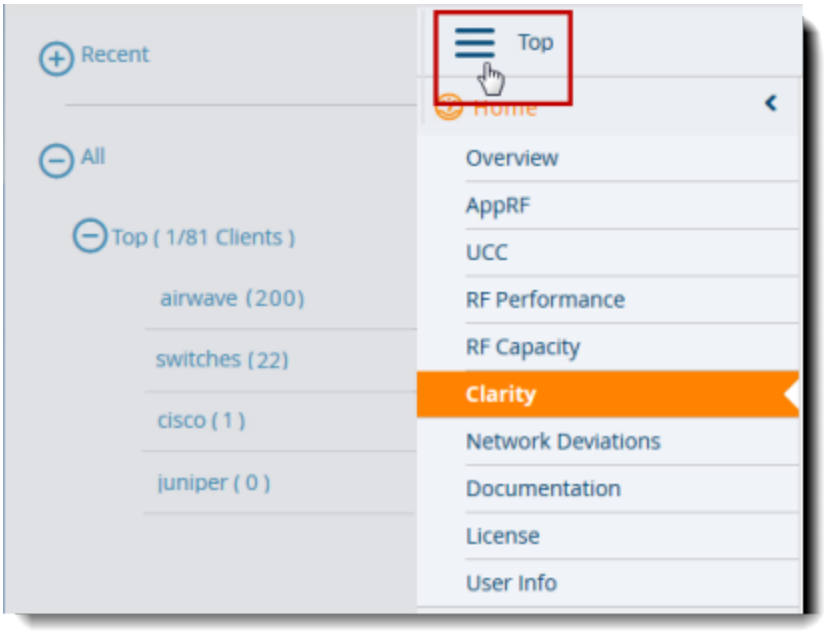
Sorting and Filtering Clarity Data

Select any column heading in a Clarity table to sort the table by that value. Each Clarity table displays entries for 25 devices with the lowest performance levels. You can also select one or more column headings in the **Details** page to sort or filter the table by the selected values.

Selecting a Folder from the Navigation Bar

The navigation bar presents your folders in an organized hierarchy. When you click ≡ in the AirWave WebUI (see Figure 201) and select a folder from the navigation bar, Clarity will present data for the devices in this folder in the Clarity Live dashboard to the right.

Figure 201: *Folder Navigation Bar*



Exporting Clarity Data

Click ≡ by a Clarity table title to display the following list of data export options and table display settings.

- **Export all data as csv**: Export the entries currently displayed in the table to a .csv formatted file.
- **Export visible data as csv**: Export all entries recorded for the selected time frame to a .csv formatted file.
- **Export all data as pdf**: Export the entries currently displayed in the table to a PDF file.
- **Export visible data as pdf**: Export all entries recorded for the selected time frame to a PDF file
- **Details**: Display the details window for the table.
- **Columns**: Click a column heading to hide or display a column in the table.

Changing the Time Range

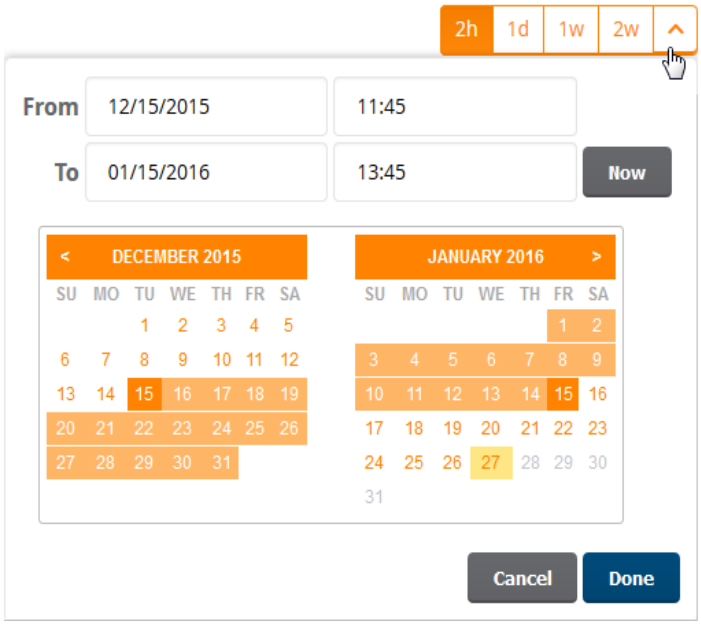
The Clarity Live dashboard displays data for the previous two hours. Clarity immediately refreshes and displays updates in the Clarity Live dashboard after any changes to the time range.

To display data for the previous day, week, or two weeks, select an option from the time range toolbar.

Figure 202: *Select a Clarity Time Range*

To select a custom time range, click the arrow on time range toolbar, then select a custom start and end time.

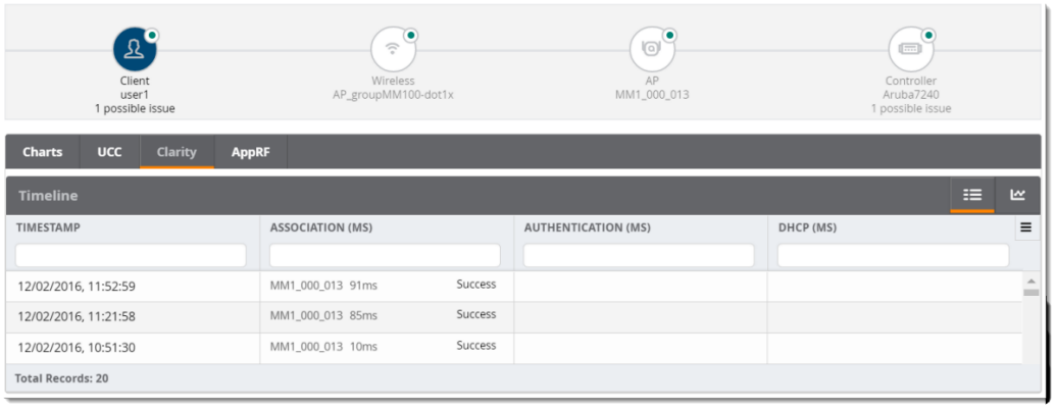
Figure 203: *Selecting a Custom Time Range*



Evaluate User Status

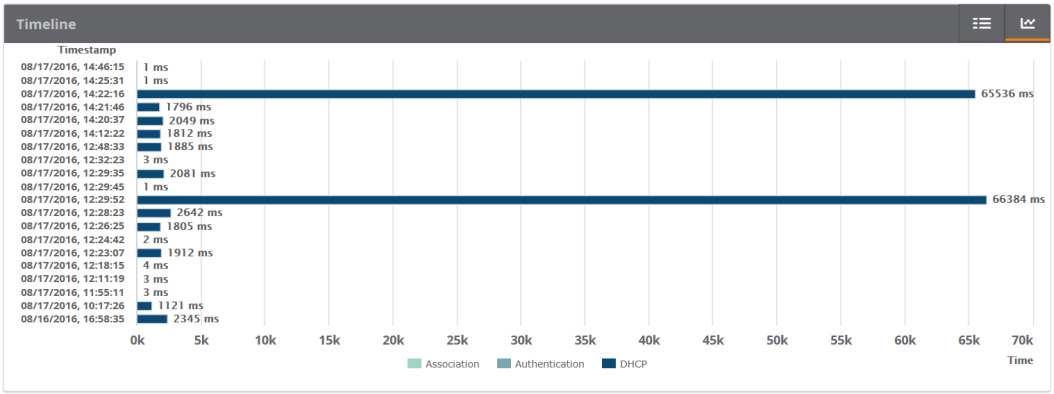
The **Clients Detail** page provides Clarity information, such as association, authentication and DHCP events for a particular client, in a table view, as shown in Figure 204.

Figure 204: *Client Diagnostics for Clarity Live Monitoring*



You can click  to display the Clarity live monitoring data in a timeline view, as shown in Figure 205.

Figure 205: *Clarity Timeline*



You can access this page by doing one of the following:

- Search for a user. In the resulting window, click the MAC address link.
- Click the MAC address link in the **Devices > Monitor** page, the **Clients > Connected** page, or the **Clients > All** page.

Using Topology

Topology looks at the devices and links in your network and puts them in an interactive topology map.

The map has several main components:

- **Zoom Control**. Click ⊕ and ⊖ to change the zoom level of your topology map, or click ⤢ to return to the full screen. In addition to using the zoom controls, you can use your mouse and keyboard, or touchscreen and trackpad to:
  - Pan and zoom to view specific parts of the map.
  - Recenter your map.
  - Drag and drop a node (in planetary view). For information about views, see "Select Your Layout" on page 288.
  - Drag and drop the bird's eye view to anywhere in the map.
- **Alert Notifications**. Click the 

icon to view changes in your network topology.
- **Search Field**. Find devices by name or IP address. For more information about finding devices in the network topology, see "Locate Your Device" on page 287.
- **Task Pane**. Click the tabs to access shortcuts to tools and tasks, such as changing the map layout or mapping your network devices, including devices that are part of a spanning tree. For more information about using these tools, see "Set up Your Map" on page 287.
- **Topology Map**. Click anywhere in the topology map to rearrange nodes, view tooltips, and access shortcuts to monitoring pages. Click 👁 to hide and unhide the bird's eye view. For more information about accessing monitoring information, see "Check the Status of Your Network" on page 294.

NOTE

When you navigate to Topology from a device monitoring page, the ⚠ Resetting filters. reminder above the zoom controls alerts you that the topology map isn't filtered. For information about excluding devices from the topology map, see "Apply Filters" on page 291.

NOTE

A high number of devices can impact Topology load times. Aruba recommends selecting the desired folders you wish to view before loading Topology. For example, to limit your view to the devices in a folder that has an ID number 5, enter the following URL into a browser: *https://example.com/topology/getTopology?folderId=5*. For more information, see the *AirWave API Guide*.

Getting Started

1. Set up Your Map
2. Check the Status of Your Network
3. Take Action from Quick Links
4. View Device and Stack Membership Details
5. Run a Command

Set up Your Map

Topology provides several ways to make finding your devices and visualizing links fast and easy. When setting up your map, you can locate your device, select your layout, pin a device, show spanning trees and show VLANs, apply filters, set a root node, save your preferences, and collapse your view.

NOTE

If you want to view the network topology in expanded view but the default view is collapsed, you need to adjust these settings on the **Devices > List** page. For more information, see "Changing the Default Expansion" on page 294.

Locate Your Device

You can search for devices by name or IP address. Topology limits the results to show devices based on your user role permissions.

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 or numbers in the search field, as shown in Figure 206.

Figure 206: *Locating a Device*

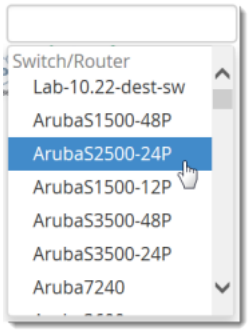
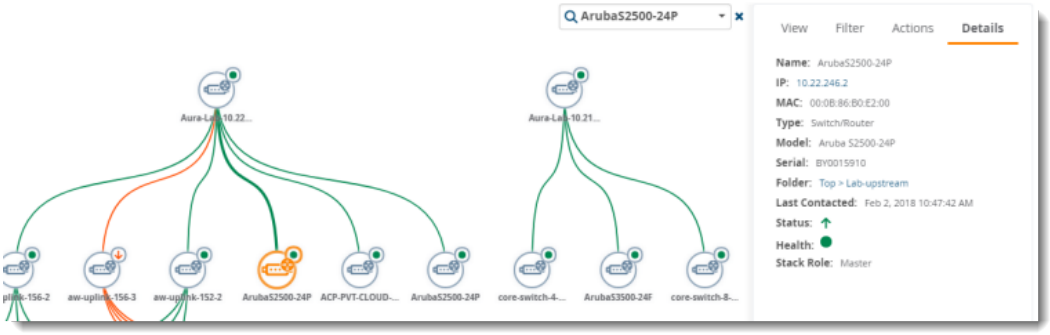


Figure 207 shows the device centered on the map and highlighted in orange with device details displayed in the task pane. For information about device status and health indicators, see "View Device and Stack Membership Details" on page 296 and "Check the Status of Your Network" on page 294.

Figure 207: *Search Result*



Select Your Layout

You can rearrange the way the topology map displays the connections from the root node to other nodes. If you select a device to reposition it on the map, the device and its connections move with it. Some nodes might not have connections and look like islands on the map.

To change the layout, choose from the following **View** options in the task pane:

- 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 and Right Left. Creates a topology map that flows from left to right, or right to left.
- Planetary. Creates topology map that shows devices connected to a hub, spread without overlapping.

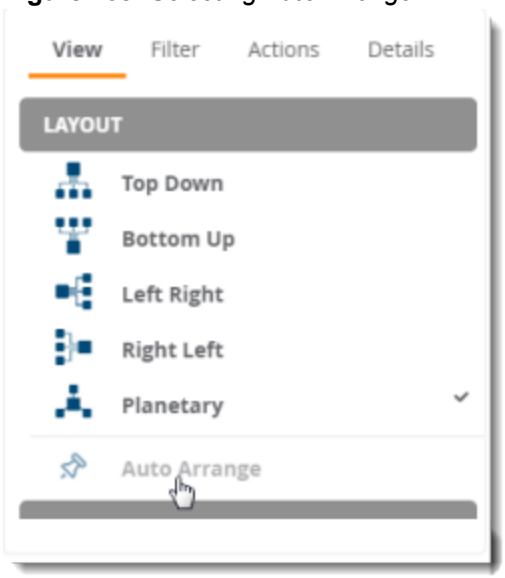
Arrange Devices on the Map

You can arrange the devices anywhere you want on the map, making it easier to see them and work with the map, by turning off Auto Arrange. When moving around the map, Topology keeps your pinned devices in the map.

To arrange a device on the map:

1. Click **Auto Arrange** from the **View** options in the task pane.

Figure 208: *Selecting Auto Arrange*



2. Drag and drop the device to a new location in the map.

To unpin the device, click **Auto Arrange** again. You'll see that Topology removes all pins and redistributes the devices evenly across the map.

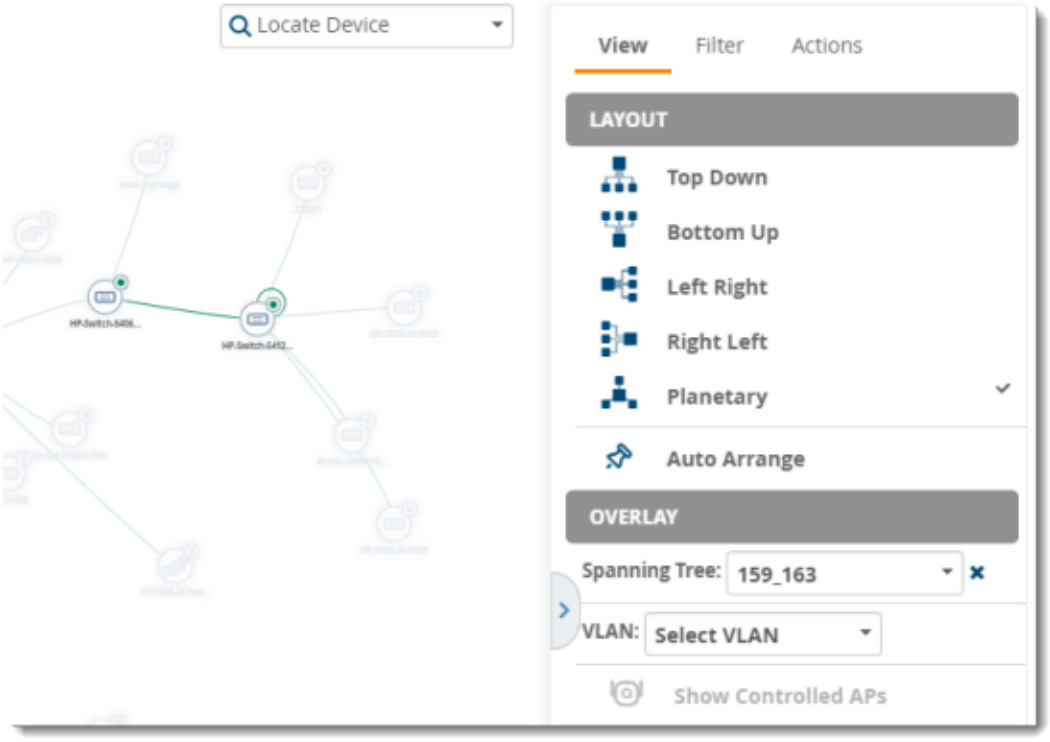
Show Spanning Tree Members

Topology learns which devices are part of a spanning tree from the switch using the STP protocol and highlights the devices that are part of the spanning tree in the topology map, as shown in Figure 209. To view the spanning tree membership, select a spanning tree from the **View > Overlay** menu in the task pane.

NOTE

Topology will show spanning tree data only for switches which support IEEE standard spanning tree MIBS.

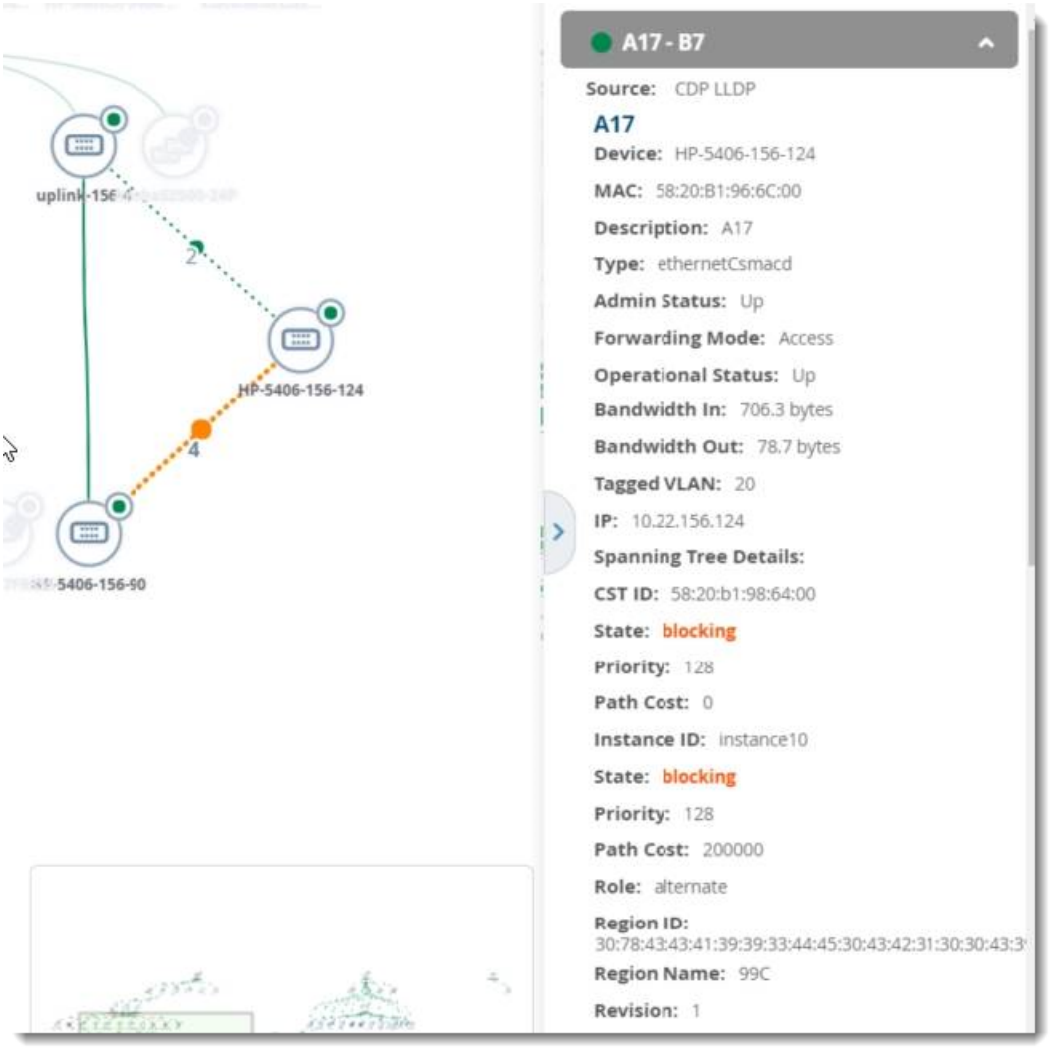
Figure 209: *Selecting a Spanning Tree Overlay*



Topology also displays STP ports that are in blocking state. When you hover over the link circle in the topology map, the tooltip shows the link types and STP port status, as shown in Figure 210.

Clicking on the link shows you link details in the task pane. A link with a circle in middle denotes an aggregated link, and a link with a number label denotes multiple links. A dotted link denotes there is a blocking port--either a single, multiple, or all ports blocked.

Figure 210: *Viewing Blocked STP Ports*

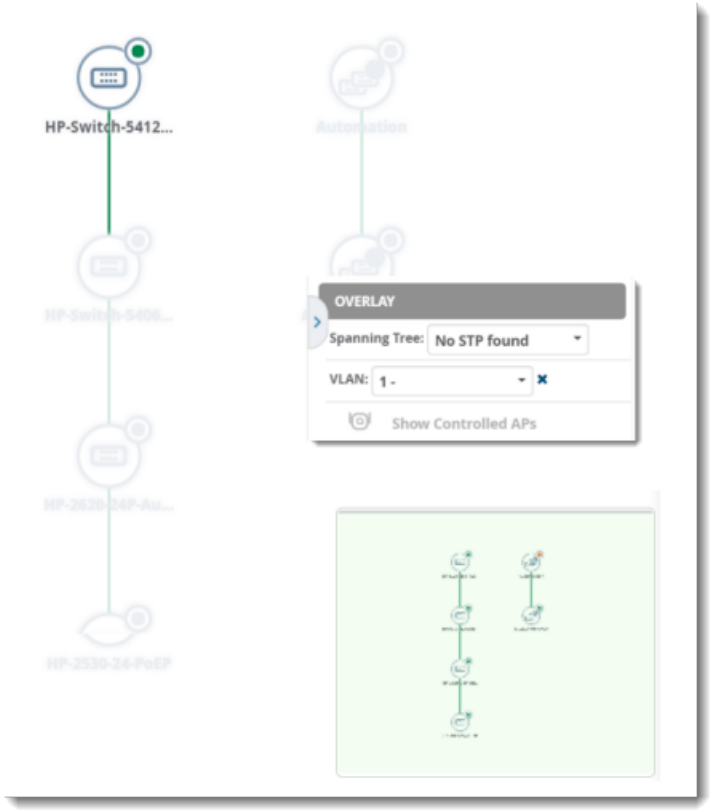


Show VLANs

When you select a VLAN from the **View > Overlay** menu in the task pane, nodes and their connections are highlighted and shadowed in the VLAN view, as shown in Figure 211.

Topology also displays and highlights down devices, obtaining the VLAN information from the last time AirWave polled the devices.

Figure 211: *Selecting a VLAN Overlay*



Apply Filters

You can customize the topology map by applying filters to your map. Filters affect which devices show up on your map. For example, you might create a filter to view only switches. When you filter by folders, user roles determine which folders are visible.

Nodes on the map can include access points, switches, switch stacks, wireless controllers, IP access controllers, and routers. By default, access points are hidden from map view to help you visualize your switching infrastructure.

NOTE

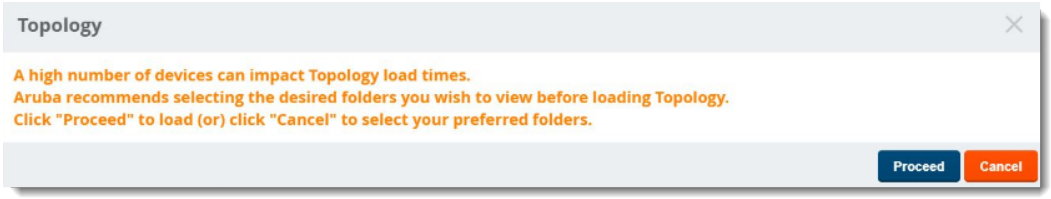
By default, AirWave hides access points from the topology map. To see access points, select AP from the filter list.

To apply a filter:

1. Select **Filter** from the task pane.
2. To show or hide a device in the topology map, click the check mark next to the device type in the **Devices** list.
3. To show only devices from a folder in the topology map, select that folder from the **Folders** drop down list. After selecting folders, AirWave alerts you to impact to performance due to the number of nodes that Topology will plot. You might want to put devices in different folders to reduce the topology load time.

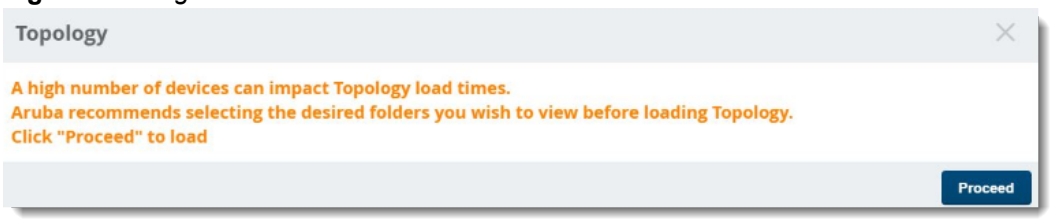
   If there are more than 250 edges in the topology, AirWave displays the message shown in Figure 212. Click **Proceed** to load, or click **Cancel** to select preferred folders.

Figure 212: *High Device Count in AirWave Notification*



If there are more than 250 devices in the selected folder, AirWave displays the message shown in Figure 213.

Figure 213: *High Device Count in Folder Notification*



The topology map shown in Figure 214 has been filtered to display only switches in the **Top > SIM > Lab_HP** folder.

Figure 214: *Filtered Map View*

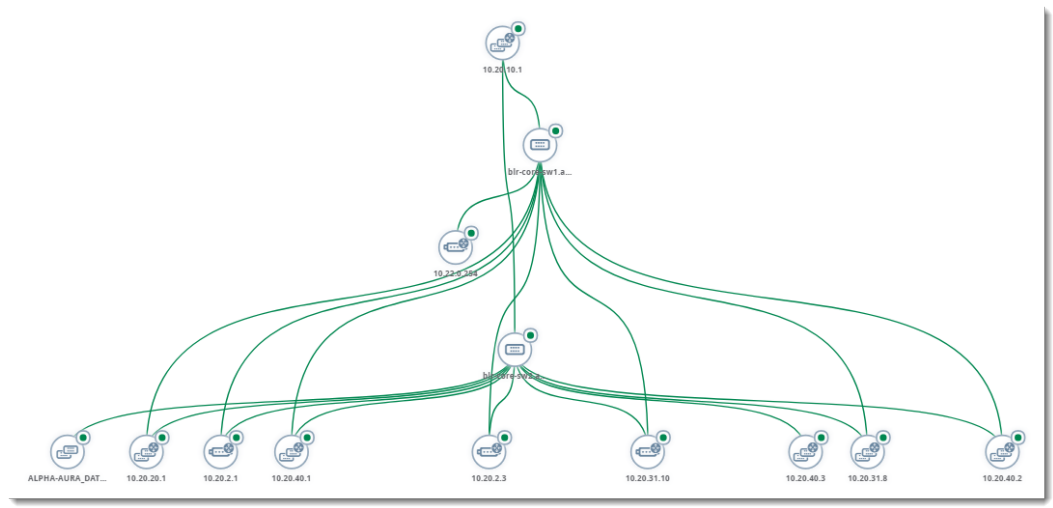


Table 114: *Device Icons*

	Controller
	Switch (L2)
	Stack switch (L2)
	Switch router (L3 Switch)

	Stack switch (L3)
	Router
	AP

Set the Root Node

You might want to change the root node that Topology places at the top of the topology map. If you have a network which is separated from another network, you can set a root node on each island.

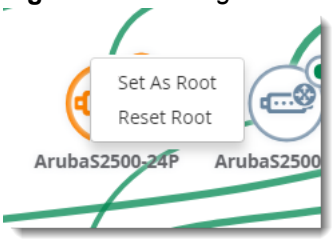
NOTE

When you set the root node, Topology saves the root node in a browser cache so that anyone with access to the AirWave server can view the root node from any client browser.

To change the root node:

1. Locate the device in the topology map.
2. Select **Actions** from the task pane.
3. Highlight the node in the map, then click **Actions** in the task pane.
4. Select **Set As Root**. Topology highlights the node and updates the map to show the new root node. Changes can be made by selecting **Reset Root Nodes**.

Figure 215: *Setting the Root Node*



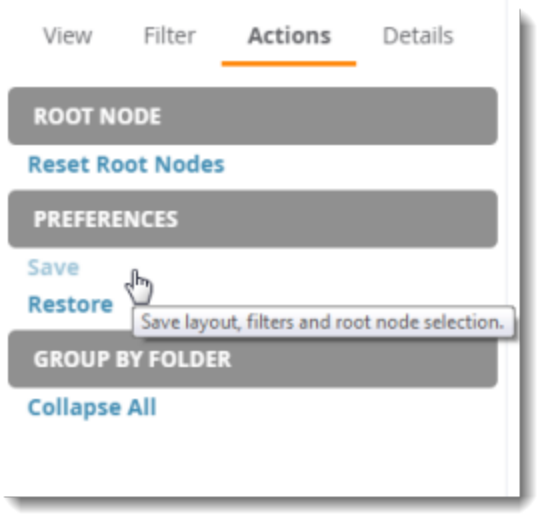
Saving Your Preferences

After changing your layout, filters, or root node, you can save your custom map.

To save your preferences:

1. Select a layout, filter, or root node.
2. Select **Actions** from the task pane.
3. Locate the Preferences section, then select **Save**. Clicking **Restore** applies your last saved preferences for layout, filters, and root nodes.

Figure 216: *Saving Your Preferences*



Changing the Default Expansion

User preferences defined on the **Devices > List** page affect the way AirWave displays the network in the topology map. The default expansion is collapsed and based on the folder level you last visited. If your view is collapsed, you will only see devices from that folder level.

To change the default expansion:

1. Navigate to **Devices > List**.
2. Click the, **Default Expansion** drop-down menu and select **Expanded**.

3. Click the Topology icon ( ) beside the **Default Expansion** menu to return to the **Home > Topology** page. The topology map displays the devices in the selected folder in expanded view.

Check the Status of Your Network

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.

Device Status

Colored circles in the topology map and colored arrows in the tooltip or Details tab indicate that:

- (next to the device icon) there are no alerts or detected rogues.
- (next to the device icon) there are 1 to 2 alerts and no detected rogues.
- (next to the device icon) there are at least 2 alerts or 1 or more detected rogues.
- the device is up.
- the device is down.

Health Status

Colored circles in the tooltip or Detail tab, or colored link lines in the topology map indicate that:

- more than 25% memory is available and less than 75% CPU is used.
- (more than 15% memory is available and less than 85% CPU is used.
- less than 15% memory is available and more than 85% CPU is used.
- less than 70% bandwidth is used.
- between 70% and 90% bandwidth is used.

Link Status

Colored link lines in the topology map indicate that:

- the link is up.
- the link is down.

Take Action from Quick Links

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

View Tooltips

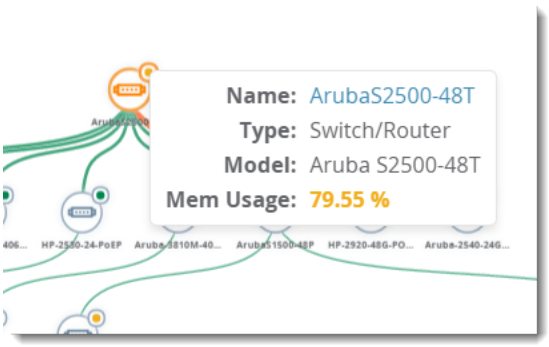
Tooltips provide quick links to the monitoring page for the device or the switch interface. Tooltips also display potential problems on a device. Alerts are colored orange in the tooltip.

To view tooltips, hover your mouse over:

- A node, which is represented by the device icon in the topology map.
- The link, which is the represented by the line between two switches.
- The link count, which is represented as a number alongside the link between two switches.

In Figure 217, the tooltip for a node shows you the name of the device, device type, model, and a health alert.

Figure 217: *Tooltip for a Node*

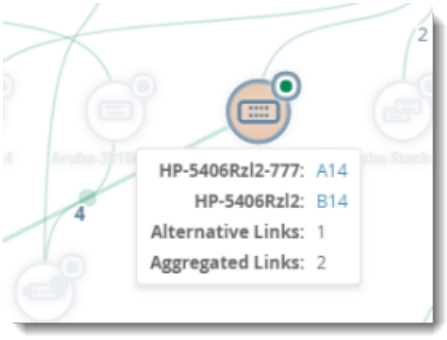


In Figure 218, the tooltip for a network link shows an alert for a down device. You can click the hyperlinks to troubleshoot the problem.

Figure 218: *Tooltip for a Link*

In Figure 219, the green link circle indicates that the link is aggregated; the link count indicates that there are 4 logical links, of which are 2 individual links and 2 aggregated links.

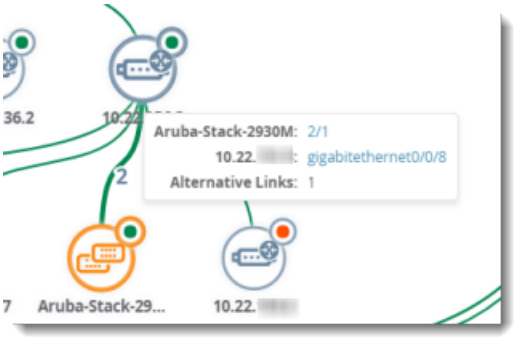
Figure 219: *Tooltip for an Aggregated Link*



The tooltip also shows whether the redundant links between tree members are dynamic, between 2 peers that support LACP, or aggregated, between 2 peers that support HP_LA. In Figure 219, "alternative link" refers to the number of non-aggregated redundant links. If you point your mouse over the link count, the tooltip provides a hyperlink to the switch interface monitoring page.

Figure 220 shows the tooltip for stack member. You can access monitoring pages from the hyperlinks in the tooltip.

Figure 220: *Tooltip for a Stack Member*



View Device and Stack Membership Details

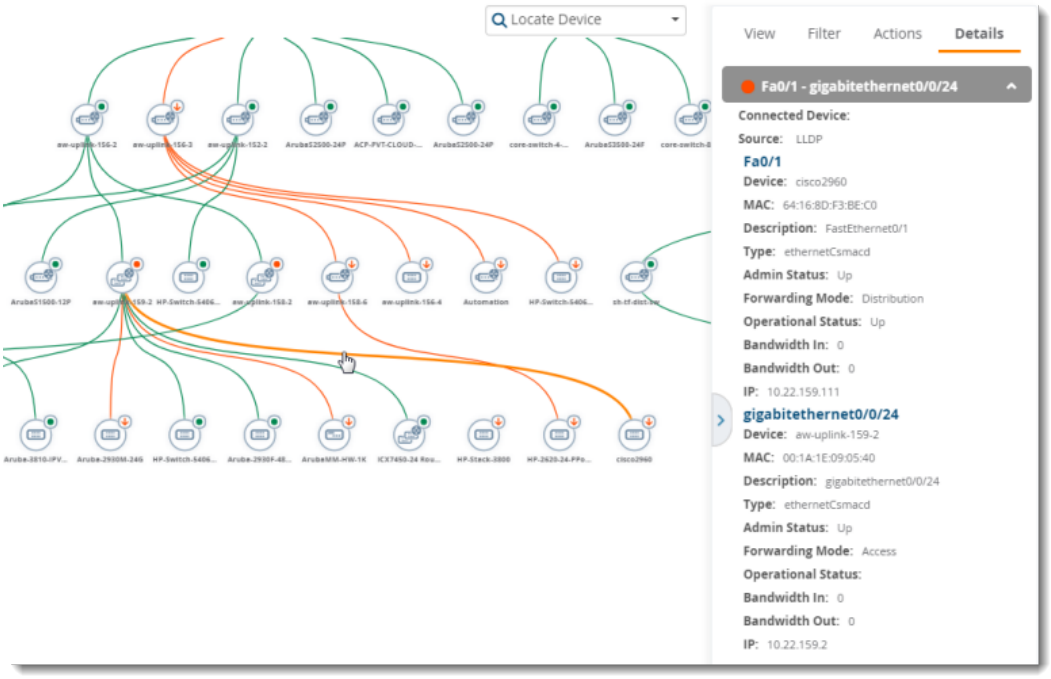
The **Details** task pane provides information, health and status indicators, and quick links to monitoring pages.

To view device and stack membership details:

- Search for a device or switch stack
- Click the node in the map
- Click a connection in the map

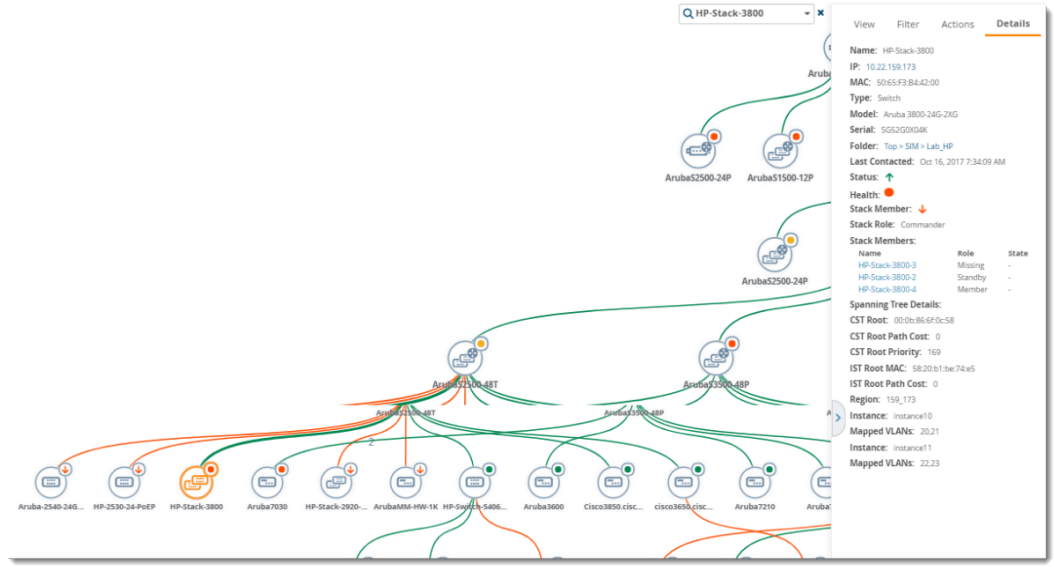
In Figure 221, you can see that the health of the network connection, represented as an orange line in the topology map, is critical. Thicker lines represent multiple links between devices. By clicking on the links to the switch ports, you can troubleshoot further.

Figure 221: *Connected Devices and Switch Interface Details*



In Figure 222, you can see information about all members in the stack commanded by the switch that is highlighted in orange on the map. The health of the network connection, represented as an orange circle in the **Details** task pane, alerts you to critical status. By clicking on the links to the stack members or folder, you can manage a stack member.

Figure 222: *Stack Member Details*



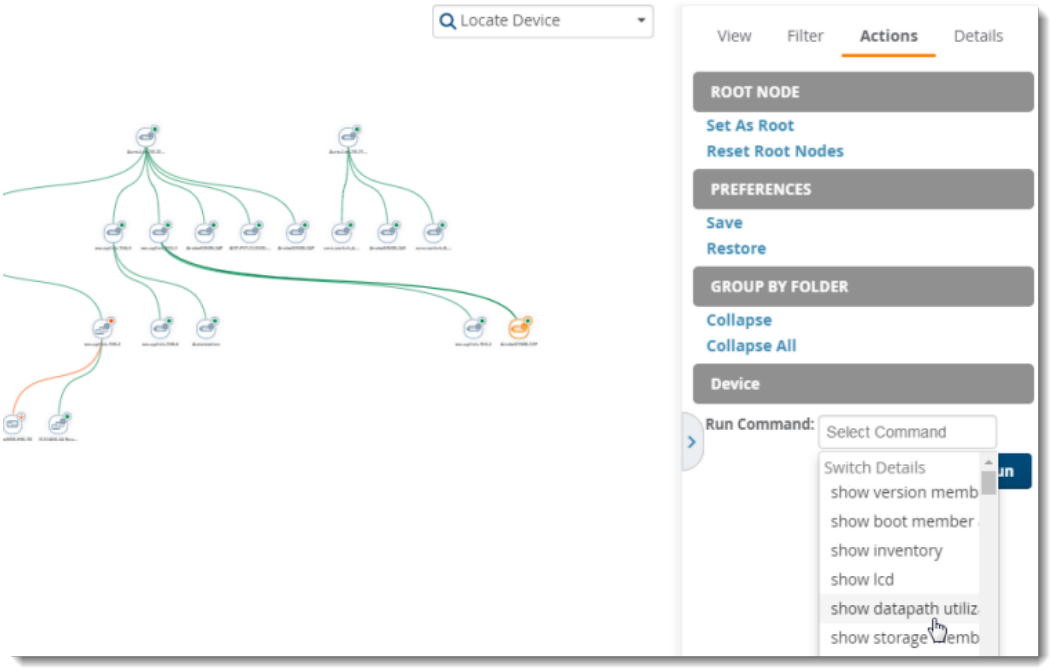
Run a Command

In addition to running a command from the monitoring page for a device, you can run a command directly from the topology map. The commands available depend on which device you select. So, if you select a switch, the commands you can choose from in the task pane are switch-related.

