AirWave 8.2.11.1

Best Practices 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.

Contacting Support v
Overview 6
Understanding Aruba Topology 6
Prerequisites for Integrating Aruba Infrastructure 6
Configuring AirWave for Global Aruba Infrastructure 8
Disabling Rate Limiting in AMP Setup > General 8
Entering Credentials in Device Setup > Communication 8
Setting Up Recommended Timeout and Retries 10
Setting Up Time Synchronization 10
Manually Setting the Clock on a Controller 10
Setting Up NTP 10
Enabling Support for Channel Utilization And Statistics 11
AirWave Setup 11
Controller Setup (Master And Local) 12
Using ArubaOS 6.x 12
Using ArubaOS 8.x 12
Configuring an Aruba Group 14
Basic Monitoring Configuration 14
Advanced Configuration 15
Discovering Aruba Infrastructure 16
Discovering or Adding Master Controllers 16
Local Controller Discovery 18
Thin AP Discovery 18
AirWave and Aruba Integration Strategies 20
Integration Goals 20
Example Use Cases 21
When to Use Enable Stats 21
When to Use WMS Offload 21
When to Use RTLS 21
When to Define AirWave as a Trap Host 22
When to Use Channel Utilization 22
Prerequisites for Integration 22
Enable Controller Statistics Using AirWave 22
WMS Offload with AirWave 23
Define AirWave as a Trap Host Using the ArubaOS CLI 24
Ensuring That IDS and Auth Traps Display in AirWave 24
Understanding WMS Offload Impact on Aruba Infrastructure 25
Aruba Specific Capabilities 28
Aruba Traps for RADIUS Auth and IDS Tracking 28
Remote AP Monitoring 29
ARM and Channel Utilization Information 30
VisualRF and Channel Utilization 31
Configuring Channel Utilization Triggers 33
Viewing Channel Utilization Alerts 33
View Channel Utilization in RF Health Reports 34

Viewing Controller License Information 35
Rogue Device Classification 35
Rules-Based Controller Classification 38
Using RAPIDS Defaults for Controller Classification 38
Changing RAPIDS Based on Controller Classification 38
Appendix A CLI Commands 40
Enable Channel Utilization Events 40
Enable Stats With the ArubaOS CLI 40
Offload WMS Using the ArubaOS CLI 40
ArubaOS CLI 40
Using ArubaOS 6.x 40
Using ArubaOS 8.x 41
Pushing Configs from Master to Local Controllers 41
Disable Debugging Utilizing the ArubaOS CLI 41
Restart WMS on Local Controllers 42
Configure ArubaOS CLI when not Offloading WMS 42
Copy and Paste to Enable Proper Traps with the ArubaOS CLI 42
Appendix B AirWave Data Acquisition Methods 46
Appendix C WMS Offload Details 50
State Correlation Process 50
Using AirWave as a Master Device State Manager 51
Appendix D Increasing Location Accuracy 52
Understand Band Steering's Impact on Location 52
Leveraging RTLS to Increase Accuracy 52
Prerequisites 52
Deployment Topology 53
Enable RTLS Service on the AirWave Server 53
Enable RTLS on the Controller 54
Troubleshooting RTLS 55
Using the WebUI to See Status 55
Wi-Fi Tag Setup Guidelines 55

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

This document provides best practices for leveraging AirWave to monitor and manage your Aruba infrastructure, which provides a wealth of functionality such as firewall, VPN, remote AP, IDS, IPS, and ARM, as well as an abundance of statistical information.

Follow the simple guidelines in this document to garner the full benefit of your Aruba infrastructure.

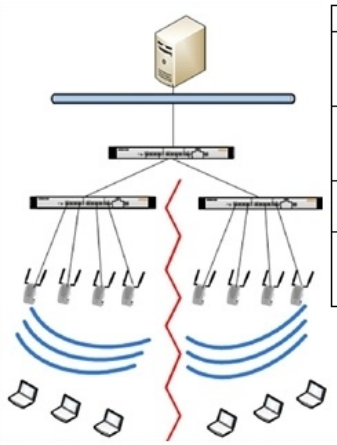
This overview chapter contains the following topics:

- "Understanding Aruba Topology" on page 6
- "Prerequisites for Integrating Aruba Infrastructure " on page 6

Understanding Aruba Topology

Figure 1 depicts a typical master-local deployment for the AirWave Wireless Management System (AWMS):

Figure 1: *Typical Aruba Deployment*



Component	Without AWMS	With AWMS
AWMS		AWMS communicates directly with local and master controllers to gather and correlate statistics
Master Controller	Correlates all state information from all downstream access points	Functions as a local controller
Local Controllers	Collect downstream AP statistical information	Collect downstream AP statistical and state information
Thin APs	Send all state information to the master controller	Send all state information to local controller

NOTE

There should never be a local controller managed by an AirWave server whose master controller is also not under management.

Prerequisites for Integrating Aruba Infrastructure

In order to integrate your Aruba infrastructure, you need the following information:

- SNMP community string for monitoring and discovery
- Telnet/SSH credentials for configuration
- **Enable** password for configuration
- SNMPv3 credentials for WMS offload

NOTE

Without proper Telnet/SSH credentials, AirWave will not be able to acquire license, serial information, and monitoring schema from controllers.

This section explains how to configure AirWave to globally manage your Aruba infrastructure.

- "Disabling Rate Limiting in AMP Setup > General" on page 8
- "Entering Credentials in Device Setup > Communication" on page 8
- "Setting Up Recommended Timeout and Retries" on page 10
- "Setting Up Time Synchronization" on page 10
- "Enabling Support for Channel Utilization And Statistics" on page 11

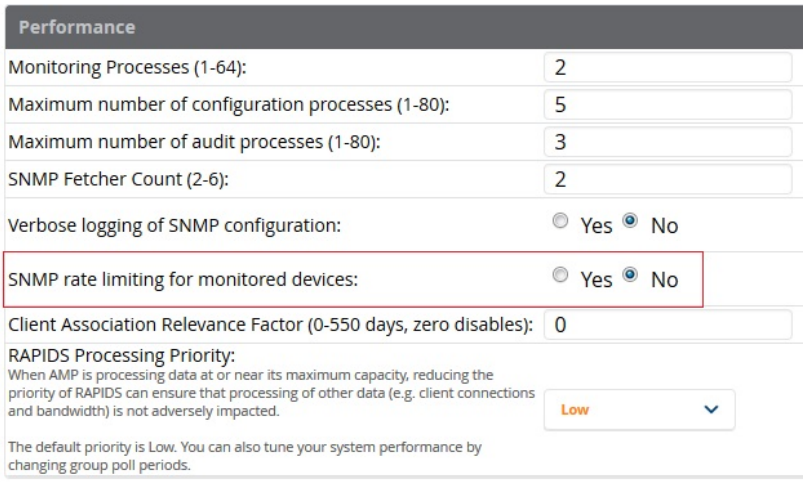
Disabling Rate Limiting in AMP Setup > General

The SNMP Rate Limiting for Monitored Devices option adds a small delay between each SNMP GET request, which results in the actual polling intervals that are longer than what is configured. For example, setting a ten-minute polling interval will result in an actual 12-minute polling interval. Disabling rate limiting is recommended in most cases unless you are using legacy Aruba devices, such as M2 devices.

To disable rate limiting in AirWave, follow these steps:

1. Navigate to **AMP Setup > General**.
2. Locate the **Performance** section.
3. In the **SNMP Rate Limiting for Monitored Devices** field, select **No**, as shown in Figure 2.
4. Click **Save**.

Figure 2: *SNMP Rate Limiting in **AMP Setup > General > Performance***



Entering Credentials in Device Setup > Communication

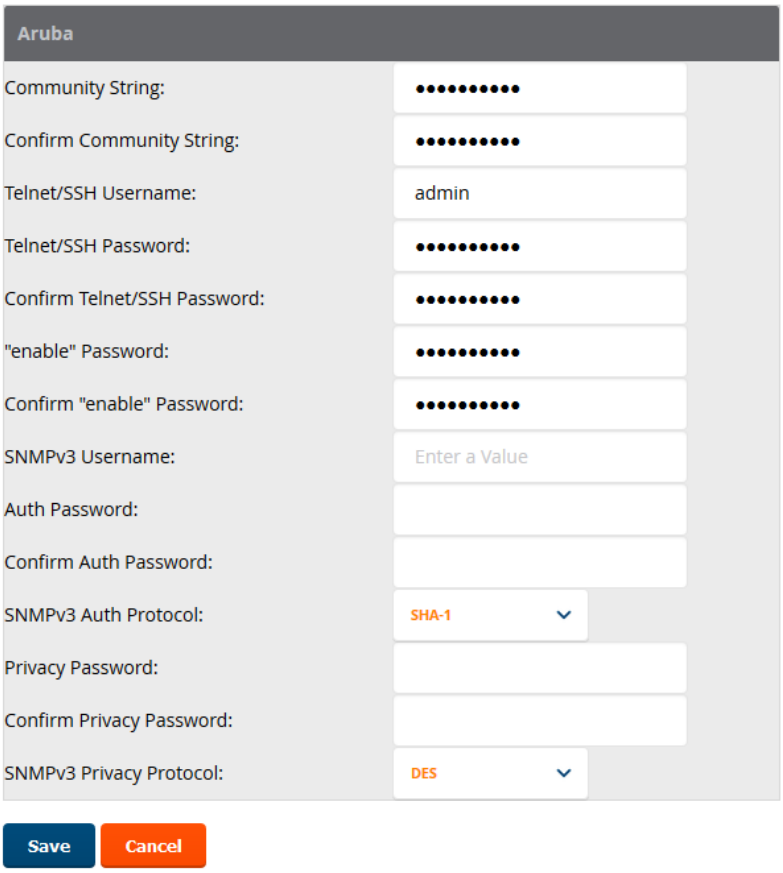
AirWave requires several credentials to properly interface with Aruba devices. To enter these credentials, follow these steps:

1. Navigate to **Device Setup > Communication**.
2. In the **Default Credentials** section, select the **Edit** link next to **Aruba**. The page illustrated in Figure 3 appears.

3. Enter the **SNMP Community String**.

Be sure to note the community string because it must match the SNMP trap community string, which is configured later in this document.

Figure 3: *Credentials in* ***Device Setup > Communication***



4. Enter the required information for configuration and basic monitoring:
   - Telnet/SSH user name
   - Telnet/SSH password
   - Enable mode password
5. Enter the required data for WMS Offload:
   - SNMPv3 user name
   - Authentication password
   - SNMPv3 authentication protocol (must be **SHA-1**)
   - Privacy password
   - SNMPv3 privacy protocol (must be **DES**)

The authentication and privacy protocols must be SHA-1 and DES for WMS Offload to work correctly.

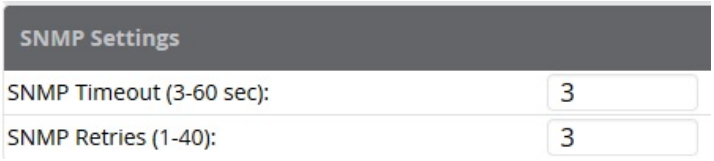
6. Click **Save**.

Setting Up Recommended Timeout and Retries

1. In the **Device Setup > Communication** page, locate the **SNMP Setting** section.
2. Change the **SNMP Timeout** setting to a value or either **3**, **4**, or **5**. This is the number of seconds that AirWave will wait for a response from a device after sending an SNMP request, so a smaller number is more ideal.
3. Change the **SNMP Retries** value to **10**. This value represents the number of times AirWave tries to poll a device when it does not receive a response within the SNMP Timeout Period or the Group's Missed SNMP Poll Threshold setting (1-100).

Although the upper limit for this value is 40, some SNMP libraries still have a hard limit of 20 retries. In these cases, any retry value that is set above 20 will still stop at 20.

Figure 4: *Timeout settings in* ***Device Setup > Communication***



4. Click **Save** when you are done.

Setting Up Time Synchronization

You can set the clock on a controller manually or by configuring the controller to use a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.

Manually Setting the Clock on a Controller

You can use either the WebUI or CLI to manually set the time on the controller's clock.

1. Navigate to the **Configuration > Management > Clock** page.
2. Under **Controller Date/Time**, set the date and time for the clock.
3. Under **Time Zone**, enter the name of the time zone and the offset from Greenwich Mean Time (GMT).
4. To adjust the clock for daylight savings time, click **Enabled** under Summer Time. Additional fields appear that allow you to set the offset from UTC and the start and end recurrences.
5. Click **Apply**.