To run a command from the topology map:

1. Click a node in the map.
2. Select **Actions** from the task pane.
3. Locate the Device section, then select a CLI command from the **Run Command** menu.

Figure 223: *Selecting a Command to Run on a Device*



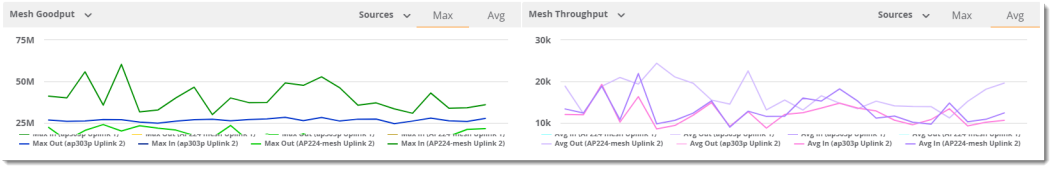
Using the Mesh Dashboard

AirWave provides a dashboard view of your mesh topology on the **Home > Mesh** page. The **Cluster** dropdown menu allows you to select an available mesh cluster that has devices with mesh portal and mesh point topology.

AirWave displays counters at the top of the page for **Mesh Portals**, **Mesh Points** and **Mesh Links** for a mesh cluster that you select from the **Cluster** drop-down menu at the top of the page.

The charts use color to display separate statistics for AP uplinks, as shown in Figure 224.

Figure 224: *Mesh Dashboard*

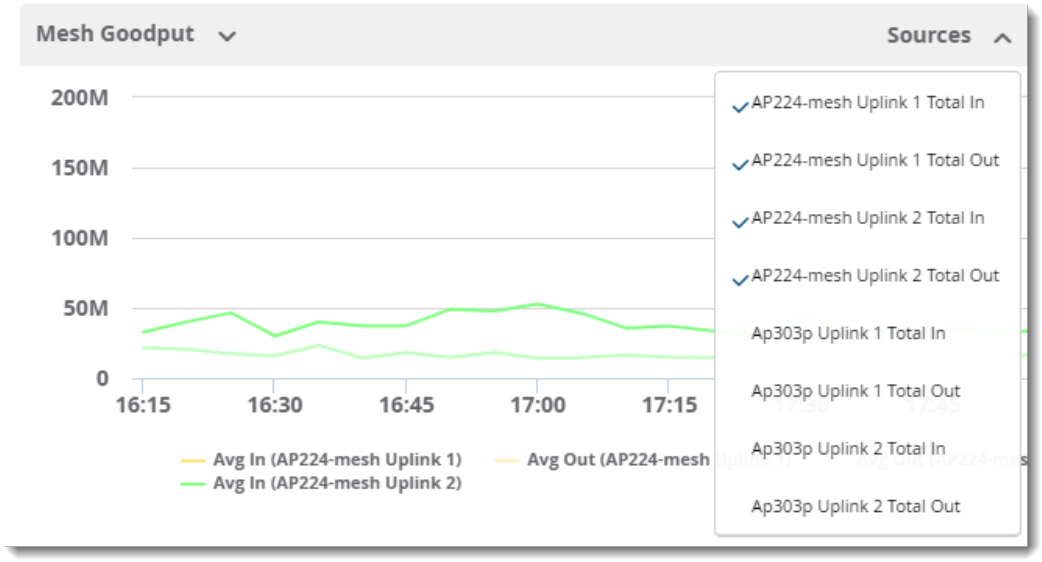


From the dashboard, you can view the following charts:

- Mesh Goodput. Shows the average load of traffic flow in and out to an uplink port by source, max, or average.
- Mesh Throughput. Shows the average rate at which traffic flows in and out to an uplink port by source, max, or average.
- Mesh SNR.

You can apply filters to your charts, as shown in Figure 225.

Figure 225: *Results Showing Filters*



Mesh Topology List

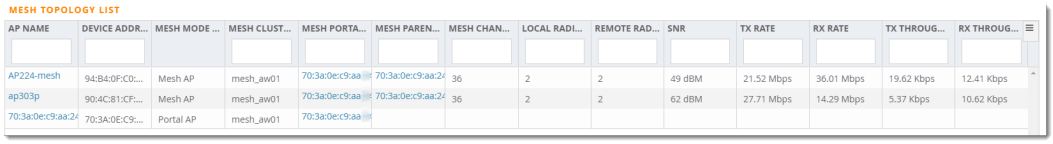


Figure 226 describes the Mesh Topology List fields. This table displays all columns by default. Click ☰ at the end of the table to select the fields you want.

Figure 226: *Mesh Topology List Fields and Descriptions*

Field	Description
AP Name	Displays the name of the mesh AP.
Device Address	Displays the MAC address of the mesh AP.
Mesh Mode	Displays whether the AP is configured as a mesh portal or mesh point.
Mesh Cluster	Name of the mesh cluster.
Mesh Portal	The gateway between the wireless mesh network and the enterprise wired LAN. You configure an Aruba AP to perform the mesh portal role, which uses its wired interface to establish a link to the wired LAN.
Mesh Parent	Displays the MAC address of the parent node for the mesh point.
Mesh Channel	Displays the channel used by the mesh cluster.
Local Radio	Radio used by local mesh points.
Remote Radio	Radio used by remote mesh portals.
SNR	Displays the mesh signal-to-noise ratio (SNR).

Field	Description
TX Rate	Displays the transmit data rate on the mesh network.
RX Rate	Displays the receive data rate on the mesh network.
TX Throughput	Displays the transmit throughput on the mesh network.
RX Throughput	Displays the receive throughput on the mesh network.

Accessing AirWave Documentation

The **Home > Documentation** page provides easy access to all relevant AirWave documentation. All of the documents on this page are hosted locally by your AirWave server. The PDF files can be viewed by any PDF viewer, and the HTML files can be viewed in any supported browser.

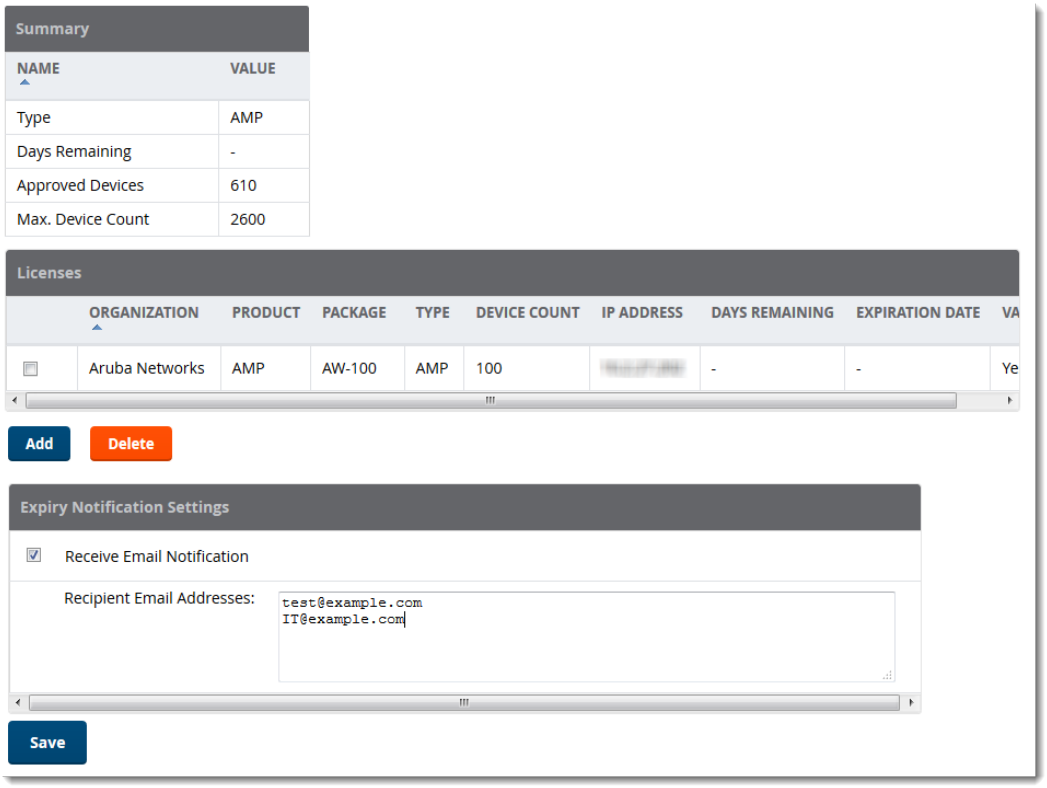
If you have any questions that are not answered by the documentation, please contact Aruba support.

Working with Licenses

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 AirWave license covers the switch stack.

Figure 227 illustrates this page, and Table 115 describes the contents.

Figure 227: *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 Aruba 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 115: *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 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.
IP Address	IP address of the 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. 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 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 User Information and Customizing the WebUI

You can update your user information and customize what you see in the AirWave in the WebUI from the User Info page (see Figure 228).

Configure Your User Information

To configure your user information:

1. Navigate to **Home > User Info**.
2. In the **User Information** section, enter the following information :
   - **Name**—Enter the ID by which you log into and operate in AirWave.
   - **Email Address**—Enter the email address to be used for alerts, triggers, and additional 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 AirWave users or administrators to understand the functions, roles, or other rights of the user being created.

Customizing the WebUI

You can customize your top header statistics, search preferences, and display preferences.

To configure what you see in the AirWave WebUI:

1. Navigate to **Home > User Info**.
2. Complete the information described in Table 116.

Figure 228: *User Info Page*

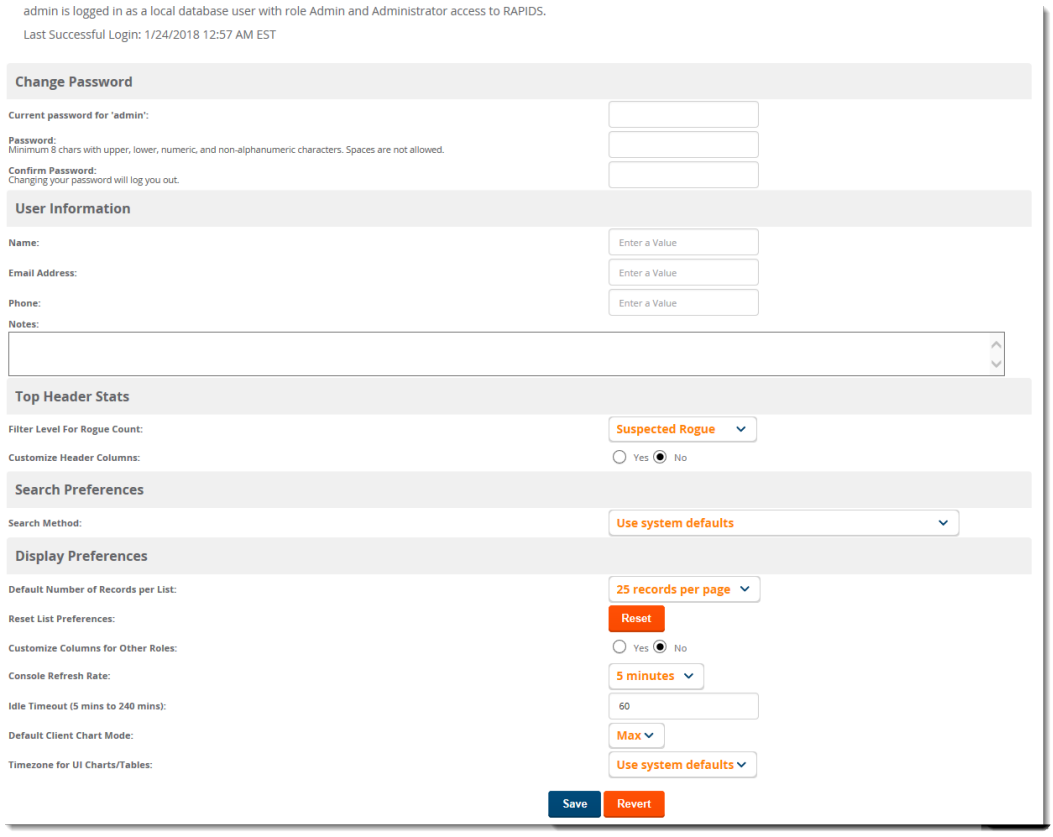


Table 116: *Home > User Info Fields and Descriptions*

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 420.
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 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 *AirWave 8.2.11.1 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 304 for details. **Note:** The severe alerts count header info will only be displayed if 'Severe Alerts' is selected in the **Stats** section above and if a severe alert exists. **Note**: This field only appears if you selected **Yes** in the **Customize Header Columns** field.
Include Device Types	Configures the types of devices that should be included in the header stats. If a device type is not selected then it will not be included in the header stats. **Note:** This field only appears if you selected **Yes** in **Customize Header Columns**.
Search Preferences	
Search Method	Specify one of the following search methods: • Use System Defaults: The Search Method will be based on the system-wide configuration setting. This method is configured on the **AMP Setup > General** page.Active clients + all devices: This looks at all active clients (not historical) and all devices. This search is not case-sensitive. • Active clients + historical clients (exact match) + all devices: Commonly referred to as Quick Search, this looks at all active and historical clients and all devices. This search is not case-sensitive. The results of this search display in a 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.

Table 116: *Home > User Info Fields and Descriptions (Continued)*

Field	Description
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 AirWave automatically ends the user session. This setting only the logged-in user of this AirWave. The default is 60 minutes. To set the max idle timeout for all users of this AirWave, see "Configuring the User Login" on page 47.

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.

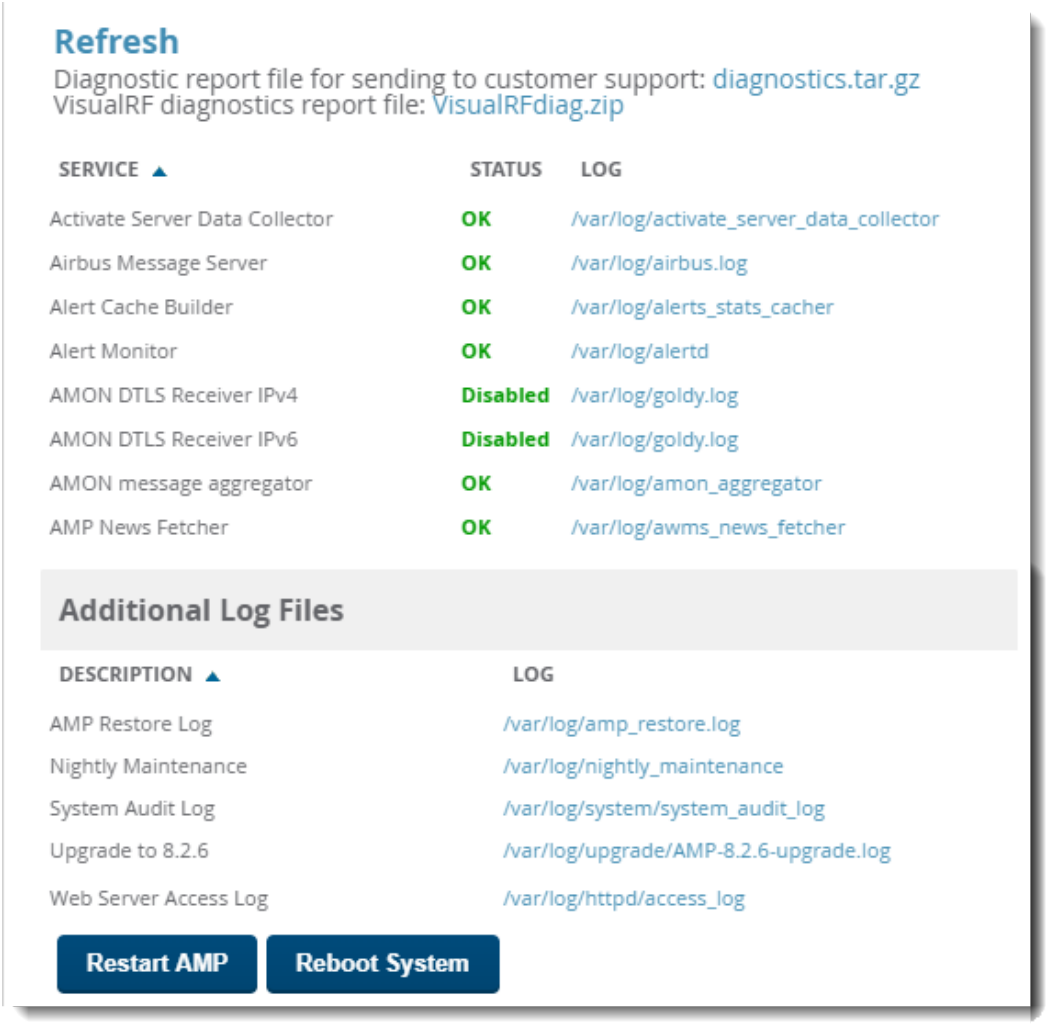
The **System** pages provide a central location for system-wide AirWave data and settings. These system pages show you syslog messages and AirWave events and let you set triggers, respond to alerts, manage configuration jobs, and monitor system performance.

Checking the Status of AirWave Services

AirWave records information about the services and puts them into log files that are available on the **System > Status** page. You can also access other AirWave logs on the **System > Download Log Files** page. For information, see "Downloading Log Files" on page 306.

Figure 229 shows an example of the System Status page. Green status descriptions indicate everything is OK or disabled. If you see status descriptions in red, contact Aruba support for help troubleshooting the service which is down.

Figure 229: *System Status Page*



In addition to viewing service status and downloading log files, you can:

- Click **Refresh** at the top of the page to update system status.

- Click the blue **diagnostics.tar.gz** link at the top of the page to get diagnostic reports and logs, or the **VisualRF.diag.zip** link to get VisualRF diagnostic information. Both will help customer support troubleshoot and solve problems.
- Click **Restart AMP** to restart AirWave services without power cycling the server or reloading the OS.
- Click **Reboot System** to power cycle your AirWave remotely.

Important AirWave Logs

Table 117 describes some of the most important AirWave logs. You can download additional logs from the /var/log and /tmp directories using SSH. If Aruba support engineers request these additional logs. you'll get instructions on how to retrieve the logs.

Table 117: *Important AirWave Logs*

Service	Log	Description
Aruba Device HTTPS Handler	device_https_ handler	Logs switch ZTP activities.
Client Monitor Worker	async_logger_ client	Logs device monitoring checks.
Configuration Server	config_pusher	Logs errors in pushing configuration to devices.
Database	pgsql	Logs database activity.
Postfix Mail Server	maillog	Applies in cases where emailed reports or alerts do not arrive at the intended recipient's address.
RADIUS Accounting Server	radius	Displays error messages associated with RADIUS accounting.
VisualRF Engine	visualrf.log	Details errors and messages associated with the VisualRF application.
Web Server	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 Aruba support whenever reporting an internal server error.

Downloading Log Files

AirWave provides logs on the **System > Download Log Files** page that help with troubleshooting problems. You can also access logs generated by services, upgrades, audits, nightly maintenance, and restore jobs on the **System > Status** page.

To download a log file:

1. Click the blue file path link to download the log. AirWave saves the file to your Download folder. If a message asks you what to do with the file, click **Open with** and select the program you want to use to open the file. Or you can click **Save file** and view the file later.
2. Locate the log and follow the onscreen instructions to open the file.

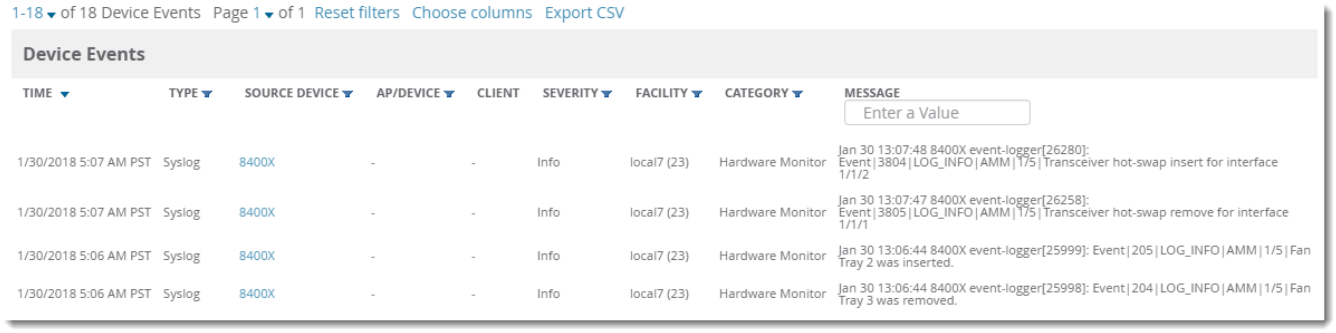
Viewing Device Events

Admins can use the **System > Syslog & Traps** page to review all syslog messages and SNMP traps that AirWave receives from the trigger type **Device Event**. For more information about triggers, see "Viewing Triggers" on page 318.

Starting with AirWave 8.2.6, you can set critical thresholds to alert when there are hardware failures on the Aruba 8400 and 8320 switches. By default, AirWave enables the trigger when you upgrade to or install AirWave 8.2.6.

Figure 230 shows an example of events for the Aruba 8400 Switch.

Figure 230: *Viewing Device Events*



Here are some of the details about the device events you can view from the Syslog & Traps page:

- Time. The time the device event occurred.
- Type. The type can be syslog or SNMP trap.
- Source Device. The name of the device that sent the message. This field provides a link to the device monitoring page if you have visibility to the device, or it can be empty if AirWave can't correlate the source IP address.
- AP/Device. This field provides a link to the device monitoring page for a device other than the source device if it correlates data contained in the message (by LAN MAC, BSSID, or IP Address) and you have visibility to the device.
- Client. The user's MAC address, if found in the message. This field provides a link to the client page if you have visibility to the user's AP, or it can be empty.
- Severity. The event severity can be emergency, alert, critical, bug, error, warning, notice, or info.
- Facility. The facility is obtained from part of the syslog spec, which is the logical source of the message. From controllers, the facility will always be one of local0 to local7. You can configure on the controller which facility you want to use in the messages when sending syslog messages to a receiver.
- Category. For SNMP traps, the category can be 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. Categories for traps and syslog messages only works for events from anArubacontroller.
- Message. The raw trap message includes the AP MAC Address, time sent, and other information. For syslog messages, AirWave doesn't display the numbers at the beginning of the message that indicate the severity and facility. For SNMP traps, AirWave tries to translate them into human-readable format. AirWave won't receive processed SNMP traps into the Device Event framework if the AirWave doesn't have the MIB file to translate the trap.

Syslog messages also appear in the **Devices > Monitor** page for controllers and in **Clients > Client Detail** pages under the **Association History** section.

You can filter most columns by clicking , and you can filter the messages after you enter a text into the **Search** field, as shown in Figure 230.

To change the historical data retention period, go to **AMP Setup > General** and update the **Device Events (Syslog, Traps)** field.

Using the Event Log

The system event log lets you troubleshoot recent AirWave events, such as APs coming up and down, services restarting, and most AirWave-related errors.

AirWave also audits activity committed by the Web or CLI so that you can analyze when a particular change might have occurred, especially for a shared system that multiple people can access.

In Figure 231, the system even log shows that AirWave audited the web session initiated by the admin user and ended the web session because of inactivity.

Figure 231: ***System > Event Log***

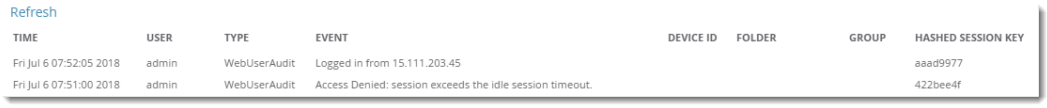


Table 118 describes the page components.

Table 118: *Event Log Fields*

Column	Description
Time	Date and time of the event.
User	The AirWave user that triggered the event. When 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 76 for more info.) • **Alert**—If a trigger is configured to report to the log, an **Alert** type event will be logged here. • **WebUserAudit**—Logging of actions performed from the AMP web interface. • **CLIUserAudit**—Logging of actions performed from the AMP CLI menu interface.
Event	The event that 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.
Hashed Session Key	Displays a partial of hash of the randomly generated key used for secure connections to help identify the session since users can have multiple sessions. **NOTE:** You can restrict the session from **AMP Setup > Authentication**.

Creating New Triggers

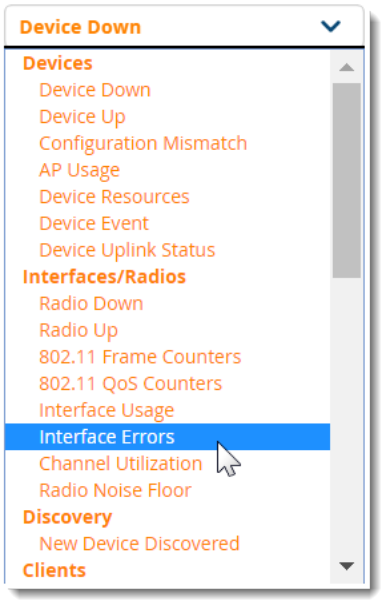
AirWave monitors key aspects of your network performance. When certain conditions or parameters arise that are outside of normal bounds, AirWave triggers alerts that enable you to address problems, often before users have a chance to report them.

To create a trigger:

1. Navigate to **System > Triggers**, then click **Add**.

2. Select the type of trigger from the drop down menu.

Figure 232: *Selecting the Type of Trigger*



3. Select the severity level.
4. Select whether AirWave matches all or any trigger conditions, then click **Add**. In many cases, you must configure at least one condition setting. For more information about trigger conditions, see "Types of Triggers" on page 309.
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 AirWave.
   - CEF Syslog Notification Options. This option allows AirWave to send alerts in CEF format when an external syslog destination is set up with CEF enabled.
   - 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 310

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 119

For more information on creating a device trigger for hardware errors, see "Triggers for hardware monitoring" on page 311. For more information on creating a device trigger for controller clusters, see "Triggers for Controller Cluster Monitoring" on page 312

Table 119: *Device Triggers*

Name	Description and Conditions
Device Down	Indicates when an authorized, monitored AP doesn't respond to SNMP queries from AirWave. When adding device down conditions, use the **Option**, **Condition**, and **Value** drop-down menus. You can configure this trigger to send alerts for thin APs when the controller is down; this behavior is turned off by default. Use the **Minutes Down** condition to compare the amount of time an AP has been down to the value set in minutes for the condition. Use the **Limit by number of down events** to set how many times the device goes up and down within a specified amount of time. AirWave will display this count in the Device Down alert.
Device Up	Indicates when an authorized, previously down AP responds to SNMP queries.
Configuration Mismatch	Indicates that the configuration on the AP does not match the defined **Group** configuration policy.
AP Usage	Indicates the total bandwidth through the device exceeds a predefined threshold for more than a specified period (for example, more than 1500 Kbps in more than 120 seconds). You can also select bandwidth direction and page or 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**. This bandwidth is monitored on the device itself, not on the network as a whole. Choose **In**, **Out**, or **Combined**. • **Severity**. Specifies the severity type for the trigger. • **Duration**. Specifies the time frame for the trigger.
Device Resources	Indicates that the CPU or memory utilization for a router or switch has exceeded a defined percentage for a specified period of time.

Table 119: *Device Triggers (Continued)*

Name	Description and Conditions
Device Event	Sends alerts based on SNMP traps and syslog messages, which are displayed in **System > Syslogs & Traps**, **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 or Failover AirWaves, 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 311
Device Uplink Status	Deploys whenever a RAP's active uplink changes from Ethernet to USB or vice versa. The corresponding events are captured in a RAP's **Devices > Monitor** page.
AP Uplink Speed	Indicates an uplink speed change in the interface. When you enable this option, you can configure a condition for different speeds on the **Uplink speed** option.
Controller Cluster Trigger	This trigger informs you when the controllers present in the cluster are reaching AP capacity, client capacity, and how much bandwidth usage (total traffic in and out) is reaching the threshold. For help creating these triggers, see "Triggers for Controller Cluster Monitoring" on page 312.

Triggers for hardware monitoring

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

To create a trigger for device hardware failures:

1. Navigate to the **System > Triggers** page, then select Device Event for the trigger type.
2. Select the event severity: Normal, Warning, Minor, Major, or Critical.
3. Click **Add** to create the trigger conditions shown in Figure 233.

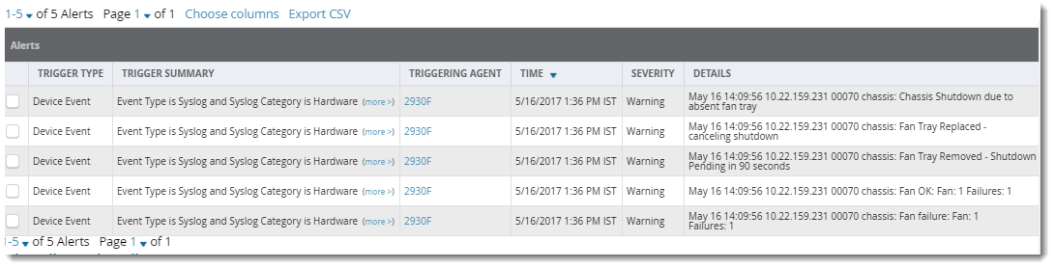
Figure 233: *Example Hardware Monitoring Trigger Conditions*

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 234.

Figure 234: *Hardware Triggers*



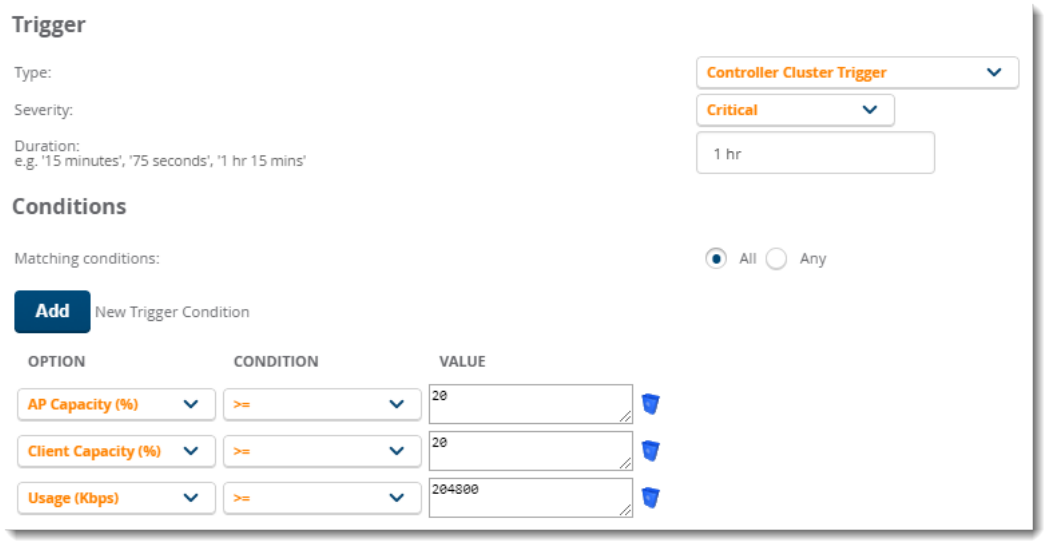
Triggers for Controller Cluster Monitoring

You can set critical thresholds to inform you of when maximum throughput or AP and client capacities are being reached.

To create a trigger for controller clusters:

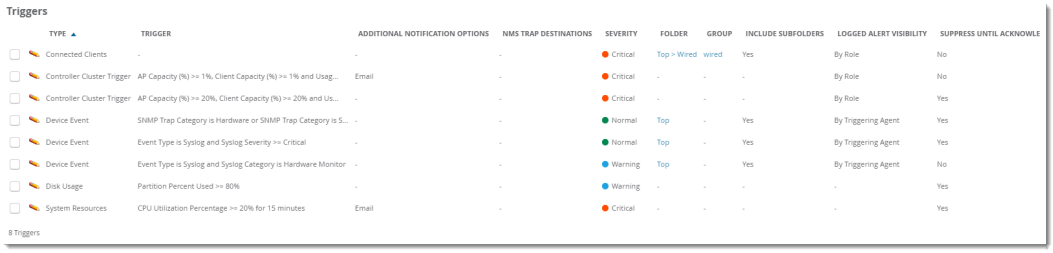
1. Navigate to the **System > Triggers** page, then create trigger as a device event.
2. Select the event severity: Normal, Warning, Minor, Major, or Critical.
3. Click **Add** to create trigger conditions as shown in Figure 235.

Figure 235: *Example Controller Cluster Trigger Conditions*



4. Click **Add** to save the trigger. The controller cluster trigger displays in the Triggers table, as shown in Figure 236.

Figure 236: ***Controller Cluster Trigger***



Interfaces and Radios 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 120.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 120: *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. You must set the condition with radio capability and value.
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 313.
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.
Channel Change	Indicates when the radio channel has changed on the AP within one day.

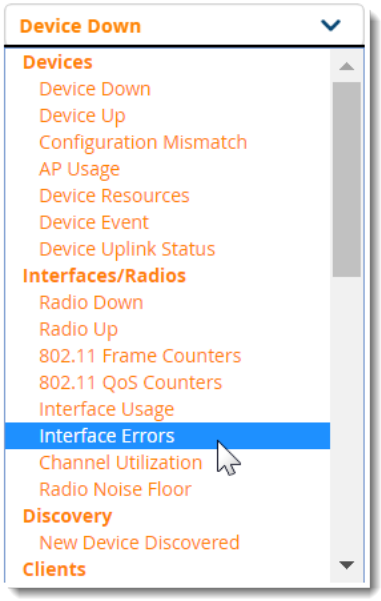
Triggers for Interface Errors

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

To create a trigger for interface errors:

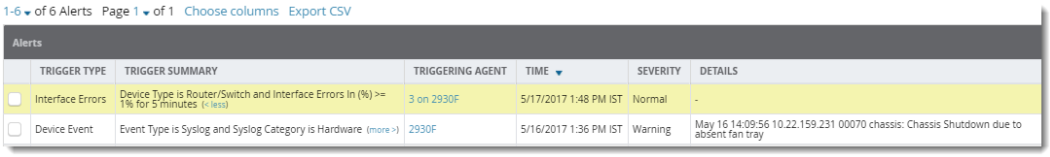
1. Navigate to **System > Triggers**, select **Interface Errors** from the list, as shown in Figure 237.

Figure 237: *Selecting the Interface Error Trigger*



2. Apply match conditions. Figure 238 shows an alert for a switch interface that is showing 1% or more input errors for 5 minutes.

Figure 238: *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 121 describes the trigger.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 121: *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 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 122.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 122: *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).
Inactive Tag	This trigger type flags events in which an RFID tag has not been reported back to 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).

Table 122: *Client Triggers (Continued)*

Name	Description and Conditions
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 123.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 123: *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.

RADIUS Accounting Triggers

To set a trigger for RADIUS accounting issues, click the **Type** drop-down list on the **System > Triggers > Add** page and select one of the RADIUS accounting triggers described in Table 124.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 124: *RADIUS Authentication Triggers*

Name	Description and Conditions
Client RADIUS Accounting 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 accounting issues per client that will trigger an issue.
Device RADIUS Accounting 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 accounting issues per device that will trigger an issue.
Total RADIUS Accounting 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 125.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 125: *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.
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" on page 415 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 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 126.

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Table 126: *Health Triggers*

Name	Description and Conditions
Disk Usage	This trigger type is based on the disk usage of AirWave. This type of trigger indicates that disk usage for the 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 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**.

Triggers for GRE Tunnels

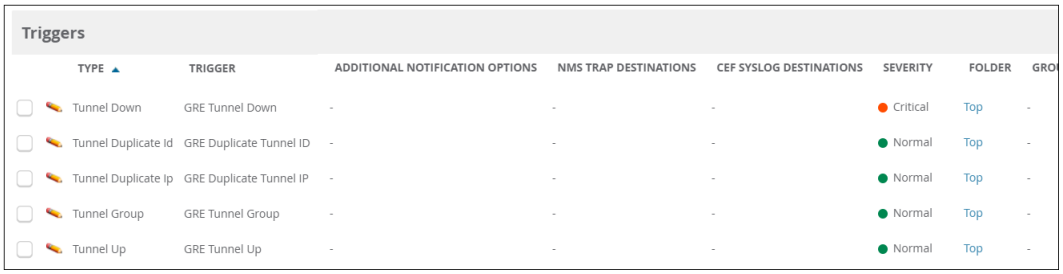
GRE tunnel triggers inform you of changes in the state, or availability of tunnels, and when tunnels have the same IP address or tunnel ID.

You can create a trigger condition by configuring the following match criteria:

- **Option**: **AP name** is the only option for this setting
- **Condition**. Available options are **in**, **not in, is**, or **is not** in the tunnel.
- **Value**: Enter a value in this field

For more information on creating a new trigger, see "Creating New Triggers" on page 308.

Figure 239: *GRE tunnel triggers*



The following table describes the available GRE tunnel triggers and condition settings.

Table 127: *GRE Tunnel Triggers*

Name	Description
Tunnel Up	Alert will raise if a GRE tunnel comes **Up** (both administratively and operationally) from a **Down** state.
Tunnel Down	Alert will raise if a GRE tunnel goes **Down** (both administratively and operationally) from a **Up** state.
Tunnel Group	Alert will raise if any of the tunnel is not part of tunnel group.
Duplicate ID	Alert will raise if same tunnel ID is configured across any of the controllers.
Duplicate IP	Alert will raise if the same IP address configured between GRE Tunnels across any of the controllers, for example, if the same L3 tunnel IP is configured.

Triggers for Clarity

To set a trigger for Clarity issues, click the **Type** drop-down list on the **System > Triggers > Add** page, and select one of the triggers described in Table 128.

For more information on creating a new trigger, see "Creating New Triggers" on page 1.

Table 128: *Clarity Triggers*

Name	Description and Conditions
Authentication Time	Generates an alert if the authentication time matches the condition on the AP, client, or authentication server and authentication type (for example, IEEE 802.1X (dot1x), captive portal, and MAC address).
DHCP Response Time	Generates an alert if the DHCP response time matches the condition on the client or DHCP server.

Viewing Triggers

AirWave shows defined system triggers on the **System > Triggers** page, as shown in Figure 240. If triggers for roles are configured, AirWave lists them in a separate table at the bottom of the page. Click any of the column headings in this table to sort the data.

Figure 240: *Triggers*

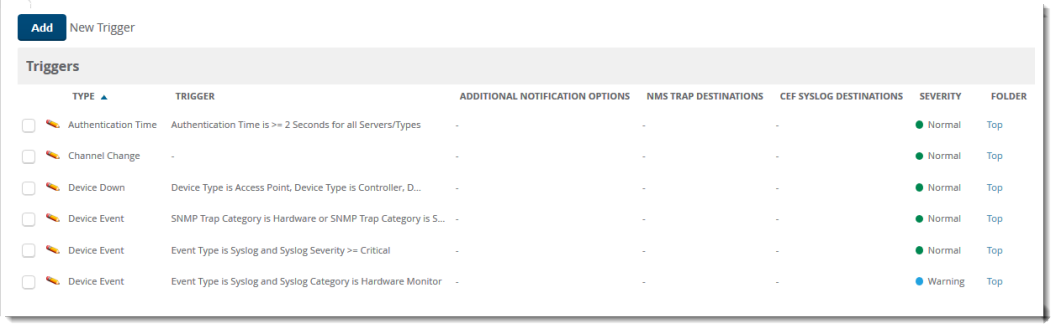


Table 129 describes the fields on the **System > Triggers** page.

Table 129: *Triggers Fields and Descriptions*

Field	Description
Type	The trigger type. For more information, see "Types of Triggers" on page 309.
Trigger	The trigger condition that generated the alert.
Additional Notification Options	If a notification option is configured, AirWave indicates that the alert will be distributed by email, to a network management system (NMS), or both.
NMS Trap Destinations	The NMS server where AirWave sends the trigger. Configure NMS trap destinations on the **AMP Setup >NMS** page. **NOTE:** This option is only available if an NMS server has been added to AirWave. For more information, see "Integrating NMS Servers" on page 76.
CEF Syslog Destinations	The external syslog destination where sends alerts in CEF format. **NOTE:** This option is available when CEF syslog notification is enabled. For more information, see "External Logging Settings" on page 27.
Severity	The severity level assigned to the trigger.
Folder	If the trigger applies only to devices in a folder, AirWave provides a link to the folder. **NOTE:** If the trigger is restricted by folder and group, the trigger applies to devices in the group and in the folder.
Group	If the trigger applies only to devices in a group, AirWave provides a link to the group. **NOTE:** If the trigger is restricted by folder and group, the trigger applies to devices in the group and in the folder.
Include Subfolders	If the trigger applies only to devices in a folder and all of its subfolders, AirWave displays **Yes**.
Logged Alert Visibility	AirWave displays whether the trigger is distributed by triggering agent, or by the associated role.
Suppress Until Acknowledged	AirWave displays how it handles the trigger: • **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.

About Alerts

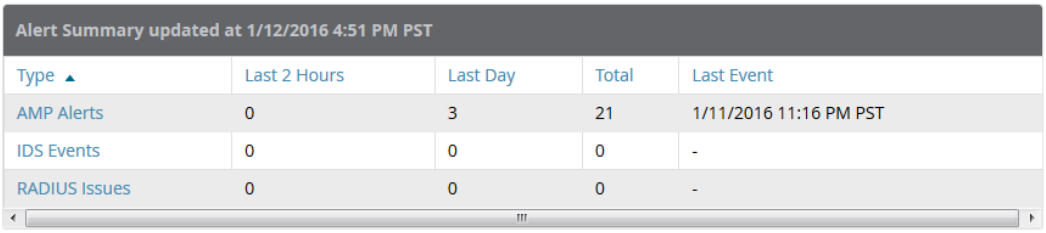
AirWave displays summary information about alerts, including the alert type and how many times an event occurred over the past 2 hours and the last 24 hours. For more information about alerts, see "Viewing System Alerts" on page 321.

You can view the Alert table from the following WebUI pages:

- **Devices > List**
- **Devices > Monitor**
- **Groups > Monitor**
- **Home > Overview**
- **Clients > Connected or Client Detail**
- **System > Alerts**

When you click the hyperlinks in the **Type** column, a detailed view for the selected type of alert opens.

Figure 241: *Alert Summary*



Alert Summary updated at 1/12/2016 4:51 PM PST

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	3	21	1/11/2016 11:16 PM PST
IDS Events	0	0	0	-
RADIUS Issues	0	0	0	-

Information about **AMP Alerts** include:

- 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

Information about **IDS Events** include:

- 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

Information about **RADIUS Accounting Issues** and **RADIUS Authentication Issues** include:

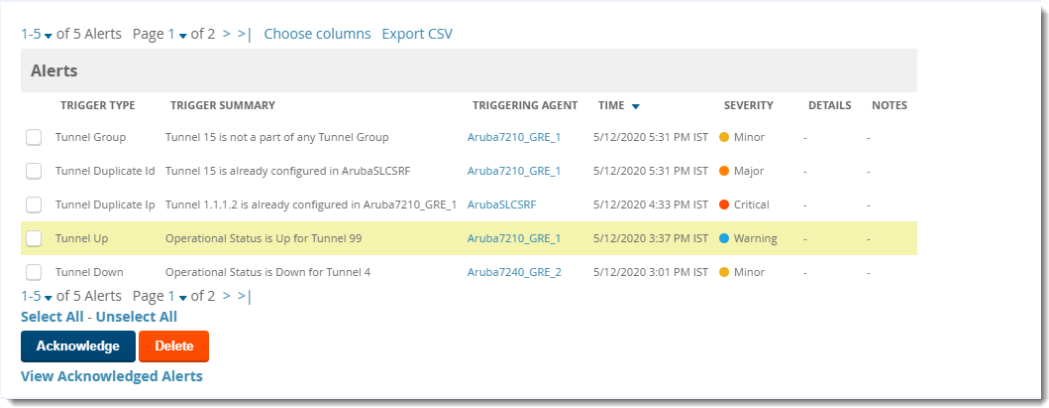
- Event: Name of the RADIUS event
- Username: user name of the device that triggered the event
- Client MAC Address: MAC address of the client that triggered the event
- Client IP address: IP address of the client that triggered the event
- AP/Device: AP or device to which the client is associated
- 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

The top header of each AirWave WebUI page provides direct links to alerts and severe alerts. You can also navigate to **System > Alerts** to view these alerts and acknowledge or delete them. You can identify alerts by color-coded icons. For example, alerts with high severity are red and warnings are blue. For information about setting the severe alert threshold, see "Setting Severe Alert Warning Behavior" on page 304.

Figure 242: *Example of GRE Tunnel Alerts*



The **System > Alerts** page displays the information described in Table 130.

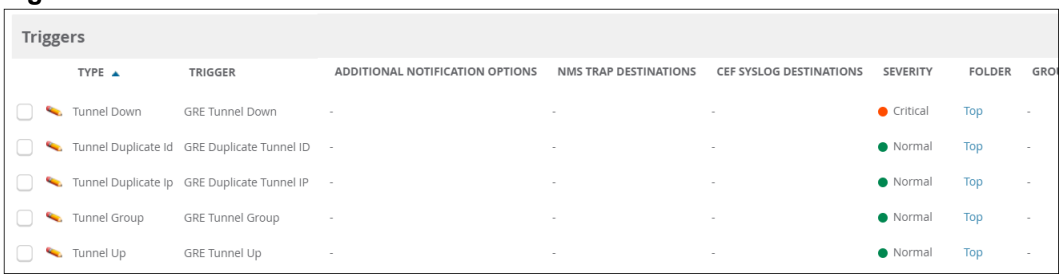
Table 130: *System > Alerts Fields and Default Settings*

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	Displays the name of the device that generated the trigger. Click the hyperlink to open the **Devices > Monitor** page for that device.
Time	Displays the date and time the trigger was generated.
Severity	Displays the severity code associated with that trigger
Details	Displays additional details for alerts.
Notes	Displays any notes that you have added.

Viewing Details

When you click the triggering agent hyperlink for a GRE Tunnel alert, AirWave displays GRE Tunnel Details in a table at the bottom of the controller monitoring page, as shown in Figure 243.

Figure 243: *GRE Tunnel Details*



Delivering Triggered Alerts

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 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

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**.

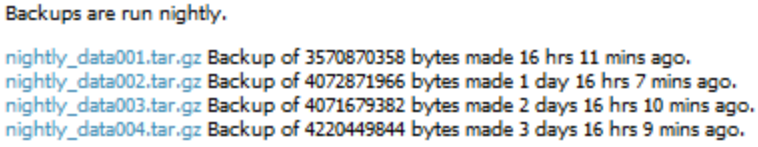
Although AirWave only keeps the last four sets of archives, the archives can be downloaded manually or automatically off-site for more extensive backup strategies. AirWave creates one data backup file each night. The data backup file contains all of the device and group information as well as historical data and system files, including IP address, NTP information, mail relay hosts, and other AirWave settings.

For information about running a backup and restoring from a backup, see "AMP Command Line Interface" on page 439.

Viewing and Downloading Backups

To view current AirWave backup files, go to the **System > Backups** page. Figure 244 illustrates this page.

Figure 244: ***System > Backups*** *Page Illustration*



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 AirWave data and save the file as nightly_data00[1-4].tar.gz. In previous AirWave versions, the scripts created both config backup and data backup files. In order to restore the AirWave data, it is only necessary to have most recent data backup file, and AirWave no longer uses or supports the config backup file, effective as of AirWave 6.3.2.

Using the System > Configuration Change Jobs Page

Schedule configuration change jobs are summarized in the **Scheduled Events** table on the **System > Configuration Change Jobs** page, illustrated in Figure 245. Select a device 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 **Devices > List** page for that folder.

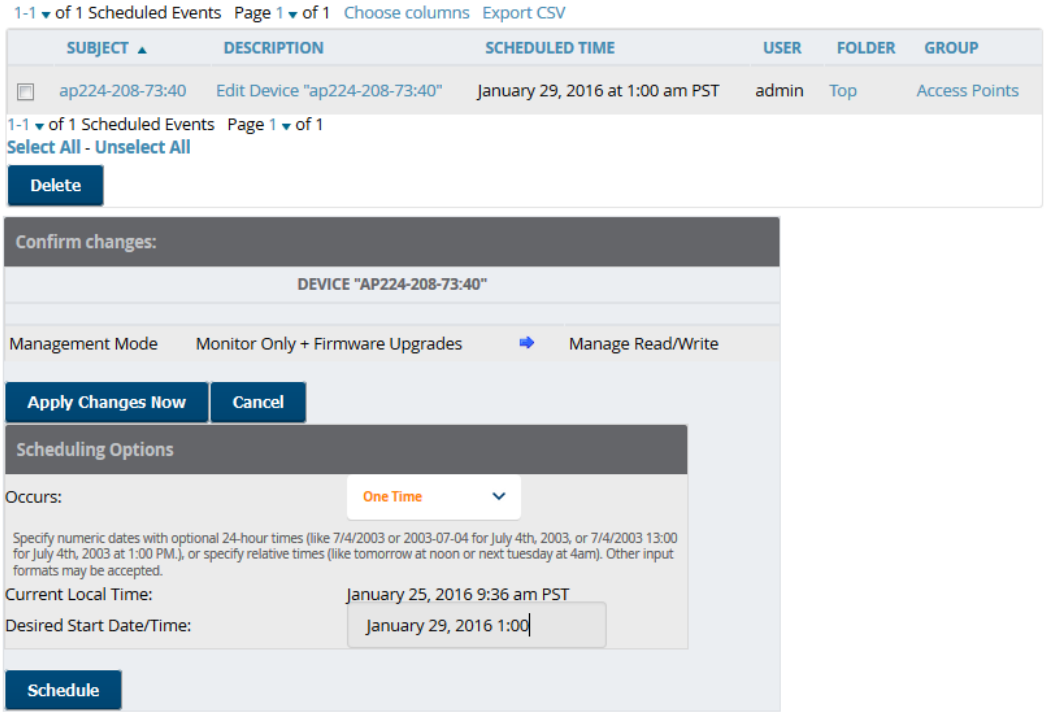
To edit an existing configuration change job:

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 device 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 folder or group page of the device.
4. Scheduled configuration change jobs will also appear on the **Manage** page for a deviceor the **Monitoring** page for a group.

Figure 245: *System > Configuration Change Jobs and System > Configuration Change Jobs Detail*



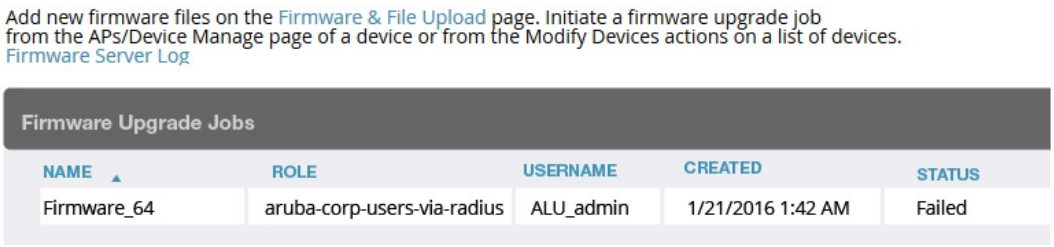
Using the System > Firmware Upgrade Jobs Page

The **System > Firmware Upgrade Jobs** page displays a list of recent firmware upgrade jobs that have been initiated in the **Devices > Manage** page or **Modify Devices** page for a controller or autonomous AP that supports firmware upgrades in 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 246: *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 **Devices > Monitor** page, or the link under **Firmware File** column to go to the **Device Setup > Upload Firmware & Files** page.

Refer also to "Uploading Firmware and Files" on page 57.

Viewing DRT Upgrade Jobs

View information about your DRT upgrade jobs from the **System > DRT Upgrade** page.

Figure 247: *DRT Upgrade Page*

From the DRT Upgrade page, you can also:

- Add a new DRT file by clicking the blue **Upload Firmware & Files** link. to upload a DRT file. Refer to "Uploading Firmware and Files" on page 57.
- Review system status messages by clicking the blue **DRT server log** link to open the Firmware Server log.

Using the System > Performance Page

The **System > Performance** page displays basic AirWave hardware information as well as resource usage over time. 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 AirWave over time.

The page is divided into the following sections:

- System Information
- Performance Graphs
- AMON Statistics
- Redis Statistics
- Database Statistics
- Disk Space

Figure 248 illustrates this page, and Table 131 describes fields and information displayed.

Figure 248: *System > Performance Page Illustration (Partial Screen)*

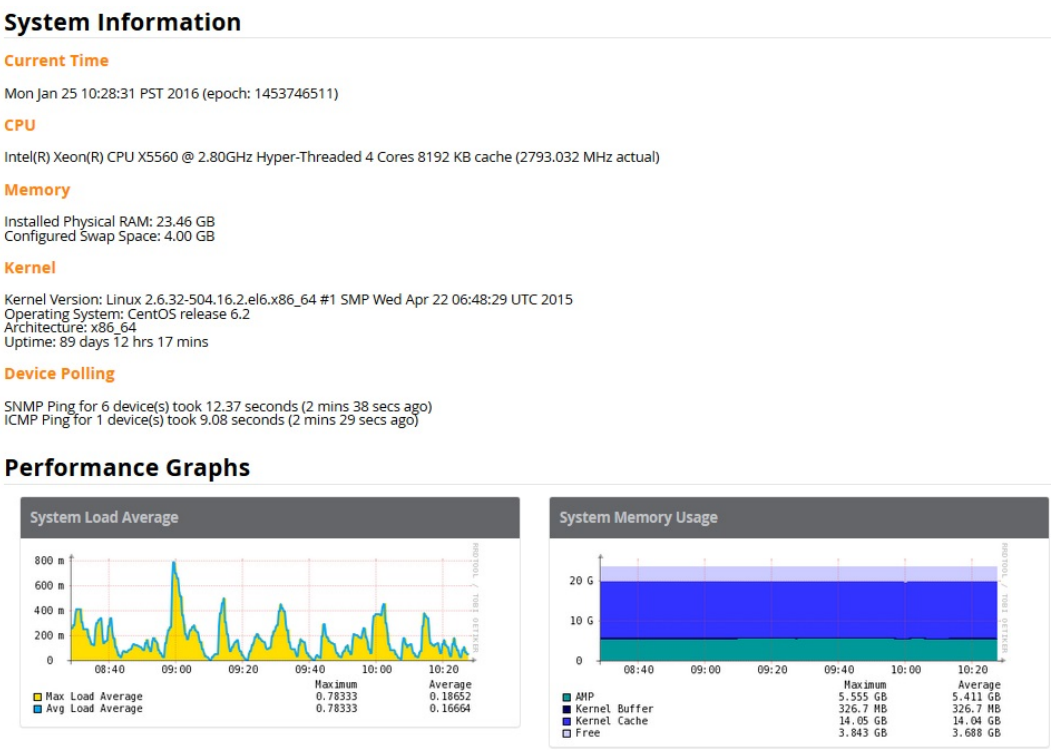


Table 131: *System > Performance Page Fields and Graphs*

Field	Description
System Information	
Current Time	Displays the current time on the AirWave server.
CPU(s)	Basic CPU information as reported by the operating system.
Memory	The amount of physical RAM and Swap space seen by the operating system. Refer to the *AirWave Server Sizing Guide* for hardware requirements.
Kernel	The version of the Linux kernel running on the box.
Device Polling	Displays some AP/Device polling statistics.
Performance Graphs	
System Load Average	The number of jobs currently waiting to be processed. Load is a rough metric that will tell you how busy a server is. A typical 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 AirWave becoming unusable. To lower the load average, try increasing a few polling periods in the **Groups > Basic** page.

Table 131: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
System Memory Usage	The amount of RAM that is currently used broken down by usage. It is normal for 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 Swap Usage	The amount of Swap memory used by AirWave. Swap is used when there is no more free physical RAM. A large performance penalty is paid when swap is used. If your AirWave consistently uses swap, you should consider installing additional RAM.
System Disk Throughput	The rate of reading and writing from and to the disk in bytes per second.
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, 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 (AirWave services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (AirWave, VisualRF and web server).
CPU Utilization by Worker/by Service	Displays reads and writes for workers (AirWave services, database, VisualRF, web server, RRD tool and AWRRD tool) and for services (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).
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).
Syslog	Displays the incoming Syslog packets on the AMP.
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.

Table 131: *System > Performance Page Fields and Graphs (Continued)*

Field	Description
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 Aruba 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 Aruba 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 Aruba 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 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 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	
Disk Space	Pie charts that display the amount of used and free hard drive space for each partition. If a drive reaches over 80% full, you may want to lower the **Historical Data Retention** settings on the **AMP Setup > General** page or consider additional drive space.

There are several initial steps that you can take to troubleshoot AirWave performance problems, including slow page loads and timeout errors. Initial troubleshooting steps would include the following:

- Increasing the polling period settings on the **Groups > Basic** page.
- Increasing the polling period time for groups with routers and switches.
- Adding additional memory to the server. Please consult the sizing information in the latest edition of the *AirWave Server Sizing Guide* or contact Aruba support for the latest recommendations.

Reports in 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

AirWave includes default reports that contain one or more sections of data, (also called widgets). The most commonly used reports are the Aruba License, Device Summary, Inventory, Client Details, Traffic Analysis, and RF Health reports . You can also create a custom report by combining individual widgets from multiple report types. The default report definitions become available after you have applied a license key.

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 331.

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 Custom Reports" on page 364 and "Cloning Reports" on page 365.

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 331.

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 332.
- 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 346.
- 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 347.
- 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 352.
- 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 356.
- 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 272.

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 334.
- 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 336.
- 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 338.
- 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 339.
- 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 AirWave only generates the report during a planned maintenance period or business days. For information, see "Using the Device Uptime Report" on page 341.
- 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 344.
- 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 360.

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 361.

Troubleshoot Device and Network Issues

- IDS Events. Use this report to respond to IDS events on the network involving APs or controller devices. 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 342.
- 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 346.
- New Clients. Use this report to see new clients that 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 349.
- New Rogue Devices. Use this report to find rogues device on your network. Before AirWave can run the report, you must define the restrictions. For information, see "Using the New Rogue Devices Report" on page 350.
- 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 354.

- 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 355.
- 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 358.
- 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 363.

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 132 describes each column for the **Reports > Generated** page.

Table 132: *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

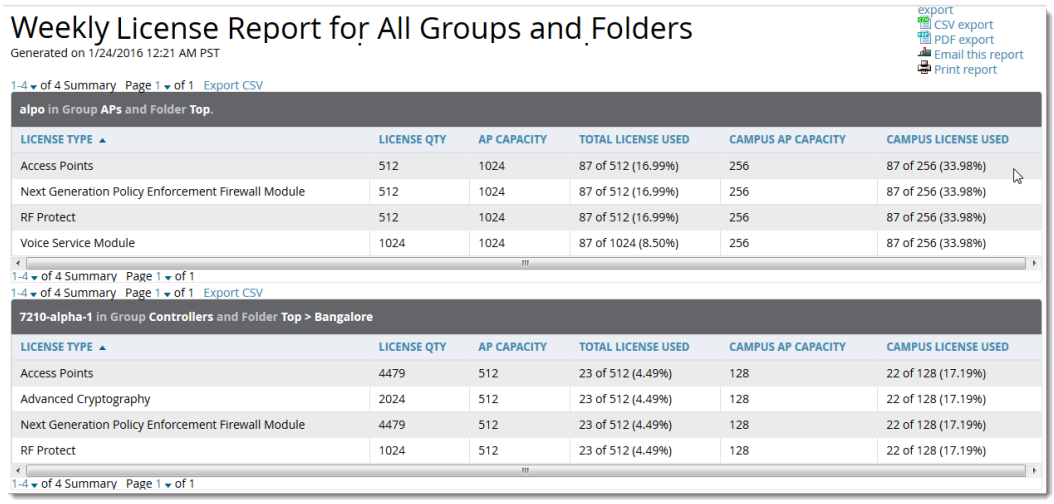
This section describes the default reports in AirWave that run daily. You can access these reports from the **Reports > Generated** page. If you need to customize a report, see "Creating Custom Reports" on page 364.

Using the License Report

The Aruba License Report tracks licenses on Aruba devices in your network. This report includes information on the type, quantity, percent used, installation date, expiration date, and the license keys.

This report includes the built-in license count only when the installed license count is less than the license limits.

Figure 249: *Aruba Detail Page*



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 347.

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 250.

Figure 250: *Capacity Planning Report*

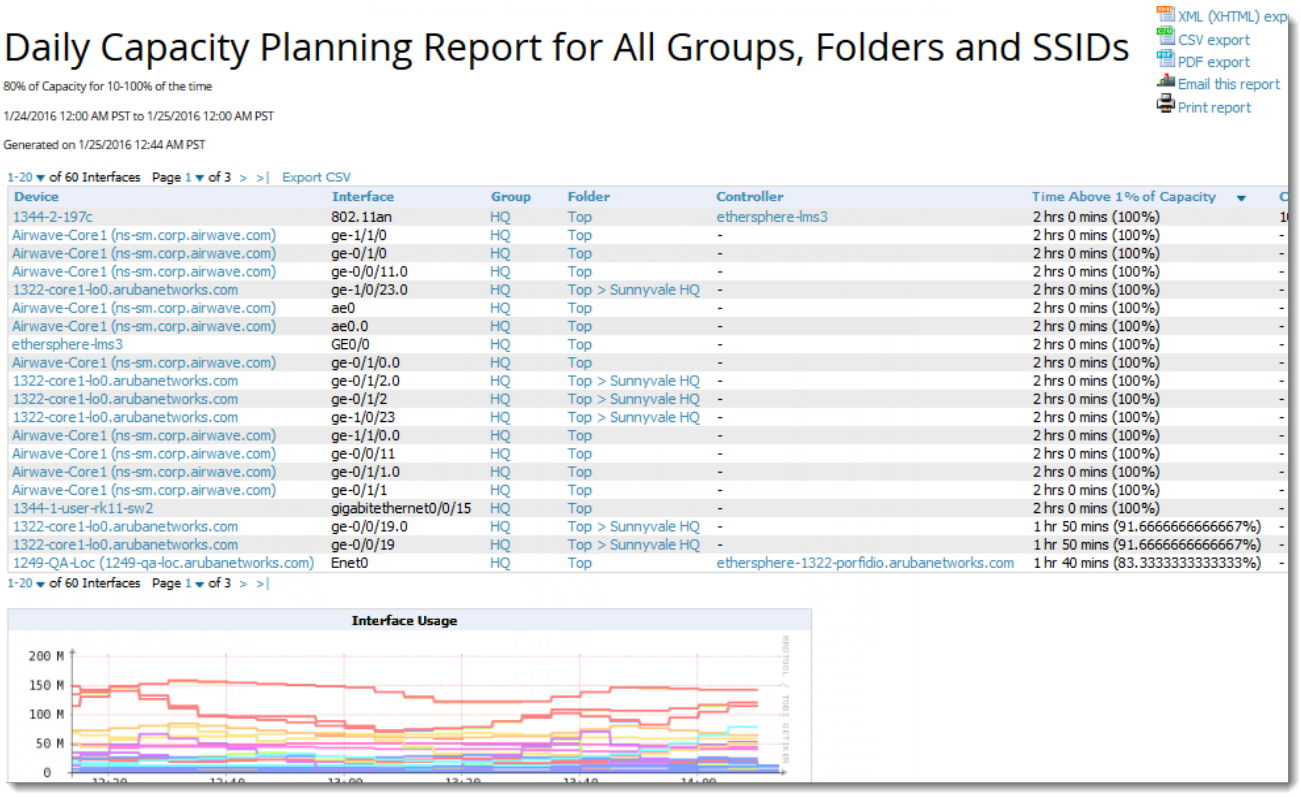


Table 133 describes the fields in the Capacity Planning Report.

Table 133: *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.
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.

Table 133: *Capacity Planning Report Fields and Descriptions (Continued)*

Field	Description
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 Aruba Role
- Last Authentication Type
- Last Connection Mode
- Last SSID
- Network Chipset - All or Matching
- Network Driver - All or Matching
- Network Vendor

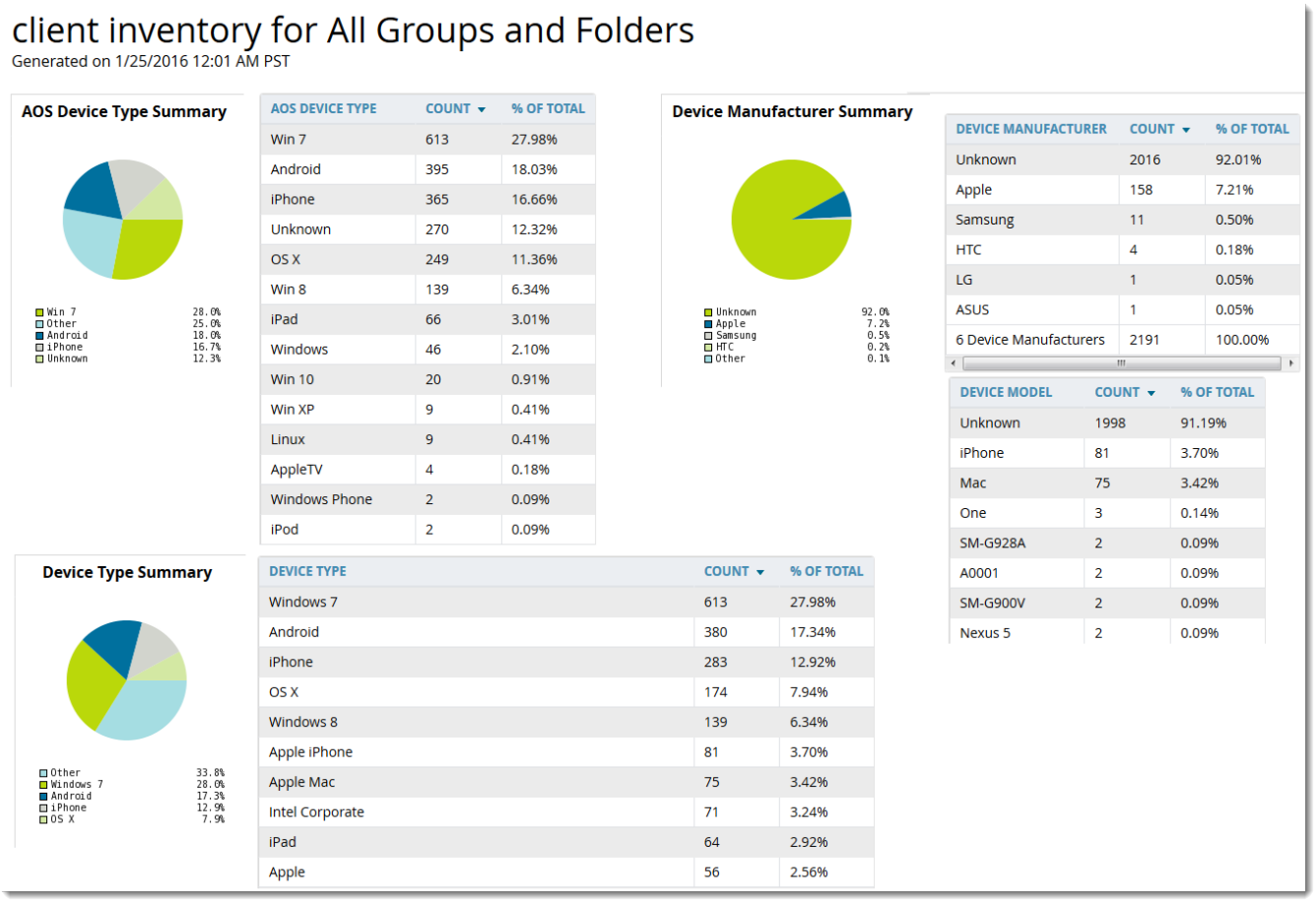
This report allows you to include details about every client, for example, the User Name, MAC Address, Role, AP Radio information, and more. Finally, you can limit this report to include devices that active or inactive at the time when this report is run.

Example 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 251.

Figure 251: *Reports > Generated > Client Inventory (partial)*



The fields on this report are described in Table 134.

Table 134: *Client Inventory Report Fields and Descriptions*

Field	Description
AOS Device Type	Displays the device type or name.

Table 134: *Client Inventory Report Fields and Descriptions (Continued)*

Field	Description
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

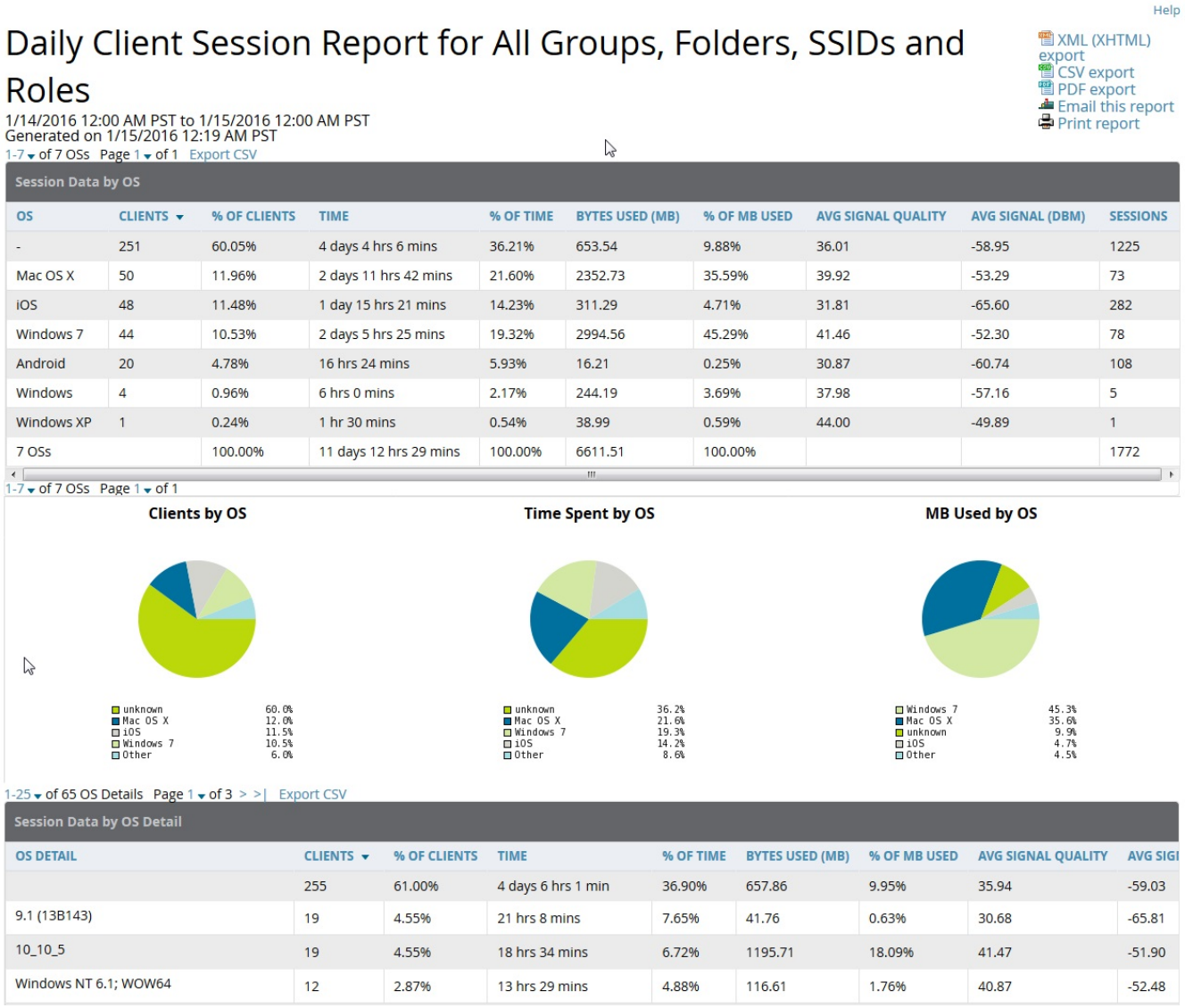
The Client Session Report itemizes user-level activity by session, meaning any instance in which a user connects to the network. In list and chart format, this report displays session information, such as: cipher; connection mode; role; SSID or VLAN ID, top clients by total MB used; device type; asset category and group; EAP supplicant; manufacturer; model; network chipset, driver, and interface vendor; and OS.

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 252: *Client Session Detail*



Each Client Session Report includes a Client Session Summary section. Table 135 describes the fields that display in this summary.

Table 135: *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.

Table 135: *Client Session Summary Fields and Descriptions (Continued)*

Field	Description
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.
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 253 and Table 136 illustrate and describe the general Configuration Audit report and related contents.

Figure 253: *Daily Configuration Audit Report Page, partial view*

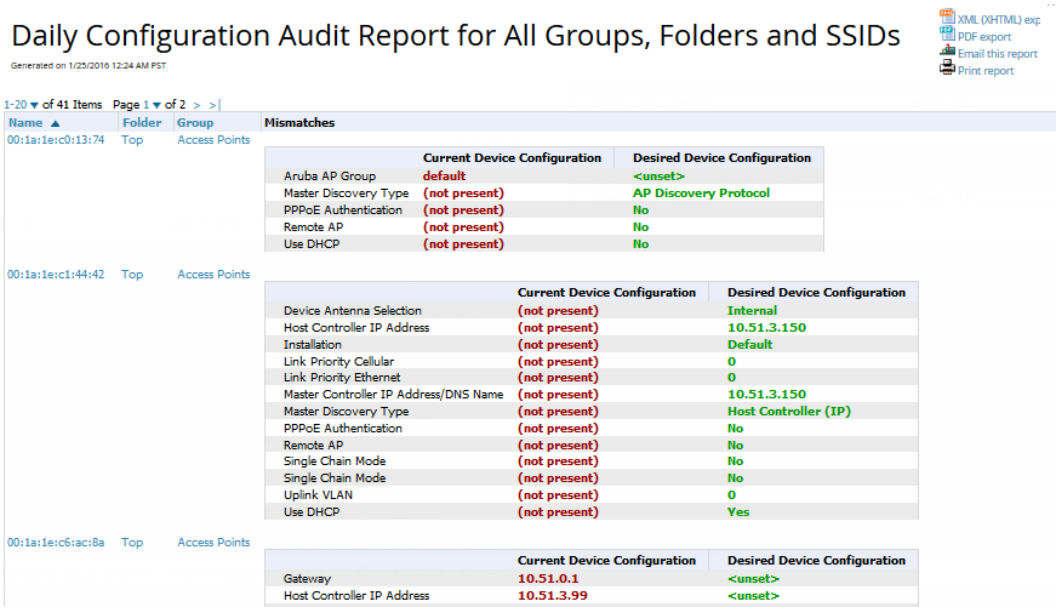


Table 136: *Daily Configuration Audit Report*

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 AirWave. Selecting the folder name in this report displays the **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. One potential use of this report is to establish more equal bandwidth distribution across multiple devices.

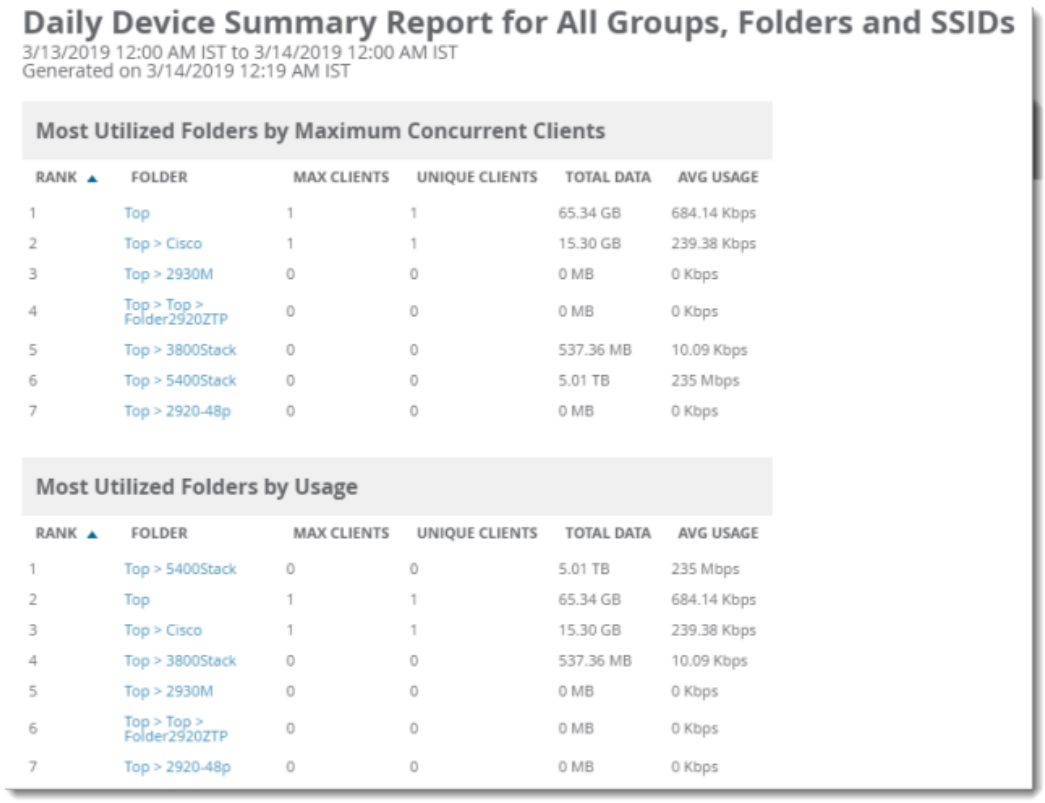
This report contains the following lists:

- **Most Utilized Folders by Maximum Concurrent Clients**—displays the top 10 folders that contain the devices supporting the highest numbers of users.
- **Most Utilized Folders by Usage**—displays the 10 folders that contain the devices that consistently have the highest bandwidth consumption during the reported time period.
- **Most Utilized by Maximum Concurrent Clients**—displays the 10 most used devices, according to the number of users.
- **Most Utilized by Usage**—displays the 10 most used devices, according to the bandwidth throughput.

- **Least Utilized by Maximum Concurrent Clients**—displays the 10 least used devices, according to the number of users.
- **Least Utilized by Usage**—displays the 10 least used devices, according to the bandwidth throughput.

These lists provide links to additional information or configuration pages for each device. Figure 254 shows some of the most used lists in the report.

Figure 254: *Device Summary Report*



Daily Device Summary Report for All Groups, Folders and SSIDs

3/13/2019 12:00 AM IST to 3/14/2019 12:00 AM IST
Generated on 3/14/2019 12:19 AM IST

Most Utilized Folders by Maximum Concurrent Clients

RANK ▲	FOLDER	MAX CLIENTS	UNIQUE CLIENTS	TOTAL DATA	AVG USAGE
1	Top	1	1	65.34 GB	684.14 Kbps
2	Top > Cisco	1	1	15.30 GB	239.38 Kbps
3	Top > 2930M	0	0	0 MB	0 Kbps
4	Top > Top > Folder2920ZTP	0	0	0 MB	0 Kbps
5	Top > 3800Stack	0	0	537.36 MB	10.09 Kbps
6	Top > 5400Stack	0	0	5.01 TB	235 Mbps
7	Top > 2920-48p	0	0	0 MB	0 Kbps

Most Utilized Folders by Usage

RANK ▲	FOLDER	MAX CLIENTS	UNIQUE CLIENTS	TOTAL DATA	AVG USAGE
1	Top > 5400Stack	0	0	5.01 TB	235 Mbps
2	Top	1	1	65.34 GB	684.14 Kbps
3	Top > Cisco	1	1	15.30 GB	239.38 Kbps
4	Top > 3800Stack	0	0	537.36 MB	10.09 Kbps
5	Top > 2930M	0	0	0 MB	0 Kbps
6	Top > Top > Folder2920ZTP	0	0	0 MB	0 Kbps
7	Top > 2920-48p	0	0	0 MB	0 Kbps

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.

Table 137 describes the fields in the report.

Table 137: *Daily Device Summary Report Unique Fields and Descriptions*

Field	Description
Rank	Ranks the device or folder from 1 to 10.

Table 137: *Daily Device Summary Report Unique Fields and Descriptions (Continued)*

Field	Description
Folder	Displays the folder information for the device.
Device	The device name or MAC address.
Max Clients	The highest number of clients that were connected to the device during the reported time period. If a range is not specified, then this value will match the value for Clients.
Unique Clients	The number of clients that were last connected to the device.
Total Data	Displays the total data usage on the device in MB, GB or TB during the reported time period.
Average Usage	Displays the average rate of data sent to the device in Kbps or Mbps during the reported time period.
Location	Displays the location information if available.
Controller	The controller that the device is associated to.
Group	Displays the group information for the device.