Setting Up NTP

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

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

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

Table 1: *AMP Setup> Network > Secondary Network Fields and Default Values*

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

Enabling Support for Channel Utilization And Statistics

To enable support for channel utilization statistics, your AirWave server and ArubaOS and Aruba Instant devices must be running the following versions of software:

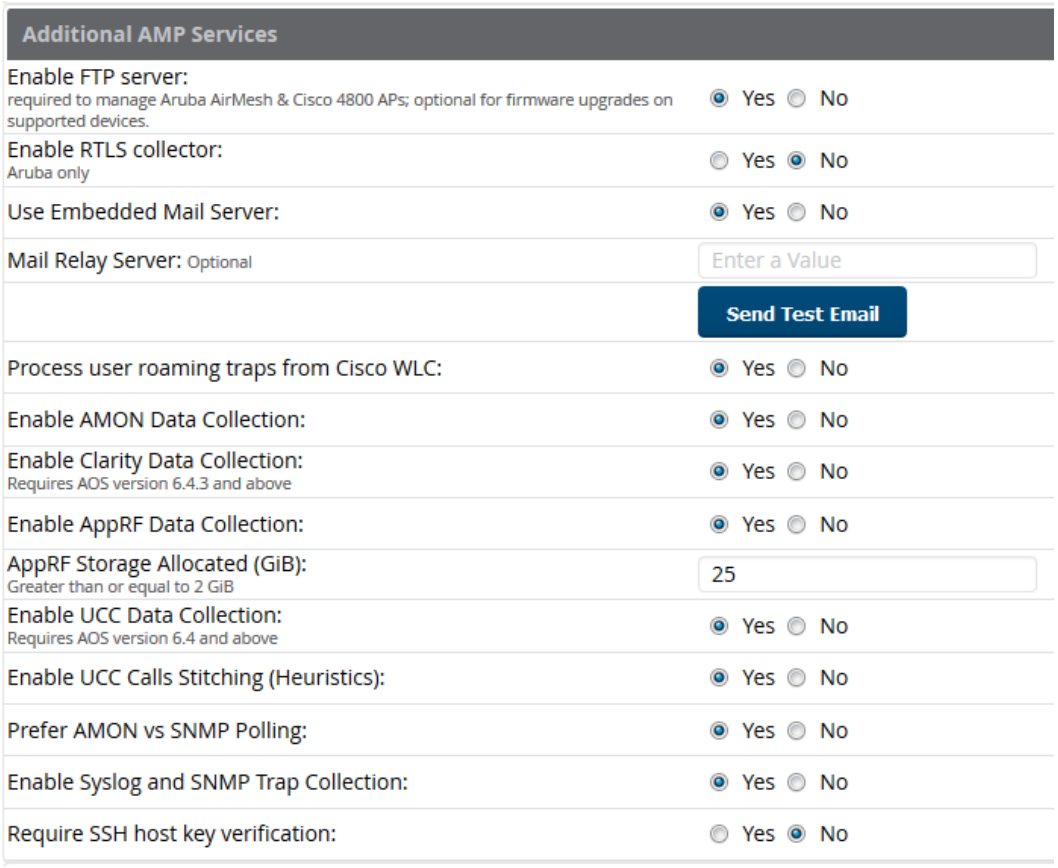
- AirWave 7.6 or later
- ArubaOS 6.0.1 or later
- Aruba Instant 3.3 or later

Devices running ArubaOS 6.0.1 can report RF utilization metrics, but ArubaOS 6.1 or later is necessary to also obtain classified interferer information.

AirWave Setup

1. Navigate to **AMP Setup > General**.
2. In the **Additional AMP Services** section, set **Enable AMON Data Collection** to **Yes**, and set **Prefer AMON vs SNMP Polling** to **Yes**.
3. Click **Save**.

Figure 5: *AMON Data Collection Setting in* ***AMP Setup > General***



Controller Setup (Master And Local)

Enabling these commands on ArubaOS versions prior to 6.0.1.0 can result in performance issues on the controller. If you are running previous firmware versions such as ArubaOS 6.0.0.0, you should upgrade to ArubaOS 6.0.1 (to obtain RF utilization metrics) or 6.1 (to obtain RF utilization *and* classified interferer information) before you enter this command.

Using ArubaOS 6.x

The following commands are for ArubaOS versions 6.3.1 and later 6.x releases. To get the commands for other versions of ArubaOS 6.x, refer to the *Command-Line Interface Reference Guide* for that version.

Use SSH to access the controller's command-line interface, enter **enable** mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # mgmt-server type amp primary-server <AMP-IP>
(Controller-Name) (config) # mgmt-server profile <profile-name>
(Controller-Name) (config) # write mem
```

Using ArubaOS 8.x

The following commands are for ArubaOS versions 8.4 and earlier 8.x releases. To get the commands for other versions of ArubaOS 8.x, refer to the *Command-Line Interface Reference Guide* for that version.

Use SSH to access Mobility Master's command-line interface, enter **enable** mode, and issue the following commands:

```
(host) [mynode] # configure terminal
```

```
Enter Configuration commands, one per line. End with CNTL/Z
(host) [mynode] (config) #mgmt-server primary-server <AMP-IP>
(host) [mynode] (config) #profile default-amp
(host) [mynode] (config) #write memory
```

You can add up to four <AMP-IP> addresses.

It is prudent to establish one or more Aruba Groups within AirWave. During the discovery process you will move new discovered controllers into this group.

This section contains the following topics:

- "Basic Monitoring Configuration" on page 14
- "Advanced Configuration " on page 15

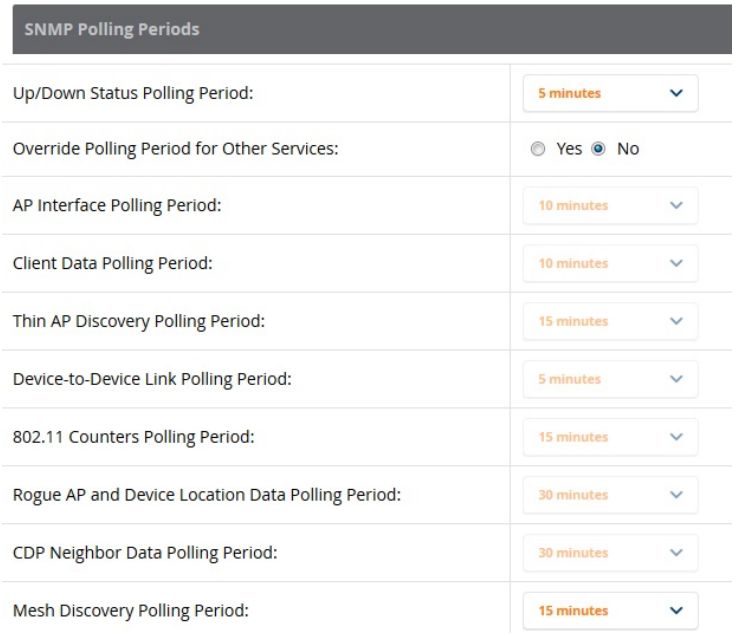
Basic Monitoring Configuration

1. Navigate to **Groups > List**.
2. Select **Add**.
3. Enter a **Name** that represents the Aruba device infrastructure from a security, geographical, or departmental perspective and select **Add**.
4. You will be redirected to the **Groups > Basic** page for the Group you just created. On this page you will need to verify and/or change the following Aruba-specific settings.
   a. Find the **SNMP Polling Periods** section of the page, as illustrated in Figure 6.
   b. Verify that the **Override Polling Period for Other Services** option is set to **Yes.**
   c. Verify that **Client Data Polling Period** is set to 10 minutes. Do not configure this interval lower than 5 minutes.

Enabling the SNMP Rate Limiting for Monitored Devices option in the previous chapter adds a small delay between each SNMP Get request, thus the actual polling interval is 12 minutes for 10 minute polling interval.

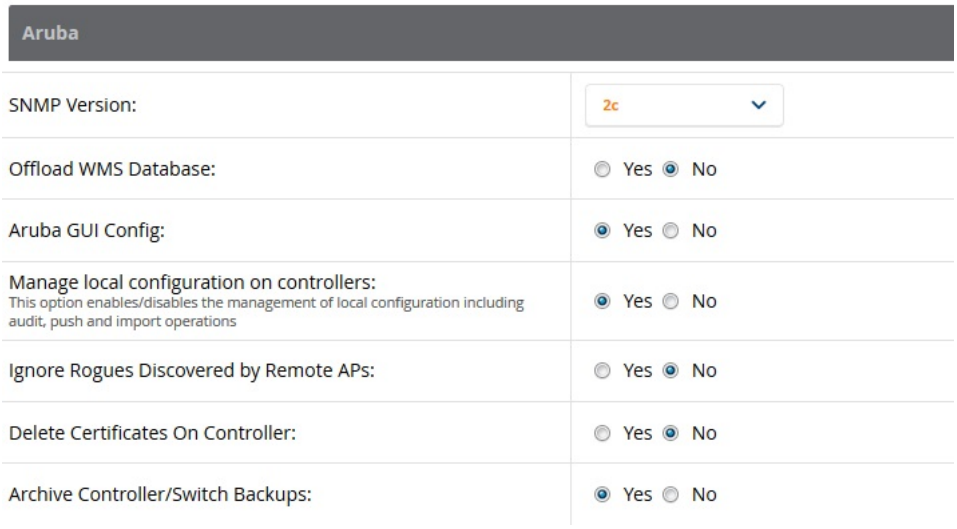
   d. Verify that the **Device-to-Device Link Polling Period** option is set to **30 minutes**.
   e. Verify that the **Rogue AP and Device Location Data Polling Period** option is set to **30 minutes**.

Figure 6: *SNMP Polling Periods section of* ***Groups > Basic***



5. Locate the Aruba section of this page. See Figure 7.
6. Configure the proper **SNMP Version** for monitoring the Aruba infrastructure.

Figure 7: *Group SNMP Version for Monitoring*



7. Click **Save and Apply** when you are done.

Advanced Configuration

Refer to the *AirWave 8.2.x Controller Configuration Guide* located at **Home > Documentation** for detailed instructions.

AirWave utilizes the Aruba topology to efficiently discover downstream infrastructure. This section guides you through the process of discovering and managing your Aruba device infrastructure.

Refer to the following earlier sections in this document before attempting discovery:

- "Configuring AirWave for Global Aruba Infrastructure" on page 8
- "Configuring an Aruba Group " on page 14

The following topics in this chapter walk through the basic procedure for discovering and managing Aruba infrastructure:

- "Discovering or Adding Master Controllers" on page 16
- "Local Controller Discovery" on page 18
- "Thin AP Discovery" on page 18

Always add one controller and its affiliated Thin APs into management or monitoring mode in a serial fashion, one at a time. Adding new devices is a very CPU intensive process for AirWave and can quickly overwhelm all of the processing power of the server if hundreds of Thin APs are added (migrated from New to Managed or Monitoring) simultaneously.

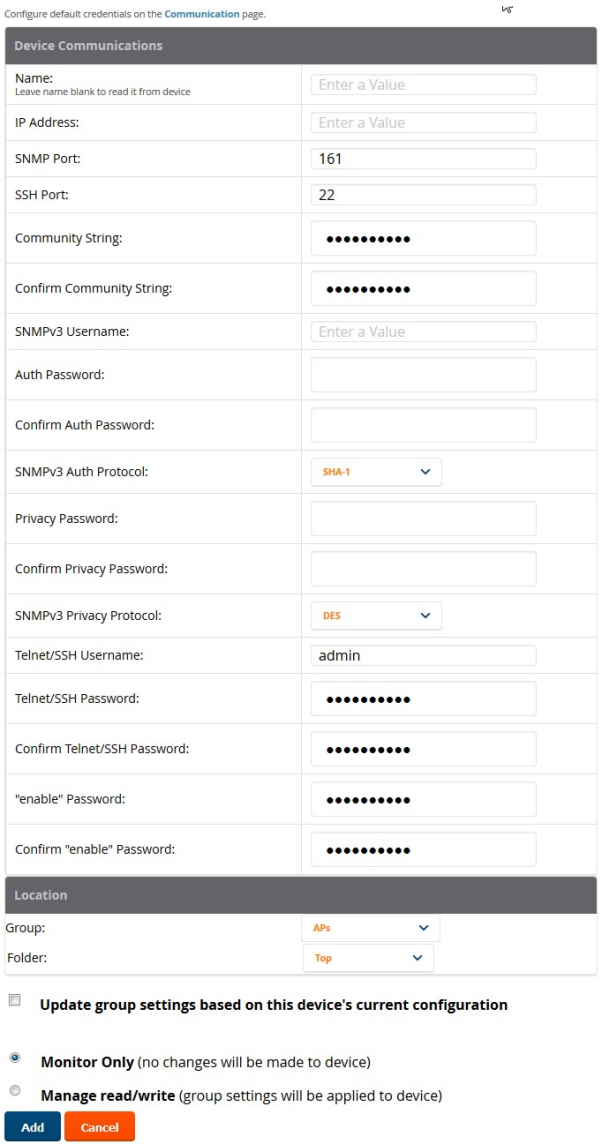
Discovering or Adding Master Controllers

Scan networks containing Aruba master controllers from the **Device Setup > Discover** page, or manually enter the master controller by following these steps in the **Device Setup > Add** page:

1. Select the **Aruba** Device type and select **Add**. The page illustrated on Figure 8 appears.
2. Enter the **Name** and the **IP Address** for the controller.
3. Enter **SNMP Community String**, which is required field for device discovery.

Be sure to note the community string because it must match the SNMP trap community string, which is configured later in this document.

Figure 8: *Aruba Credentials in* ***Device Setup > Add***



4. Enter the required fields for configuration and basic monitoring:
   - Telnet/SSH user name
   - Telnet/SSH password
   - Enable password
5. Enter the required fields for WMS Offload
   - SNMPv3 authentication protocol (must be **SHA-1**)
   - SNMPv3 privacy protocol (must be **DES**)
   - SNMPv3 user name
   - Authentication password
   - Privacy password

The protocols for SNMPv3 authentication and SNMPv3 privacy must be SHA-1 and DES in order for WMS Offload to work.

CAUTION

If you are using SNMPv3, and the controller's date/time is incorrect, the SNMP agent will not respond to SNMP requests from the AirWave SNMP manager. This will result in the controller and all of its downstream access points showing as Down in AirWave.

6. Assign the controller to a Group and Folder.
7. Ensure that the **Monitor Only** option is selected.

CAUTION

If you select Manage read/write, AirWave will push the group setting configuration, and existing device configurations will be deleted/overwritten.

8. Select **Add**.
9. Navigate to the **Devices > New** page.
10. Select the Aruba master controller you just added from the list of new devices.
11. Ensure **Monitor Only** option is selected.
12. Select **Add**.

Local Controller Discovery

Local controllers are added to AirWave via the master controller by a discovery scan, or manually added in **Device Setup > Add**. After waiting for the Thin AP Polling Period interval or executing a Poll Now command from the **Devices > Monitor** page, the local controllers will appear on the **Devices > New** page.

Add the local controller to the Group defined previously. Within AirWave, local controllers can be split away from the master controller's Group.

NOTE

Local Controller Discovery/monitoring may not work as expected if AirWave is unable to communicate directly with the target device. Be sure and update any ACL/Firewall rules to allow AirWave to communicate with your network equipment.

Thin AP Discovery

Thin APs are discovered via the local controller. After waiting for the Thin AP Polling Period or executing a Poll Now command from the **Devices > Monitor** page, thin APs will appear on the **Devices > New** page.

Add the thin APs to the Group defined previously. Within AirWave, thin APs can be split away from the controller's Group. You can split thin APs into multiple Groups if required.

This section describes strategies for integrating AirWave and Aruba devices and contains the following topics:

- "Integration Goals" on page 20
- "Example Use Cases" on page 21
- "Prerequisites for Integration" on page 22
- "Enable Controller Statistics Using AirWave" on page 22
- "WMS Offload with AirWave" on page 23
- "Define AirWave as a Trap Host Using the ArubaOS CLI" on page 24
- "Understanding WMS Offload Impact on Aruba Infrastructure" on page 25

Integration Goals

Table 2 summarizes the types of integration goals and strategies for meeting them in certain architectural contexts:

Table 2: *Integration Goals in All Masters or Master/Local Architectures*

Integration Goals	All Masters Architecture	Master/Local Architecture
Rogue And Client Info		enable stats
Rogue containment only	ssh access to controllers	ssh access to controllers
Rogue And Client containment	WMS Offload	WMS Offload
Reduce Master Controller Load		WMS Offload debugging off
IDS And Auth Tracking	Define AirWave as a trap host	Define AirWave as a trap host
Track Tag Location	enable Real Time Location System (RTLS) WMS Offload	enable RTLS WMS Offload
Channel Utilization	enable Application Monitoring (AMON)	enable AMON
Spectrum	enable AMON	enable AMON
Traffic Analysis Visibility	enable AMON	enable AMON
UCC Visability	enable AMON	enable AMON
Health Information	enable Adaptive Radio Management (ARM)	enable ARM

Key integration points to consider include the following:

- IDS Tracking does not require WMS Offload in an all-master or master/local environment.
- IDS Tracking does require enable stats in a master/local environment.
- WMS Offload will hide the Security Summary tab on master controller's web interface.
- WMS Offload encompasses enable stats or enable stats is a subset of WMS Offload.
- Unless you enable stats on the local controllers in a master/local environment, the local controllers do not populate their MIBs with any information about clients or rogue devices discovered/associated with their APs. Instead the information is sent upstream to master controller.

Example Use Cases

The following are example use cases of integration strategies:

- "When to Use Enable Stats" on page 21
- "When to Use WMS Offload" on page 21
- "When to Use RTLS" on page 21
- "When to Define AirWave as a Trap Host" on page 22
- "When to Use Channel Utilization" on page 22

When to Use Enable Stats

You want to pilot AirWave, and you do not want to make major configuration changes to their infrastructure or manage configuration from AirWave.

Enable Stats still pushes a small subset of commands to the controllers via SSH.

See "Enable Controller Statistics Using AirWave" on page 22.

When to Use WMS Offload

- You have older Aruba infrastructure in a master/local environment and the master controller is fully taxed. Offloading WMS will increase the capacity of the master controller by offloading statistics gathering requirements and device classification coordination to AirWave.
- You want to use AirWave to distribute client and rogue device classification amongst multiple master controllers in a master/local environment or in an All-Masters environment.
- See the following topics:
  - "WMS Offload with AirWave" on page 23
  - "Understanding WMS Offload Impact on Aruba Infrastructure" on page 25
  - "WMS Offload Details" on page 50

When to Use RTLS

- A hospital wants to achieve very precise location accuracy (5 -15 feet) for their medical devices which are associating to the WLAN.
- You want to locate items utilizing Wi-Fi Tags.

RTLS can negatively impact your AirWave server's performance.

- See "Leveraging RTLS to Increase Accuracy" on page 52.

When to Define AirWave as a Trap Host

- You want to track IDS events within the AirWave UI.
- You are in the process of converting their older third-party WLAN devices to Aruba devices and want a unified IDS dashboard for all WLAN infrastructure.
- You want to relate Auth failures to a client device, AP, Group of APs, and controller. AirWave provides this unique correlation capability.

See "Define AirWave as a Trap Host Using the ArubaOS CLI" on page 24.

When to Use Channel Utilization

- You have a minimum version of ArubaOS 6.1.0.0.

Prerequisites for Integration

If you have not discovered the Aruba infrastructure or configured credentials, refer to the previous chapters of this book:

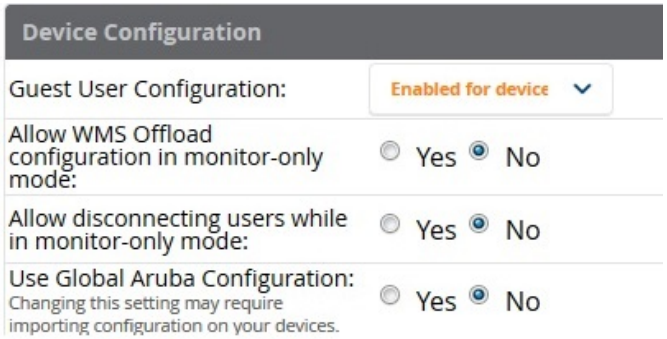
- "Configuring AirWave for Global Aruba Infrastructure" on page 8
- "Configuring an Aruba Group " on page 14
- "Discovering Aruba Infrastructure" on page 16

Enable Controller Statistics Using AirWave

To enable stats on the Aruba controllers, follow these steps:

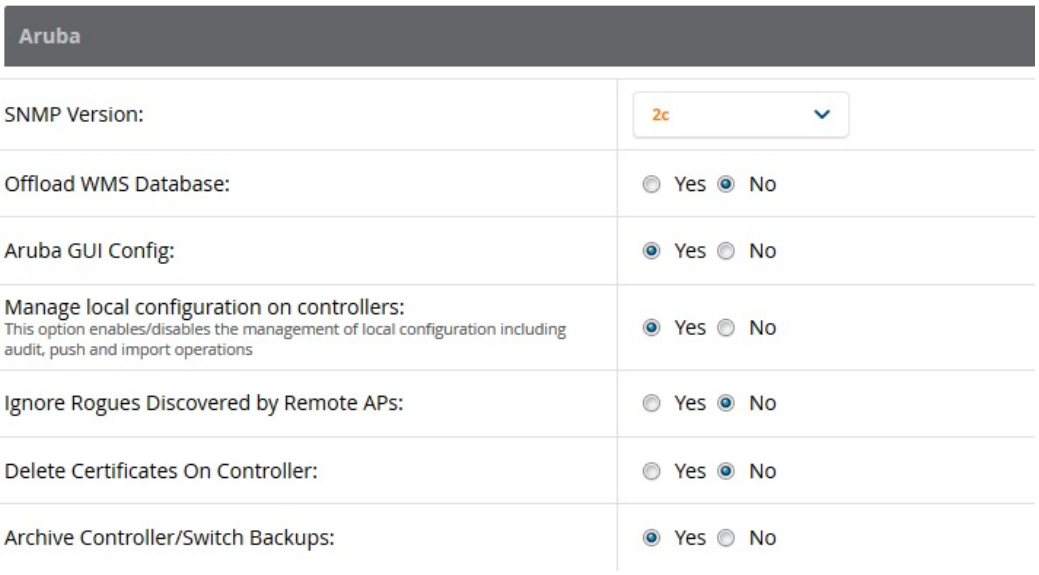
1. Navigate to **AMP Setup > General** and locate the **Device Configuration** section.
2. Set the **Allow WMS Offload Configuration in Monitor-Only Mode** field to **Yes**, as shown in Figure 9:

Figure 9: *WMS Offload Configuration in **AMP Setup > General***



3. Navigate to **Groups > Basic** for the group that contains your Aruba controllers.
4. Locate the Aruba section on the page.
5. Set the **Offload WMS Database** field to **No,** as shown in Figure 10:

Figure 10: *Offload WMS Database field in* ***Groups > Basic***



6. Select **Save and Apply**.
7. Select **Save**.

This will push a set of commands via SSH to all Aruba local controllers. AirWave must have read/write access to the controllers in order to push these commands.

NOTE

This process will not reboot your controllers.

CAUTION

If you do not follow the above steps, local controllers will not be configured to populate statistics. This decreases AirWave's capability to trend client signal information and to properly locate devices. See "ArubaOS CLI" on page 40 for information about how to utilize the ArubaOS CLI to enable stats on Aruba infrastructure.

If your credentials are invalid or the changes are not applied to the controller, error messages will display on the controller's **Devices > Monitor** page under the **Recent Events** section. If the change fails, AirWave does not audit these setting (display mismatches) and you will need to apply to the controller by hand. See "ArubaOS CLI" on page 40 for detailed instructions.

These are the commands pushed by AirWave while enabling WMS Offload. Do not enter these commands:

```
configure terminal
no mobility-manager <Active WMS IP Address>
wms
general collect-stats enable
stats-update-interval 120
show wms general
write mem
```

WMS Offload with AirWave

To offload WMS on the Aruba controllers using AirWave:

1. In **AMP Setup > General**, locate the **Device Configuration** section and enable or disable **Allow WMS Offload Configuration in Monitor-Only Mode.**

2. Select **Save and Apply**. This will push a set of commands via SSH to all Aruba master controllers. If the controller does not have an SNMPv3 user that matches the AirWave database it will automatically create a new SNMPv3 user. AirWave must have read/write access to the controllers to push these commands
3. Navigate to **Groups > Basic** and locate the **Aruba** section.
4. Set the **Offload WMS Database** field to **Yes**.

NOTE

This process will not reboot your controllers. See "CLI Commands" on page 40 for information on how to utilize the ArubaOS CLI to enable stats for WMS Offload.

CAUTION

The SNMPv3 user's Auth Password and Privacy Password must be the same.

Do not enter these commands; these are pushed by AirWave while enabling WMS Offload.

```
configure terminal
mobility-manager <AMP IP> user <AMP SNMPv3 User Name> <AMP Auth/Priv PW>
stats-update-interval 120
write mem
```

NOTE

AirWave will configure SNMPv2 traps with the **mobile manager** command.

Define AirWave as a Trap Host Using the ArubaOS CLI

To ensure the AirWave server is defined as a trap host, access the command line interface of each controller (master and local), enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # snmp-server host <AMP IP ADDR> version 2c <SNMP Community String of Controller>
```

NOTE

Ensure the SNMP community matches those that were configured in "Configuring AirWave for Global Aruba Infrastructure" on page 8.

```
(Controller-Name) (config) # snmp-server trap source <Controller-IP>
(Controller-Name) (config) # write mem
```

NOTE

AirWave supports SNMP v2 traps and SNMP v3 informs in ArubaOS 3.4 and higher. SNMP v3 traps are not supported.

Ensuring That IDS and Auth Traps Display in AirWave

Validate your ArubaOS configuration by exiting the configure terminal mode and issue the following command:

```
(Controller-Name) # show snmp trap-list
```

If any of the traps in the output of this command do not appear to be enabled, enter **configure terminal** mode and issue the following command:

```
(Controller-Name) (config) # snmp-server trap enable <TRAPS FROM LIST ABOVE>
```

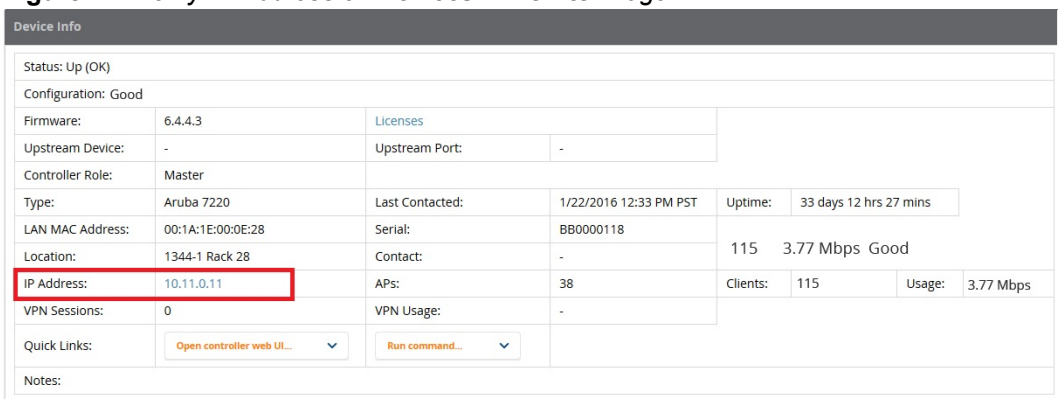
NOTE

See "ArubaOS CLI" on page 40 for the full command that can be copied and pasted directly into the ArubaOS CLI.

```
(Controller-Name) (config) # write mem
```

Ensure the source IP of the traps match the IP that AirWave uses to manage the controller, see Figure 11. Navigate to **Devices > Monitor** to validate the IP address in the **Device Info** section.