Using the Device Uptime Report

The Device Uptime report covers protocol-oriented, device-oriented, or SSID-oriented information. You can use this report to monitor and optimize the network by tracking the bootstrap count, reboot count, uptimes, and downtimes. Or, you can ignore downtime during maintenance periods and run the report on business days by setting the "Restrict to daily time window" and "Include weekends" options in the **Reports > Definitions** page.

These time restrictions are only applicable to Device Uptime reports and not applicable when creating other reports or custom reports.

Figure 255 shows the details from a Daily Device Uptime report.

Figure 255: *Device Uptime Report*

The Device Uptime report lists the following information as percentages by device, AP, controller, or switch, group, and folder:

- **Device Uptime**: The length of time that the device was up.
- **SNMP Comm Uptime**: The percentage of time the device was reachable via ICMP. AirWave polls the device via SNMP at the rate specified on the **Groups > Basic** page.
- **ICMP Comm Uptime**: 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. AirWave only pings the device if SNMP fails and then it pings at the SNMP polling interval rate.
- **HTTPS Comm Uptime**: The percentage of time the device was reachable via HTTPS.
- **Group**: The average device uptime by device group.
- **Folder**: The average device uptime by device folder.

Using the IDS Events Report

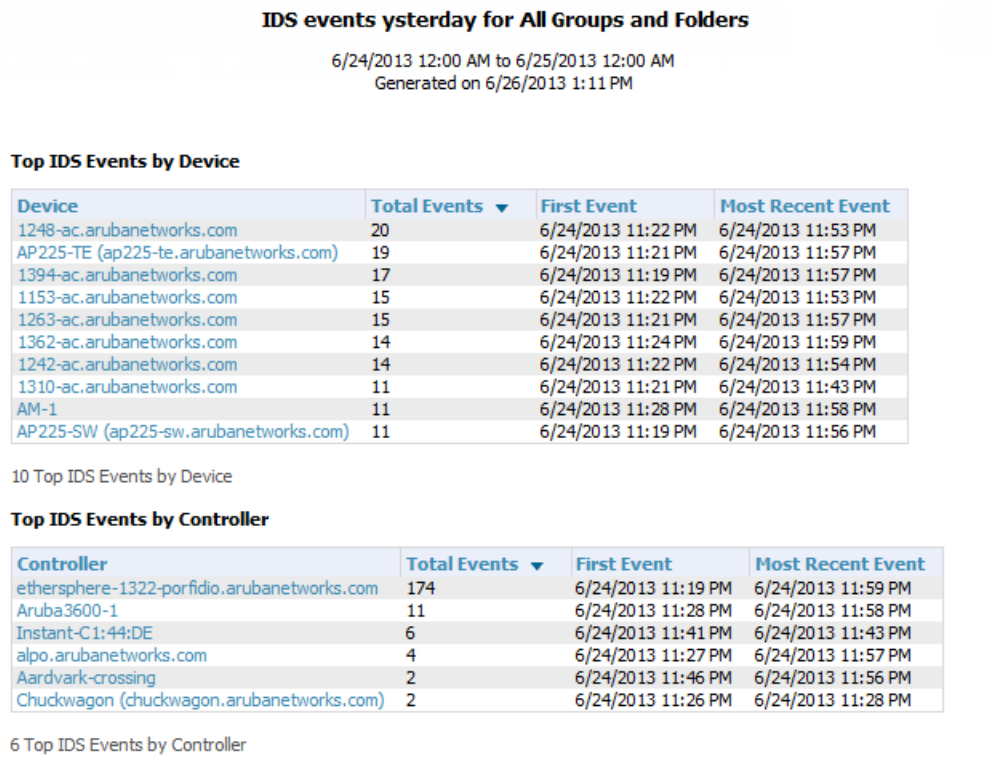
The IDS Events Report lists and tracks IDS events on the network involving APs or controller devices. This report cites the number of IDS events for devices that have experienced the most instances in the prior 24 hours, and provides links to support additional analysis or configuration in response. 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.

Your role must be enabled to view RAPIDS in order to see this report. In addition, this report requires that you enter a start and stop time range.

The **Home > Overview** page also cites IDS events. Triggers can be configured for IDS events. Refer to "Creating New Triggers" on page 308 for additional information.

Figure 256 and Table 138 illustrate and describe the IDS Events Detail report. Selecting the AP device or controller name takes you to the **Devices > List** page.

Figure 256: *IDS Events Report Illustration*



IDS events ysterday for All Groups and Folders

6/24/2013 12:00 AM to 6/25/2013 12:00 AM
Generated on 6/26/2013 1:11 PM

Top IDS Events by Device

Device	Total Events	First Event	Most Recent Event
1248-ac.arubanetworks.com	20	6/24/2013 11:22 PM	6/24/2013 11:53 PM
AP225-TE (ap225-te.arubanetworks.com)	19	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1394-ac.arubanetworks.com	17	6/24/2013 11:19 PM	6/24/2013 11:57 PM
1153-ac.arubanetworks.com	15	6/24/2013 11:22 PM	6/24/2013 11:53 PM
1263-ac.arubanetworks.com	15	6/24/2013 11:21 PM	6/24/2013 11:57 PM
1362-ac.arubanetworks.com	14	6/24/2013 11:24 PM	6/24/2013 11:59 PM
1242-ac.arubanetworks.com	14	6/24/2013 11:22 PM	6/24/2013 11:54 PM
1310-ac.arubanetworks.com	11	6/24/2013 11:21 PM	6/24/2013 11:43 PM
AM-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
AP225-SW (ap225-sw.arubanetworks.com)	11	6/24/2013 11:19 PM	6/24/2013 11:56 PM

10 Top IDS Events by Device

Top IDS Events by Controller

Controller	Total Events	First Event	Most Recent Event
ethersphere-1322-porfidio.arubanetworks.com	174	6/24/2013 11:19 PM	6/24/2013 11:59 PM
Aruba3600-1	11	6/24/2013 11:28 PM	6/24/2013 11:58 PM
Instant-C1:44:DE	6	6/24/2013 11:41 PM	6/24/2013 11:43 PM
alpo.arubanetworks.com	4	6/24/2013 11:27 PM	6/24/2013 11:57 PM
Aardvark-crossing	2	6/24/2013 11:46 PM	6/24/2013 11:56 PM
Chuckwagon (chuckwagon.arubanetworks.com)	2	6/24/2013 11:26 PM	6/24/2013 11:28 PM

6 Top IDS Events by Controller

Table 138: *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 **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.
SNR	Displays the signal-to-noise (SNR) radio associated with the IDS event.
Precedence	Displays precedence information associated with the IDS event, when known.
Time	Displays the time of the IDS event.

Using the Inventory Report

The **Inventory Report** itemizes all devices on the network. The output breaks down this information by vendor, model (including firmware and bootloader), and device type.

Example 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 257.

Figure 257: *Inventory Report*

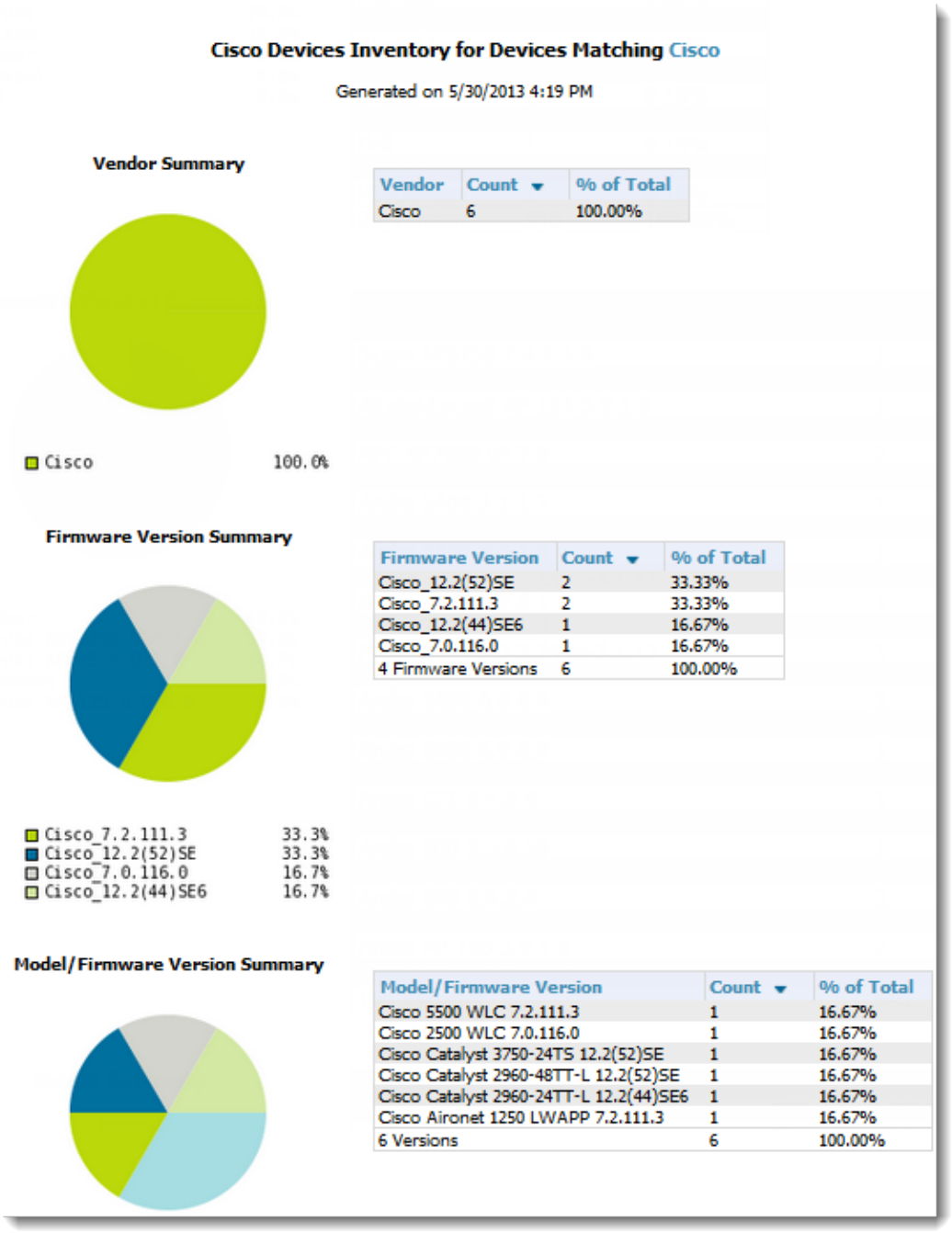


Table 139: *Inventory Report Fields and Descriptions*

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.

Table 139: *Inventory Report Fields and Descriptions (Continued)*

Field	Description
% 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 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 258.

Figure 258: *Example of a Match Event Report*

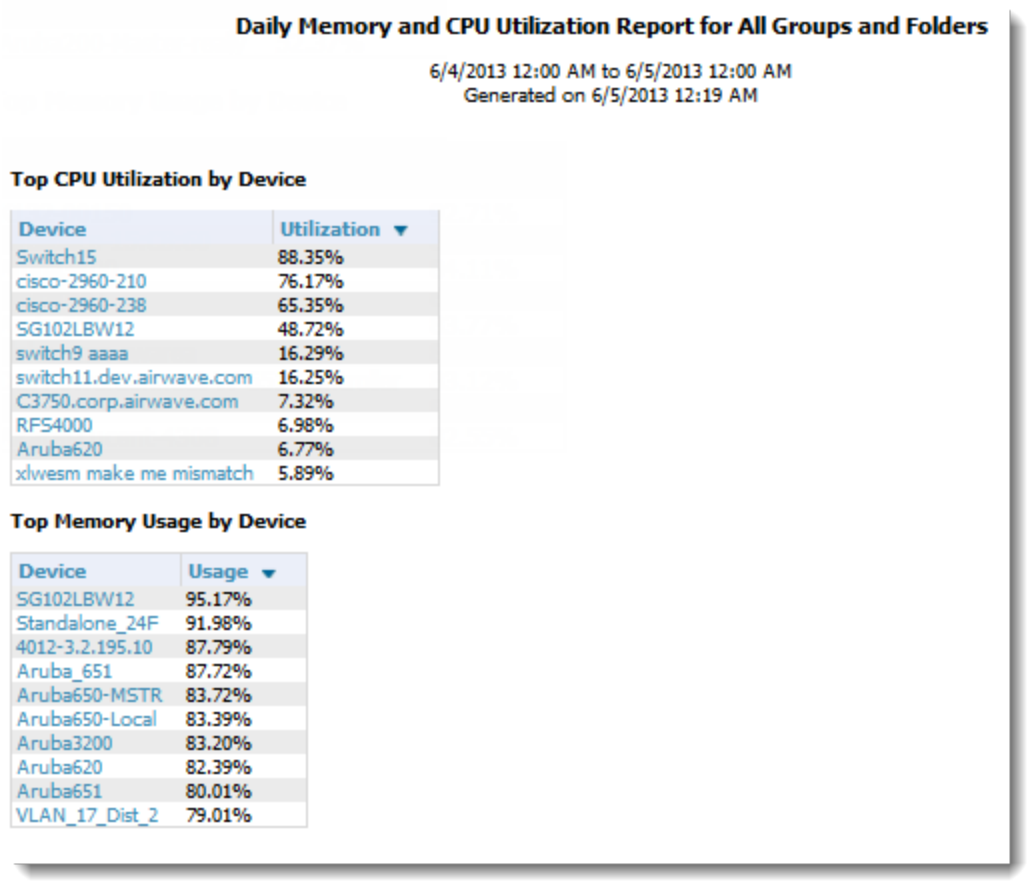
Table 140: *Match Event Report output details*

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 Memory and CPU Utilization Report

The Memory and CPU Utilization report, as shown in Figure 259, 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 259: *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 Figure 260, 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 260: *Network Usage Report*

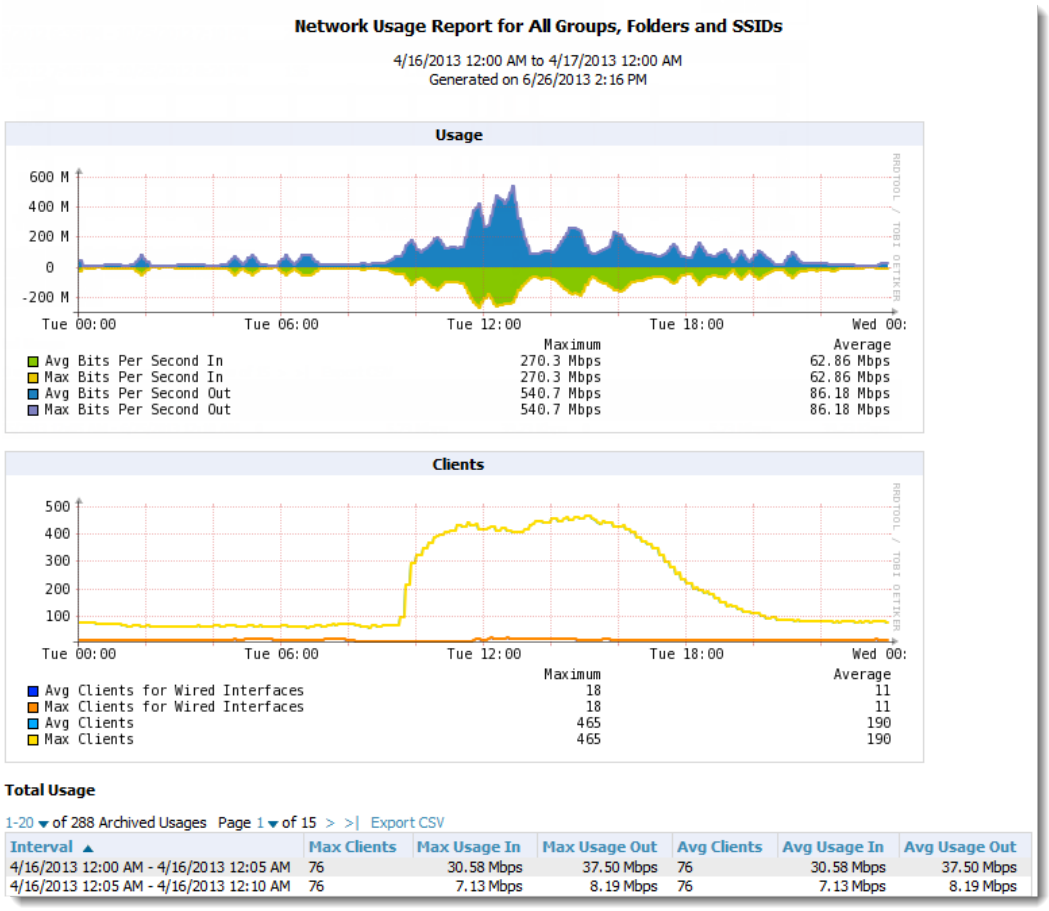


Table 141: *Network Usage Report Fields and Descriptions*

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.

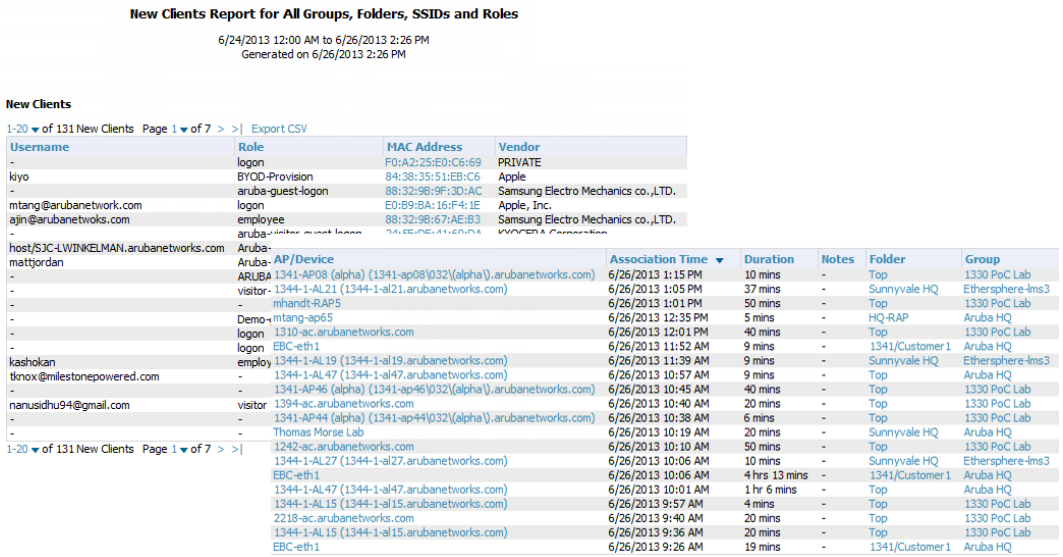
Using the New Clients Report

The New Clients Report lists all new users that have appeared on the network during the time duration defined for the report. This report covers the user identifier, the associated role when known, device information and more. This report gives you the option to filter instead on specific devices and/or users. Whether viewing information for devices or clients, the report can configured to display additional options. For many of these options, you can choose to view all information or a specific set of information (Matching option). If Matching is selected, a text entry field displays. When you put your cursor in the text entry field, an additional side menu displays providing you with a list of available options that you can select.

- SSID - All or Selected
- Aruba Role - All or Selected
- Classification (for possible Rogue devices) - All or Selected
- Device Type - All or Matching
- AOS Device Type - All or Matching
- Manufacturer - All or Matching
- Model - All or Matching
- OS - All or Matching
- OS Detail - All or Matching
- Network Chipset - All or Matching
- Network Driver - All or Matching
- EAP Supplicant - All or Matching
- Asset Group - All or Matching
- Asset Category - All or Matching

Figure 261 illustrates the fields and information in the New Clients Report. The fields that display on this output are described in Table 142.

Figure 261: *New Clients Report Illustration (split view)*



New Clients Report for All Groups, Folders, SSIDs and Roles

6/24/2013 12:00 AM to 6/26/2013 2:26 PM
Generated on 6/26/2013 2:26 PM

New Clients

1-20 of 131 New Clients Page 1 of 7 > >| Export CSV

Username	Role	MAC Address	Vendor
-	logon	F0:A2:25:E0:C6:69	PRIVATE
kiyo	BYOD-Provision	84:38:35:51:EB:C6	Apple
-	aruba-guest-logon	88:32:9B:9F:3D:AC	Samsung Electro Mechanics co.,LTD.
mtang@arubanetwork.com	logon	E0:B9:BA:16:F4:1E	Apple, Inc.
ajin@arubanetwoks.com	employee	88:32:9B:67:AE:B3	Samsung Electro Mechanics co.,LTD.
-	aruba-		
host/SJC-LWINKELMAN.arubanetworks.com	Aruba-		
mattjordan	Aruba-		
-	ARUBA		
-	visitor-		
-	-		
-	Demo-		
-	logon		
-	logon		
kashokan	employ		
tknox@milestonepowered.com	-		
-	-		
nanusidhu94@gmail.com	visitor		
-	-		
-	-		

1-20 of 131 New Clients Page 1 of 7 > >|

AP/Device	Association Time	Duration	Notes	Folder	Group
1341-AP08 (alpha) (1341-ap08\032\(alpha\).arubanetworks.com)	6/26/2013 1:15 PM	10 mins	-	Top	1330 PoC Lab
1344-1-AL21 (1344-1-al21.arubanetworks.com)	6/26/2013 1:05 PM	37 mins	-	Sunnyvale HQ	Ethersphere-lms3
mhandt-RAP5	6/26/2013 1:01 PM	50 mins	-	Top	1330 PoC Lab
mtang-ap65	6/26/2013 12:35 PM	5 mins	-	HQ-RAP	Aruba HQ
1310-ac.arubanetworks.com	6/26/2013 12:01 PM	40 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 11:52 AM	9 mins	-	1341/Customer 1	Aruba HQ
1344-1-AL19 (1344-1-al19.arubanetworks.com)	6/26/2013 11:39 AM	9 mins	-	Sunnyvale HQ	Ethersphere-lms3
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:57 AM	9 mins	-	Top	Aruba HQ
1341-AP46 (alpha) (1341-ap46\032\(alpha\).arubanetworks.com)	6/26/2013 10:45 AM	40 mins	-	Top	1330 PoC Lab
1394-ac.arubanetworks.com	6/26/2013 10:40 AM	20 mins	-	Top	1330 PoC Lab
1341-AP44 (alpha) (1341-ap44\032\(alpha\).arubanetworks.com)	6/26/2013 10:38 AM	6 mins	-	Top	1330 PoC Lab
Thomas Morse Lab	6/26/2013 10:19 AM	20 mins	-	Sunnyvale HQ	Aruba HQ
1242-ac.arubanetworks.com	6/26/2013 10:10 AM	50 mins	-	Top	1330 PoC Lab
1344-1-AL27 (1344-1-al27.arubanetworks.com)	6/26/2013 10:06 AM	10 mins	-	Sunnyvale HQ	Ethersphere-lms3
EBC-eth1	6/26/2013 10:06 AM	4 hrs 13 mins	-	1341/Customer 1	Aruba HQ
1344-1-AL47 (1344-1-al47.arubanetworks.com)	6/26/2013 10:01 AM	1 hr 6 mins	-	Top	Aruba HQ
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:57 AM	4 mins	-	Top	1330 PoC Lab
2218-ac.arubanetworks.com	6/26/2013 9:40 AM	20 mins	-	Top	1330 PoC Lab
1344-1-AL15 (1344-1-al15.arubanetworks.com)	6/26/2013 9:36 AM	20 mins	-	Top	1330 PoC Lab
EBC-eth1	6/26/2013 9:26 AM	19 mins	-	1341/Customer 1	Aruba HQ

Table 142: *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

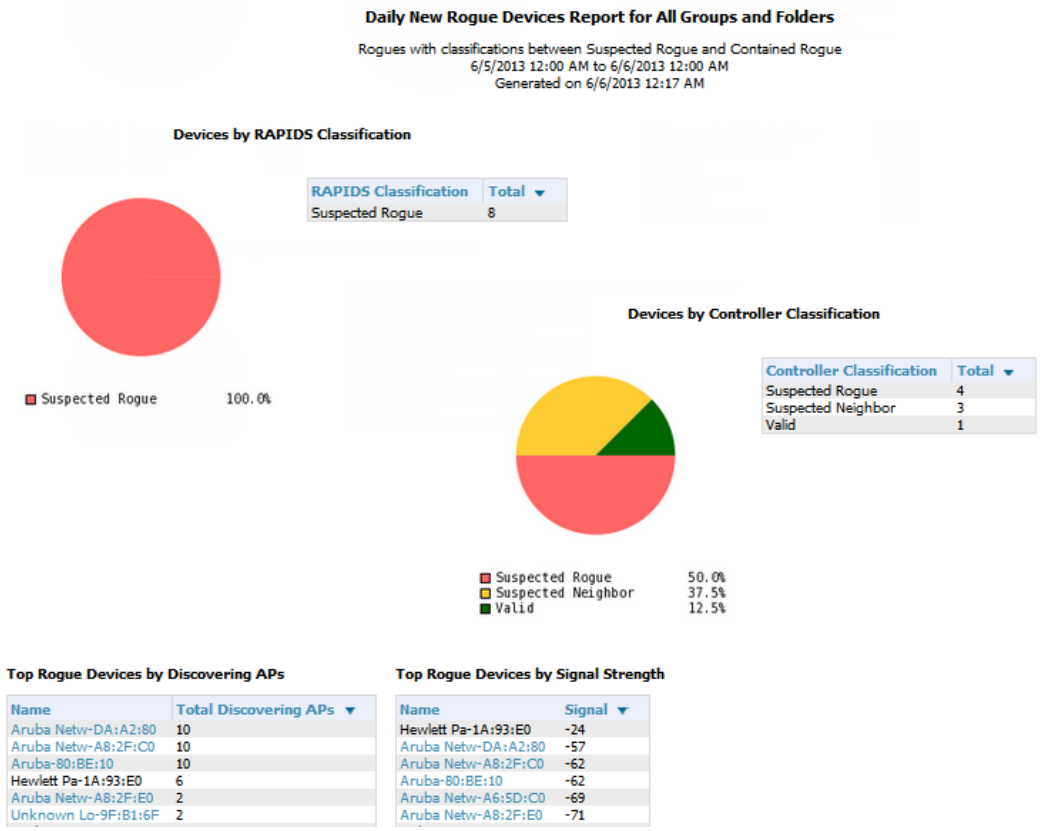
The New Rogue Devices Report summarizes rogue device information including the following categories of information:

- Rogue devices by RAPIDS classification—described in "Using RAPIDS" on page 415
- 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 AirWave pages
- Detailed and text-based table of all rogue devices supporting all discovery methods with extensive device parameters and hyperlink interoperability to additional 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 AirWave pages

This report is not run by default, but is available after you define it.

Refer to Figure 262 for a sample illustration of this report.

Figure 262: *New Rogue Devices Report Illustration (partial view)*



The rogue device inventories that comprise this report contain many fields, described in Table 143.

Table 143: *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" on page 415 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" on page 415 for additional information.
Ack	Indicates whether the device has been acknowledged with the network.
First Discovered	Displays the date and time that the rogue device was first discovered on the network.
First Discovery Method	Displays the method by which the rogue device was discovered.
First Discovery Agent	Displays the network device that first discovered the rogue device.
Last Discovering AP	Displays the network device that most recently discovered the rogue device.

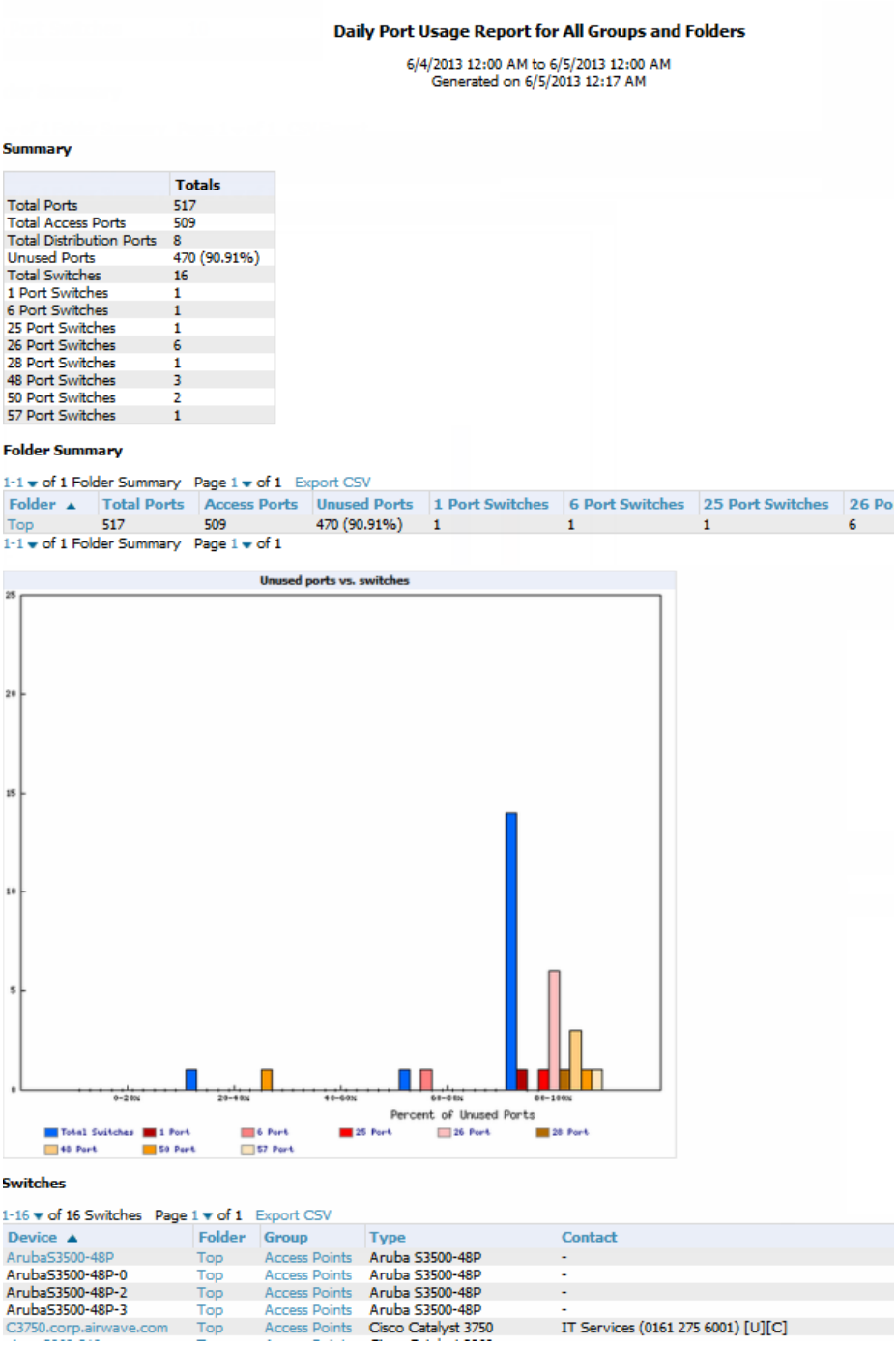
Table 143: *New Rogue Devices Report Fields (Continued)*

Field	Description
Model	Displays the rogue device type when known.
Operating System	Displays the operating system for the device type, when known.
IP Address	Displays the IP address of the rogue device when known.
SSID	Displays the SSID for the rogue device when known.
Network Type	Displays the network type on which the rogue was detected, when known.
Channel	Displays the wireless RF channel on which the rogue device was detected.
WEP	Displays WEP encryption usage when known.
RSSI	Displays Received Signal Strength (RSSI) information for radio signal strength when known.
Signal	Displays signal strength when known.
LAN MAC Address	Displays the MAC address for the associated LAN when known.
LAN Vendor	Displays LAN vendor information associated with the rogue device, when known.
Radio MAC Address	Displays the MAC address for the radio device, when known.
Radio Vendor	Displays the vendor information for the radio device when known.
Port	Displays the router or switch port associated with the rogue device when known.
Last Seen	Displays the last time in which the rogue device was seen on the network.
Total Discovering APs	Displays the total number of APs that detected the rogue device.
Total Discovery Events	Displays the total number of instances in which the rogue device was discovered.

Using the 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 263, also provides a histogram of unused ports vs. unused switches by type (access or distribution).

Figure 263: *Port Usage Report*



Daily Port Usage Report for All Groups and Folders

6/4/2013 12:00 AM to 6/5/2013 12:00 AM
Generated on 6/5/2013 12:17 AM

Summary

	Totals
Total Ports	517
Total Access Ports	509
Total Distribution Ports	8
Unused Ports	470 (90.91%)
Total Switches	16
1 Port Switches	1
6 Port Switches	1
25 Port Switches	1
26 Port Switches	6
28 Port Switches	1
48 Port Switches	3
50 Port Switches	2
57 Port Switches	1

Folder Summary

1-1 of 1 Folder Summary Page 1 of 1 Export CSV

Folder	Total Ports	Access Ports	Unused Ports	1 Port Switches	6 Port Switches	25 Port Switches	26 Po
Top	517	509	470 (90.91%)	1	1	1	6

1-1 of 1 Folder Summary Page 1 of 1

Switches

1-16 of 16 Switches Page 1 of 1 Export CSV

Device	Folder	Group	Type	Contact
ArubaS3500-48P	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-0	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-2	Top	Access Points	Aruba S3500-48P	-
ArubaS3500-48P-3	Top	Access Points	Aruba S3500-48P	-
C3750.corp.airwave.com	Top	Access Points	Cisco Catalyst 3750	IT Services (0161 275 6001) [U][C]

Table 144 describes the fields in the Switches table that is in this report.

Table 144: *Switch Table Fields and Descriptions*

Field	Description
Device	The name of the device

Table 144: *Switch Table Fields and Descriptions (Continued)*

Field	Description
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 RADIUS Reports

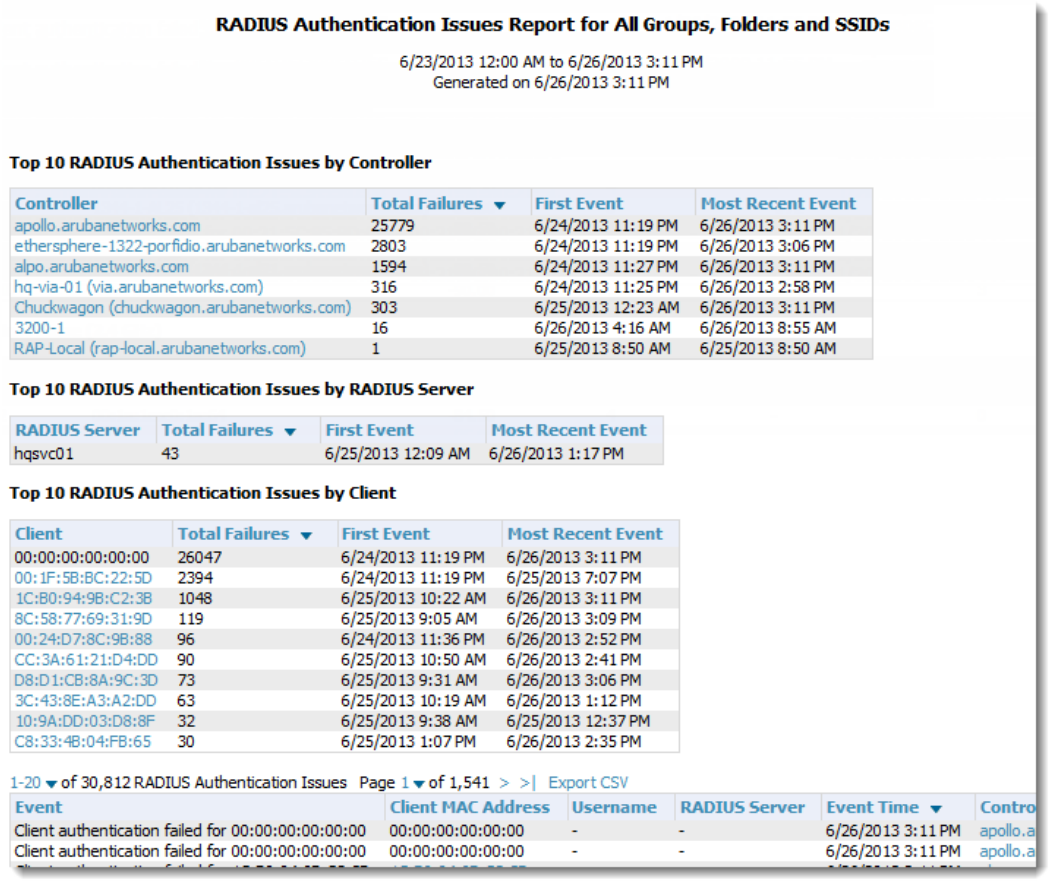
These reports display issues that may appear with controllers, RADIUS servers, and users, or about RADIUS accounting issues.

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, AirWave summarizes authentication issues for each event.

Figure 264: *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

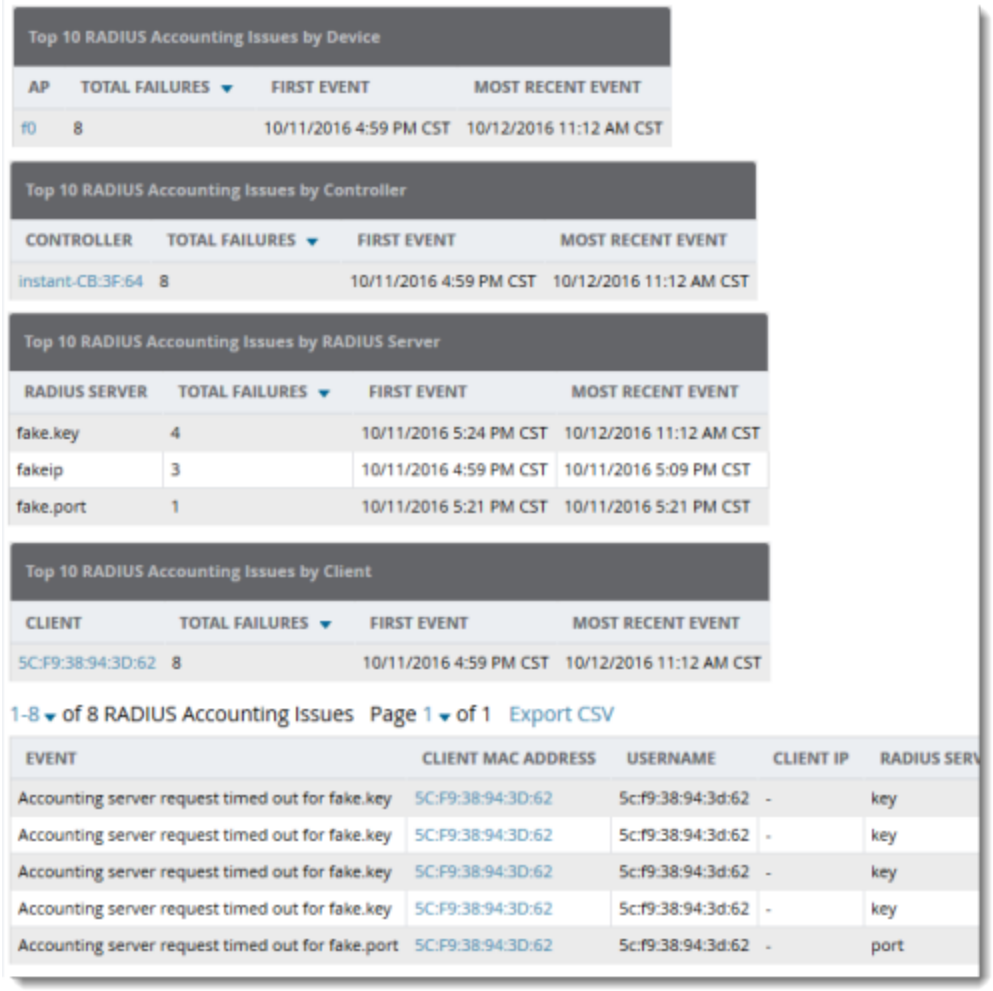
Event	Client MAC Address	Username	RADIUS Server	Event Time	Contro
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a
Client authentication failed for 00:00:00:00:00:00	00:00:00:00:00:00	-	-	6/26/2013 3:11 PM	apollo.a

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 265: *RADIUS Accounting Issues Report*



Top 10 RADIUS Accounting Issues by Device

AP	TOTAL FAILURES	FIRST EVENT	MOST RECENT EVENT
f0	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

Top 10 RADIUS Accounting Issues by Controller

CONTROLLER	TOTAL FAILURES	FIRST EVENT	MOST RECENT EVENT
instant-CB:3F:64	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

Top 10 RADIUS Accounting Issues by RADIUS Server

RADIUS SERVER	TOTAL FAILURES	FIRST EVENT	MOST RECENT EVENT
fake.key	4	10/11/2016 5:24 PM CST	10/12/2016 11:12 AM CST
fakeip	3	10/11/2016 4:59 PM CST	10/11/2016 5:09 PM CST
fake.port	1	10/11/2016 5:21 PM CST	10/11/2016 5:21 PM CST

Top 10 RADIUS Accounting Issues by Client

CLIENT	TOTAL FAILURES	FIRST EVENT	MOST RECENT EVENT
5C:F9:38:94:3D:62	8	10/11/2016 4:59 PM CST	10/12/2016 11:12 AM CST

1-8 of 8 RADIUS Accounting Issues Page 1 of 1 Export CSV

EVENT	CLIENT MAC ADDRESS	USERNAME	CLIENT IP	RADIUS SERV
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.key	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	key
Accounting server request timed out for fake.port	5C:F9:38:94:3D:62	5c:f9:38:94:3d:62	-	port

Using the RF Health Report

The RF Health Report assists in pinpointing the most problematic devices on your network, and lists the top devices by problem type. The default RF Health report shows the max concurrent clients count per radio band.