Figure 11: *Verify IP Address on **Devices > Monitor** Page*



Verify that there is a SNMPv2 community string that matches the SNMP Trap community string on the controller.

```
(Controller-Name) # show snmp community
SNMP COMMUNITIES
----------------
COMMUNITY ACCESS      VERSION
--------- ------      -------
public    READ_ONLY V1, V2c

(Controller-Name) # #show snmp trap-host

SNMP TRAP HOSTS
---------------
HOST           VERSION     SECURITY NAME  PORT    TYPE TIMEOUT RETRY
----           -------     -------------- ----    ---- ------- -----
10.2.32.4      SNMPv2c     public          162     Trap N/A       N/A
```

Understanding WMS Offload Impact on Aruba Infrastructure

When offloading WMS, it is important to understand what functionality is migrated to AirWave and what functionality is deprecated.

The following ArubaOS tabs and sections are deprecated after offloading WMS:

- **Plan** - The tab where floor plans are stored and heatmaps are generated. Before offloading WMS, ensure that you have exported floor plans from ArubaOS and imported them into AirWave. All functionality within the Plan Tab is incorporated with the VisualRF module in AirWave.
- **Dashboard > Security Summary** - The **Security Summary** section (Figure 12) disappears after offloading WMS. The data is still being processed by the master controller, but the summary information is not available. You must use AirWave to view data for APs, clients and events in detail and summary from.
  - AirWave displays information on Rogue APs in the **RAPIDS > Overview** pages.
  - Information on Suspected Rogue, Interfering and known interfering APs is available in AirWave on each **Devices > Manage** page.
  - IDS events data and reports appear on AirWave's **Reports > Generated > IDS Events** page.

Figure 12: *Security Summary on the Master Controller*

See "Rogue Device Classification" on page 35 for more information about security, IDS, WIPS, WIDS, classification, and RAPIDS.

This section discusses Aruba specific capabilities in AirWave and contains the following topics:

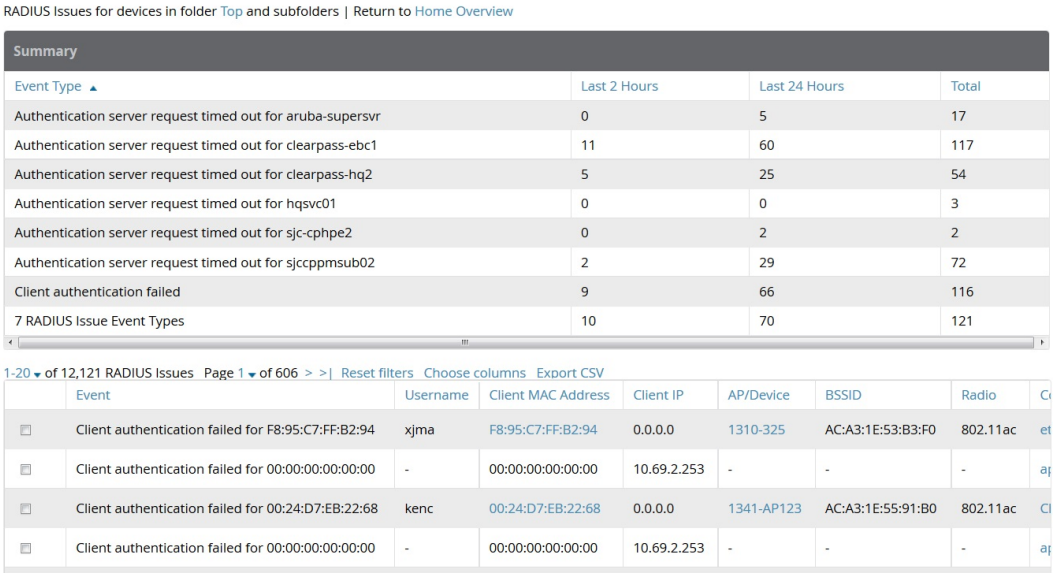
- "Aruba Traps for RADIUS Auth and IDS Tracking" on page 28
- "Remote AP Monitoring" on page 29
- "ARM and Channel Utilization Information" on page 30
- "Viewing Controller License Information" on page 35
- "Rogue Device Classification" on page 35
- "Rules-Based Controller Classification" on page 38

Aruba Traps for RADIUS Auth and IDS Tracking

The authentication failure traps are received by the AirWave server and correlated to the proper controller, AP, and user.

View a list of recent RADIUS authentication issues by navigating to the **Home >Overview** page, and selecting the **RADIUS Issues** link in the **Alert Summary** table at the bottom of the page. Figure 13 shows all authentication failures related to RADIUS data.

Figure 13: *RADIUS Issues Summary*


RADIUS Issues for devices in folder Top and subfolders | Return to Home Overview

Summary

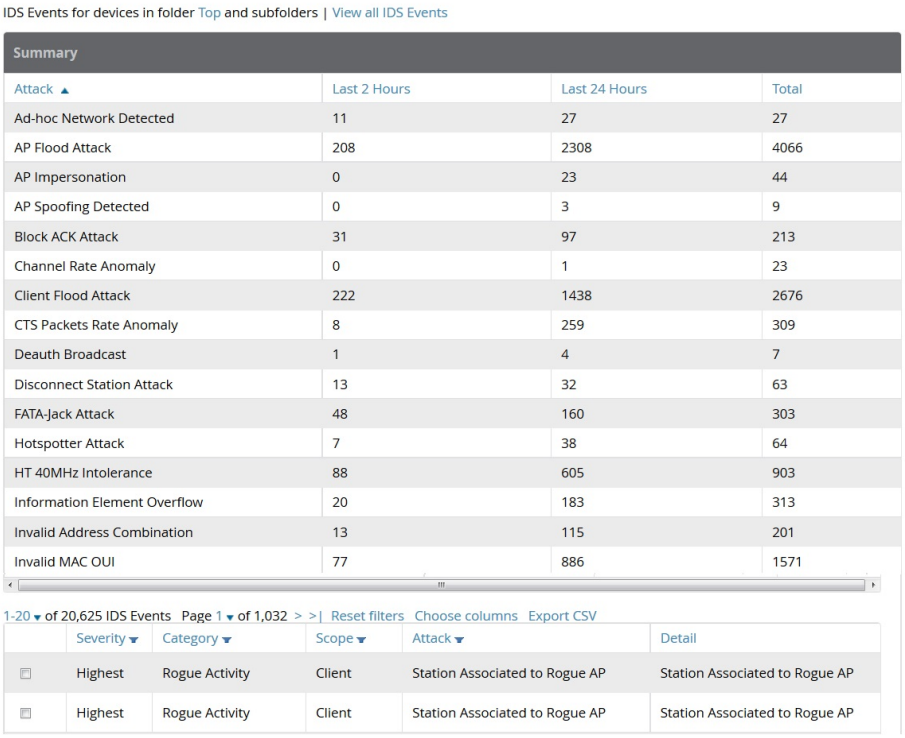
Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Authentication server request timed out for aruba-supersvr	0	5	17
Authentication server request timed out for clearpass-ebc1	11	60	117
Authentication server request timed out for clearpass-hq2	5	25	54
Authentication server request timed out for hqsvc01	0	0	3
Authentication server request timed out for sjc-cphpe2	0	2	2
Authentication server request timed out for sjccppmsub02	2	29	72
Client authentication failed	9	66	116
7 RADIUS Issue Event Types	10	70	121

1-20 of 12,121 RADIUS Issues Page 1 of 606 > >| Reset filters Choose columns Export CSV

Event	Username	Client MAC Address	Client IP	AP/Device	BSSID	Radio	C
Client authentication failed for F8:95:C7:FF:B2:94	xjma	F8:95:C7:FF:B2:94	0.0.0.0	1310-325	AC:A3:1E:53:B3:F0	802.11ac	et
Client authentication failed for 00:00:00:00:00:00	-	00:00:00:00:00:00	10.69.2.253	-	-	-	ap
Client authentication failed for 00:24:D7:EB:22:68	kenc	00:24:D7:EB:22:68	0.0.0.0	1341-AP123	AC:A3:1E:55:91:B0	802.11ac	Cl
Client authentication failed for 00:00:00:00:00:00	-	00:00:00:00:00:00	10.69.2.253	-	-	-	ap

There are two ways to navigate to the list of recent IDS events. You can go to the **Home >Overview** page and select the **IDS Events** link in the **Alert Summary** table at the bottom of the page, or go directly to **RAPIDS > IDS Events**. The IDS Events Summary page includes a table that shows the numbers of events in each IDS category, as well as a sortable table of each event. (See Figure 14.)

Figure 14: *IDS Events in AirWave*



IDS Events for devices in folder Top and subfolders | View all IDS Events

Summary

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Ad-hoc Network Detected	11	27	27
AP Flood Attack	208	2308	4066
AP Impersonation	0	23	44
AP Spoofing Detected	0	3	9
Block ACK Attack	31	97	213
Channel Rate Anomaly	0	1	23
Client Flood Attack	222	1438	2676
CTS Packets Rate Anomaly	8	259	309
Deauth Broadcast	1	4	7
Disconnect Station Attack	13	32	63
FATA-Jack Attack	48	160	303
Hotspotter Attack	7	38	64
HT 40MHz Intolerance	88	605	903
Information Element Overflow	20	183	313
Invalid Address Combination	13	115	201
Invalid MAC OUI	77	886	1571

1-20 ▾ of 20,625 IDS Events Page 1 ▾ of 1,032 > >| Reset filters Choose columns Export CSV

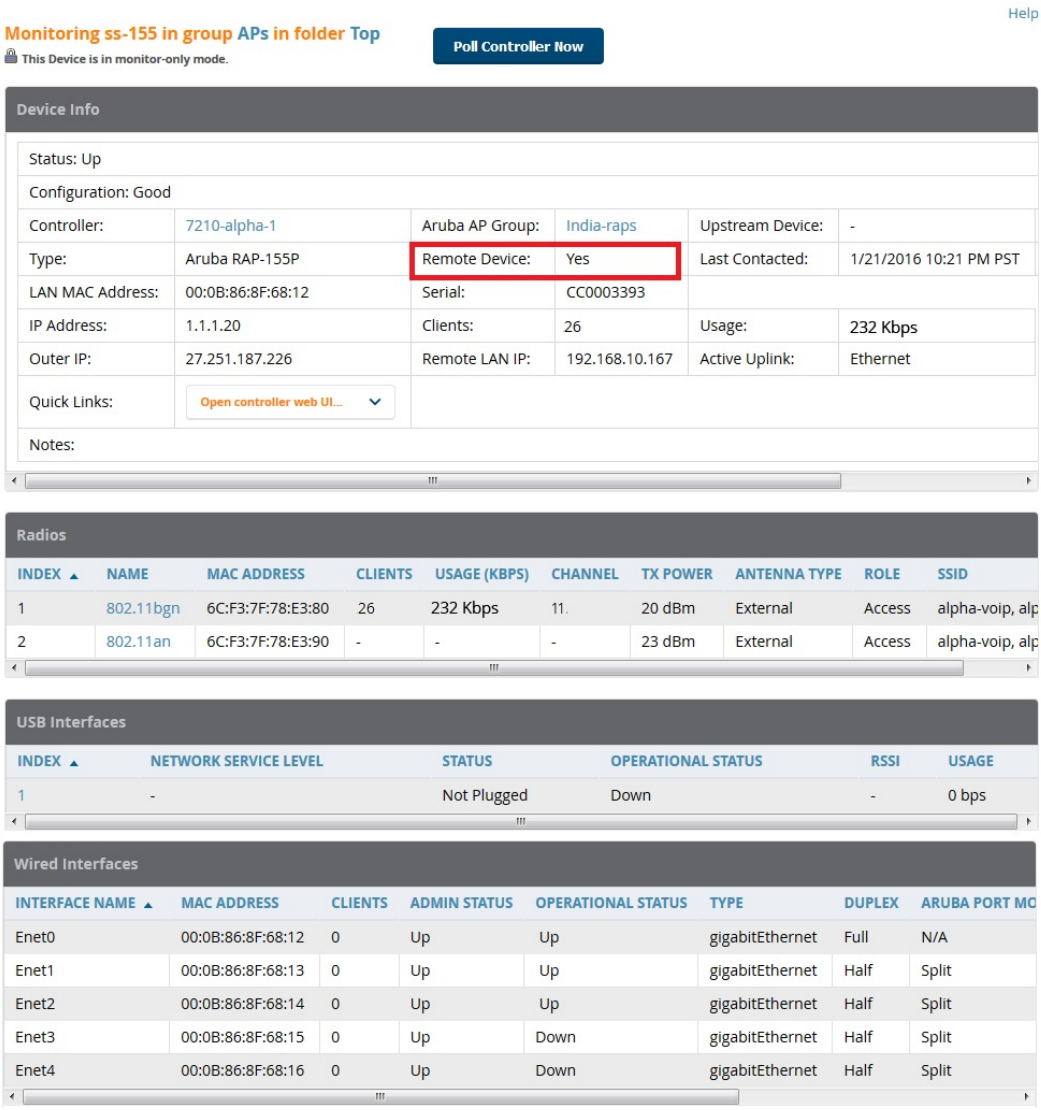
	Severity ▾	Category ▾	Scope ▾	Attack ▾	Detail
☐	Highest	Rogue Activity	Client	Station Associated to Rogue AP	Station Associated to Rogue AP
☐	Highest	Rogue Activity	Client	Station Associated to Rogue AP	Station Associated to Rogue AP

Remote AP Monitoring

To monitor remote APs, follow these steps:

1. From the **Devices > List** page, filter on the **Remote Device** column to find remote devices.
2. To view detailed information about the remote device, select the device name. The page illustrated in Figure 15 appears.