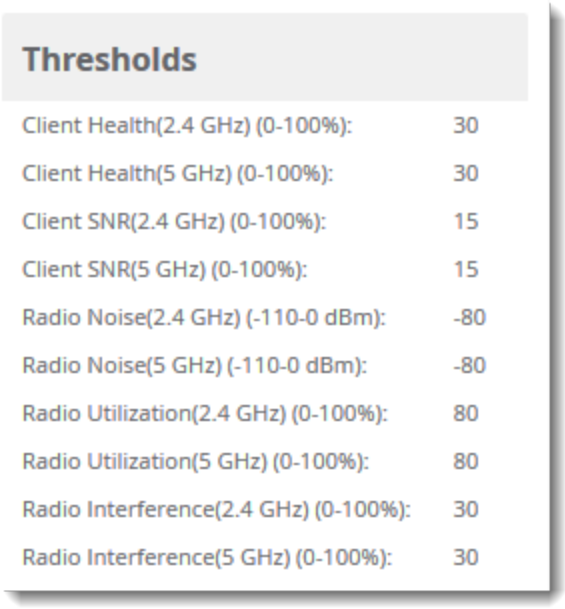
When creating a custom RF Health report, you can select the following widgets from the custom options:

- Max concurrent clients (2.4 GHz)
- Max concurrent clients (5 GHz)

From the generated report, you can open the monitoring page for the selected radio by clicking a hyperlink in the AP Name column.

Thresholds

Thresholds for the radio statistics are reported as a percentage (%) or a power measurement (dBm). For information on changing the threshold values, see "Changing Your Report Summary and Thresholds" on page 357.

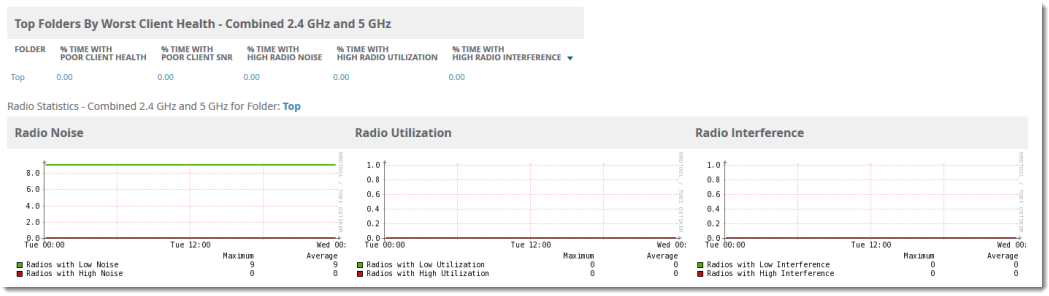


Top Folders and Radio Statistics

A report can be summarized by the following statistics:

- 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.



Changing Your Report Summary and Thresholds

To select a new summary method:

1. Log in to AirWave.
2. Navigate to **Reports > Definitions**, then click **Add**.
3. Select **Daily RF Health Report**.
4. In the Report Restrictions area, select the **Summarize report by** options that you want.
5. Select the statistics to be displayed from the **Top Folder Sorting Column** drop-down menu.
6. Define the thresholds for 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 Custom Reports" on page 364 section of this chapter.

Lists of Top Radio Issues

AirWave tracks the top AP radio issues and lists them by problems. A device will make it into the list of problems if it violates two or more thresholds. For more on the thresholds that indicate problems, refer to "Viewing the Radio Statistics Page" on page 162.)

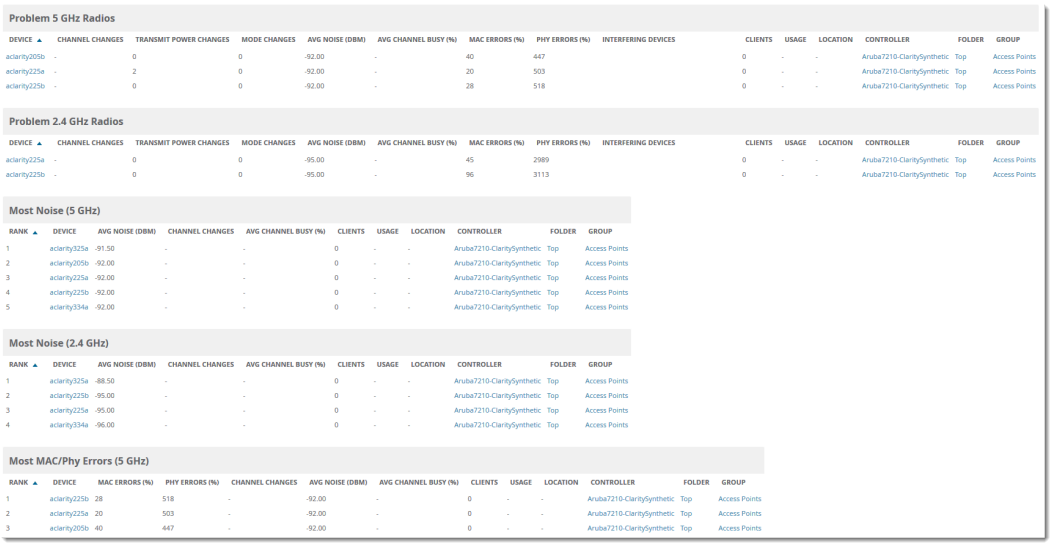
The lists for most mode changes and most interfering are available if there are ARM events.

Other lists include:

- Most or Least Utilized by Channel Usage
- Most MAC/Phy Errors
- Most Channel Changes
- Most Transmit Power Changes
- Clients with Least Goodput
- Clients with Least Speed
- Radios with Least Goodput

Figure 266 illustrates some of the lists on the Daily RF Health Report.

Figure 266: *Lists of Problems and Radio 8888 Issues*



The RF Health report lists devices that are ranked and then sorted by the third column in the table. Click the blue **Device** link to access the **Devices > Monitor > Radio Statistics** page for the radio band.

NOTE

AirWave limits data storage to 183 days, which is approximately six months, per radio. If you create an RF Health report with range of more than 183 days, the report 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. Most reports have data (like bandwidth and users) that maxes out at 425 days. AirWave validates reports so you can only run them over a 366-day duration.

Using the Rogue Clients Report

The Rogue Clients report tracks the number of valid users that connected to rogues in the specified time frame, and can be filtered by rogue classification. You can specify to include ad-hoc devices can be included and detailed information about the clients.

By default, the minimum RAPIDS classification is Suspected Rogue, and the maximum is Contained Rogue.

Figure 267: *Rogue Clients Report Page Illustration*

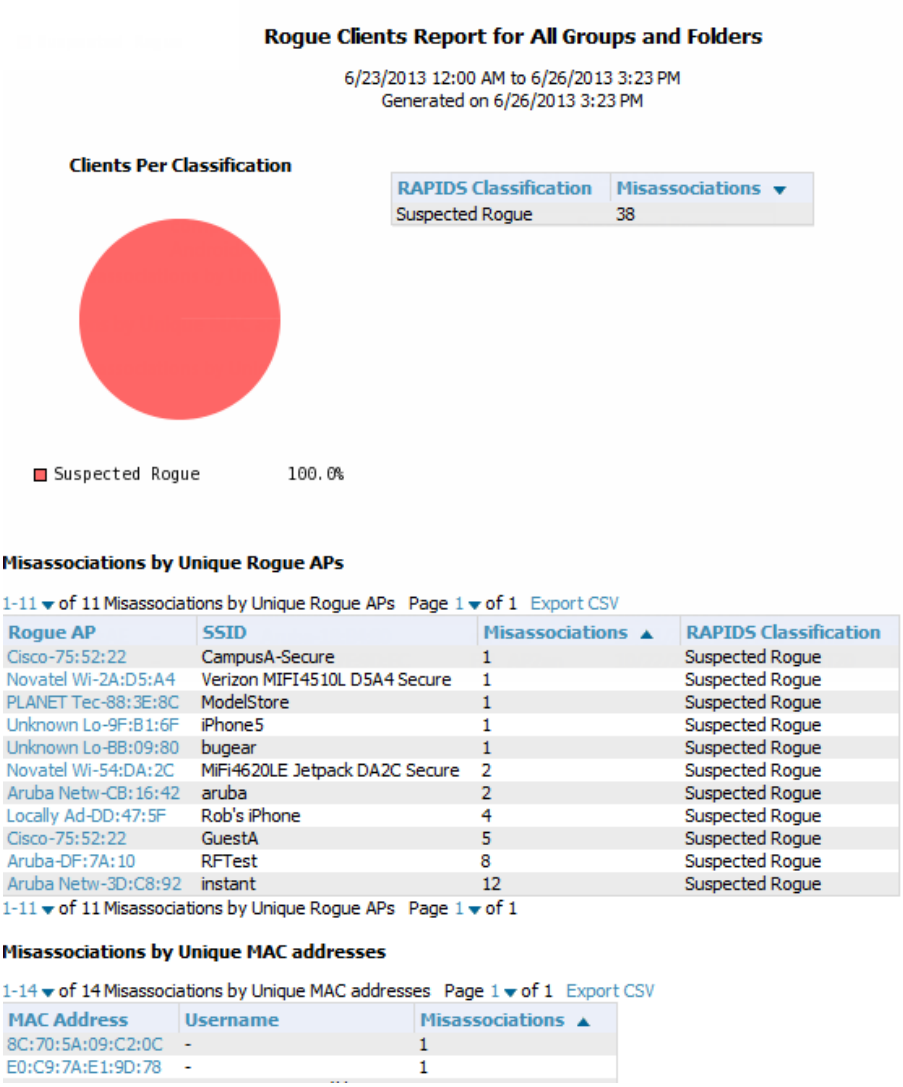


Table 145: *Rogue Clients fields and descriptions*

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

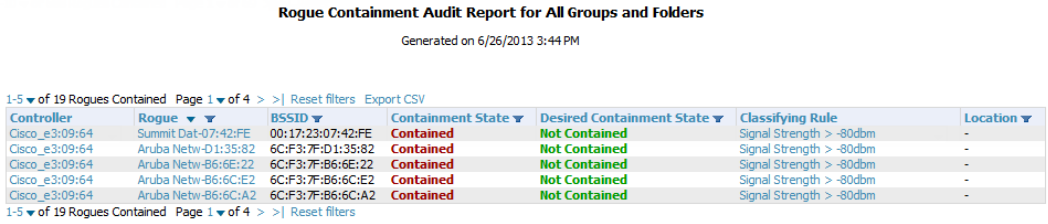
Table 145: *Rogue Clients fields and descriptions (Continued)*

Field	Description
First Heard	The date/time when the rogue client was first detected on the network
Ch BW	The channel bandwidth of the client, if 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 Rogue Containment Audit Report

The Rogue Containment Audit report that lets you know if any containment is failing. Figure 268 illustrates the output of this report, and Table 146 describes the fields available in the report.

Figure 268: *Rogue Containment Audit Report Page Illustration*



Rogue Containment Audit Report for All Groups and Folders

Generated on 6/26/2013 3:44 PM

1-5 of 19 Rogues Contained Page 1 of 4 > >| Reset filters Export CSV

Controller	Rogue	BSSID	Containment State	Desired Containment State	Classifying Rule	Location
Cisco_e3:09:64	Summit Dat-07:42:FE	00:17:23:07:42:FE	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-D1:35:82	6C:F3:7F:D1:35:82	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6E:22	6C:F3:7F:B6:6E:22	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:E2	6C:F3:7F:B6:6C:E2	Contained	Not Contained	Signal Strength > -80dbm	-
Cisco_e3:09:64	Aruba Netw-B6:6C:A2	6C:F3:7F:B6:6C:A2	Contained	Not Contained	Signal Strength > -80dbm	-

1-5 of 19 Rogues Contained Page 1 of 4 > >| Reset filters

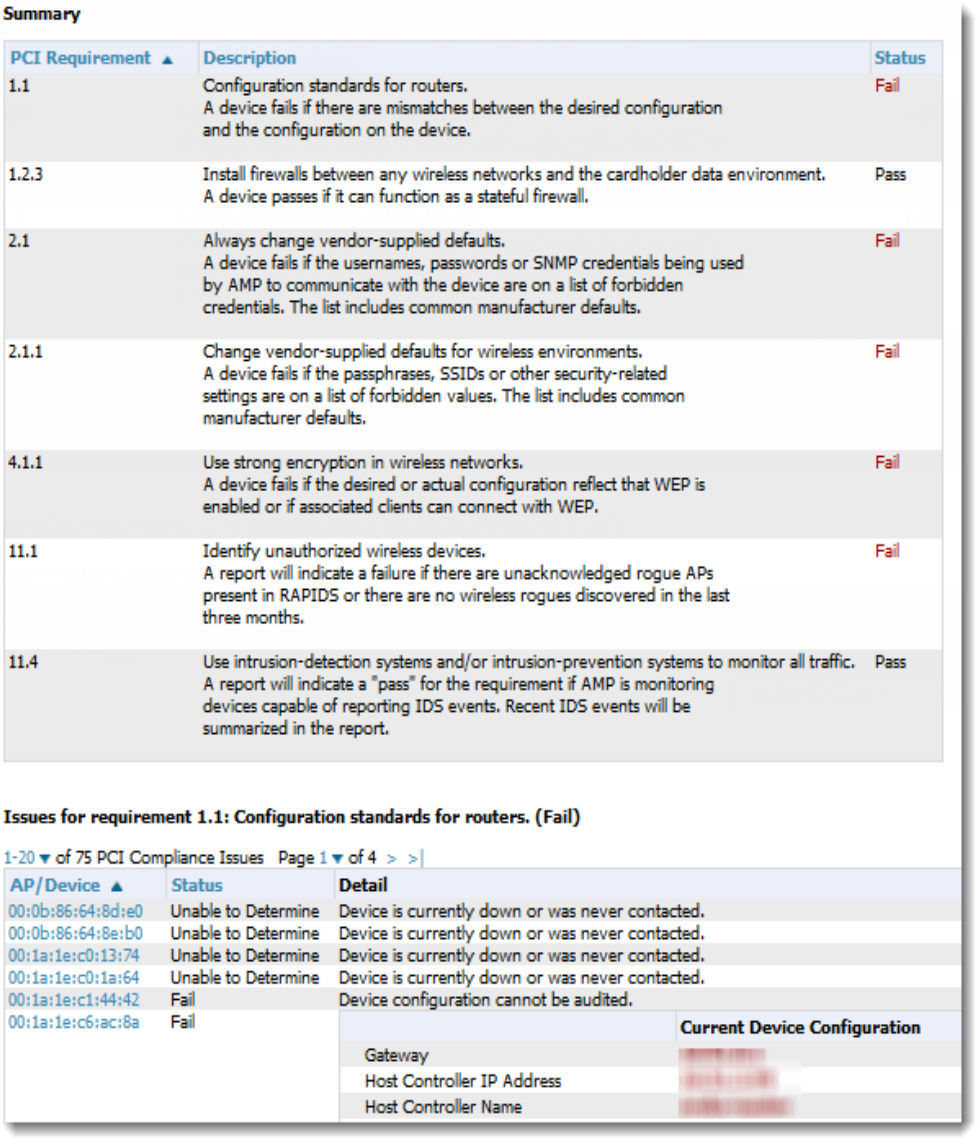
Table 146: *Rogue Containment Report fields and descriptions*

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

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 269: *PCI Compliance Report*



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	

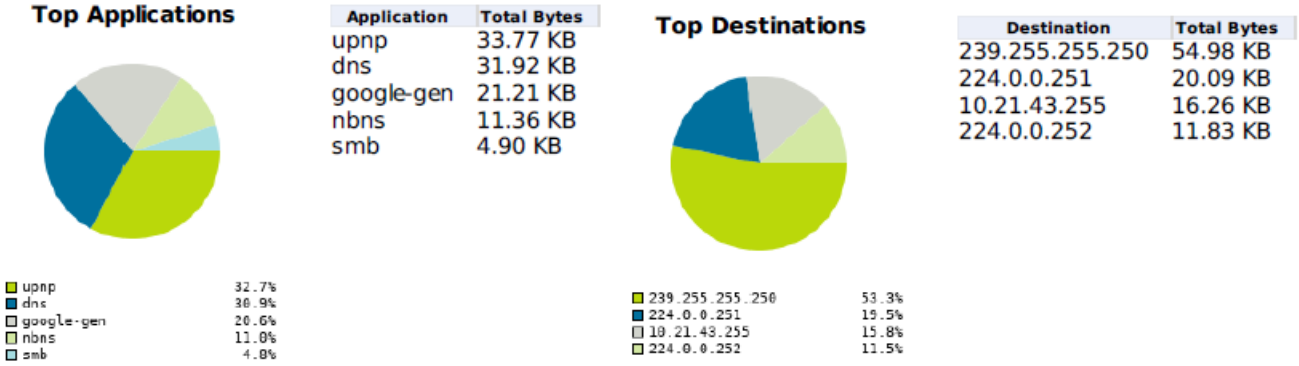
	Current Device Configuration
Gateway	[redacted]
Host Controller IP Address	[redacted]
Host Controller Name	[redacted]

For information about turning on this feature, see "Enabling PCI Compliance Monitoring" on page 77.

Using the Traffic Analysis Report

AirWave allows you to generate reports on the highest volume of web traffic, as shown in Figure 270.

Figure 270: *Top Applications and Top Destinations Reports*



AirWave also provides traffic analysis reports filtered by device type, role, or SSID, as shown inFigure 271

Figure 271: *Top 10 Application Reports*

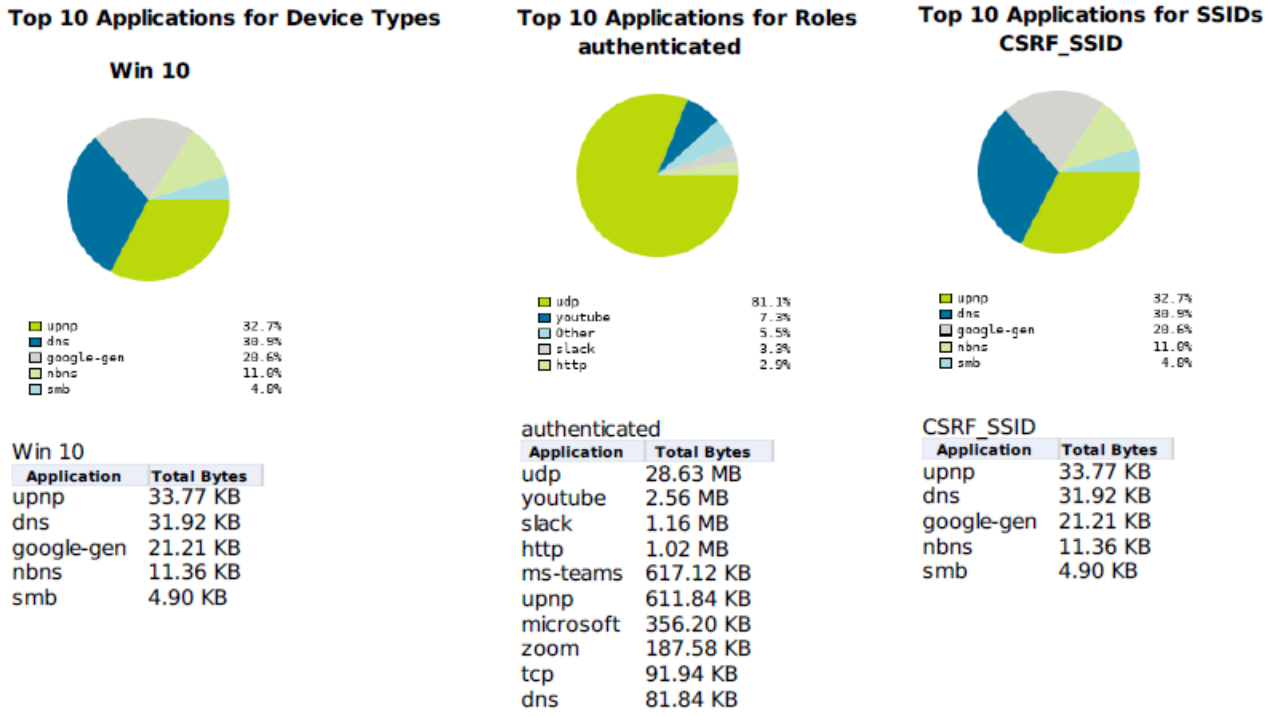
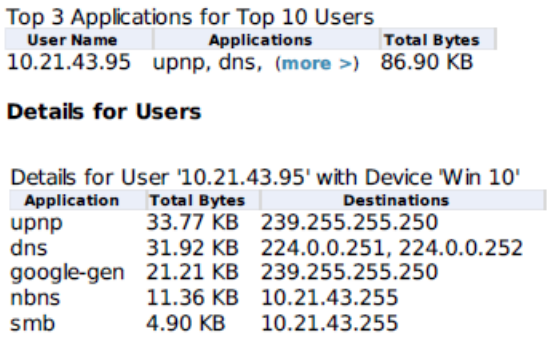


Figure 272 shows an example of traffic analysis without regard to role or SSID even if you specify them in the report definition. Keep in mind that the top users might change if you run the report for a longer time period.

Figure 272: *Top Three Applications for Top Ten Users Report*



Top 3 Applications for Top 10 Users

User Name	Applications	Total Bytes
10.21.43.95	upnp, dns, (more >)	86.90 KB

Details for Users

Details for User '10.21.43.95' with Device 'Win 10'

Application	Total Bytes	Destinations
upnp	33.77 KB	239.255.255.250
dns	31.92 KB	224.0.0.251, 224.0.0.252
google-gen	21.21 KB	239.255.255.250
nbns	11.36 KB	10.21.43.255
smb	4.90 KB	10.21.43.255

Table 147 describes the fields in the Traffic Analysis reports.

Table 147: *Traffic Analysis Report Fields and Descriptions*

Field	Description
Application	The application detected on your network.
Total Bytes	The number of packets, in bytes, sent by an application or received by the client.
Destinations	The client IP address for application traffic.

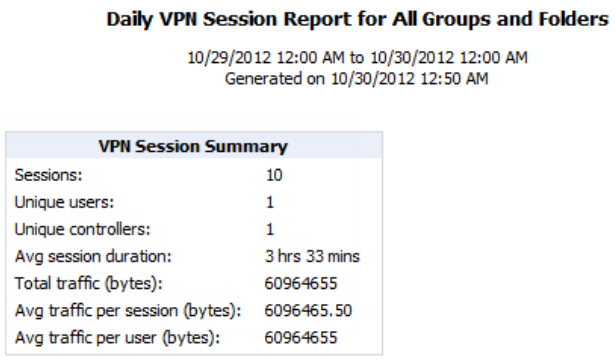
Using the VPN Session Report

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 273: *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 148 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 148: *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 Custom 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. AirWave reports and information displayed in the WebUI varies depending on configurations, user roles, and folders.

Report Restrictions

Keep these considerations in mind when working with the Reports Definitions page:

- You might see conflicting device counts in reports that are restricted by time range, such as client session data, and reports that show all data, such as client inventory.

  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.
- All reports allow you to make restrictions based on groups, folders, and device types. However, when creating a Traffic Analysis report, if you set the **Select by APs/Device Name** option to **Yes**, you can't select groups and folders
- When you select custom options to include in a report, additional restrictions become available.

To create a custom report:

1. Go to **Reports > Definitions**, then click **Add**. Or click to edit a report.
2. Enter the name of the report in the **Title** field.
3. From the **Type** drop-down menu, select **Custom**.
4. 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.
5. Complete the **Report Restrictions** section.
6. 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.

7. If you want non-admin users to see a generated reports, choose **By Subject**. By default, any report can be seen by an AirWave admin.
8. Click **Yes** if you want to email the report. They can be sent in HTML, PDF, and CSV formats.
9. Click **Yes** to you want to share the report by FTP or SCP to an external server.
10. Click **Add** to save your report. The report displays on the **Report Definitions** page.

Running Reports on Selected Devices

Using the Modify Devices tool to select devices and run a report will take you to the **Reports Definitions** page, where you can select a report definition template.

Currently, all report definitions are available to choose from even though you can't run the following client-based reports: new rogue device, rogue clients, rogue containment audit, traffic analysis, and UCC.

To run reports on selected devices:

1. Navigate to one of the following pages that has a Device List:
   - **Devices > List**. You can also click the Up, Down, Mismatched hyperlinks on the List page to open monitoring pages for the devices with those devices states.
   - **Groups > Monitor**.
2. Click  at the top right corner of the device list, then select the devices that you want to include in a report.
3. From the **Device Actions** drop-down menu, select **Run report on selected devices**.
4. Click **Run Report**. AirWave opens the **Report Definitions** page.
5. Enter a title for the report.
6. Select a device-level report.
7. 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.
8. 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.
9. If you want non-admin users to see a generated reports, choose **By Subject**. By default, any report can be seen by an AirWave admin.
10. Click **Yes** if you want to email the report. They can be sent in HTML, PDF, and CSV formats.
11. Click **Yes** to you want to share the report by FTP or SCP to an external server.
12. Click **Add** to save your report. The report displays on the **Report Definitions** page.

Cloning Reports

There are two places where you can clone and run a report. One is where you select a report definition from the Report Definition list. The other is where you use the Modify Devices option from a device list view, which you can access from **Groups** or **Devices**.

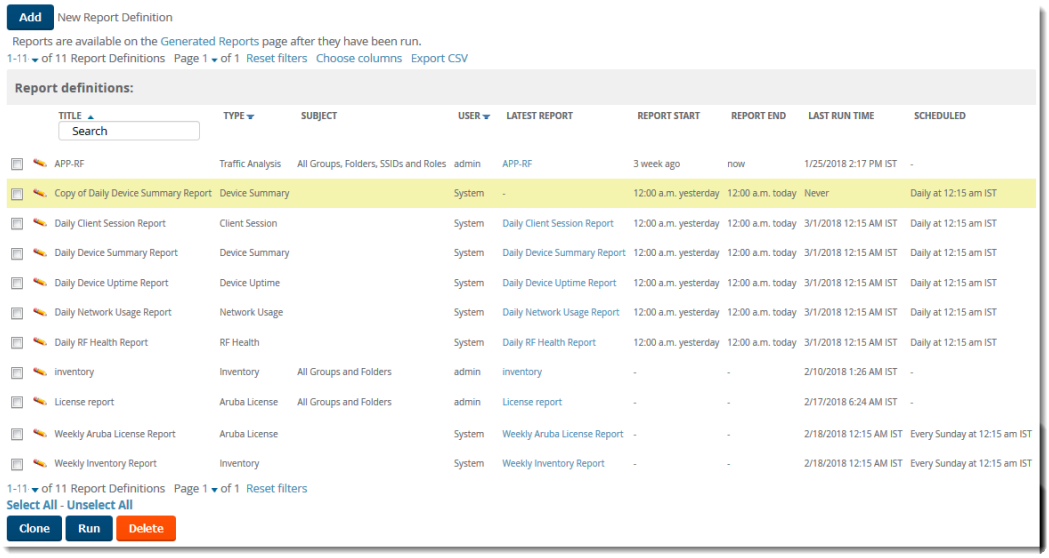
Selecting the Report Definition

To clone a report using a report definition:

1. Navigate to **Reports > Definitions** then select a report definition.

2. Click **Clone**. The copied report will be added to the report definition list with "copy of" appended in front of the report name.

Figure 274: *Cloning a Report*



3. Click to modify the report settings.
4. Change the title of the report.
5. Click **Save**.

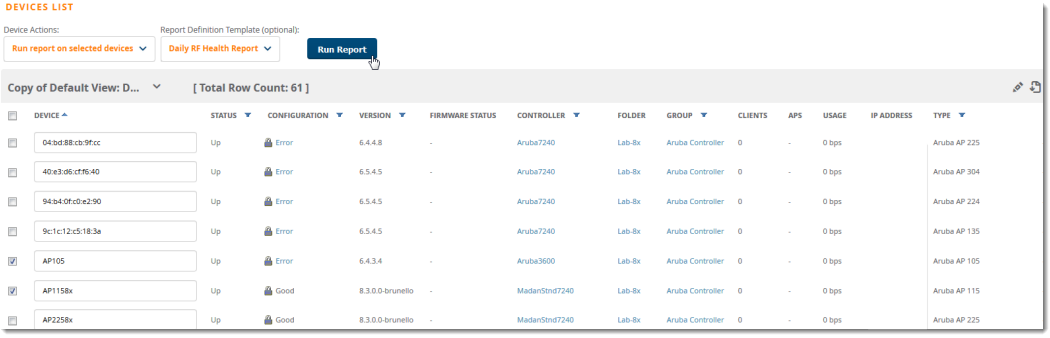
Selecting the Devices and a Report Template

You can select devices from the device list and modify the clone using a report template or by choosing report widgets. If you want to customize the report with widgets, see "Selecting the Devices Without Using a Report Template" on page 367.

To clone a report from the Modify Devices list using a report template:

1. Navigate to **Groups** and select a group, or **Devices > List**, then click  to select the devices from the Modify Devices list.
2. From the Device Actions drop down menu, select **Run report on selected devices**.
3. Choose a report definition template.

Figure 275: *Running a Report Using a Definition Template*



4. Click **Run Report**. AirWave opens the Reports Definitions page. The copied report will be added to the report template with "copy of" appended in front of the report name.
5. Choose additional restrictions for the copy of the report.

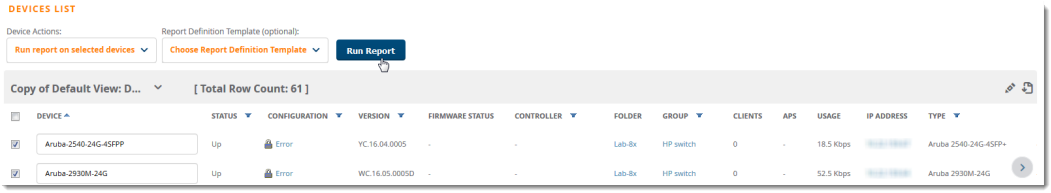
6. Cick **Save and Run**. The newly created report is added in the Report Definitions page. You can make further report modifications at any time from the Report Definitions page.

Selecting the Devices Without Using a Report Template

To clone a report from the Modify Devices list without using a report template:

1. Navigate to **Devices**, then click  to select the devices from the Modify Devices list.
2. From the Device Actions drop down menu, select **Run report on selected devices**.

Figure 276: *Running a Report Without a Template*



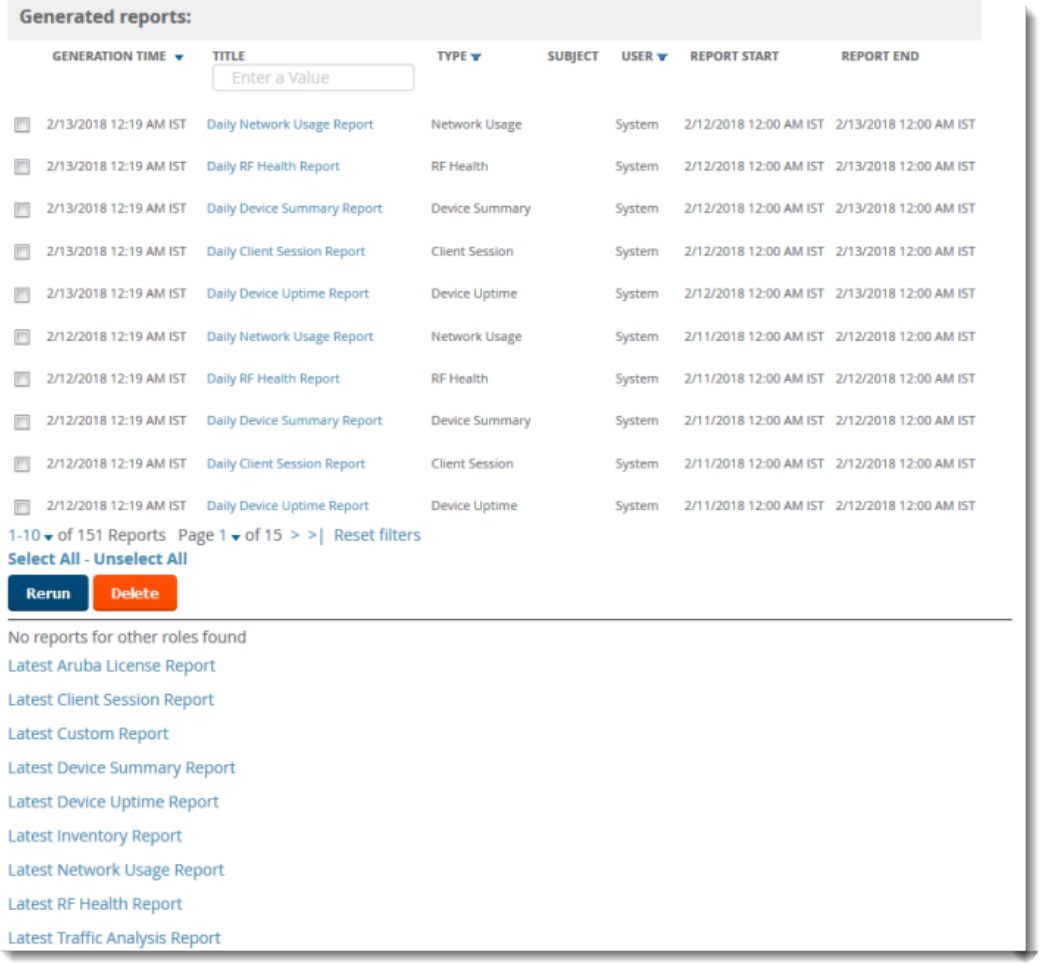
3. Click **Run Report**. AirWaveopens the Custom Options page with the selected devices listed in the Report Restrictions area.
4. Choose report widgets and other report options.
5. Click **Add and Run**. The newly created report is added in the Report Definitions page. You can make further report modifications at any time from the Report Definitions page.

Viewing Generated Reports

The **Reports > Generated** page lists reports that have been run and the latest version of all daily reports. From the Generated reports list, you can click the title hyperlink to view the report details. By default, AirWave orders reports by generation time. You can sort reports by any other column header in sequential or reverse sequential order. You can also choose columns, export the list in CSV format, and modify the pagination.

An Admin user can see and edit all report definitions. Users with "Monitor Only" roles can see reports and definitions only if they have access to all devices in the reports. AirWave displays reports for the current role and for additional roles.

Figure 277: *Generated Reports Page*



Here are some of the details you can view about a generated report:

- Generated Time. 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. The user-configured title of the report.
- Type. The type of the report.
- User. The user who created the customized report.
- Subject. The scope of the report, including groups, folders, SSIDs, or a combination of these included in the report.
- Report Start. The designated start of the time period to be covered by the report. You can enter a start date of 6 months 3 weeks 5 days 9 hours ago, or 5/5/2018 13:00. This field is supported by most report types. When this field isn't available, the report provides a snapshot of current status.
- Report End. The designated end of the time period covered by the report. You can enter an end date of 4 months 2 weeks 1 day ago, or 6/6/2018 9:00. This field is supported by most report types. When this field isn't available, the report provides a snapshot of current status.

Get an Updated Report

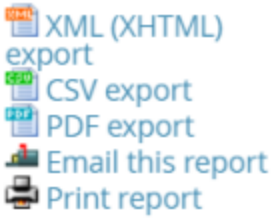
There are several ways to get an updated report:

- From the generated reports list, select a check box beside a report and click **Rerun**. When you run or rerun a report, the Generation Time column changes to pending until the report is completed.
- From the latest reports list at the bottom of the page, click the report hyperlink.

Sending Reports

All reports contain links to export, email, and print reports at the top right of the page (see Figure 278). Graphics and links are included with exported reports. When sending reports to multiple email addresses, separate them with commas.

Figure 278: *Send Report Options*



Exporting Reports in CSV Format

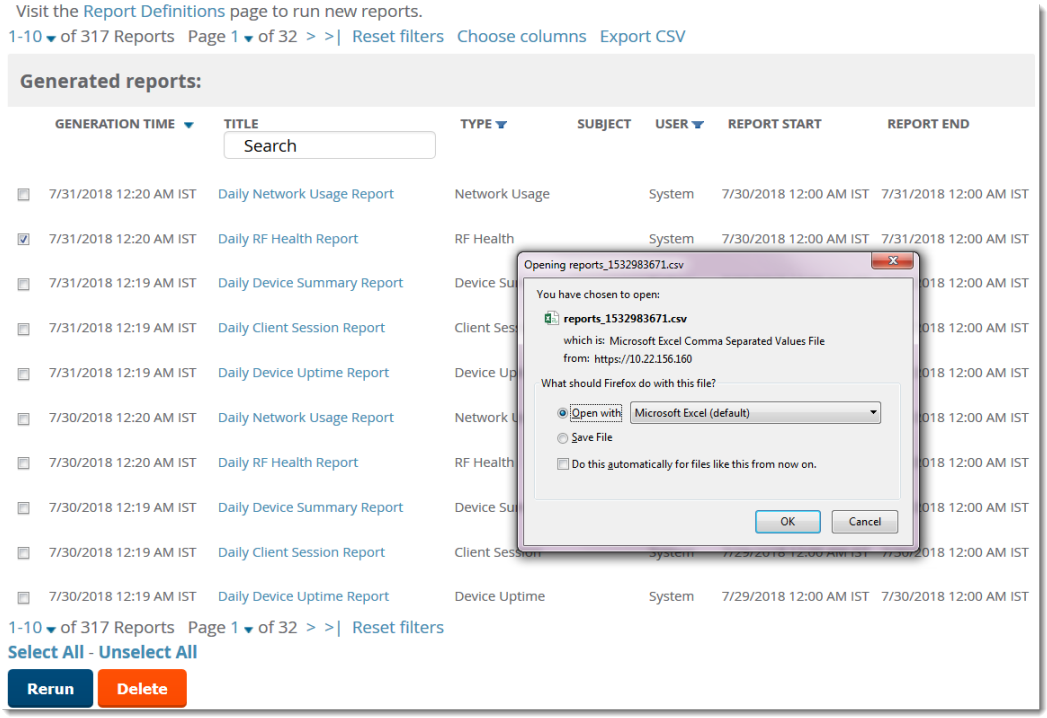
You can export reports (and some tables) from the WebUI. AirWave will append a number to the file name like **1532986103**. This number changes every time you generate the report.

Exporting a Report

If you want to export an individual report, follow these steps:

1. Go to **Reports > Generated** and select a report from the report table.
2. Click the blue **Export CSV** link above the report table. If a message asks you what to do with the file, click **Open**. Or you can click **Save file** and view the file later.
3. Click **OK**.

Figure 279: *Exporting a Report in CSV Format*



Exporting Multiple Reports

When you export all files at once, AirWave creates a zip file of all the CSV files and saves it to a temporary or download directory on your local AirWave server.

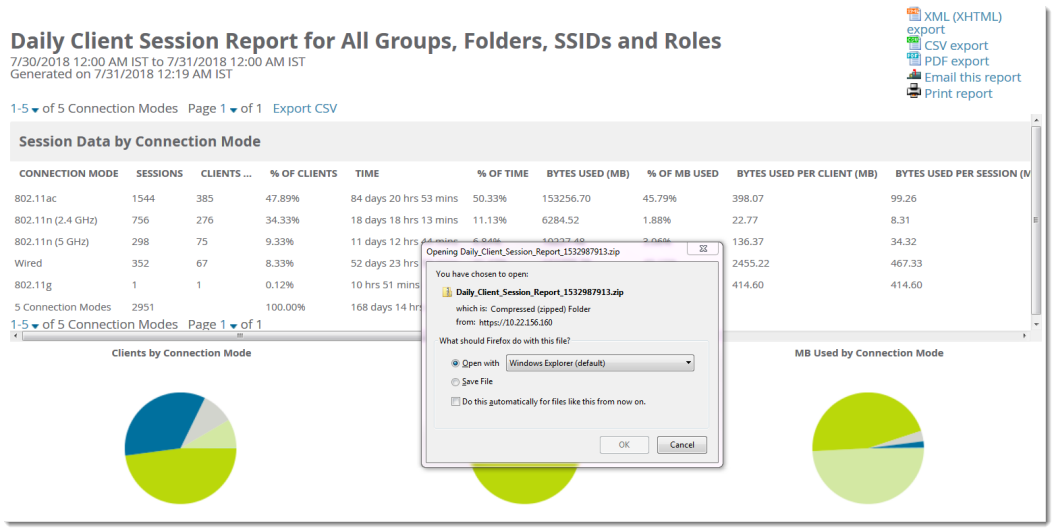
NOTE

If you are exporting reports to a remote server and name the report when you enter the file path, AirWave will append a report ID to the CSV files and put it in a folder in a zip file on the remote server.