Figure 15: *Remote AP Detail Page*



You can also see if there are users plugged into the wired interfaces in the **Connected Clients** list below the **Clients** and **Usage** graphs at the bottom of this page.

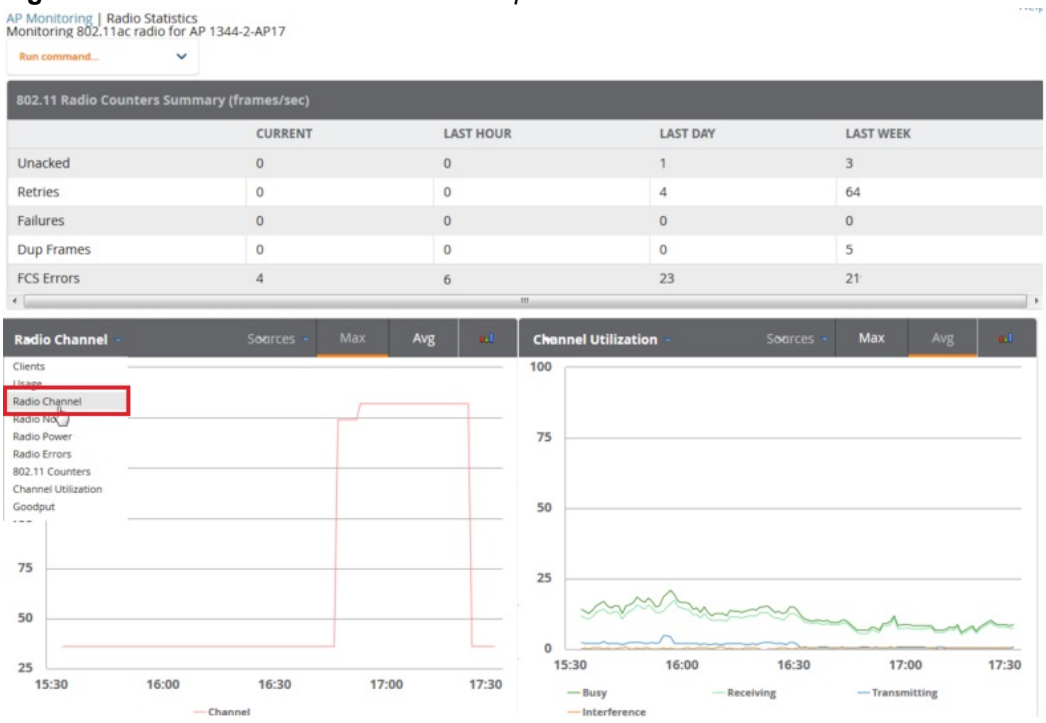
This feature is only available when the remote APs are in split tunnel and tunnel modes.

ARM and Channel Utilization Information

ARM statistics and Channel utilization are very powerful tools for diagnosing capacity and other issues in your WLAN.

1. Navigate to an **Devices > Monitor** page for any AP that supports ARM and channel utilization.
2. In the **Radios** table, select a radio link under the **Name** column for a radio.
3. The graphs default to Client and Usage. Select an icon for each to change the graphs to display Radio Channel and Channel Utilization.

Figure 16: *ARM and Channel Utilization Graphs*



See the *AirWave 8.2.11.1 User Guide* in **Home > Documentation** more information about the data that displays in the **Radio Statistics** page for these devices.

VisualRF and Channel Utilization

1. Navigate to a floor plan by navigating to **VisualRF > Floor Plans** page.
2. Click the **list** link at the top of the Floor Plans page, and select a floor plan from the list.
3. Click the **View** tab
4. Select the **Overlays** menu.
5. Select the **Ch. Utilization** overlay.
6. Select **Current** or **Maximum** (over last 24 hours).
7. Use the Data Set drop-down list to display **Total**, **Receive** (Rx), **Transmit** (Tx), or **Interference** utilization data.
8. Select the option to view information for the current floor only, or to include information about the floor above, and/or the floor below.
9. Select a frequency **(5 GHz** and/or **2.4 GHz**).

Figure 17: *Overlays*

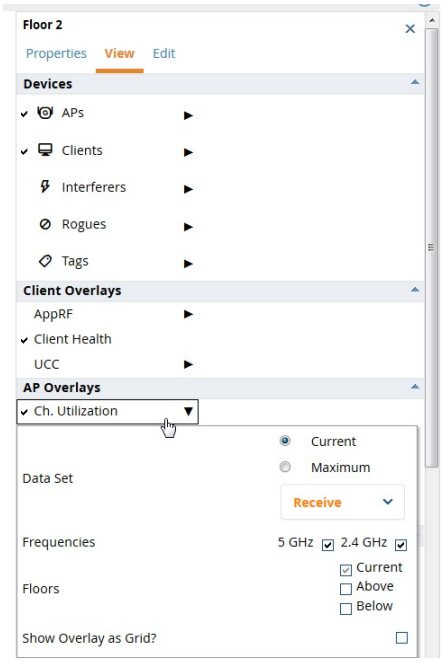
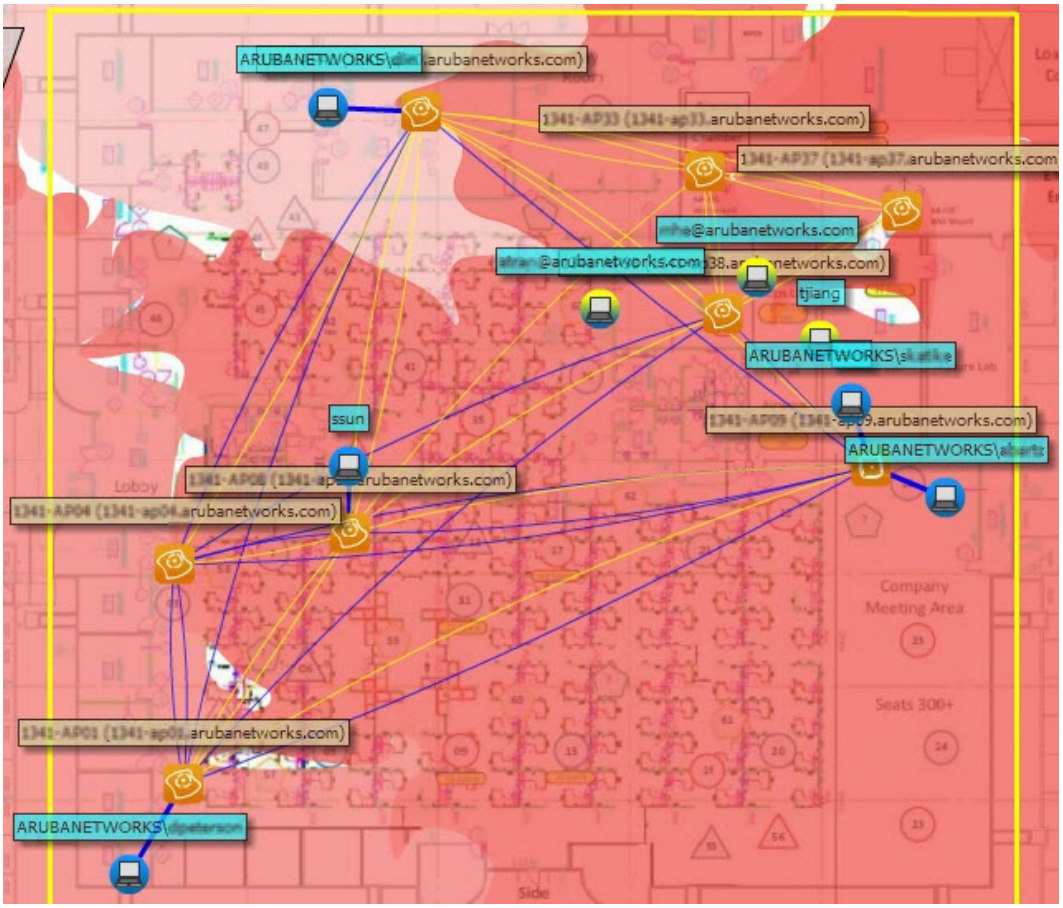


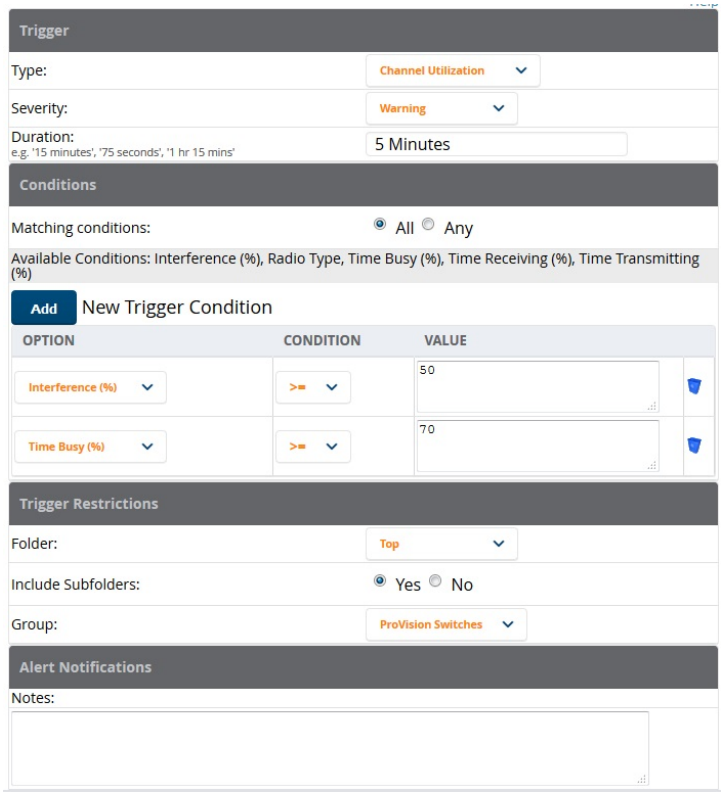
Figure 18: *Channel Utilization in VisualRF (Interference/2.4 GHz)*



Configuring Channel Utilization Triggers

1. Navigate to **System > Triggers** and select **Add**.
2. Select **Channel Utilization** from the **Type** drop-down menu as seen on Figure 19:

Figure 19: *Channel Utilization Trigger*



3. Enter the duration evaluation period.
4. Click the **Add New Trigger Condition** button.
5. Create a trigger condition for **Radio Type** and select the frequency to evaluate.
6. Select total, receive, transmit, or interference trigger condition.
7. Set up any restrictions or notifications. (Refer to the *AirWave 8.2.11.1 User Guide* in **Home > Documentation** for more details.)
8. When you are finished, click **Add**.

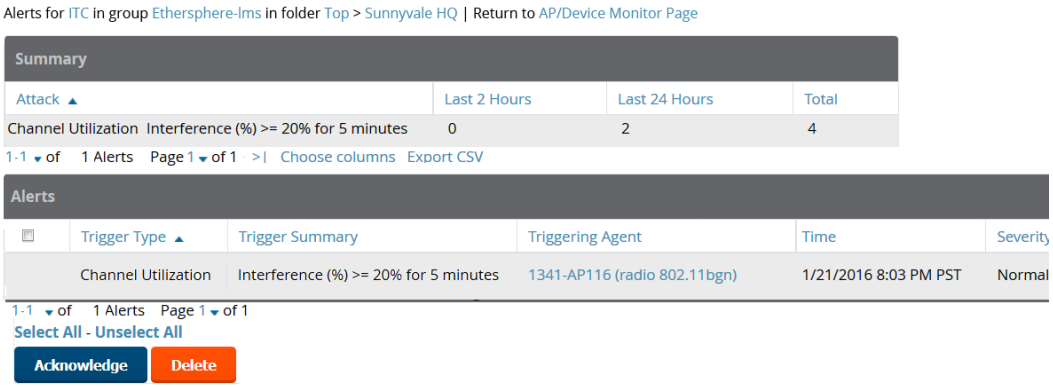
Viewing Channel Utilization Alerts

You can view Channel Utilization alerts from the **Devices > Monitor** page and on the **System > Alerts** page.

To view channel utilization alerts on the **Devices > Monitor** page:

1. Navigate to the **Devices > list** page and select a device.
2. Navigate to the **Devices> Monitor** page for that device.
3. Scroll down to the **Alert Summary** table and select **AirWave Alerts**.

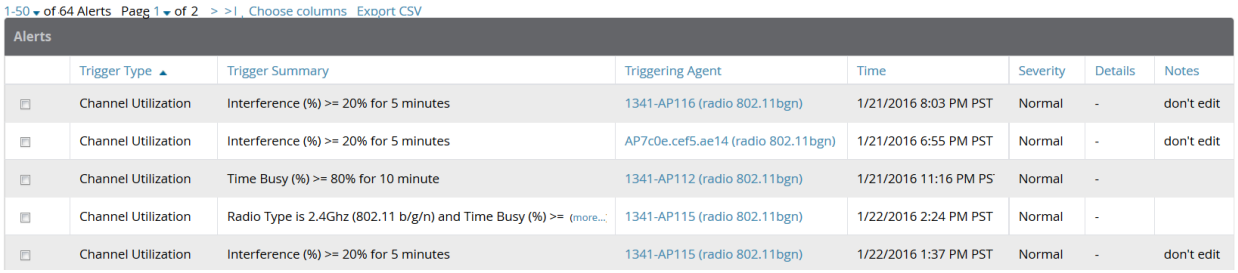
Figure 20: *Channel Utilization alerts*



To view channel utilization alerts on the **System > Alerts** page:

1. Navigate to the **System > Alerts** page.
2. Sort the table using the **Trigger Type** column to display **Channel Utilization** alerts.

Figure 21: *Channel Utilization alerts on the System > Alerts page*



View Channel Utilization in RF Health Reports

1. Navigate to **Reports > Generated**.
2. Find and select an RF Health report.
3. Scroll down to view the **Most Utilized by Channel Usage (5 GHz)** and **Most Utilized by Channel Usage (2.4 GHz)** graphs.

Figure 22: *Channel Utilization in an RF Health Report (partial view)*

Most Utilized by Channel Usage (5 GHz)

Rank	Device	Channel Busy (%)	Interference (%)	Clients	Usage	Location	Controller	Folder	Group
1	1341-AP122	22.44	0.39	3	417.48 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
2	1341-AP121	22.05	0.00	1	155.74 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
3	1341-AP131	22.05	0.00	1	190.26 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
4	1341-AP105	21.65	-0.00	1	231.72 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
5	1341-AP120	21.26	-0.00	0	4.10 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
6	1341-AP127	20.87	0.00	0	11.98 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
7	1341-AP130	20.87	0.00	3	628.27 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
8	1341-AP107	20.47	-0.39	3	406.21 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
9	1341-AP117	20.47	-0.00	1	24.13 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
10	1341-AP112	20.08	-0.39	1	87.25 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ

Most Utilized by Channel Usage (2.4 GHz)

Rank	Device	Channel Busy (%)	Interference (%)	Clients	Usage	Location	Controller	Folder	Group
1	1341-AP125	77.95	17.32	0	17.48 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
2	AP7c0e.cef5.ae14	76.77	76.77	0	11.98 Kbps	default location	Cisco8510	Top	Cisco Gear
3	1341-AP127	74.02	14.96	0	8.08 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
4	APd072.dce0.225c	73.23	73.23	0	6.21 Kbps	default location	Cisco7500	Top	Cisco Gear
5	1341-X-AP09	72.83	26.77	0	4.13 Kbps	-	alpo	Top > Sunnyvale HQ	Aruba HQ
6	1341-AP114	70.08	10.63	0	68 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
7	1341-AP124	69.29	9.84	0	47 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
8	1341-AP132	68.50	9.06	0	2 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
9	1341-AP117	67.32	10.24	0	0 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
10	1341-AP116	66.54	8.27	0	0 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ

Viewing Controller License Information

Follow these steps to view your controller's license information in AirWave:

1. Navigate to the **Devices > List page** and select a controller.
2. Navigate to the **Devices > Monitor** page for that controller.
3. In the **Device Info** table at the top of the page, select the **Licenses** link. A pop-up window appears listing all licenses.

Figure 23: *Controller License Popup from the **Devices > Monitor** page*

License Table for Chuck:

Service Type	Installed	Expires	Flag	Key
Access Points: 512	10/21/2012		E	F/luldyB-tPp9X7q5-SRXPUdRJ-gKmr5CPP-j2D
Internal Test Functions	10/16/2015		E	nbq1fJtt-Eq44rroM-06zsbiXT-9Ht8WFPV-3AxrZ
Next Generation Policy Enforcement Firewall Module: 512	10/21/2012		E	XxD6a4uH-BGWea+XP-DPRYRrg7-eut+loHA
Policy Enforcement Firewall for VPN users	10/21/2012		E	Eb/n2d02-9AeE6coJ-3J0Orfij-iaBu7tpX-Bi8sw6J
RF Protect: 512	10/21/2012		E	859Gc/BG-nQnXivjb-WMmHOVDT-dCjJOOvQ
Voice Service Module: 8192	10/20/2012		E	YNIGZ88x-UtVfvPlv-WKSX1LzM-564tsWH8-x

Rogue Device Classification

Complete the steps in this section if you have completed the WMS Offload procedure. After offloading WMS, AirWave maintains the primary ARM, WIPS, and WIDS state classification for all devices discovered over-the-air. See Table 3 below for details.

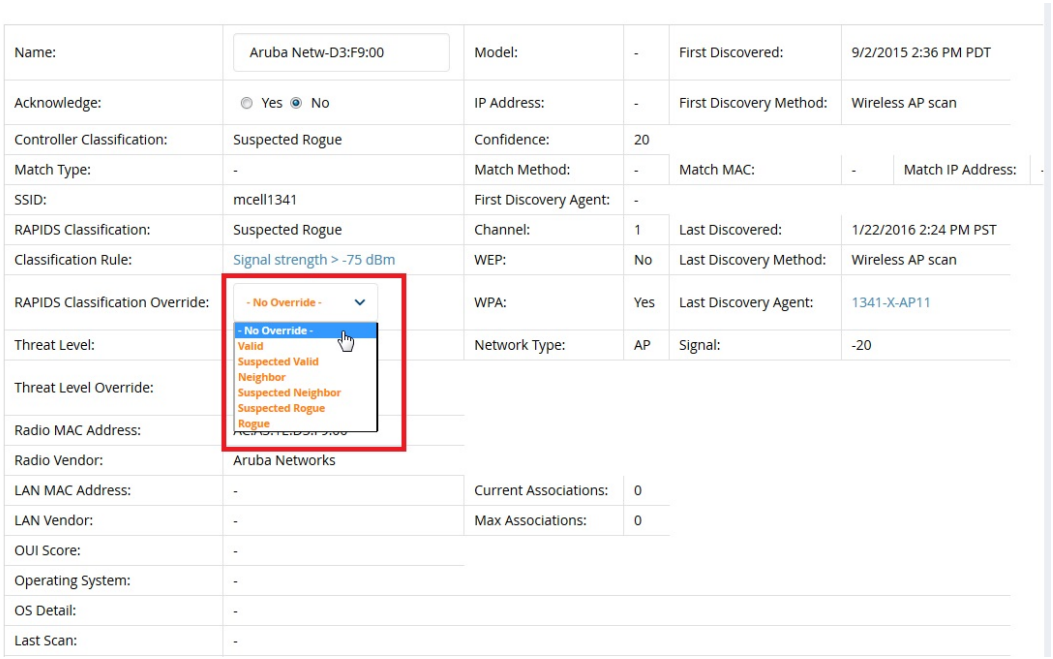
Table 3: *WIPS/WIDS to AirWave Controller Classification Matrix*

AirWave Controller Classification	ArubaOS (WIPS/WIDS)
Unclassified (default state)	Unknown
Valid	Valid
Suspected Valid	Suspected Valid
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Suspected Rogue	Suspected Rogue
Rogue	Rogue
Contained Rogue	DOS

To check and reclassify rogue devices, follow these steps:

1. Navigate to the **RAPIDS > Detail** page for a rogue device (see Figure 24 below).
2. Select the proper classification for the device from the **RAPIDS Classification Override** drop-down list.

Figure 24: *Rogue Detail Page Illustration*



CAUTION

Changing the controller's classification within the AirWave WebUI will push a reclassification message to all controllers managed by the AirWave server that are in Groups with Offloading the WMS database set to **Yes**. To reset the controller classification of a rogue device on AirWave, change the controller classification on the AirWave WebUI to unclassified.

Controller classification can also be updated from **RAPIDS > List** via the **Modify Devices** link.

All rogue devices will be set to a default controller classification of **unclassified** when WMS is first offloaded except for devices classified as valid. Rogue devices classified in ArubaOS as valid will also be classified within AirWave as valid for their controller classification as well. As APs report subsequent classification information about rogues, this classification will be reflected within AirWave WebUI and propagated to controllers that AirWave manages. The device classification reflected in the controller's WebUI and in the AirWave WebUI will probably not match, because the controller/APs do not reclassify rogue devices frequently.

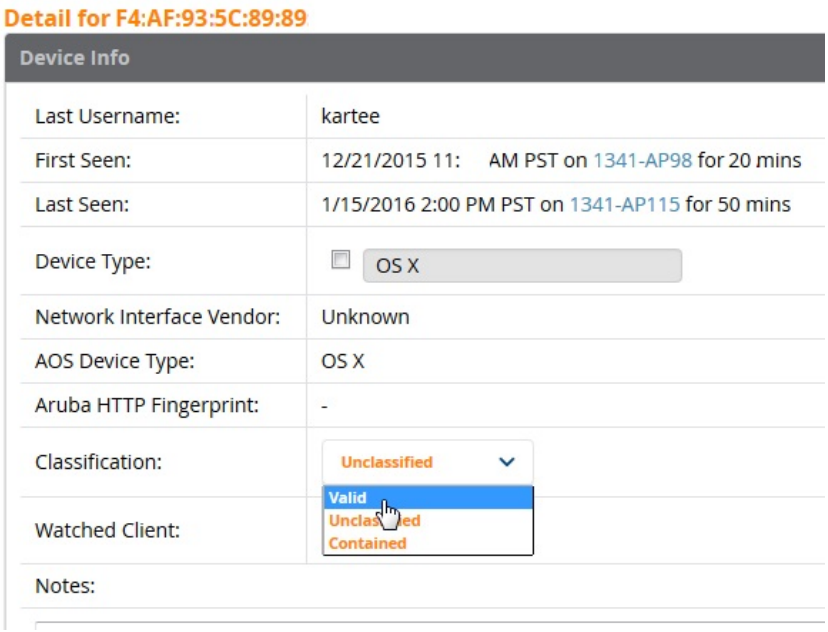
To update a group of devices' controller classification to match the ArubaOS device classification, navigate to **RAPIDS > List** and utilize the **Modify Devices** checkbox combined with the multiple sorting a filtering features.

Table 4: *ARM to AirWave Classification Matrix*

AirWave	AOS (ARM)
Unclassified (default state)	Unknown
Valid	Valid
Contained	DOS

1. Navigate to the **Clients > Client Detail** page for the user.
2. In the **Device Info** section, select the proper classification from the **Classification** drop-down list (see Figure 25):

Figure 25: *User Classification*



CAUTION

Changing User Classification within the AirWave WebUI will push a user reclassification message to all controllers managed by the AirWave server that are in Groups with Offloading the WMS database set to **Yes**.

All users will be set to a default classification of unclassified when WMS is first offloaded. As APs report subsequent classification information about users, this classification will be reflected within the AirWave WebUI and propagated to controllers that AirWave manages. It is probable that the user's classification reflected in the controller's WebUI and in the AirWave WebUI will not match, because the controllers/APs do not reclassify users frequently.

There is no method in the AirWave WebUI to update user classification before bulk to match the controller's classification. Each client must be updated individually within the AirWave WebUI .

Rules-Based Controller Classification

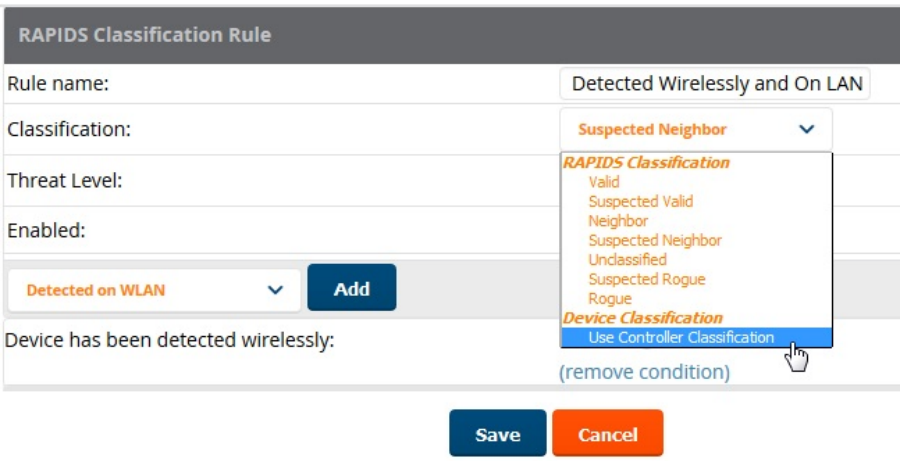
This section contains the following topics:

- "Using RAPIDS Defaults for Controller Classification" on page 38
- "Changing RAPIDS Based on Controller Classification" on page 38

Using RAPIDS Defaults for Controller Classification

1. Navigate to the **RAPIDS > Rules** page and select the pencil icon beside the rule that you want to change.
2. In the **Classification** drop-down list, select **Use Controller Classification** (see Figure 26 below).
3. Click **Save**.