To export multiple reports:

1. Go to **Reports > Generated** and select a report from the list. Or you can scroll down to the bottom of the page, then click the blue link for the latest version of the report.
2. From the detailed report, click the **CSV Export** link at the top right of page.
3. Follow the onscreen instructions to open the CSV files, or save the zip file.
4. Click **OK**. Figure 280 shows an example of exporting client session reports in CSV format.

Figure 280: *Exporting Multiple CSV Files*



Sending Reports to a Smart Host

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 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.

To add a forwarding email address:

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:

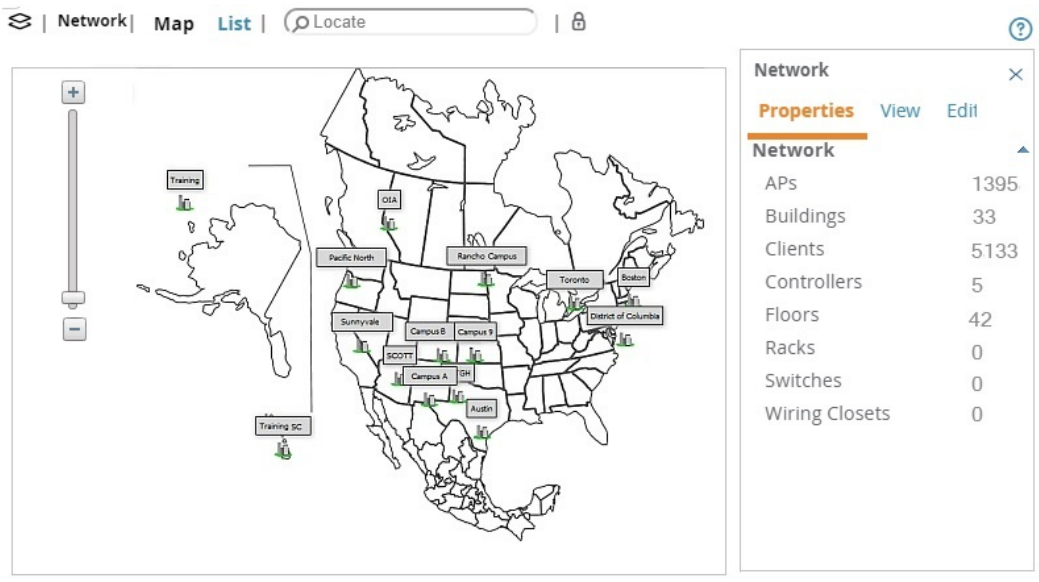
   `tail -f /var/log/maillog`

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 281: *Example VisualRF Page Showing all networks*



Features

- Mesh monitoring page specially for viewing Aruba AirMesh devices. VisualRF automatically renders Mesh APs based on GPS coordinates.

- Floor plan upload wizard enables direct importation of JPG/JPEG, GIF, PNG, PDF (single page only) and CAD files for floor plans. **NOTE**: PDF floor plans must be generated from a source file. Other PDFs, such as those scanned from a printer, will not import properly. Similarly, CAD files must be generated by AutoCAD.
- Batch upload wizard enables batch uploads of multiple CAD files with corresponding walls, and access points.
- Accurate calculation of the location of all client devices (laptops, RFID Tags, PDAs, Phones) using RF data from your existing APs and controllers. Increased accuracy of device placement can be achieved with periodic site surveys.
- Graphical navigation allows your Help Desk to view floor plans simply by clicking on the appropriate campus, building, or floor.
- Tree view allows you to navigate to a specific campus, building, or floor via a tree navigation.
- Heatmaps depict the strength of RF coverage in each location.
- Speed (data rate) view which depicts the highest 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. 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 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. 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 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. AirWave also uses these signal strength readings to more accurately place these unassociated clients.
- **VisualRF** - The AirWave service that calculates location, calculates path loss, and provides floor plan editing capabilities.

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**.

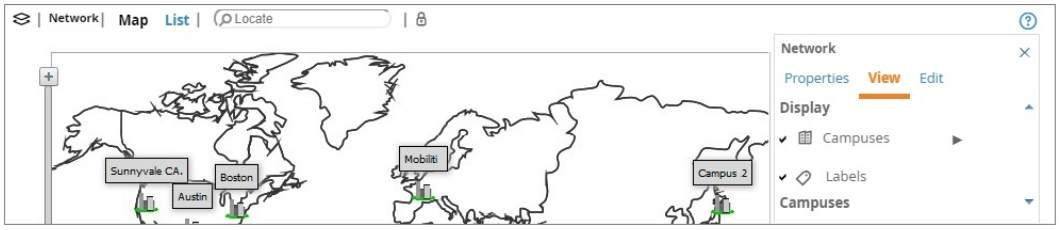
To enable VisualRF, follow these instructions while logged in as an administrator:

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 282.

Figure 282: *Default VisualRF Top Level Menu - Network View*



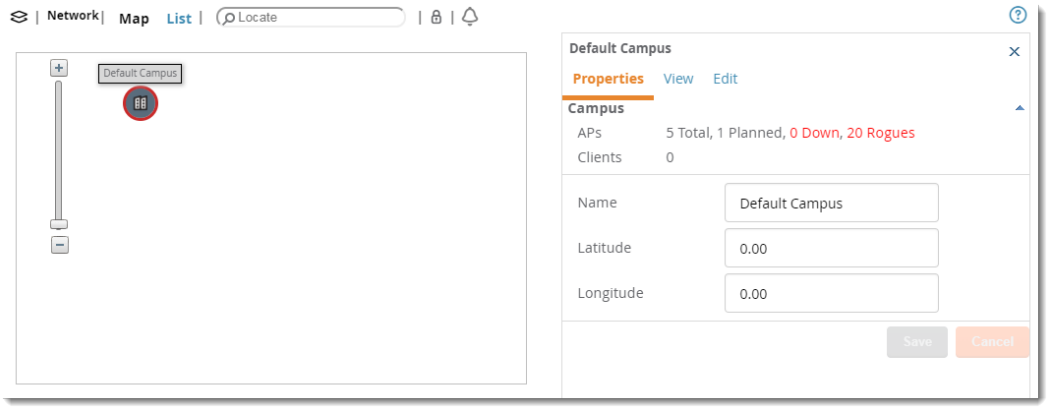
The top-level Network view can display network campuses on a map, or in a list. You can toggle between these two displays by clicking the **Map** or **List** links at the top of the Network view.

Network View Navigation

The Network view provides page specially for viewing campuses, buildings and floors within your network.

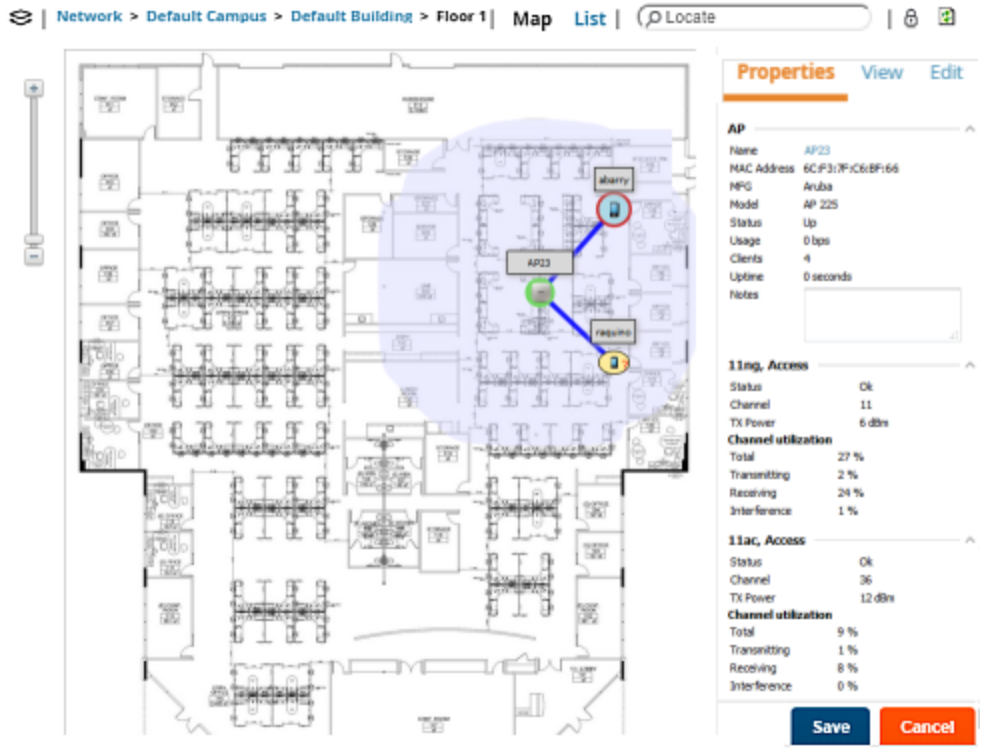
You can select any campus or building to view the numbers of APs and clients at that location. Figure 283 displays an example of a campus view with a building icon selected:

Figure 283: *Viewing a Campus Network*



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 284

Figure 284: *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 ArubaOS devices running 6.1 or greater that have run the **mgmt-server type** 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:

- **Traffic Anaylsis**, 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 ArubaOS 6.3 or greater. For more information on how this value is calculated, see "Useful Terms" on page 373.
- **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 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, or Walls. If you created a client survey in 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.

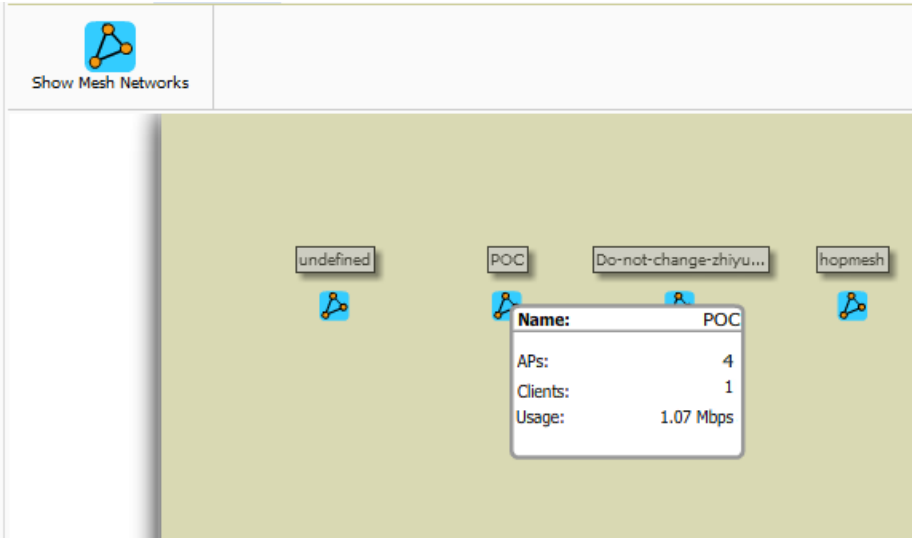
To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. VisualRF uses the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position.

Mesh View Navigation

Mesh view provides a visual Mesh monitoring page specially for viewing Aruba 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 285 displays an example of a Mesh Network view with a mouseover above a network icon:

Figure 285: *Viewing Mesh Networks in VisualRF*



Click on an AirMesh network to display the APs with labels, as shown in Figure 286

Figure 286: *APs in a mesh network*

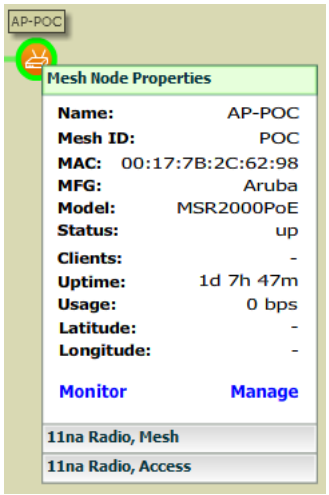
Select an AirMesh AP icon to bring up the pop up menu showing the Mesh Node Properties by default. This window shows the node's name, MeshID, MAC, Manufacturer, and other information. Clicking the blue **Monitor** link inside this window opens the **Devices > Monitor** page in a new tab. Clicking the blue **Manage** link inside this window opens the **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 149 describes these icons and their functions in the VisualRF Mesh view.

Table 149: *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
Help		Launch the online help. **NOTE:** This User Guide currently contains the most up-to-date help information for the VisualRF interface.

Figure 287: *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. For additional troubleshooting, refer to VisualRF and Performance on page 449.

NOTE

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.

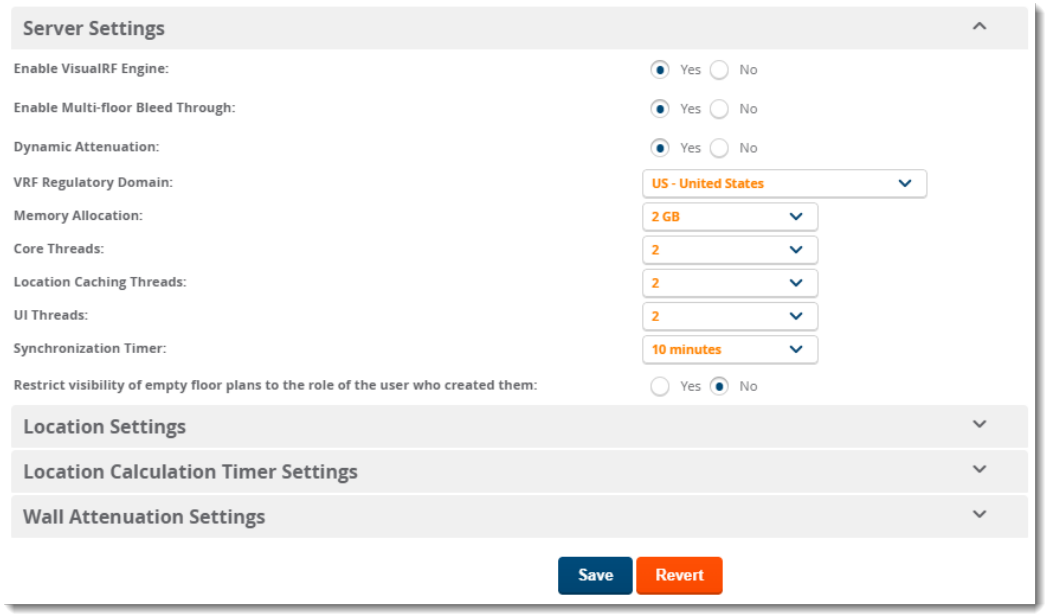
Server Settings

To enable VisualRF and tune memory and performance, navigate to the **Server Settings** section on the **VisualRF > Setup** page.

NOTE

In previous versions of AirWave, you set measurement preferences on the **VisualRF > Setup** page. In AirWave 8.2.5.1 and later versions, this preference is set by choosing the "Meters" or "Feet " option on the **VisualRF > Floor Plans > Network >Edit** page. For more information about setting your preferences, see "Change Settings in Floor Plans" on page 389.

Figure 288: *Server Settings*



The server settings are detailed in Table 150.

Table 150: *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.

Table 150: *Server Settings (Continued)*

Setting	Default	Description
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.
VRF Regulatory Domain	United States	Sets the regulatory domain in AirWave.
Memory Allocation	512 MB	The amount of memory dedicate to VisualRF. It is not dynamically allocated and all the memory is consumed upon starting the service. Be sure to check the memory and swap utilization in the **Systems > Performance** page before making any changes. The exact amount of memory used per floor plan will vary heavily based on the size, number of devices and number of grid cells on the floor plan. • 25 floors or less 512 MB • 25 to 50 floors 768 MB • 50 to 75 floors 1 GB • 75 to 100 floors 1.5 GB • 100 to 200 floors 3 GB • 200 to 300 floors 5 GB (64-bit only) • Above 300 8 GB (64-bit only) **NOTE:** If you see Out of Memory errors in the httpd/error_log on the **System > Status** page, you should increase memory allocation.
Core Threads	1x number of cores	Number of threads that calculate path loss for each floor. These threads also regenerate a floor's RF properties when new APs, walls, or regions are added to a floor plan.
Location Caching Threads	1x number of cores	Number of threads that calculate the location of all clients associated with access points on this floor plan.
UI Threads	1x number of cores	Number of threads that service the users accessing VisualRF, as well as 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 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  to access the location settings on the **VisualRF > Setup** page.

Figure 289: *Location Settings*

The location settings are detailed in Table 151

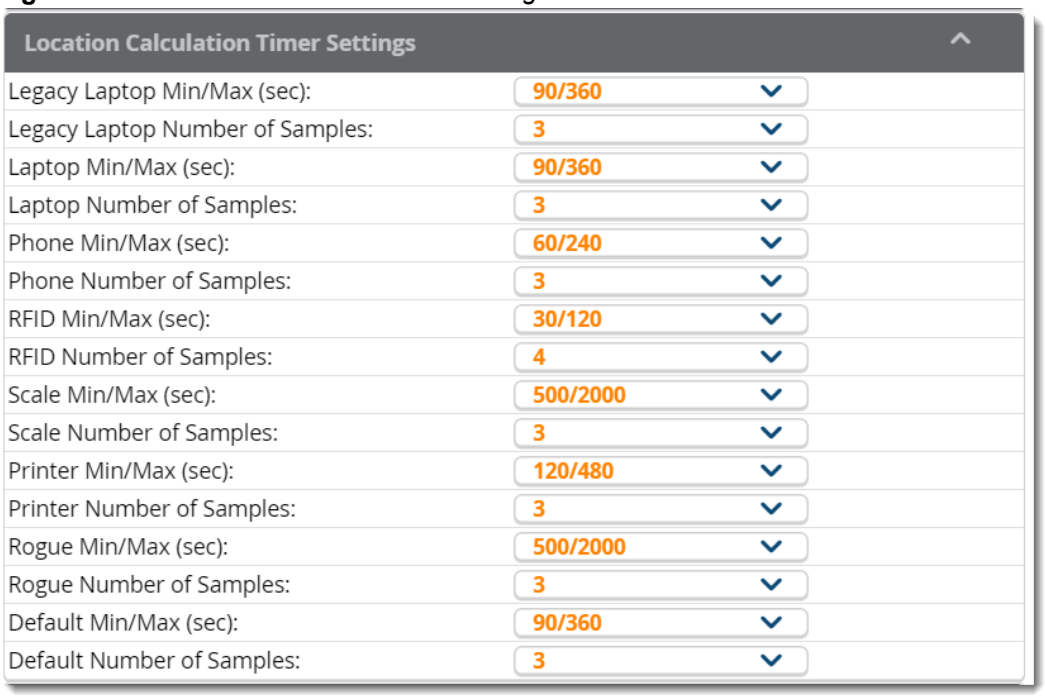
Table 151: *Location Settings*

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.
Maximum Rogue APs per Floor Plan	20	Sets the maximum number of rogues 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 290: *Location Calculation Timer Settings*



The location calculation timer settings are described in Table 152

Table 152: *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.
Legacy Laptop Number of Samples	3	See definition above.

Table 152: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
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 Number of Samples	3	

Table 152: *Location Calculation Timer Settings (Continued)*

Setting	Default	Description
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.

Disabling Client Calculation

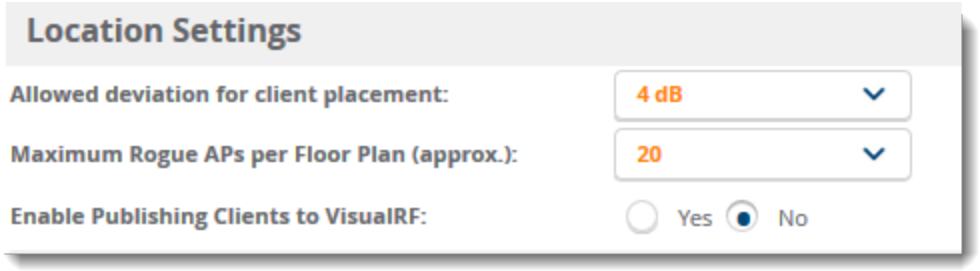
You can enable or disable the client calculation from the **VisualRF > Setup** page. Clients that are currently in VisualRF stay until they expire, and then VisualRF removes them.

To immediately remove all clients, first remove the **visualrf_bootstrap** file to flush the client information and then restart VisualRF. You can do this from the CLI by selecting **11** to open the Enter Commands menu. At the prompt, enter **remove_visualrf_cache**.

To disable client calculations:

1. Go to **VisualRF > Setup**, then click Location Settings.

Figure 291: *Disabling the Client Calculation Feature*



2. Select **No** for the **Enable Publishing Clients to VisualRF** option.
3. Click **Save**.

Wall Attenuation Settings

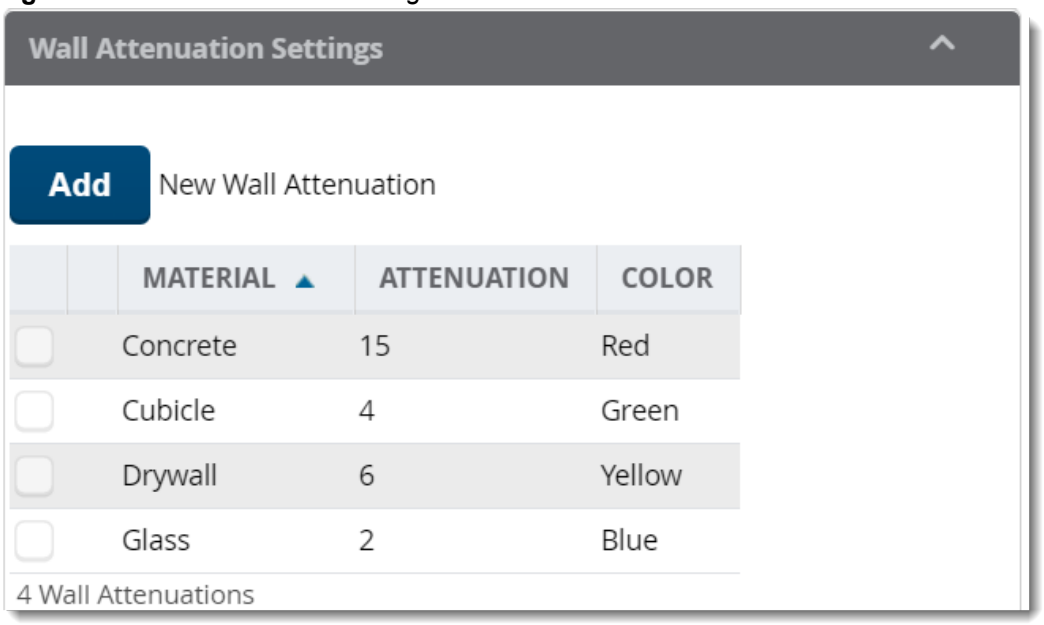
Signal attenuation is the loss of signal strength during transmission. You can indicate the causes of attenuation using attenuation settings on the **VisualRF > Setup** page.

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 292: *Wall Attenuation Settings*



The default wall attenuation settings are described in Table 153.

Table 153: *Default Wall Attenuations*

Item	Description
Material	Type of material that reduces the signal strength, including concrete, cubicle, dry wall, and glass.

Table 153: *Default Wall Attenuations (Continued)*

Item	Description
Attenuation	Signal loss represented in decibels (dB).
Color	Color representation in the floor plan.

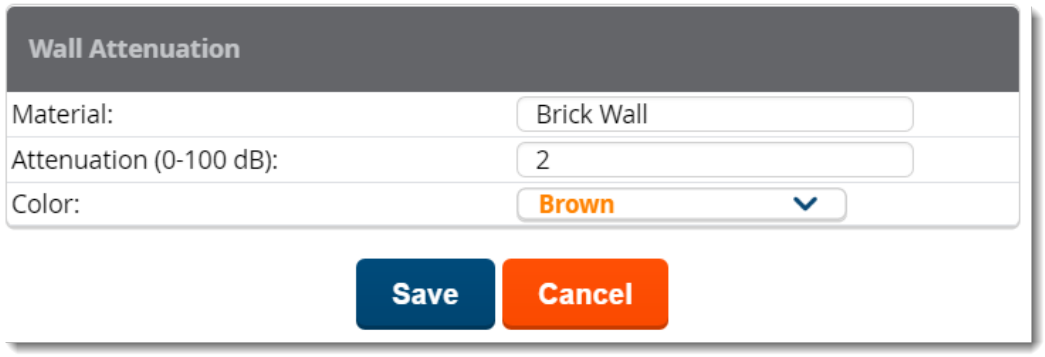
Adding a Wall Attenuation

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.

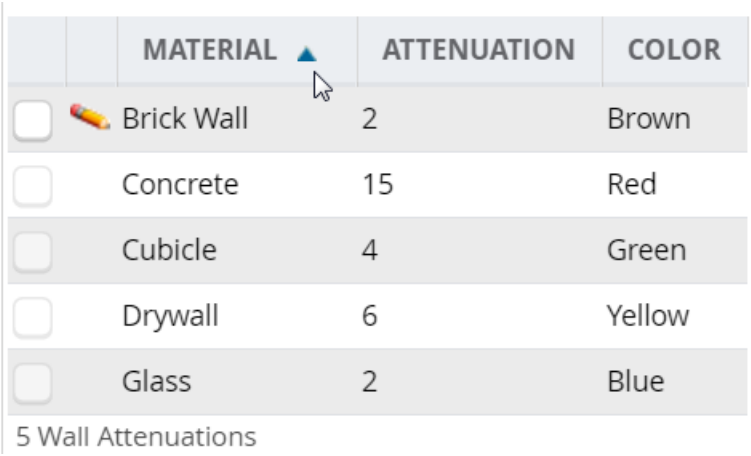
   Figure 293 shows an example of RF signal power decreasing by 3 db of attenuation for brick walls.

Figure 293: *Adding a Wall Attenuation*



5. Click **Save**. The brick wall attenuation you added in Step 4 displays in the Wall Attenuation table.

Figure 294: *Wall Attenuation*



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.

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

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 **New 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 **New Building**.

3. When the **New Building** window appears, enter the following information:

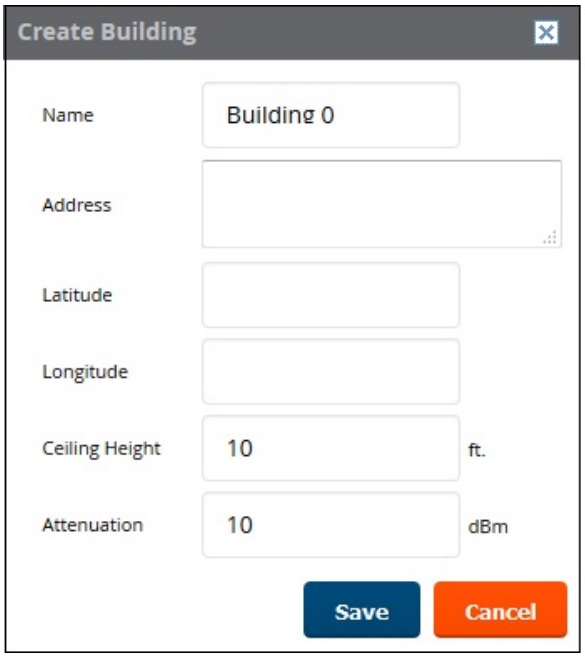
Table 154: *New Building Fields and Descriptions*

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 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 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 295: *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.

When importing a floor plan, ensure that the devices to be included are also available in the device catalog.

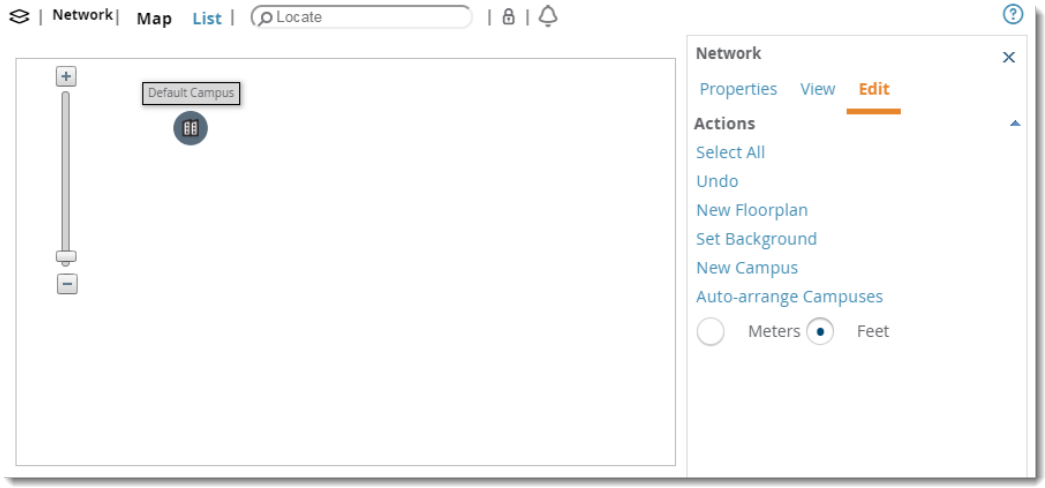
To add a floor plan:

1. Go 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. Right-click anywhere on the floor plan, then select **New Floorplan**. Or, you can 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.

Change Settings in Floor Plans

You can customize your floor plans in VisualRf by changing the settings on the **VisualRF > Floor Plans > Network >Edit** page. For example, options that determine whether floor plan measurements are in meters or feet are located at the bottom of the Edit task pane. Options to change backgrounds and replace floor plans are also available from the **Edit** taskpane.

Figure 296: *Setting the Unit of Measurement*



Editing a Floor Plan Image

There are several ways to edit a floor plan that you have uploaded, as explained in the following topics:

- "Replacing the Background" on page 390
- "Cropping the Floor Plan Image" on page 391
- "Sizing a Non-CAD Floor Plan " on page 392

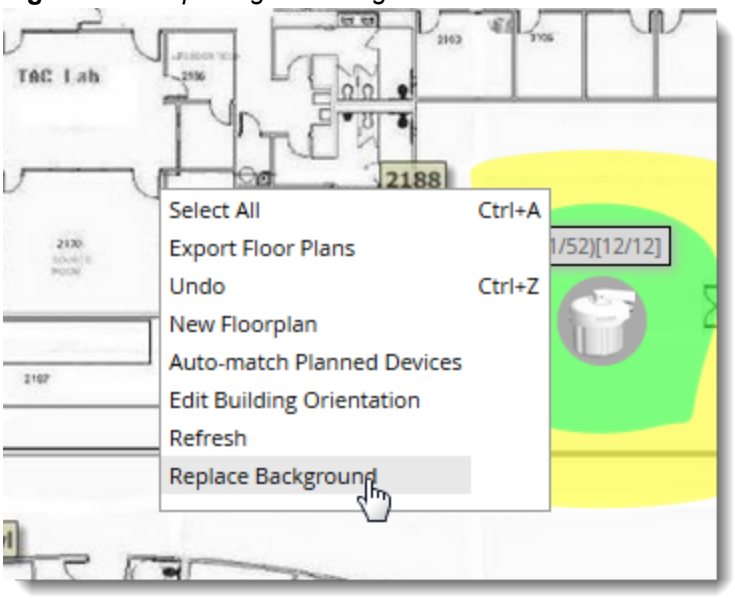
Replacing the Background

You can change your background when you update your floor plan and prefer not to delete the original floor plan and upload a new one.

To replace the background:

1. Navigate to **VisualRF > Floor Plans** and drill down into the network and campus maps to select the building floor plan you want to change.
2. Right-click anywhere on the floor plan, then select **Replace Background**.

Figure 297: *Replacing the Background*



3. Click **Browse** to find the image file in your hard drive, then click **Next**. AirWave applies the background to the floor plan.
4. Rescale and set the dimensions for the background.
5. Click **Finish**.

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 389.
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.

Decreasing the grid cell size will increase accuracy, but it also increase CPU consumption by the floor caching threads and the location caching threads. Check the **System > Performance** page to ensure your server is functioning properly when you make a change to this setting.

Other items worth noting:

- If this is a CAD file, then the Floor Plan creation wizard will automatically inherit height and width from the drawing.
- If this is a non-CAD file, then the height and width is zero.
- CAD files are converted to a JPG with a resolution of 4096 horizontal pixels at 100% quality prior to cropping. If you crop, then you will lose clarity.
- CAD files must be generated from AutoCAD and may not exceed 10 MB.
- Metric CAD files are supported.

- Importing GIF files for floor plans can result in blank 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.

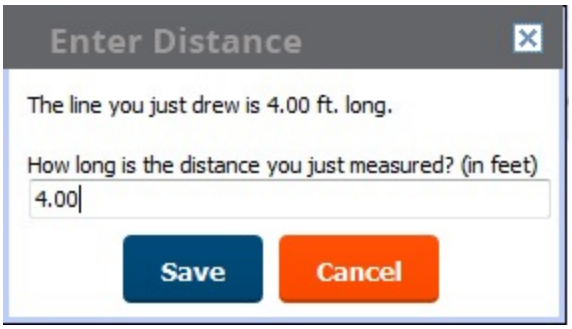
Sizing a Non-CAD Floor Plan

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 298.
5. Click **OK**.

Figure 298: *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 389.
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, Switches or Generic Markers onto the Floor Plan" on page 396 and "Adding Deployed APs onto the Floor Plan" on page 395.

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 155: *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.

Table 155: *Fields in the Region Properties Window (Continued)*

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 156. 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 156: *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.

Table 156: *Floor Plan Properties (Continued)*

Setting	Default	Description
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.

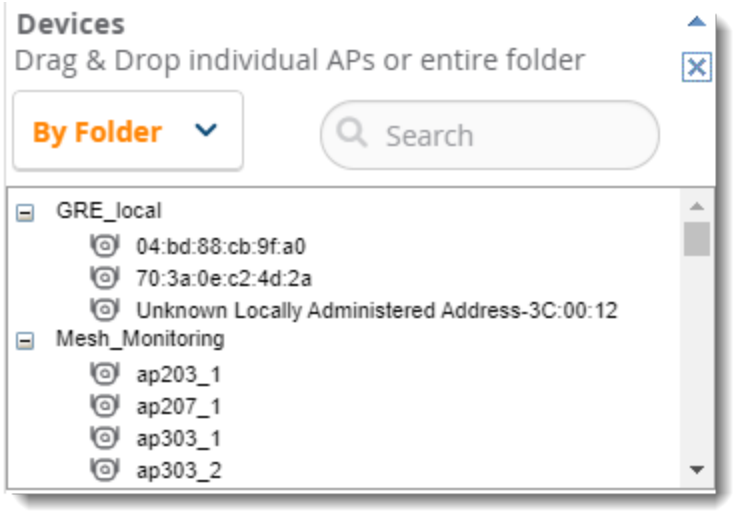
Adding Deployed APs onto the Floor Plan

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.

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 AirWave appears, as shown in Figure 299.
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 the proper location on the floor.
6. If you are adding APs to a floor using the Floor Upload wizard, click the **Finish** button.

Figure 299: *List of Deployed APs*



Adding Planned APs, Switches or Generic Markers onto the Floor Plan

You can plan for and provision new APs when you create a new floor plan, or add individual APs, switches or generic markers to an existing floor plan using the **Edit** menu for that floor.

Adding Planned Devices to a New Floor Plan

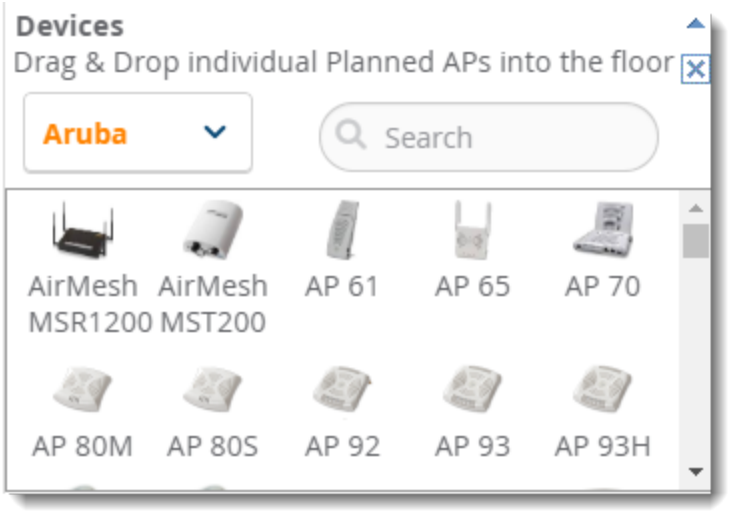
To add planned devices as you are creating a new floor plan:

1. **VisualRF > Floor Plans** page, then select **Campus > Building.**
2. Click the **Edit** menu and select New Floorplan.
3. Click **Choose File** and select a floorplan image file.
4. Specify campus, building and floorplan number and image, then click **Save**.
5. Once you have defined the scale, region and CAD layer information for the new floor, select **Access Points**.
6. Select **Add Planned APs**.
7. Click the **Type** drop-down menu and select the type of AP, switch or default marker you want to add to the floor plan.
8. If you are adding access points, select the number of APs or sensors of that device type you want to add.
9. Click **Add APs to Floorplan**.
10. Move the devices to the desired location on the floor plan.

Adding Planned Devices to an Existing Floor Plan

1. Go to the **VisualRF > Floor Plans** page, then click through **Campus > Building > Floor** to the floor plan.
2. Click **Edit** in the task pane.
3. Select **Add Planned Devices**.
4. Click the **Type** drop-down list and select a device type from the list of available devices, or use the Search utility.

Figure 300: *Available Planned Devices*



5. Drag and drop the AP, switch or generic marker to the desired location on the floor plan.
6. (Optional) If you are adding a generic marker, select the marker and enter a name and description for the marker in the **Properties** field.

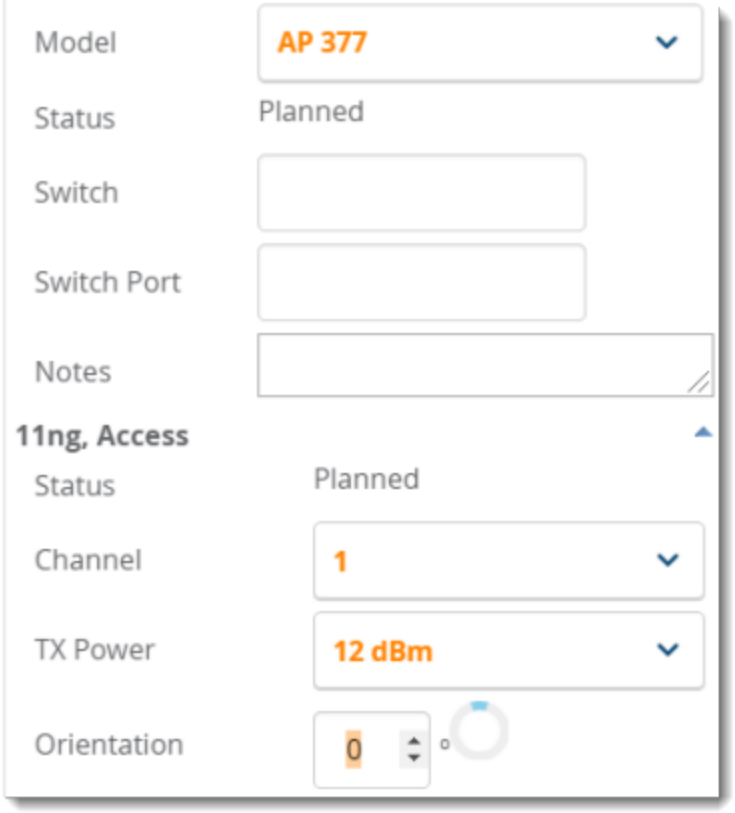
Configure Tilt Settings

VisualRF includes an addition **Orientation** setting to help you with planning and provisioning APs that point downward, or tilt at an angle.

1. Go to the **VisualRF > Floor Plans** page, then click through **Campus > Building > Floor** to the floor plan.
2. Adding Planned APs, Switches or Generic Markers onto the Floor Plan
3. Select the AP on the floor plan.
4. Locate the **Orientation** field in the **Properties** taskpane.
5. Set the angle of the AP by entering the degree or rotating the dial on the circle for both antennas (11ng and 11ac).