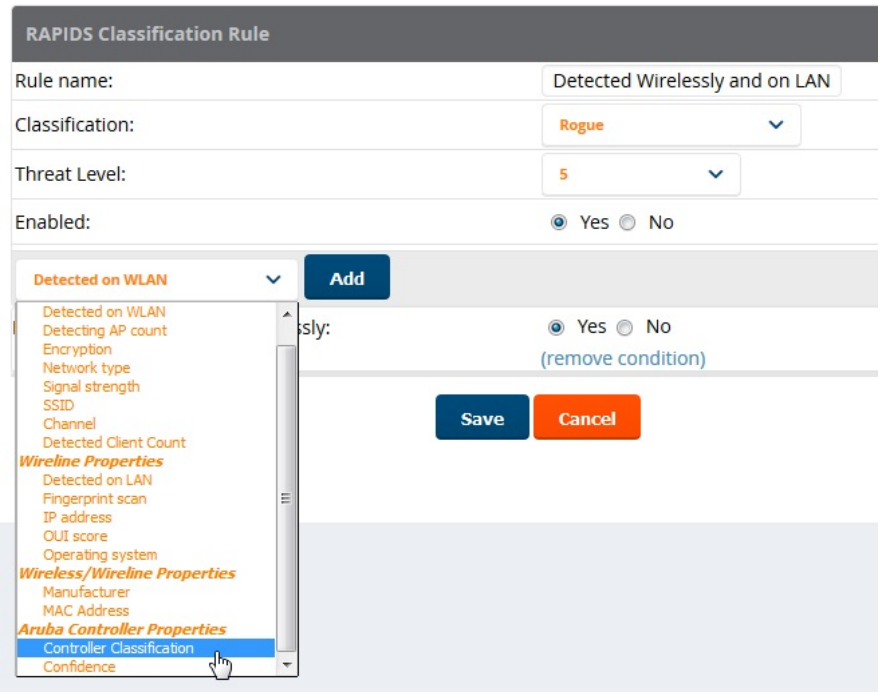
Figure 26: *Using Controller Classification*



Changing RAPIDS Based on Controller Classification

1. Navigate to **RAPIDS > Rules** and select the desired rule.
2. In the **Classification** menu, select the RAPIDS classification.
3. Select **Controller Classification** (see Figure 27 below).

Figure 27: *Configure Rules for Classification*



4. Click **Add**. A new Controller Classification field displays.
5. Select the desired controller classification to use as an evaluation in RAPIDS.
6. Click **Save**.

Enable Channel Utilization Events

Enabling these commands on ArubaOS versions prior to 6.1 can result in performance issues on the controller.

To enable channel utilization events utilizing the ArubaOS CLI, use SSH to access a local or master controller's command-line interface, enter **enable** mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # mgmt-server type amp primary-server <AMP IP> profile <profile-name>
(Controller-Name) (config) # write mem
```

Enable Stats With the ArubaOS CLI

The following commands enable collection of statistics (up to 25,000 entries) on the master controller for monitored APs and clients.

Do not use these commands if you use the AirWave WebUI to monitor APs and Clients. Enabling these commands on ArubaOS versions prior to 6.1 can result in performance issues on the controller.

Use SSH to access the command-line interface of the master controller or Mobility Master, enter **enable** mode, and issue the following commands:

```
(host) [mynode]  # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(host) [mynode] # ids wms-general-profile collect-stats
(host) [mynode] (IDS WMS General Profile) # exit
(host) [mynode]  # write mem
```

Offload WMS Using the ArubaOS CLI

Do not use these commands if you use the AirWave WebUI to monitor APs and clients.

Additional commands can be used to offload WMS using the ArubaOS command-line interface or the AirWave SNMP Walk. For information, see "ArubaOS CLI" on page 40.

ArubaOS CLI

Using ArubaOS 6.x

SSH into all ArubaOS 6.x controllers (local and master) , enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # mobility-manager <AMP IP> user <MMS-USER> <MMS-SNMP-PASSWORD>
(Controller-Name) (config) # write mem
```

This command allows the controller to communicate with an MMS server by creating an SNMPv3 user on the controller with the default authentication protocol configured to **SHA** and privacy protocol **DES**. The user and password must be at least eight characters because the Net-SNMP package in AirWave adheres to this IETF recommendation. ArubaOS automatically creates Auth and Privacy passwords from this single password. If mobility-manager is already using a preconfigured SNMPv3 user, ensure the privacy and authentication passwords are the same.

Using ArubaOS 8.x

SSH into all ArubaOS 8.x Mobility Master and managed devices, enter enable mode, and issue the following commands:

```
(host) [mm]) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(host) [mm] (config) #mobility-manager <AMP-IP> user <MMS-User> <MMS-Password> auth-prot md5
priv-prot DES
(Controller-Name) (config) # write mem
```

This command allows a managed device to communicate with a mobility manager server (MMS) and creates an SNMPv3 user on the controller with the authentication protocol configured to **MD5** and privacy protocol **DES**. The user and password must be at least eight characters because the Net-SNMP package in AirWave adheres to this IETF recommendation. ArubaOS automatically creates Auth and Privacy passwords from this single password. If mobility-manager is already using a preconfigured SNMPv3 user, ensure the privacy and authentication passwords are the same.

Pushing Configs from Master to Local Controllers

Use the following ArubaOS CLI commands to ensure that the master controller is properly pushing configuration settings from the master controller to local controllers. This command ensures configuration changes made on the master controller will propagate to all local controllers.

Do not use these commands if you use the AirWave WebUI to monitor APs and clients.

```
(Controller-Name) (config) # cfgm mms config disable
(Controller-Name) (config) # write mem
```

Disable Debugging Utilizing the ArubaOS CLI

If you are experiencing performance issues on the master controller, ensure that debugging is disabled. It should be disabled by default. Debugging coupled with gathering the enhanced statistics can put a strain on the controller's CPU, so it is highly recommended to disable debugging.

To disable debugging, SSH into the controller, enter enable mode, and issue the following commands:

```
(Controller-Name) # show running-config | include logging level debugging
```

If there is output, then use the following commands to remove the debugging:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # no logging level debugging <module from above>
(Controller-Name) (config) # write mem
```

Restart WMS on Local Controllers

To ensure local controllers are populating rogue information properly, use SSH to access the command-line interface of each local controller or managed device, enter enable mode, and issue the following commands:

```
(host) [mynode] # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(host) [mynode] # process restart wms
```

After executing the **restart wms** command in ArubaOS, you will need to wait until the next Rogue Poll Period on AirWave and execute a **Poll Now** operation for each local controller or managed device on the **Devices > List page** before rogue devices begin to appear in AirWave.

Configure ArubaOS CLI when not Offloading WMS

To ensure proper event correlation for IDS events when WMS is not offloaded to AirWave, access the command line interface of each controller (master and local), enter enable mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(Controller-Name) (config) # ids management-profile
(Controller-Name) (config) # ids general-profile <name>
(Controller-Name) (config) # ids-events logs-and-traps
(Controller-Name) (config) # write mem
```

Copy and Paste to Enable Proper Traps with the ArubaOS CLI

To ensure the proper traps are configured on Aruba controllers, copy and paste the following command in config mode:

```
snmp-server trap enable wlsxNUserAuthenticationFailed
wlsxAdhocNetworkBridgeDetected
wlsxAdhocNetworkBridgeDetectedAP
wlsxAdhocNetworkBridgeDetectedSta
wlsxAdhocNetworkDetected
wlsxAdhocUsingValidSSID
wlsxAPChannelChange
wlsxApFloodAttack
wlsxAPImpersonation
wlsxAPModeChange
wlsxAPPowerChange
wlsxAPSpoofingDetected
wlsxBlockAckAttackDetected
wlsxChannelFrameErrorRateExceeded
wlsxChannelFrameFragmentationRateExceeded
wlsxChannelFrameRetryRateExceeded
wlsxChannelRateAnomaly
wlsxChopChopAttack
wlsxClientAssociatedToHostedNetwork
wlsxClientAssociatingOnWrongChannel
wlsxClientFloodAttack
wlsxCTSRateAnomaly
wlsxDisconnectStationAttackAP
wlsxDisconnectStationAttackSta
wlsxEAPRateAnomaly
wlsxFataJackAttack
wlsxFrameBandWidthRateExceeded
wlsxFrameFragmentationRateExceeded
wlsxFrameLowSpeedRateExceeded
wlsxFrameNonUnicastRateExceeded
wlsxFrameReceiveErrorRateExceeded
```

```
wlsxFrameRetryRateExceeded
wlsxHostOfWirelessNetworkContainment
wlsxHotspotterAttackDetected
wlsxHT40MHzIntoleranceAP
wlsxHT40MHzIntoleranceSta
wlsxHtGreenfieldSupported
wlsxInvalidAddressCombination
wlsxInvalidMacOUIAP
wlsxInvalidMacOUISta
wlsxMalformedAssocReqDetected
wlsxMalformedAuthFrame
wlsxMalformedFrameLargeDurationDetected
wlsxMalformedFrameWrongChannelDetected
wlsxMalformedHTIEDetected
wlsxNAccessPointIsDown
wlsxNAccessPointIsUp
wlsxNAdhocNetwork
wlsxNAdhocNetworkBridgeDetectedAP
wlsxNAdhocNetworkBridgeDetectedSta
wlsxNAdhocUsingValidSSID
wlsxNAPMasterStatusChange
wlsxNAuthServerReqTimedOut
wlsxNDisconnectStationAttack
wlsxNIpSpoofingDetected
wlsxNodeRateAnomalyAP
wlsxNodeRateAnomalySta
wlsxNSignatureMatch
wlsxNSignatureMatchAirjack
wlsxNSignatureMatchAsleap
wlsxNSignatureMatchDeauthBcast
wlsxNSignatureMatchDisassocBcast
wlsxNSignatureMatchNetstumbler
wlsxNSignatureMatchNullProbeResp
wlsxNSignatureMatchWellenreiter
wlsxNStaUnAssociatedFromUnsecureAP
wlsxNUserAuthenticationFailed
wlsxNUserEntryAuthenticated
wlsxOmertaAttack
wlsxOverflowEAPOLKeyDetected
wlsxOverflowIEDetected
wlsxPowerSaveDosAttack
wlsxRepeatWEPIVViolation
wlsxReservedChannelViolation
wlsxRTSRateAnomaly
wlsxSequenceNumberAnomalyAP
wlsxSequenceNumberAnomalySta
wlsxSignalAnomaly
wlsxSignAPAirjack
wlsxSignAPAsleap
wlsxSignAPDeauthBcast
wlsxSignAPNetstumbler
wlsxSignAPNullProbeResp
wlsxSignatureMatchAP
wlsxSignatureMatchSta
wlsxSignStaAirjack
wlsxSignStaAsleap
wlsxSignStaDeauthBcast
wlsxSignStaNetstumbler
wlsxSignStaNullProbeResp
wlsxStaAssociatedToUnsecureAP
wlsxStaImpersonation
```

```
wlsxStaPolicyViolation
wlsxStaRepeatWEPIVViolation
wlsxStaUnAssociatedFromUnsecureAP
wlsxStaWeakWEPIVViolation
wlsxTKIPReplayAttack
wlsxUserEntryAttributesChanged
wlsxValidClientMisassociation
wlsxValidClientNotUsingEncryption
wlsxValidSSIDViolation
wlsxWeakWEPIVViolation
wlsxWEPMisconfiguration
wlsxWindowsBridgeDetected
wlsxWindowsBridgeDetectedAP
wlsxWindowsBridgeDetectedSta
wlsxWirelessBridge
wlsxWirelessHostedNetworkContainment
wlsxWirelessHostedNetworkDetected
```

You will need to issue the `write mem` command.

Appendix B
AirWave Data Acquisition Methods

The tables below describe the different methods through which AirWave acquires data from Aruba devices on the network.

The tables use the following symbols:

- ← Initiated by AirWave
- → Initiated by Controller, Switch, or Instant Virtual Controller
- ↑ Initiated by AirWave to a separate device

Table 5: *Data Flow between Controllers and AirWave*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
802.11 Counters	←											
AP Up/Down Status	←	→										
ARM Events				→								
Channel Utilization				→								
Client Hostname											↑	
Client Match Events				→								
Client Monitoring	←			→								If Prefer AMON enabled it's done by AMON. Requires ArubaOS 6.3 or later and AirWave 7.7.7 or later.
Configuration Audit			←									
Configuration Push			←									
Controller Up/Down Status	←							←				

Table 5: *Data Flow between Controllers and AirWave (Continued)*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Device CPU/Memory	←											
Enabling of WMS Offload			←									
Exec UI							→					When AMON is used for client monitoring, AirWave uses this at startup time to get current user status.
Firewall Stats				→								
Firmware Images							↑			←		Images are sent to controller over FTP/TFTP. They can be transferred to AirWave via HTTPS from a user or from https://images.arubanetworks.com .
IDS Events		→										
Interface Monitoring	←											
Lync/UCC/Voice				→								Available in AirWave 8.0 and later.
Neighbor Clients	←			→								
Network Derivations			←									
RADIUS Auth Issues		→										
RAPIDS	←											
RF Capacity				→								
RF Health				→								

Table 5: *Data Flow between Controllers and AirWave (Continued)*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Rogue AP OS									↑			
Rogue Classification	←				←							If WMS Offload enabled, AirWave updates rogue classifications on a controller using PAPI; otherwise it's done with SNMP.
Rogue Clients	←											
Syslog						→						
VisualRF	←			→								VisualRF's client data comes from AirWave, which gets its data from SNMP + AMON.