The example in Figure 301 shows the tilt orientation set to 180 degrees for the 11ng antenna on an AP-377.

Figure 301: *Configuring the AP Orientation*



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.

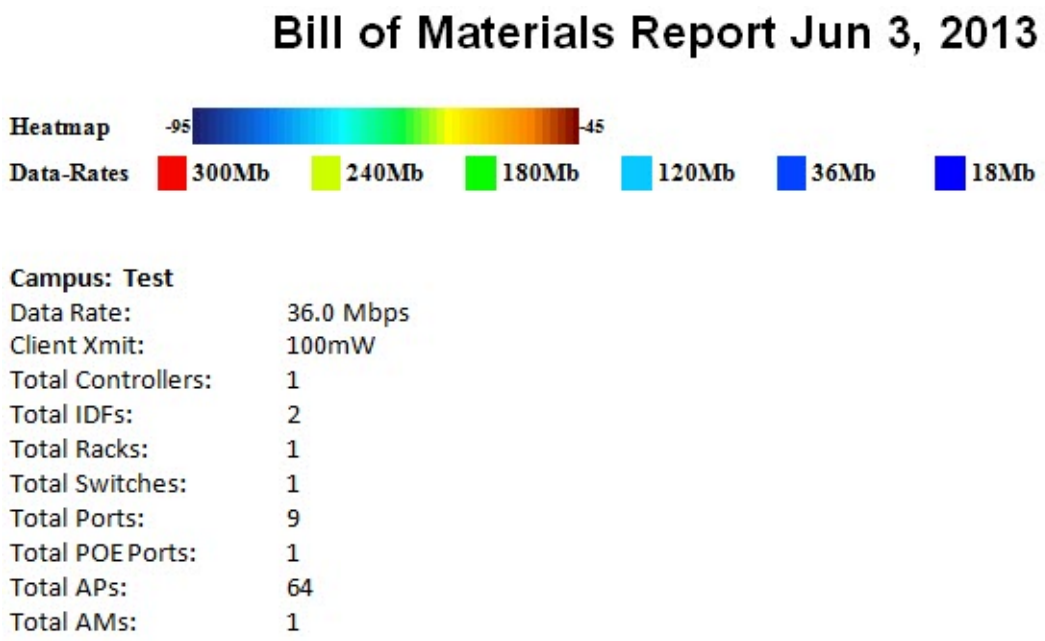
Printing a Bill of Materials Report

You can generate a Bill of Materials (BOM) Report from within VisualRF in Word format. The generated report includes a floor plan view with background grid lines.

To create a BOM report:

1. Navigate back to the Network view.
2. Right-click a campus icon, a building icon, or a builiding floor, then select **Bill of Materials**.
3. Select options such as show heatmap, speed, sensor coverage, wired range, and summary. You can include the kit, serial number, and notes.
4. Select **OK**. A BOM report appears in Microsoft Word as shown in Figure 302.

Figure 302: *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 157:

Table 157: *Elements Read From Controllers to Increase Location Accuracy*

MFG/Model	Client Signal Associated AP	AP-to-AP Signals (Dynamic Attenuation)	Unassociated Client Signal	Rogue AP Signal
Aruba	Yes	Yes	Yes	Yes
Cisco LWAPP	Yes	Yes	Yes	Yes
Cisco IOS	Yes	No	No	With WLSE
Cisco VxWorks	Yes	No	No	No
Trapeze	Yes	No	No	Yes
Meru	No	No	No	Yes

Table 157: *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

AirWave provides four main methods to increase accuracy once your access points are deployed:

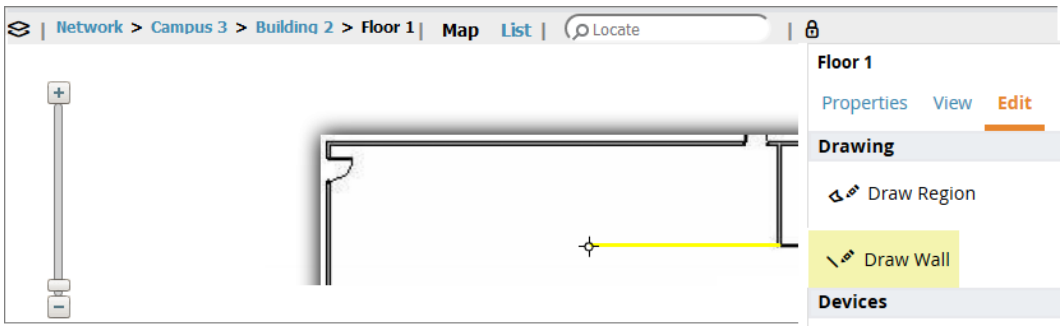
- Adding Exterior Walls - increases location accuracy by reducing the statistical probability of placements outside the office confines. See "Adding Exterior Walls" on page 400.
- Remote Client Surveys - provides additional attenuation inputs for corners and low-coverage areas without the burden of actually 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 303.

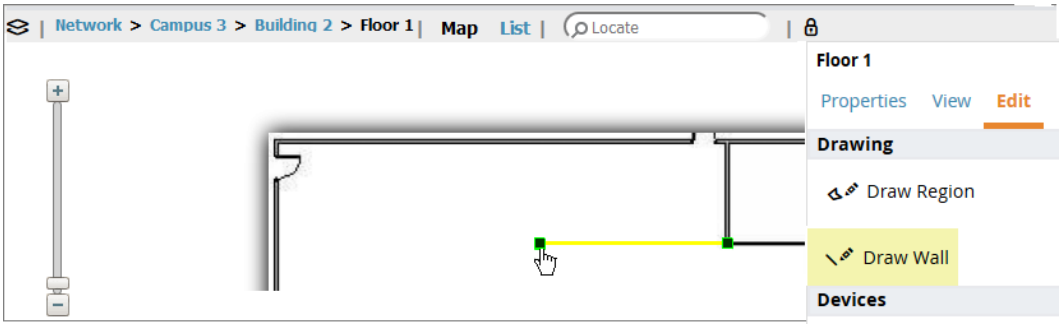
Figure 303: *Drawing a wall*



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 304.

Figure 304: *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.

NOTE

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.

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 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.

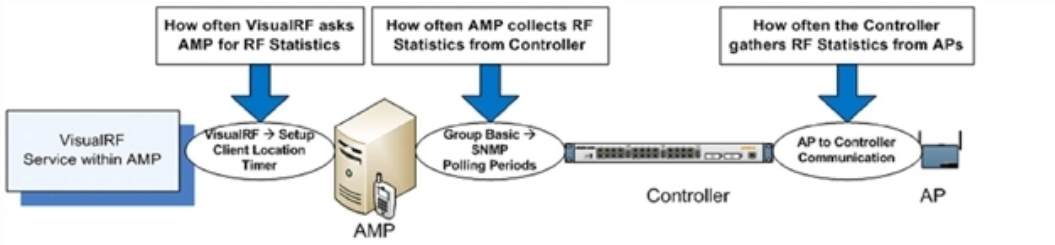
Enabling Dynamic Attenuation

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 AirWave queries those MIB entries, and how often VisualRF service queries AirWave for this RF information.

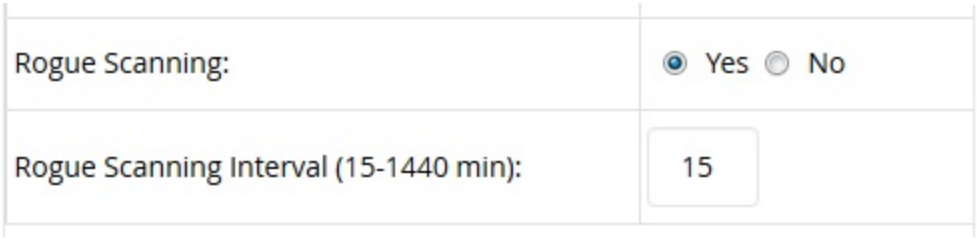
Figure 305: *Timing Factors Impacting Location Accuracy*



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 306.

Figure 306: *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 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 three radios can hear each client devices at -85 dBm or stronger.
- 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 307 for an example.

Figure 307: *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

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, click the VisualRF thumbnail, located next to the **Current Association** section at the bottom of the of this page (as shown in Figure 308). This opens a window that displays VisualRF data in a focused client view.

Figure 308: *VisualRF thumbnail in Clients > Client Detail*

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.

- Only the user in focus is displayed
- Only the access point in which the focus client is associated with is displayed
- The heatmap represents only the radio to which the client in focus is associated
- All rogues are off
- All client/rogue surveys are off
- Only lines shown are between the client to and its associated AP
- All labels are disabled

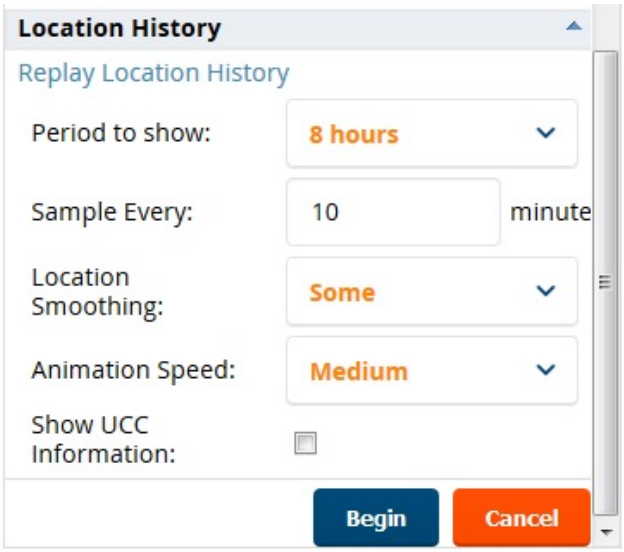
Tracking Location History

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 309, appears at the bottom of the VisualRF window.

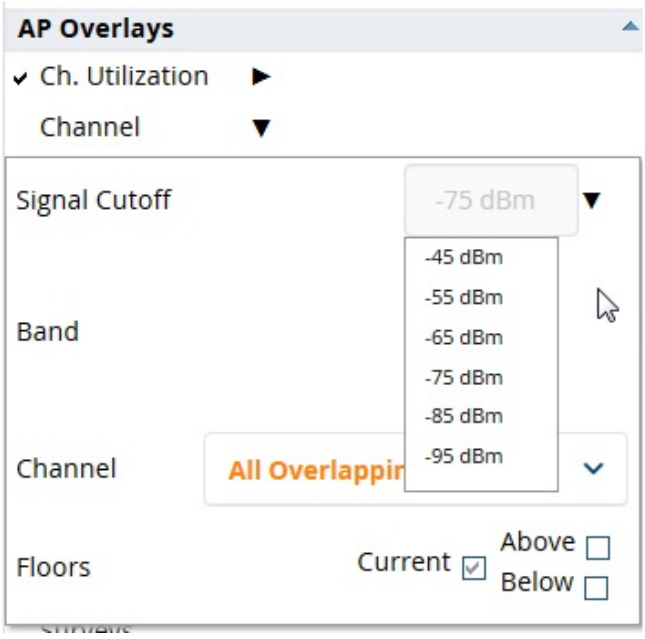
Figure 309: *Location History Player*



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 310. The heatmap updates immediately.

Figure 310: *Signal Cutoff dBm Dropdown Menu*



Viewing an AP's Wireless RF Environment

To view an access point's RF environment from **Devices > Monitor** page:

1. Select a device of interest from **Devices > List**, or any other AirWave page that lists your APs. The **Devices > Monitor** page opens.

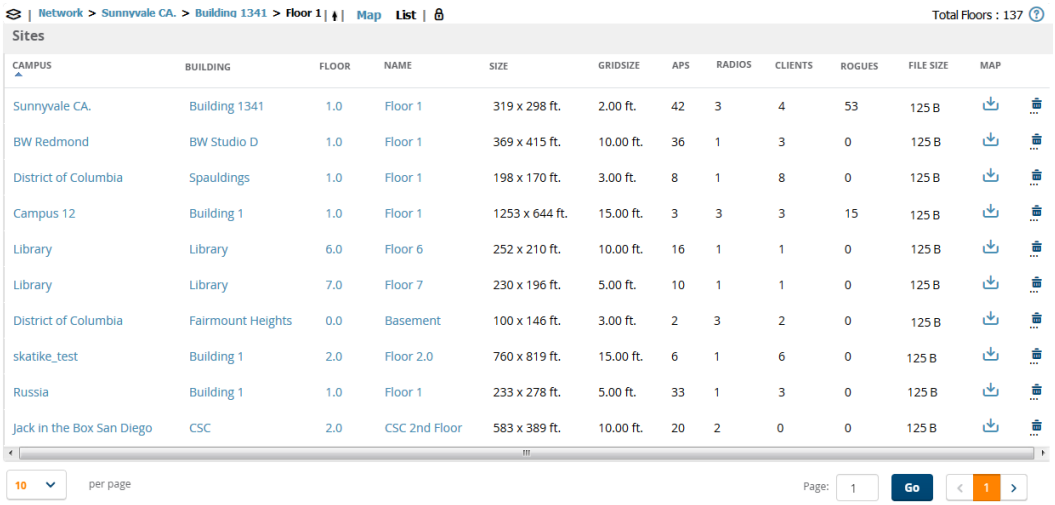
2. If the AP is associated with a floor plan, the page displays a VisualRF thumbnail showing the location of the AP. Click this thumbnail to open the floor plan in VisualRF.

Figure 311: *VisualRF Thumbnail on the **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 312: *Floor Plans List View*



The **VisualRF > Floor Plans** page provides a snapshot of how VisualRF is performing, as described in Table 158:

Table 158: *Floor Plans list columns*

Field	Description
Campus	Campus associated to the floor.
Building	Building associated to the floor.

Table 158: *Floor Plans list columns (Continued)*

Field	Description
Floor	Floor number. The decimal place can be used for mezzanine levels.
Name	Optional name of a floor. (If the name is not changed, it displays the name as Floor [Number] by default.)
Size	The height and width in feet of the floor plan, including white space.
Grid Cell Size	The size of the grid cells, in feet.
APs	The number of access points on the floor.
Radios	The number of radios associated with access points on the floor.
Clients	The number of wireless clients associated with access points on the floor. **NOTE:** Locating clients consumes significant VisualRF resources. A floor with hundreds or thousands of clients can take a long time to process.
Rogues	The number of rogue devices heard by access points on the floor. This number reflects the filters configured on the **VisualRF > Setup**. This means that while APs on the floor might hear more rogue devices, they are being filtered because of weak signal, they haven't been heard recently, or they are ad-hoc.
File Size	The floor plan background or image reported, in kilobytes. The larger the file, the longer it will take to render in the canvas.
Original Floor Plan	A link to download the original image background file.

Viewing a Network, Campus, Building's RF Environment

To view floors from a geographical perspective:

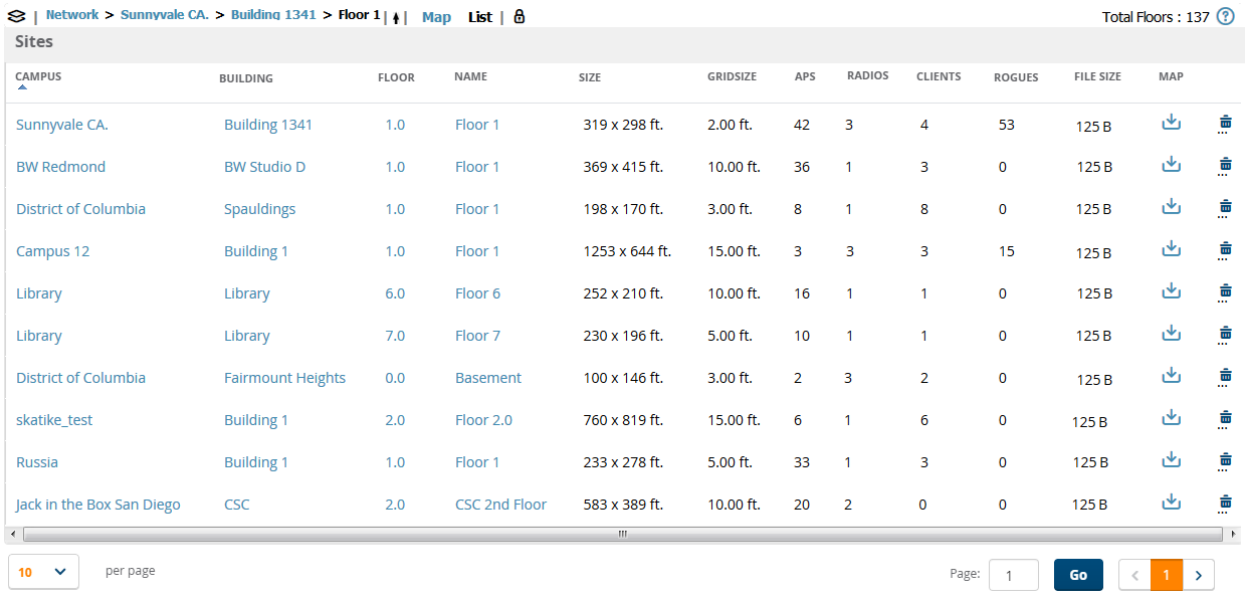
1. Navigate to the **VisualRF > Floor Plans** page.
2. Click on each network, campus, or building successively to drill down further until you reach the floor plan. This navigation provides information in each view as follows:
   - Network View - Contains all campuses within your WLAN
   - Campus View - All buildings within a campus
   - Building View - All floors within a building
   - Floor Plan View - All regions and 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 313, 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 313: *Network List View*



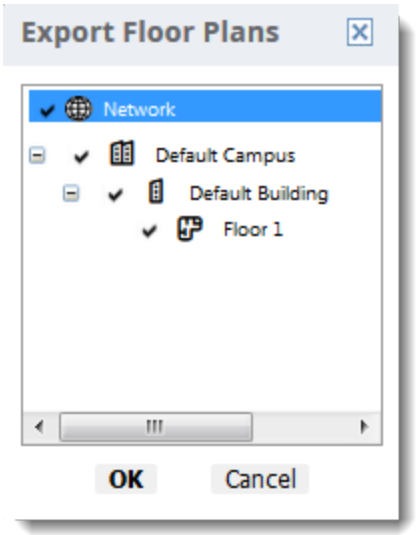
3. Click any of the links to view that location, or click a column heading to sort the list by that column criteria. The **Original Floor Plan** column contains links to download the floor plan graphic for the selected floor.
4. To return to the Map view, click the **Map** link at the top right of the page.

Importing and Exporting in VisualRF

You can export a floor plan from a building view, or an individual floor plan view, and import the file later into another AirWave server.

To export a floor plan:

1. Navigate through the Network view and select the campus, building or floor that you want to view. Or you can work from the List view and click the blue **Building**, **Floor**, or **Name** links to make your selections.
2. Right-click to choose **Export Floor Plans** from the shortcut menu.
3. Select a campus, building, or floor to export, then click **OK**.



4. Select **Save File** to save the **backup.zip** file to your local hard drive.

5. Click **OK**.

At this point, you can deploy a production AirWave and manage devices by importing your exported floor plan. For more information, see "Adding a Floor Plan" on page 389.

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. Select **Browse** to launch the File Explorer Window.
5. Select the zip file containing the upload instructions and click the **Open** button. The **File Explorer** Window will disappear, and you will return to the **Batch Floor Upload Wizard**.
6. Select **Next**.
7. The application validates the following information
   - Well-formed XML
   - All drawing files are accessible
   - All APs are present
   - All Building and Campuses are present
8. If there are any errors, none of the floor plans are created.

Post Processing Steps

1. Decrease the Location Caching Timer to previous value.
2. Review the **VisualRF > Floor Plans** page to ensure server is keeping up.

Sample Upload Instruction XML File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<visualrf:site_batch xmlns:visualrf="http://www.airwave.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1" origin="lower-left">
        <floor name="1st Floor" number="43" building-name="Library" campus-name="University">
                <image filename="blueprint1.dwg"/>
                <access-points>
                        <access-point name="ART.1.1" x="190.26" y="222.31"/>
                        <access-point name="ART.1.2" x="136.12" y="208.60"/>
                        <access-point name="ART.1.3" x="75.02" y="221.47"/>
                        <access-point name="ART.1.4" x="73.41" y="132.48"/>
                        <access-point name="ART.1.9" x="196.67" y="98.34"/>
                        <access-point name="ART.1.8" x="179.07" y="55.97"/>
                        <access-point name="ART.1.7" x="119.64" y="56.12"/>
                        <access-point name="ART.1.6" x="74.53" y="56.36"/>
                        <access-point name="ART.1.5" x="59.18" y="38.01"/>
                </access-points>
        </floor>
        <floor name="2nd Floor" number="44" building-name="Library" campus-name="University">
                <image filename="blueprint2.dwg"/>
                <access-points>
                        <access-point name="ART.2.12" x="196.31" y="92.19"/>
                        <access-point name="ART.2.11" x="204.82" y="55.78"/>
                        <access-point name="ART.2.10" x="133.08" y="55.81"/>
                        <access-point name="ART.2.9" x="73.79" y="55.78"/>
                        <access-point name="ART.2.8" x="73.72" y="104.26"/>
                        <access-point name="ART.2.7" x="73.91" y="134.88"/>
                        <access-point name="ART.2.6" x="73.83" y="162.72"/>
                        <access-point name="ART.2.5" x="73.82" y="183.61"/>
                        <access-point name="ART.2.4" x="63.74" y="125.48"/>
```

```
                </access-points>
        </floor>
</visualrf:site_batch>
```

Common Importation Problems

- Improper or undefined UNITS or MEASURE
- Text embedded into the Model view which causes an inconsistent bounding box
- Large dimensions which cause grainy resolution upon zoom
- Legacy CAD versions prior to Release 15 or AutoCAD 2000.

Importing from an Aruba Controller

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into an Aruba controller.

Pre-Conversion Checklist

Prior to importing floor plans, ensure that 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 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 AirWave

1. Navigate to **VisualRF > Import**.
2. Select the **Import floor plans from an Aruba/ Controller** link.
3. Select the **Begin Importing Floor Plans** link.
4. When prompted for input file, use the file saved from the controller process.

Importing from Ekahau Backups

If you use Ekahau 9.2 for Wi-Fi planning and site surveying, you can import data from a backup into VisualRF.

Before you begin

To ensure a seamless import:

- Configure the manufacturer and model of your APs in Ekahau.
- Check your memory allocation by going to the **VisualRF > Setup**. We recommend the following allowance:

  .5 GB for 1 to 75 floor plans, 1 GB for 76 to 250 floor plans, 1.5 GB for 251 to 500 floor plans, and 2 GB for 501 to 1,000 floor plans.

To import from your backup:

1. Navigate to **VisualRF > Import**, then click "Import Floor Plans From a Ekahau Backup".

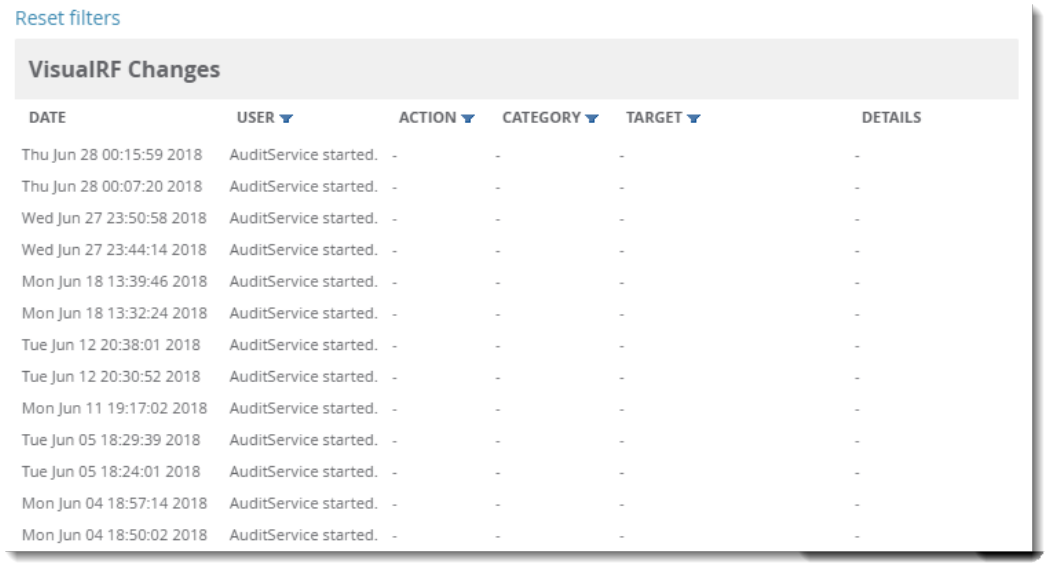
2. Click "Begin Importing Floor Plans".
3. Follow the onscreen instructions and wait for the process to finish completely.

Using the VisualRF Audit Log

You can changes to VisualRF in the audit log by navigating to **VisualRF > Audit Log**. AirWave records when the change occurred, who made the change, and details about the change event, as shown in Figure 314.

If you apply filters to your view, click **Reset filters** at the top of the page to go back to the unfiltered view.

Figure 314: *VisualRF Audit Log*



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 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 AirWave service on the Web. You can use VisualRF Plan to do basic planning procedures like adding a floor plan, provisioning APs, and generating a Bill of Materials (BOM) report. VisualRF Plan is free to use for anyone with an Aruba support account. No license is required.

The client can be downloaded from the Aruba Support Portal.

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

If installing VisualRF Plan on a VMware virtual machine hosted by a Mac computer, you must disable **Folder Sharing.**

After you have downloaded VisualRF Plan from the Aruba support site, the installer will prompt you for the location of the data directory. You must have access to the directory you choose for the installation. Also choose a directory for auto-backup. (The default is the user directory.) Follow the rest of the instructions on your installation screen.

Table 159: *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	
View deployed switches	X	
View signal strength	X	
Planning and provisioning	X	X
Import and Export	X	X

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.
- 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

To set up a scan, refer to "How to Set Up Device Discovery" on page 130.

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

- **Aruba WIP**—Wireless Intrusion Protection (WIP) module integrates wireless intrusion protection into the mobile edge infrastructure. The WIP module provides wired and wireless AP detection, classification and containment; detects DoS and impersonation attacks; and prevents client and network intrusions.
- **Cisco WLSE** (1100 and 1200 IOS)—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 AirWave.
- **AirDefense**—Uses the AirWave XML API to keep its list of managed devices up to date.
- **WildPackets OmniPeek**—Retrieves a list of managed APs from AirWave.

Viewing RAPIDS Summary

The **RAPIDS > Overview** page displays pie charts and device counts by RAPIDS classifications (see Figure 315). Clicking the hyperlinks opens the RAPIDS list for the selected classification.

Figure 315: *RAPIDS > Overview Page*

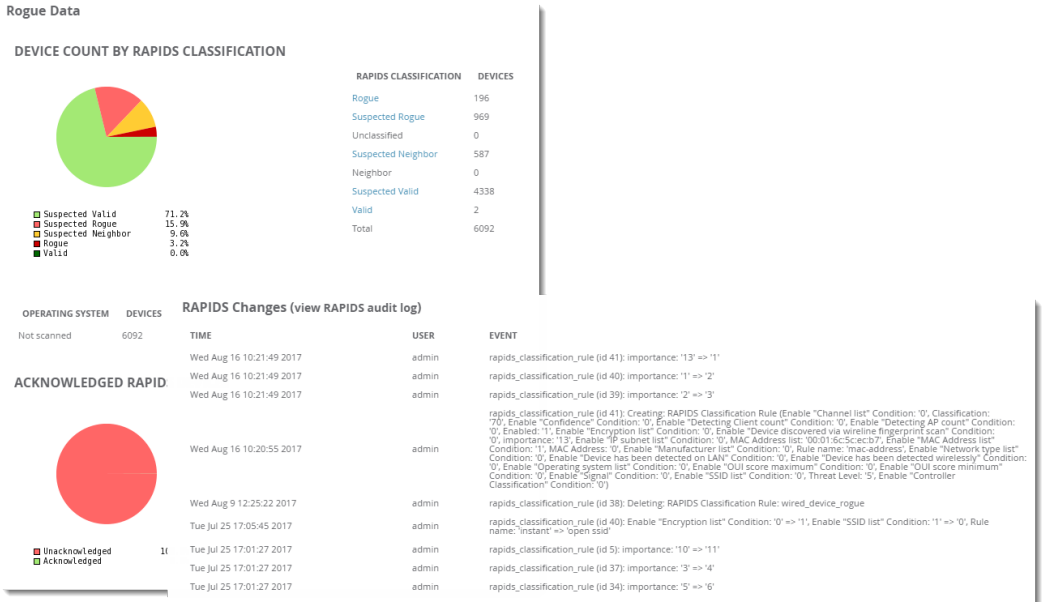


Table 160 defines the summary information that appears on the page.

Table 160: *RAPIDS > Overview Fields and Descriptions*

Summary	Description
Device Count by RAPIDS Classification	A pie chart of rogue device percentages by RAPIDS classification.
RAPIDS Classification	A summary list with details of the statistics depicted in the Device Count by RAPIDS Classification pie chart. Click the linked classification name to be taken to a filtered rogue list.
RAPIDS Devices by OS	A pie chart of RAPIDS percentages by the detected operating system.
Operating System	Detected operating systems represented in this summary listing. Click on the linked Operating System name to see the rogues list filtered by that classification. OS scans can be run manually or enabled to run automatically on the **RAPIDS > Setup** page.
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 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 AirWave will process rogues.

Refer to the following sections:

- "RAPIDS Setup" on page 417
- "Additional Settings" on page 420

RAPIDS Setup

Basic Configuration

On the **RAPIDS > Setup** page, the **Basic Configuration** section allows you to define RAPIDS behavior settings.

Figure 316: *Basic Configuration Settings*

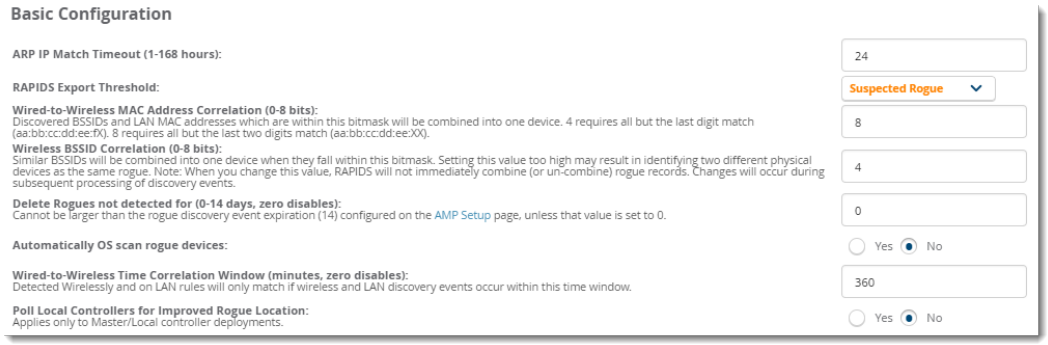


Table 161: *RAPIDS > Setup > Basic Configuration Fields and Default Values*

Field	Default	Description
ARP IP Match Timeout (1-168 hours)	24	If you have routers and switches on 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.

Table 161: *RAPIDS > Setup > Basic Configuration Fields and Default Values (Continued)*

Field	Default	Description
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

The classification option settings determine how AirWave acknowledges rogues and classifies them.

Figure 317: *Classification Options*

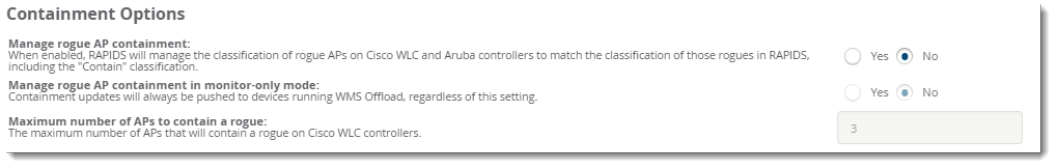
Table 162: *RAPIDS > Setup > Classification Options Fields and Default Values*

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, AirWave can shield rogue devices from associating to Cisco WLC controllers (versions 4.2.114 and later), and Aruba controllers (running ArubaOS versions 3.x and later). AirWave will alert you to the appearance of the rogue device and identify any mismatch between controller configuration and the desired configuration.

Figure 318: *Containment Options*



WMS Offload is not required to manage containment in AirWave.

Table 163: *RAPIDS > Setup > Containment Options Fields and Default Values*

Field	Default	Description
Manage rogue AP containment	No	Specifies whether RAPIDS will manage the classification of rogue APs on Cisco WLC and Aruba controllers to match the classification of those rogues in RAPIDS. This includes the "Contained" classification. If this setting is enabled, then the **Maximum number of APs to contain a rogue** setting can be configured. Similarly, if this is enabled, then the Contained Rogue option will appear in the classification drop down menu when you add a new classification rule. (See "Viewing and Configuring RAPIDS Rules" on page 422 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.

Figure 319: *Filtering Settings*

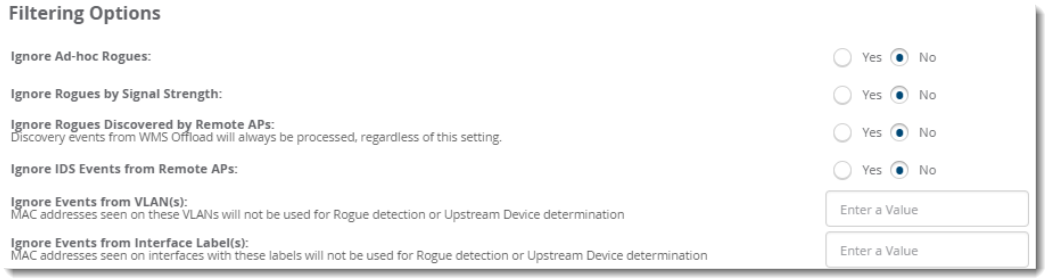


Table 164: *RAPIDS > Setup > Filtering Options Fields and Default Values*

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 AirWave to drop all rogue discovery information coming from remote APs.

Table 164: *RAPIDS > Setup > Filtering Options Fields and Default Values (Continued)*

Field	Default	Description
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 AirWave User Roles" on page 41.

Defining RAPIDS Rules

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

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

This section contains the following topics:

Controller Classification with WMS Offload

This classification method is supported only when WMS offload is enabled on Aruba WLAN switches. Controller classification of this type remains distinct from RAPIDS classification. WLAN switches feed wireless device information to AirWave, which AirWave then processes. 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.

RAPIDS classification is not pushed to the devices.

The following table compares how default classification may differ between AirWave and ArubaOS for scenarios involving WMS Offload.

Table 165: *Rogue Device Classification Matrix*

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 *AirWave 8.2.11.1 Best Practices Guide* on the **Home > Documentation** page.

Device OUI Score

The Organizationally Unique Identifier (OUI) score is based on the LAN MAC address of a device. RAPIDS can be configured to poll your routers and switches for the bridge forwarding tables. RAPIDS then takes the MAC addresses from those tables and runs them through a proprietary database to derive the OUI score. The OUI score of each device is viewable from each rogue's detail page. Table 166 provides list the OUI scores definitions.

Table 166: *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

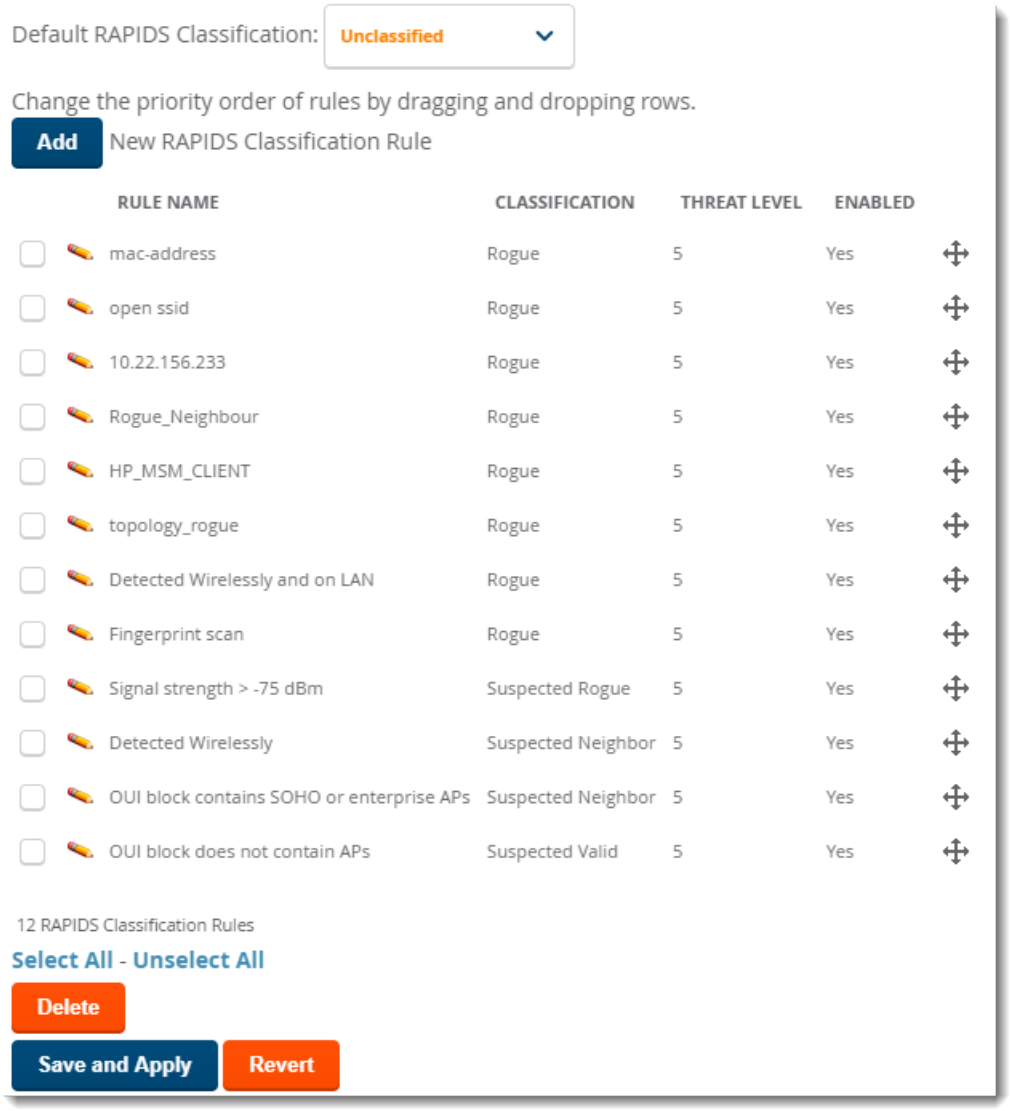
The threat level classification adds granularity for each general RAPIDS classification. Devices of the same classification can have differing threat scores based on the classifying rule, ranging from 1 to 10 with a default value of **5**. This classification process can help identify the greater threat. 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

AirWave displays RAPIDS rules on the **RAPIDS > Rules** page (Figure 320). By default, rogues that don't match any rules are unclassified, but you can set the default classification using the Default RAPIDS Classification drop-down menu at the top of the page.

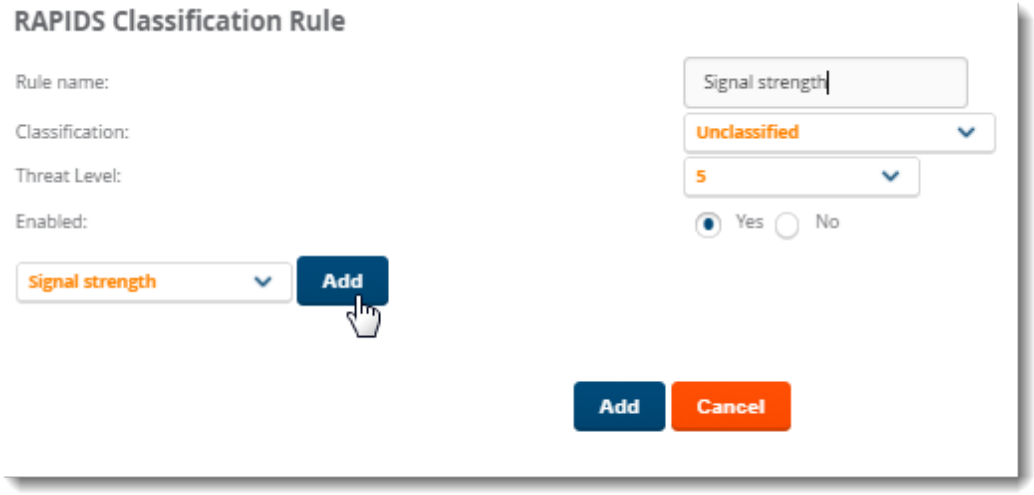
Figure 320: *RAPIDS > Rules Page*



To create a new RAPIDS classification rule:

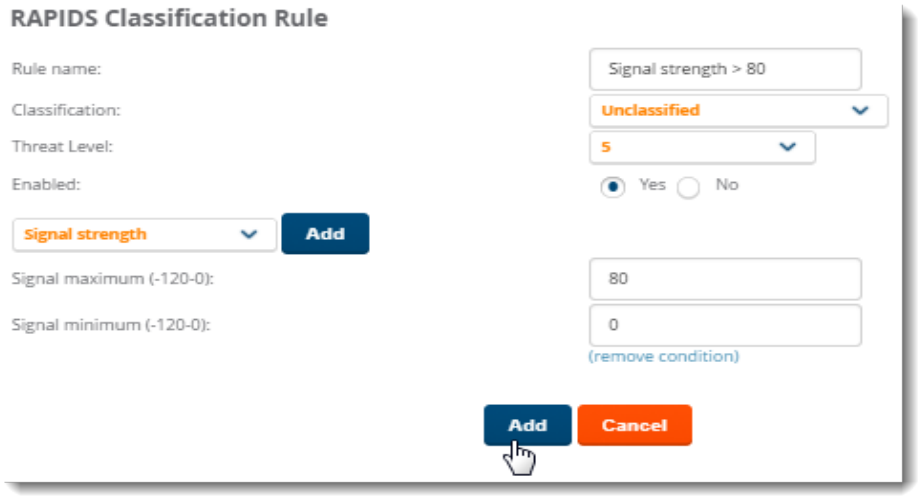
1. Navigate to **RAPIDS > Rules**, then select the **Add**.
2. Enter a name for this RAPIDS classification rule. Rule names should describe your rule's core purpose.
3. Select the classification that a device will receive if rules are met.
4. Select the threat level for the rogue device. See "Rogue Device Threat Level" on page 421 for additional information.
5. Select a rule from the drop-down menu, then click **Add**. Rule conditions become available for you to configure.

Figure 321: *Adding a Rule Condition*



6. Repeat Step 5 to create additional rule conditions. Figure 322 shows a condition being created for a maximum signal strength of 80 dBm
7. Click **Add** at the bottom of the page.

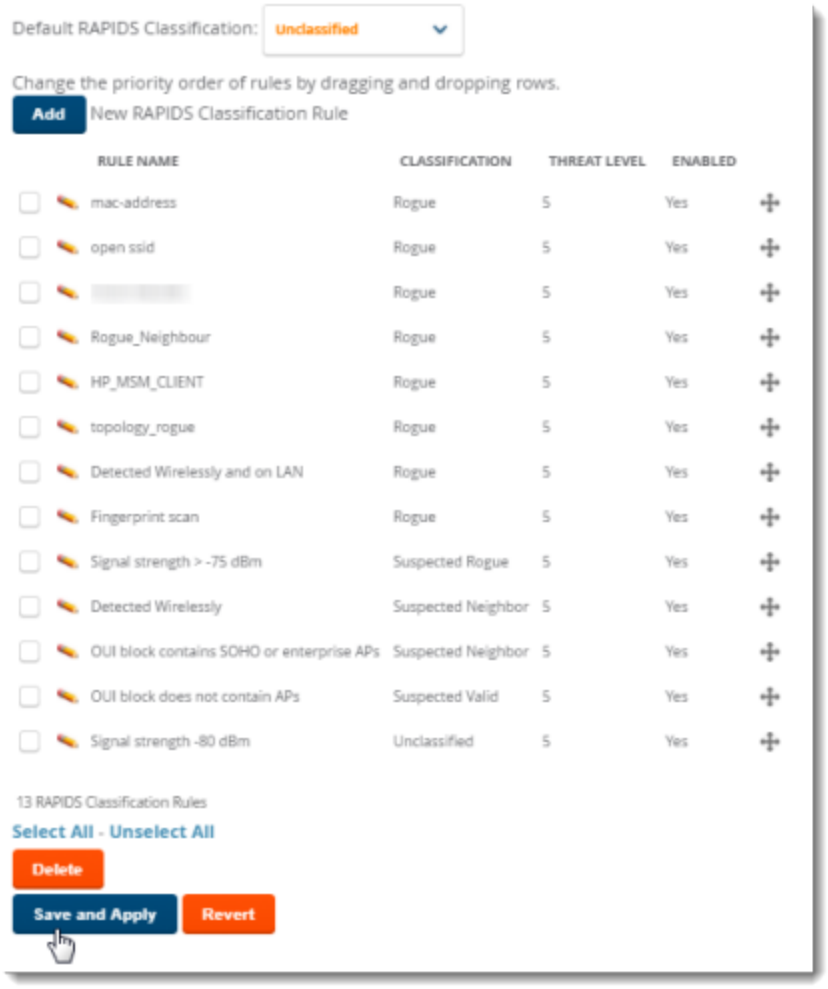
Figure 322: *Creating a Rule for Signal Strength*



AirWave displays the newly created rule on the Rules page.

Figure 323:

Figure 324: *Newly Created Signal Strength Rule*



8. Click **Save and Apply** to have the new rule take effect.

RAPIDS Classification Rule Properties

Table 167 defines the properties that you can add to a RAPIDS classification rule.

Table 167: *Rule Properties*

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.**

Table 167: *Rule Properties (Continued)*

Option	Description
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, AirWave processes only alpha-numeric characters and the asterisk wildcard character (*****). 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.
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.
Aruba Controller Properties	
Controller Classification	Rogue matches the specified controller classification.
Confidence	Rogue falls within a specified minimum and maximum confidence level, ranging from 1 to 100.

Deleting or Editing a Rule

To delete a rule:

1. Go to the **RAPIDS > Rules** page.
2. Select the check box next to the rule you want to delete, and click **Delete**. Or, click to apply changes to a rule, then click **Save**.

Changing the Rule Priority

To change the sequence in which rules apply to any rogue device, drag and drop the rule to a new position in the rules sequence.

Recommended RAPIDS Rules

- **If Any Device Has Your SSID, then Classify as Rogue**

  The only devices broadcasting your corporate SSID should be devices that you are aware of and are managed by AirWave. Rogue devices often broadcast your official SSID in an attempt to get access to your users, or to trick your users into providing their authentication credentials. Devices with your SSID generally pose a severe threat. This rule helps to discover, flag, and emphasize such a device for prompt response on your part.
- **If Any Device Has Your SSID and is Not an Ad-Hoc Network Type, then Classify as Rogue**

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

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

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

Using RAPIDS Rules with Additional AirWave Functions

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

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

Viewing Rogues

There are several ways to view rogue devices, listed by rogue classification.

To view the list of rogue devices:

- Click the rogue count in the header statistics at the top of the AirWave WebUI.

- Go to **RAPIDS > Overview**, then click the RAPIDS classification link.
- Go to **RAPIDS > List** and select a RAPIDS classification from the drop-down menu, as shown in Figure 325.

You can sort the table columns by selecting the column head. Most columns can be filtered by clicking the funnel icon . The hyperlinks on this page open additional pages for RAPIDS configuration or device processing.

Predefined, Default Views for Rogue Devices

AirWave displays a default view for rogue devices on the **RAPIDS > List** page. Default views have predefined columns that cannot be modified.

Figure 325: *Predefined, Default Views for Rogue Devices*

Table 168 describes the information displayed in the default view.

Table 168: *Default View for Rogue Devices*

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 AirWave user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 417).
RAPIDS Classification	Displays the RAPIDS classification of the discovered device, including: valid, suspected valid, neighbor, suspected neighbor, unclassified, suspected rogue, rogue, and contained rogue. RAPIDS classifies the discovered devices based on rules that you customize on the **RAPIDS > Rules** page (see "Defining RAPIDS Rules" on page 420).
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 421. The threat level is also supported with Triggers (see "Using the System Pages" on page 305).
Name	Displays the alpha-numeric name of the rogue device, as known. By default, AirWave assigns each rogue device a name derived from the OUI vendor and the final six digits of the MAC address. Clicking the linked name will redirect you to the **RAPIDS > Detail** page for that rogue device. Refer to "Overview of the RAPIDS > Detail Page" on page 430.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 422).

Table 168: *Default View for Rogue Devices (Continued)*

Column	Description
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.
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.
First Discovering AP	Displays when a rogue was first seen. You can sort on this field to decide whether to be concerned with the rogue.
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 AirWave. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.

Filtered Views for Rogue Devices

You can create a new view, or edit and copy a view, and save the view to access information you frequently use.

For more information on filtering data from your view, see "Creating Filtered Views" on page 150.

Table 169: *Additional Columns for Custom Views*

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 AirWave user has investigated them and determined that they are not a threat (see "RAPIDS Setup" on page 417).
Ch	Indicates the most recent RF channel on which the rogue was detected. **NOTE:** The rogue can be detected on more than one channel if it contains more than one radio.
Classifying Rule	Displays the RAPIDS Rule that classified the rogue device (see "Viewing and Configuring RAPIDS Rules" on page 422).
Confidence	The confidence level of the suspected rogue. How confidence is calculated varies based on the version of ArubaOS. When an ArubaOScontroller 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.
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.
Current Associations	The number of current rogue client associations to this device.
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.

Table 169: *Additional Columns for Custom Views (Continued)*

Column	Description
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.
First Discovering Time	Displays the time the rogue was first discovered.
Floor Coordinates	Displays the x and y coordinates taken from VisualRF for rogues.
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.
LAN MAC Address	The LAN MAC address of the rogue device.
LAN Vendor	Indicates the LAN vendor of the rogue device, when known.
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 AirWave. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.
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.
Max Associations	The highest number of rogue client associations ever detected at one time.
Model	Displays the model of rogue device, if known. This is determined with a fingerprint scan, and this information may not always be available.
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.
Notes	Indicates any notes about the rogue device that may have been added.
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.
Port	Indicates the physical port of the switch or router where the rogue was last seen.

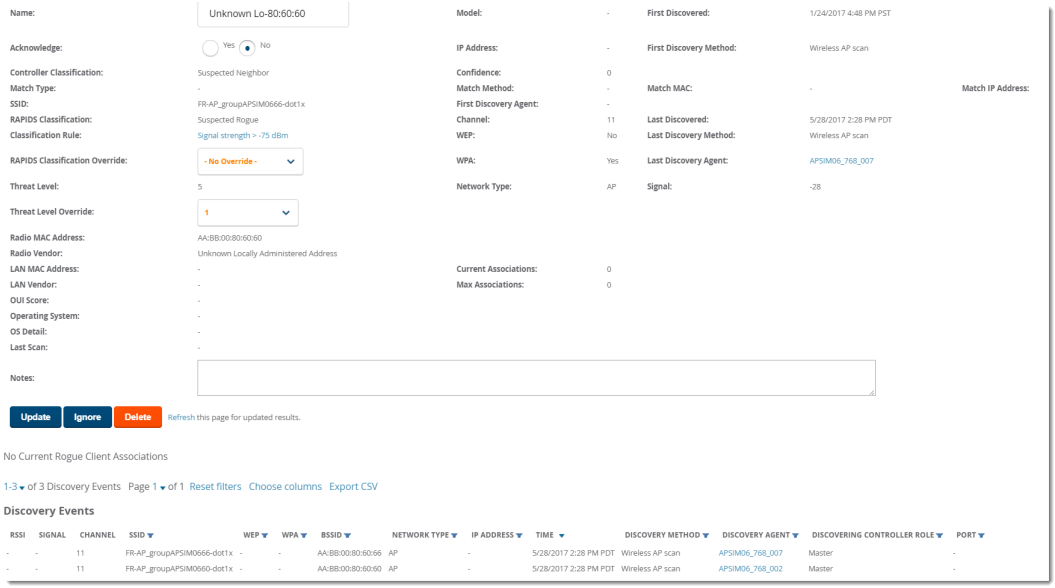
Table 169: *Additional Columns for Custom Views (Continued)*

Column	Description
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.
RSSI	Displays the signal strength in dBm. In AirWave, the signal strength is a calculation based on RSSI measurements received in the radio signal from the AP. This RSSI data is relative and varies by AP.
Signal	Displays the strongest signal strength detected for the rogue device.
SSID	Displays the most recent SSID that was heard from the rogue device.
Switch/Router	Displays the switch or router where the device's LAN MAC address was last seen.
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 421. The threat level is also supported with Triggers (see "Using the System Pages" on page 305).
Wired	Displays whether the rogue device has been discovered on one of your wired networks by polling routers/switches, your SNMP/HTTP scans, or Aruba WIP information. This column displays **Yes** or is blank if wired information was not detected.
WMS Classification AP	The AP that provided the information used to classify the device. Click the linked device name to be redirected to the **Devices > Monitor** page for that AP.
WMS Classification Date	The date that WMS set the classification.

Overview of the RAPIDS > Detail Page

Clicking a hyperlink in the **Name** column on the **RAPIDS > List** page opens a detailed view for the selected device (Figure 326).

Figure 326: *RAPIDS > Detail Page*



Important Considerations

Keep in mind the following considerations when working with rogue devices:

- Users with the role of **Admin** can see all rogue AP devices.
- Users with roles limited by folder can see a rogue AP if there is at least one discovering device that they can see.
- 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.
- 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.
- 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.

Filter the Device Data

You can use filters to narrow results or work with large amounts of data.

To filter the device data:

- Use global filtering options on the **RAPIDS > Setup** page to filter rogue devices according to signal strength, ad-hoc status, and discovered by remote APs.
- Click to filter columns in the **Discovery Events** table .

Update Rogue Devices

In addition to updating the **Name** and **Notes** fields to identify the AP and document its location, you can:

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 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 AirWave processing.

Viewing Ignored Rogue Devices

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

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

Using RAPIDS Workflow to Process Rogue Devices

One suggested workflow for using RAPIDS is as follows:

- Start from the **RAPIDS > List** page. Sort the devices on this page based on classification type. Begin with Rogue APs, working your way through the devices listed.
- Select **Modify Devices**, then select all devices that have an IP address and select **Identify OS**. AirWave performs a port scan on the device and attempts to determine the operating system. (See "Setting Up RAPIDS" on page 417.)

  You should investigate devices running an embedded Linux OS installation. The OS scan can help identify false positives and isolate some devices that should receive the most attention.
- Find the port and switch at which the device is located and shut down the port or follow wiring to the device.
- To manage the rogue, remove it from the network and acknowledge the rogue record. If you want to allow it on the network, classify the device as valid and update with notes that describe it.

Not all rogue discovery methods will have all information required for resolution. For example, the switch/router information, port, or IP address are found only through switch or router polling. Furthermore, RSSI, signal, channel, SSID, WEP, or network type information only appear through wireless scanning. Such information can vary according to the device type that performs the scan.

Score Override

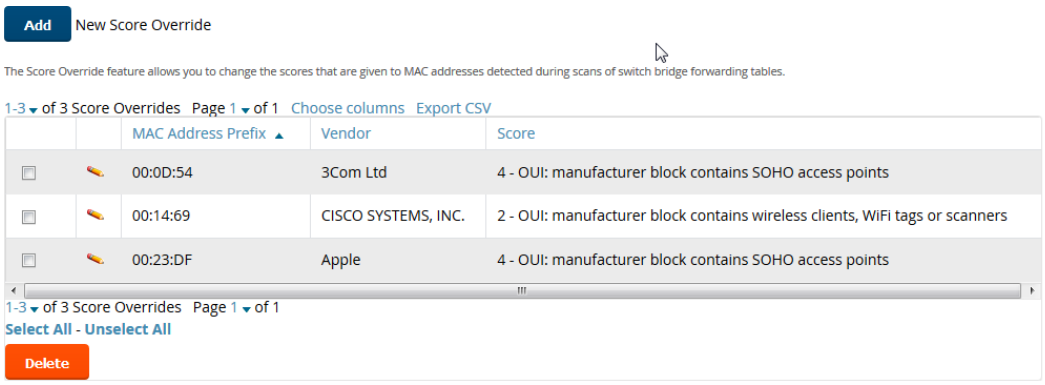
On the **RAPIDS > Score Override** page you can change the OUI scores that are given to MAC addresses detected during scans of bridge forwarding tables on routers or switches. Figure 327, Figure 328, and Table 170 illustrate and describe RAPIDS Score Override. Perform these steps to create a score override.

Once a new score is assigned, all devices with the specified MAC address prefix receive the new score.

Note that 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 327: *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 328).

Figure 328: *Add/Edit Score Override Page*

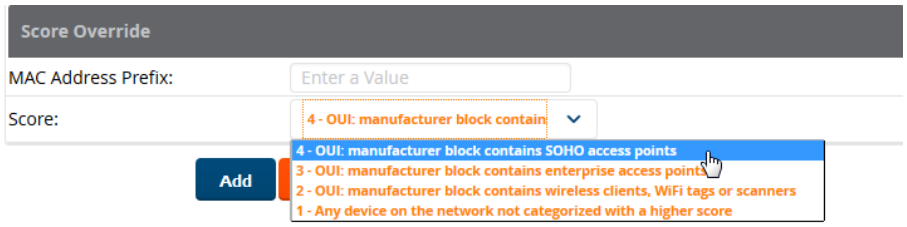


Table 170: *RAPIDS > Add/Edit Score Override Page Fields*

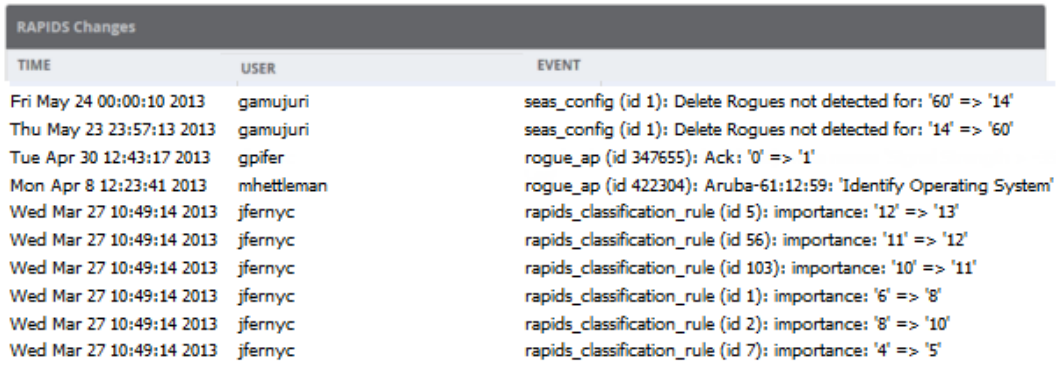
Field	Description
MAC Address Prefix	Use this field to define the OUI prefix to be re-scored.
Score	Use this field to set the score that a device, with the specified MAC address prefix, will receive.

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 329.

Figure 329: *Audit Log Page Illustration*



RAPIDS Changes

TIME	USER	EVENT
Fri May 24 00:00:10 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '60' => '14'
Thu May 23 23:57:13 2013	gamujuri	seas_config (id 1): Delete Rogues not detected for: '14' => '60'
Tue Apr 30 12:43:17 2013	gpifer	rogue_ap (id 347655): Ack: '0' => '1'
Mon Apr 8 12:23:41 2013	mhettleman	rogue_ap (id 422304): Aruba-61:12:59: 'Identify Operating System'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 5): importance: '12' => '13'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 56): importance: '11' => '12'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 103): importance: '10' => '11'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 1): importance: '6' => '8'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 2): importance: '8' => '10'
Wed Mar 27 10:49:14 2013	jfernyc	rapids_classification_rule (id 7): importance: '4' => '5'

Additional Resources

The following 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 Creating New Triggers.
- **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 350.

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

- "Configuring Security for Device Groups" on page 105
- "Configuring Cisco WLC Security Parameters and Functions" on page 123
- "Configuring SSIDs and VLANs for Device Groups" on page 110
- "Using the System Pages" on page 305

You can monitor multiple AirWave servers using the Master Console. After you add the AirWave servers to Master Console, they will be polled for basic 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 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 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 AirWave station. The **Master Console** or **Failover** server can also send email or NMS notifications about the event.

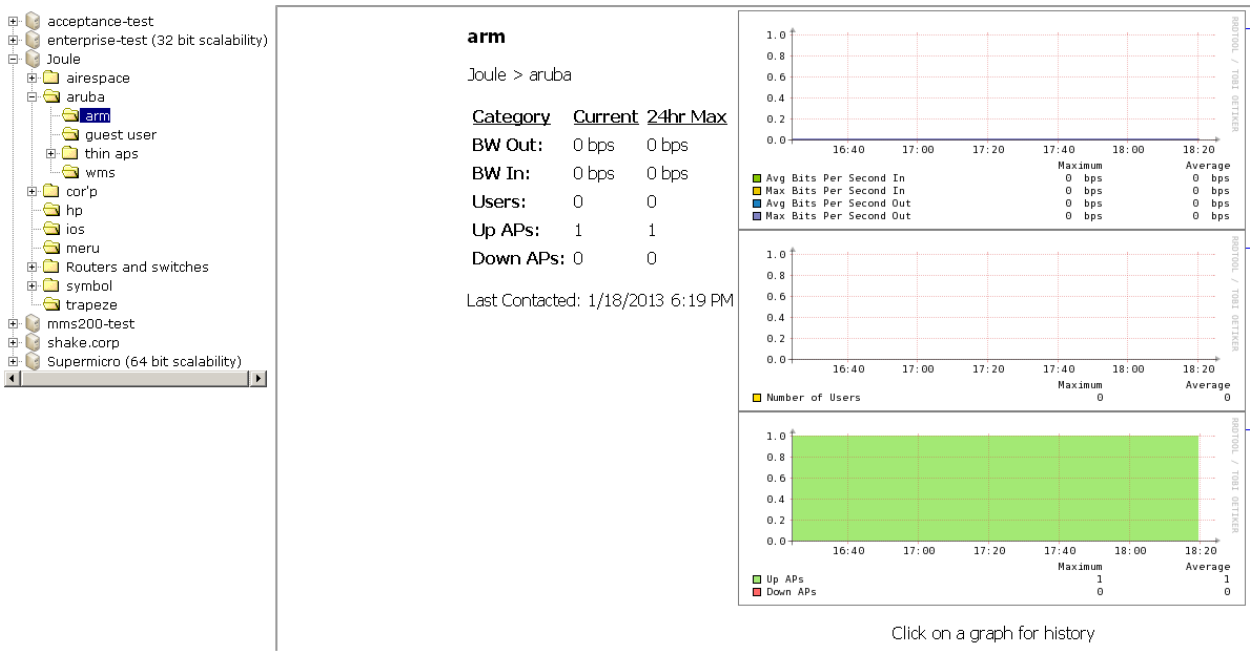
XML APIs are not supported on the Master Console.

If you have the Master Console license, you can also monitor your multiple AirWave servers using AirWave Glass. For more information, see the *AirWave Glass 1.2.3 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 AirWave. This feature is disabled by default for security reasons; no 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 AirWave, the public portal is disabled by default, regardless of the type of license.

Figure 330: *Public Portal Page Illustration*



The Public Portal supports configuration of the iPhone interface, which can be configured using the Master Console AirWave page.

Adding a Managed AMP with the Master Console

Perform the following steps to add a managed 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 171.

Table 171: *Managed AMP fields and default values*

Field	Default	Description
Hostname / IP Address	N/A	Enter the IP address or Hostname of the AirWave server to be managed.
Polling Enabled	Yes	Enables or disables the Master Console polling of managed AirWave server.
Polling Period	5 minutes	Determines how frequently the Master Console polls the managed AirWave server.
Username	N/A	The user name used by the Master Console to login to the managed AirWave server. The user needs to be an AP/Device Manager or AirWave Administrator.
Password (Confirm Password)	N/A	The password used by the Master Console to login to the managed AirWave server.
HTTP Timeout (5-1000 sec)	60	Defines the timeout period used when polling the managed AirWave server.

Table 171: *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 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 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 AirWave User Guide, except that there is no process by which templates can be fetched from devices in the subscriber group on managed 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 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 AirWave servers; make sure that the **Manage Group Configuration** option is enabled for each managed AirWave.

Once Global Groups have been configured on the **Master Console**, groups must be created or configured on the managed 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 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 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 AirWave User Guide"Using Device Groups" on page 81.

Enabling FIPS 140-2 Approved Mode

Users who are subject to government or industry regulations must enable FIPS 140-2 approved mode when using AirWave. When FIPS 140-2 approved mode is on, users can connect to the 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 AirWave server reboots automatically after it turns on FIPS mode.

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

You can access the CLI through an SSH connection by logging in to the AirWave server with the admin user created when you install or upgrade your software to AirWave 8.2.11.1. For information about the admin user, see the *AirWave 8.2.11.1 Installation Guide*.

When the database is down and you access the CLI through an SSH connection, AirWave will skip the click through agreement and advance to the AMP CLI menu.

CLI Options

Table 173 lists the CLI commands that are available in AirWave 8.2.11.1. If there are other important tasks that you can't do from the CLI, contact technical support for help.

Table 172: *CLI Options*

Option	Description
1 Files	Displays AMP file options
1-1 Upload File	Uploads a file to the AMP server you're currently logged in to using SCP for Unix.
1-2 Download File	Downloads a file from the local AMP to another server using SCP for Unix.
1-3 Delete File	Deletes a file from the AMP server. Files shown for deletion might include downloaded files, temporary files, and backup files.
2 Backup	Displays AMP backup and restore options.
2-1 Backup >	Displays AMP backup options.
2-1-1 Backup Now	Runs the back up now.
2-1-2 Configure Automatic Transfer	Sets the destination for nightly backup files. When you configure the automatic backup transfer, you won't see the backup file on the external server until the next nightly maintenance window passes.
2-1-3 Local Backup Retention	Changes how many backups AirWave retains (maximum of 4).

Option	Description
2-2 Restore >	Displays restore options.
2-2-1 AMP Restore	Restores the AMP server from an on-demand, nightly, or imported backup that you select.
2-2-2 VisualRF Restore	Restores the VisualRF database from the **visualrf_backup.pl** file that you select. Files shown for backup might include downloaded files, temporary files, and backup files.
3 Configuration	Displays AMP configuration options
3-1 Configure Network Settings	Configures network settings. You will be prompted to select an interface. Once an interface is selected, you can modify any of the following settings: 1) IPv4 Address 2) IPv4 Netmask 3) IPv4 Gateway 4) IPv6 Address (optional) 5) IPv6 Gateway (optional) 6) Primary DNS Server 7) Secondary DNS Server
3-2 Set Hostname	Sets the hostname of the AMP server.
3-3 Set Timezone	Sets the timezone of the AMP server. You will be prompted to select a continent/ocean, country and region, or specify the time zone using the Posix TZ format.
3-4 Certificates >	Displays certificate options.
3-4-1 Add SSL Certificate	Installs the SSL certificate, used to establish secure web sessions, on your AMP server.
3-4-2 Generate Certificate Signing Request	Creates a CSR that identifies which server will use the certificate.
3-4-3 Install Signed Certificate	Installs a signed certificate. AirWave supports signed certificates in PEM format with *.crt file extensions.
3-4-4 Install Self-Signed Certificate	Regenerates the self-signed certificate created when you installed AirWave.
3-4-5 Add DTLS Certificates	Installs the DTLS certificates, used to encrypt secure AMON traffic, on your AMP server.

Option	Description
3-4-6 OCSP >	Displays options for OCSP responders.
3-4-6-1 Make OCSP Optional/Required	Toggles on or off OCSP certificate validation when certificate authentication is required from the UI. **NOTE:** When configuring OCSP and CRL, one type of validation must be made mandatory if the other is optional. The optional validation type will be used if the initial validation type fails. When OCSP is optional, AirWave will first check for CRL certificate validation, and only check OCSP validation if CRL validation fails.
3-4-6-1 Manage OCSP URIs	This setting allows you to ad OCSP URIs. Click the a option to add a new URI.
3-4-7 CRL >	Manage AMP Certificate Revocation List (CRL) options for certificate path discovery and validation.
3-4-7-1 Make CRL Optional/Required	Toggles on or of CRL validation. **NOTE:** When configuring OCSP and CRL, one type of validation must be made mandatory if the other is optional. The optional validation type will be used if the initital validation type fails. When CRL is optional, AirWave will first check for OCSP certificate validation, and only check CRL validation if OCSP validation fails.
3-4-7-2 Manage CRL distribution URLs	Select this option to delete an existing URL, or click the **a** option to add a new URL
3-4-7-3 Manage CRL files	Select this option to delete an CRL file, or click the **a** option to add a new file.
3-5 SSHD >	Displays options for the SSH daemon (SSHD).
3-5-1 Set MaxAuthTries	Sets a limit on how many authentication attempts are allowed per user session.
3-5-2 Use Compatible Ciphers	Use this command to enable weak ciphers *aes128-cbc*, *aes192-cbc*, and *aes256-cbc* if the config file has ciphers set and these algorithms are not part of the existing AirWave ciphers.
3-6 CLT >	Configure AirWave to support Contact & Location Tracing (CLT) Analytics
3-6-1 Configure CLT	Use this command to configure the CLT feature. **NOTE:** Before you can use CLT, you are first required to sign up for this feature in Aruba Central, as the CLT configuration steps in AirWave require you to enter the Customer ID, Email and Secret used on Central.

Option	Description
3-6-2 Reconfigure CLT	Reconfigure CLT with an existing Central customer ID. To use CLT with a new customer ID, you will need to remove the old customer ID and then configure a new one again.
3-6-3 Remove CLT	Disable CLT by removing a previouisly configured CLT customer ID
3-6-4 Test CLT GW connectivity	Use this command to establish a TCP connection to https://nookgw.netinsight.arubanetworks.com. The output of this command can be used to identify any firewall issues that could impact CLT.
4 System	Displays AirWave system options.
4-1 Upgrade	Runs the AirWave software upgrade.
4-1-1 Aruba Support Portal (asp.arubanetworks.com)	Download the upgrade package from the Aruba Support Portal at asp.arubanetworks.com
4-1-2 HPE My Networking Portal	Download the upgrade package from the HPE My Networking Portal
4-2 Disable AMP	Toggles on and off the stopping and starting of all AMP services.
4-3 Restart AMP	Restarts the AMP services.
4-4 Reboot System	Reboots the AMP server.
4-5 Shutdown System (halt)	Shuts down the AMP server gracefully.
4-6 Show EngineID	Displays the SNMPv3 engine ID.
4-7 Module Key >	Displays module key options.
4-7-1 Show	Displays module key options.
4-7-2 Save	Saves a copy of the module key to the file <host>.module.key (e.g., AirWave.example.com.module.key).
5 **Users**	Displays User options.
5-1 Reset Web admin Password >	Resets the WebUI login password for the admin user.
5-1-1 admin	Changes the password for the WebUI admin user.
5-2 Change CLI User Password >	Changes the CLI log in password.
5-2-1 ampadmin	Changes the password for the CLI ampadmin user.

Option	Description
5-2-2 amprecovery	Changes the amprecovery password.
5-3 Add File Transfer User	Creates a new file transfer user account that works to transfer files between the AMP server and an SSHD client.
5-4 Remove amprecovery Account	Remove an AMP recovery user account.
5-5 Advanced >	Remove an AMP recovery user account.
5-5-1 Enable/Disable Complex Password Rules	Toggles on or off the configuration of password rules. This option only appears if STIGs are not applied to the AirWave server.
5-5-2 Set Lockout Threshold	Sets the number of failed log in attempts before the CLI user account is locked.
5-5-3 Set Lockout Timer	Sets the waiting period before the CLI user account is unlocked.
5-5-4 Set Password Length	Sets the length of the password.
5-5-5 Set Inactivity Threshold for CLI Users	Sets the period of inactivity before logging out the CLI user.
5-5-6 Unlock Web Users	Unlocks the Web user account. You will be prompted to select a user.
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.
6-7 Paste Encoded Text	Provides the option to paste the encoded format of the support_connection.tar file instead of upload the package.
7 Security	Displays AirWave security options.

Option	Description
7-1 Apply STIGs	Applies and enforces the Security Technical Implementation Guide (STIG) modules according to the Defense Information Systems Agency (DISA) for STIG compliance. If you enable this setting, it can't be changed.
7-2 Enable FIPs (requires reboot)	Toggles on or off FIPS 140-2 Approved Mode (requires a reboot).
7-3 Configure SELinux >	Toggles on or off Security-Enhanced Linux (SELinux), which provides users more access control of security policies.
7-3-1 Leave Disabled	Leave SELinux disabled.
7-3-2 Permissive (requires reboot)	in **Permissive** mode, SELinux displays warnings only but does not enforce the security policy. This mode is useful for debugging permissions issues.
7-3-3 Enforcing (requires reboot)	In **Enforcing** mode, the SELinux security policy is enforced.
7-4 Enable Firmware Integrity Check	Toggles on or off a validation check of the firmware code.
8 Advanced	Displays advanced system options.
8-1 Custom Commands >	Displays the custom command option.
8-1-1 Add New Menu Module	If you have already requested a new CLI module encrypted with a module key from customer support, you can use this command to select and add that module.
8-2 Enter Commands >	Some read-only commands are available from this menu. To see a list of commands, type a question mark (?) at the prompt. For more information, see Table 174.
8-3 Configure Network Settings	Configures network settings.
8-4 Enable DB transaction logging	Use this option to enable or disable additional logging of postgres database transactions. This option only appears when STIGs are applied to the AirWave server. **NOTE:** Enabling this option will increase disk usage and impact performance.
b >> Back (or Ctrl+c)	Returns to the previous menu.
c >> Cancel	Cancels the key request.
q	Exits the CLI session.

Table 173: *CLI Options*

Table 174 lists the running enter commands that are available when you select **11** from the CLI.

Table 174: *Running Enter Commands*

Command	Description
?	Displays the list of commands.
help <topic>	Displays the help for the <topic>.
man <topic>	Invokes the linux `man` command for the <topic>.
quit	Returns to CLI menu.
q	Returns to CLI menu.
exit	Returns to CLI menu.
history	Displays the history of commands you have typed.
h	Displays the history of commands you have typed.
h <pattern>	Displays history of all commands, matching the specified <pattern> input.
ch	Clears the history of commands displayed on the screen.
r	Repeats the previous command.
r <number>	Repeats the command, specified by the <number> from the history list.
r /x/y	Repeats the previous command, replacing x with y.
clear	Clears the terminal screen.
date	Displays the current date and time.
date MMDDhhmm	Changes the date and time on the AMP server.
top	Displays the status of running processes.
daemons	Displays the running daemons.
wd	Displays the monitoring of running daemons, refreshing after 1-second intervals.
wd <n>	Displays the monitoring of running daemons, refreshing after the <n> interval.
ls	Lists the files in the AMP CLI directory. **NOTE:** You can use shell patterns with *, ?, and [ ].
rm	Removes files from the AMP CLI directory. **NOTE:** You can use shell patterns with *, ?, and [ ].
cleanup	Deletes files that are no longer needed, including log files, old source files, and pre-upgrade backups.

Table 174: *Running Enter Commands (Continued)*

Command	Description
rd	Restarts the daemons.
psg <pattern>	Displays the running processes, matching the <pattern> you typed.
pss <pattern>	Displays the running processes like grep but shows more detailed information, matching the <pattern> you typed.
show_tech_support	Displays information about the AMP server to show technical support.
dbsize	Displays the 30 largest database tables.
dbsize <n>	Displays the <n> largest database tables.
dbsize -l	Displays details of disk space consumed, tuple spaces, and the actual size of the 30 largest tables.
dbsize -l <n>	Displays details of disk space consumed, tuple spaces, and the actual size of the <n> largest tables.
osrel	Displays the release version of the operating system.
license	Displays the license for the AMP server.
amp_version	Displays the AirWave version on your AMP server.
df -h	Shows disk space usage.
git diff	Checks for patches.
hostname	Displays the DNS name of the AMP server.
amp_backup	Runs a backup and puts the file in the AMP CLI directory.
amp_restore <filename>	Restores the AMP server from the backup.
remove_visualrf_cache	Clears the **visualrf_bootstrap** file.
iptables -L	Displays the IP tables.
dmidecode	Displays the serial number of the AMP server along with BIOS information.
network	Runs the network setup wizard.
dci	Displays the device communication interface, which configures the ethernet interface used for communication with devices.
ifconfig <interface>	Displays the status of the network interfaces.
ip route	Displays the IP routing tables.

Table 174: *Running Enter Commands (Continued)*

Command	Description
disable_whitelist	Resets the AMP whitelist to allow access (and restarts the AMP web server).
sw <ap id> args	Uses SNMP v1GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
sw2 <ap id> args	Uses SNMP v2c GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
sw3 <ap id> args	Uses SNMP v3 GETBULK to send a request to the database and walks back a list of all items up to a specified limit.
tcpdump args	Sends TCP packet data to an output file that you can use for later troubleshooting.
ping args	Sends ICMP echo request to confirm whether your network is reachable.
nslookup args	Queries the Internet name server, or the host name of the name server.
traceroute args	Tracks the route packets from an IP network to a host, using the IP protocol's time to live (TTL) value and getting an ICMP time exceeded response from each gateway along the path to the host.
free args	Displays the amount of free and used memory in the system.
service iptables	Displays the full status for IP tables.
service	Lists all services and allows you to manage them.
service <service> status|start|stop|restart	Manages the <service> you typed.
service <service>	Displays the status of the service.
qlog	Lists the status of available qlog topics.
qlog enable <topic>	Enables debugging. As files are created, they appear in the AMP CLI directory. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
qlog disable <topic>	Disables debugging for an individual topic. **NOTE:** You can give a unique prefix or a unique substring.
qlog disable all	Disables debugging for all qlog topics. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.
snoop	Displays the list of work queue snoop debug topics. **NOTE:** If there is more than 1 qlog topic matching the substring, a numbered picklist will be displayed. Enter the desired qlog topic number or multiple numbers separate by spaces. You can give a unique prefix or a unique substring.

Table 174: *Running Enter Commands (Continued)*

Command	Description
snoop <topic>	Enables work queue snoop debug for the desired topics. **NOTE:** You can give a unique prefix or a unique substring.
snoop active	Displays the active work queue snoop topics.
snoop stop <topic>	Stops work queue snoop on the selected topic. **NOTE:** You can give a unique prefix or a unique substring.
snoop stop all	Stops all active work queue snoop debugging.
ethernet_bonding <ip><netmask><gateway>	Enables ethernet bonding of two network interfaces. **NOTE:** If you enter ethernet_bonding without variables, you will be prompted for 3 input variables.
docker <bridge_ip_ address/cidr_bits>	Configures the AirWave Glass feeder service. **NOTE:** If you enter docker without variables, you will be prompted for 2 input variables.

The first place to check for performance issues is the **VisualRF > Floor Plans** page. If any floor's location calculation duration exceeds the location calculation timer setting, which is configured on **VisualRF > Setup** page, then VisualRF will not be able to calculate locations for clients within the desired time interval.

How Floor Components Impact Performance

Floor plan components that affect VisualRF performance include:

- Number of clients. VisualRF calculates the location for every client associated with access points on the floor per the value of location calculation timer. Hundreds or thousands of clients on a floor might cause location calculations for that floor to take minutes instead of seconds.
- Dimensions of the floor plan. VisualRF calculates path loss for every radio to every cell on the floor plan. If the floor is 2,000 feet by 1,500 feet, the grid cell size is 5 x 5, and there are 50 dual radio access points, then VisualRF will need to make 12,000,000 path loss calculations (400 cells * 300 cells * 100 radios).
- Number of APs or radios on a floor plan. VisualRF calculates path loss for every radio to every cell on the floor plan.
- Floor plan image size. The bigger the file size, the longer VisualRF takes to render the floor.
- Number of rogue devices on a floor plan. VisualRF calculates location for every rogue device heard by APs on the floor per the value of the rogue calculation timer.

Identifying Performance Problems

In addition to checking the floor plan calculations, you can monitor system performance with the following graphs:

- System Memory Usage. Ensure there is free memory, and check trending after adding new floors or changing settings on the **VisualRF > Setup** page.
- System Swap Usage. Ensure the server is not swapping.
- System CPU Utilization. Ensure the server has average idle time.
- System Load Average. Ensure that load average is below 2 times the number of cores. For example, if you have a dual dual-core server, the average load time should be at or below 8.

Resolving Performance Problems

If the floor location calculation takes longer than the Client Location Timer:

- Migrate to faster hardware
- Increase Core Caching Threads
- Increase Location Caching Threads
- Decrease the Location Caching Timer
- Increase Grid Cell Size

For memory or swap issues:

- Add more memory
- Reduce polling intervals on the AirWave server on the **VisualRF > Setup** page

- Reduce polling interval polling for router and switches

For server load issues:

- Migrate to faster hardware
- Decrease polling frequency of various polling buckets on **Groups > Basics** page
- Increase Min/Max timers and samples per devices on **VisualRF > Setup** page
- Increase Cell Grid Size
- Increase the AMP synchronization timer on **VisualRF > Setup** page
- Adjust rogue location filters

D

M

N

O

P

Q

R

S

V

W

Z