Table 6: *Data Flow between Instant Devices and AirWave*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
All Monitoring Data							→					VC sends data to AirWave every minute in an HTTP POST.
Configuration Commands							→					When AirWave needs to send data to a VC, it sends it in the HTTPS response.
Diagnostic Commands							→					
Firmware Images							→					

Table 7: *Data Flow between MAS and AirWave*

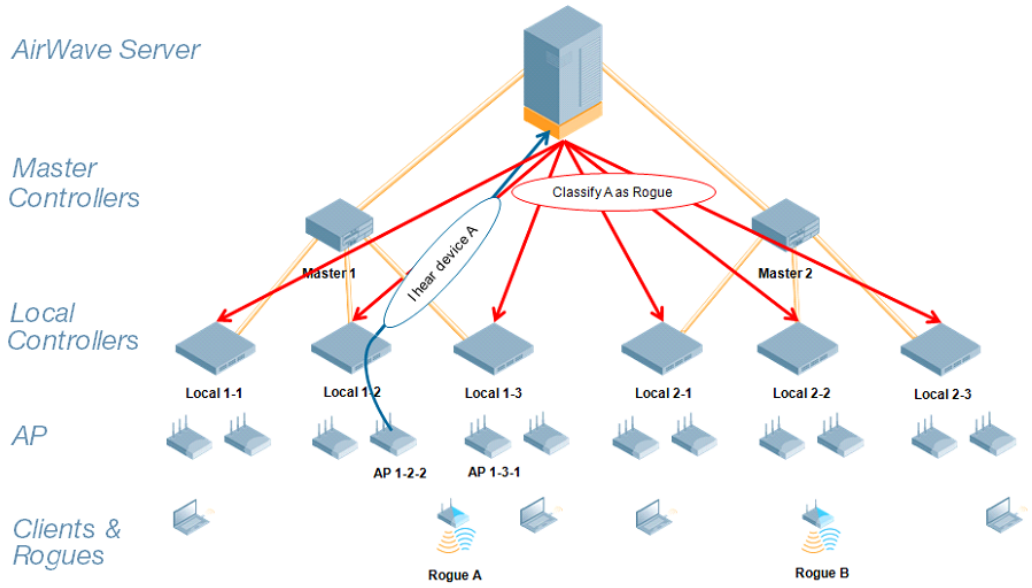
Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Configuration			←									

Table 7: *Data Flow between MAS and AirWave (Continued)*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Firmware Images										←		
Monitoring Data	←											
Syslog						→						
Traps		→										
Up/Down Status	←							←				
Zero-Touch Provisioning			←				→					

WMS Offload instructs the master controller to stop correlating ARM, WIPS, and WIDS state information among its local controllers because AirWave will assume this responsibility. Figure 28 depicts how AirWave communicates state information with local controllers.

Figure 28: *ARM/WIPS/WIDS Classification Message Workflow*



State Correlation Process

1. AP-1-3-1 hears rogue device A.
2. Local controller 1-3 evaluates devices and does initial classification and sends a classification request to AirWave.
3. AirWave receives message and reclassifies the device if necessary and reflects this within the AirWave WebUI and via SNMP traps, if configured.
4. AirWave sends a classification message back to all local controllers managed by master controller 1, (1-1, 1-2, and 1-3).
5. AirWave sends a classification message back to all additional local controllers managed by the AirWave server. In this example all local controllers under master controller 2, (2-1, 2-2, and 2-3) would receive the classification messages.
6. If an administrative AirWave user manually overrides the classification, then AirWave will send a re-classification message to all applicable local controllers.
7. AirWave periodically polls each local controller's MIB to ensure state parity with the AirWave database. If the local controller's device state does not comply with the AirWave database, AirWave will send a re-classification message to bring it back into compliance.

NOTE

The Rogue Detail page includes a BSSID table for each rogue that displays the desired classification and the classification on the device.

Using AirWave as a Master Device State Manager

AirWave offers the following benefits as a master device state manager:

- Ability to correlate state among multiple master controllers. This will reduce delays in containing a rogue device or authorizing a valid device when devices roam across a large campus.
- Ability to correlate state of third party access points with ARM. This will ensure that Aruba infrastructure inter-operates more efficiently in a mixed infrastructure environment.
- Ability to better classify devices based on AirWave wire-line information not currently available in ArubaOS.
- AirWave provides a near real-time event notification and classification of new devices entering air space.
- RAPIDS gains additional wire-line discovery data from Aruba controllers.

This appendix describes the impact that band steering can have on location accuracy. It also explains how RTLS can be used to increase location accuracy.

Understand Band Steering's Impact on Location

Band steering can negatively impact location accuracy when testing in a highly mobile environment. The biggest hurdles to overcome are scanning times in 5 GHz frequency.

Table 8: *Location accuracy impact*

Operating Frequency	Total Channels	Scanning Frequency	Scanning Time	Total Time One Pass
2.4 GHz	11 (US)	10 seconds	110 milliseconds	121.21 seconds
5 GHz	24 (US)	10 seconds	110 milliseconds	242.64 seconds

Leveraging RTLS to Increase Accuracy

This section provides instructions for integrating the AirWave and Aruba WLAN infrastructure with Aruba's RTLS feed to more accurately locate wireless clients and Wi-Fi Tags.

Prerequisites

You will need the following information to monitor and manage your Aruba infrastructure.

- Ensure that the AirWave server is already monitoring Aruba infrastructure.
- Ensure that the WMS Offload process is complete.
- Ensure that the firewall configuration for port 5050 (default port) supports bidirectional UDP communication between the AirWave server's IP address and each access point's IP address.

Deployment Topology

Figure 29: *Typical Client Location*

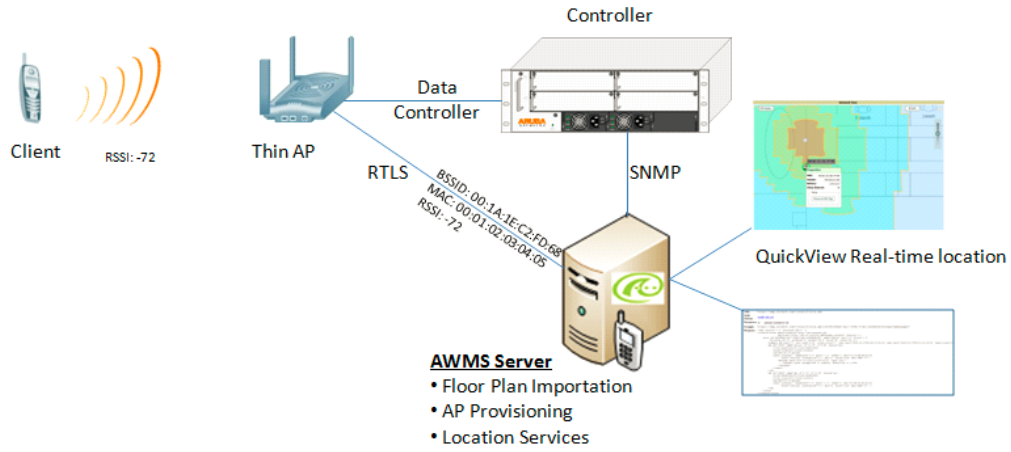
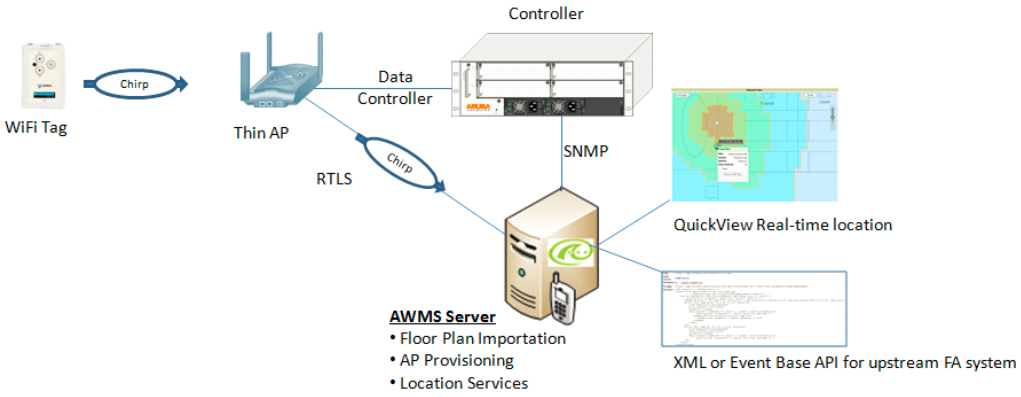


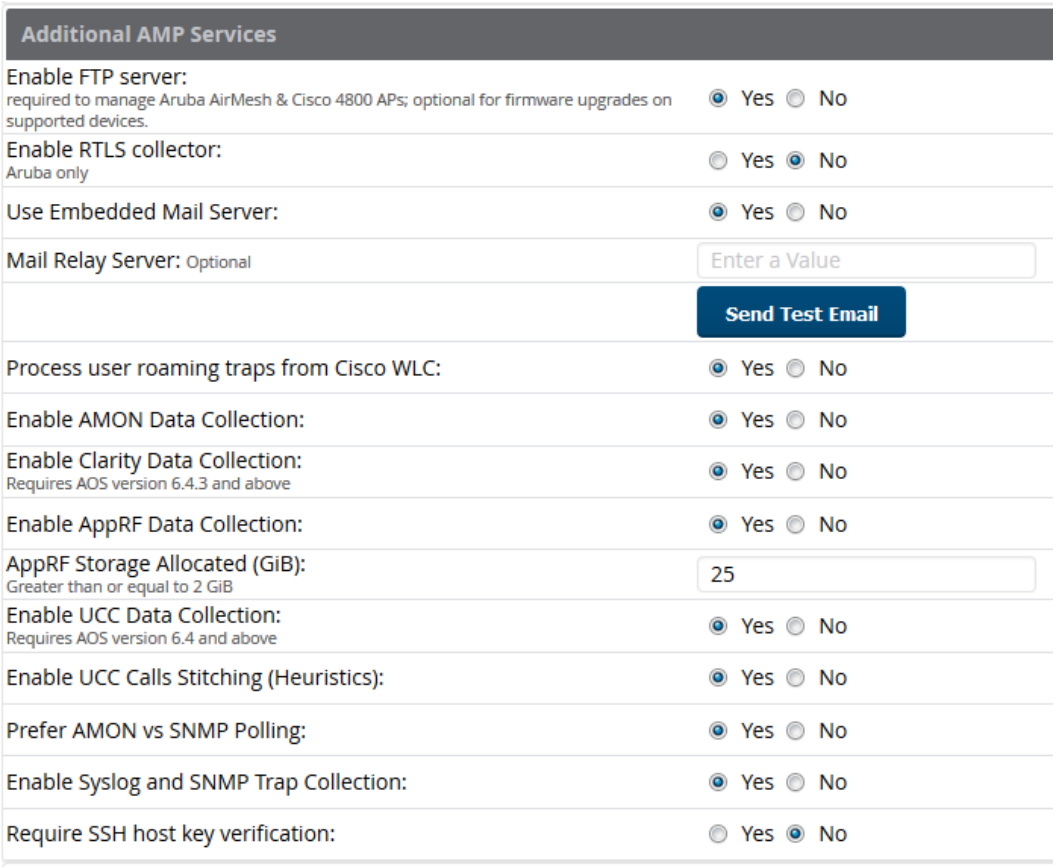
Figure 30: *Typical Tag Deployment*



Enable RTLS Service on the AirWave Server

1. Navigate to **AMP Setup > General** and locate the **Additional AMP Services** section.
2. Select **Yes** for the **Enable RTLS Collector** option (see Figure 31 below).
3. A new section will automatically appear with the following settings:
   - **RTLS Port**—The match controller default is 5050.
   - **RTLS Username—**This must match the SNMPv3 MMS user name configured on the controller.
   - **RTLS Password—**This must match the SNMPv3 MMS password configured on the controller.
4. Click **Save**.

Figure 31: *RTLS Fields in* ***AMP Setup> General> Additional AMP Services***



Enable RTLS on the Controller

RTLS can only be enabled on the master controller and it will automatically be propagated to all local controllers.

SSH into master controller, enter **enable** mode, and issue the following commands:

```
(Controller-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(Controller-Name) (config) # ap system-profile <Thin-AP-Profile-Name>

(Controller-Name) (AP system profile default) # rtls-server ip-addr <IP of AirWave Server> port
5050 key <Controller-SNMPv3-MMS-Password>

(Controller-Name) (AP system profile default) # write mem
```

To validate exit configuration mode:

```
(Controller-Name) # show ap monitor debug status ip-addr <AP-IP-Address>
...
RTLS configuration
------------------
Type       Server IP   Port Frequency Active
----       ---------   ---- --------- ------
MMS        10.51.2.45  5070  120
```

```
Aeroscout  N/A          N/A   N/A
RTLS       10.51.2.45   5050  60          *
```

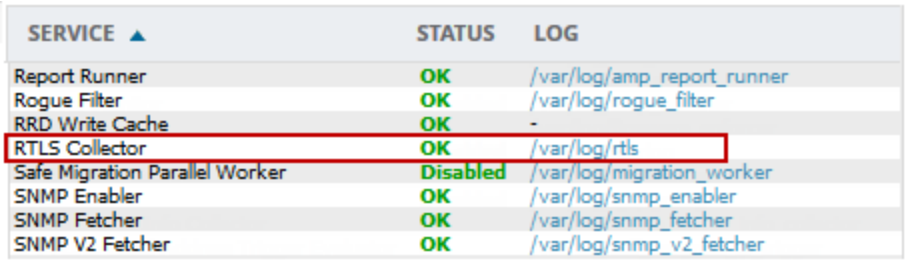
Troubleshooting RTLS

You can use either the WebUI or CLI to ensure the RTLS service is running on your AirWave server.

Using the WebUI to See Status

1. In the AirWave WebUI, navigate to the **System > Status** page.
2. Scroll down through the Services list to locate the RTLS service, as shown below.

Figure 32: *RTLS System Status*



SERVICE ▲	STATUS	LOG
Report Runner	OK	/var/log/amp_report_runner
Rogue Filter	OK	/var/log/rogue_filter
RRD Write Cache	OK	-
RTLS Collector	OK	/var/log/rtls
Safe Migration Parallel Worker	Disabled	/var/log/migration_worker
SNMP Enabler	OK	/var/log/snmp_enabler
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher

Wi-Fi Tag Setup Guidelines

- Ensure that the tags can be heard by at least three access points from any given location. The recommended value is four APs.
- Ensure that the tags chirp on all regulatory channels.