Dell Networking W-AirWave 7.7

Best Practices Guide

Copyright

Open Source Code

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Chapter 1 Overview

This document provides best practices for leveraging AirWave to monitor and manage your Dell Networking W-Series infrastructure. Dell Networking W-Series wireless infrastructure 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 Dell Networking W-Series infrastructure.

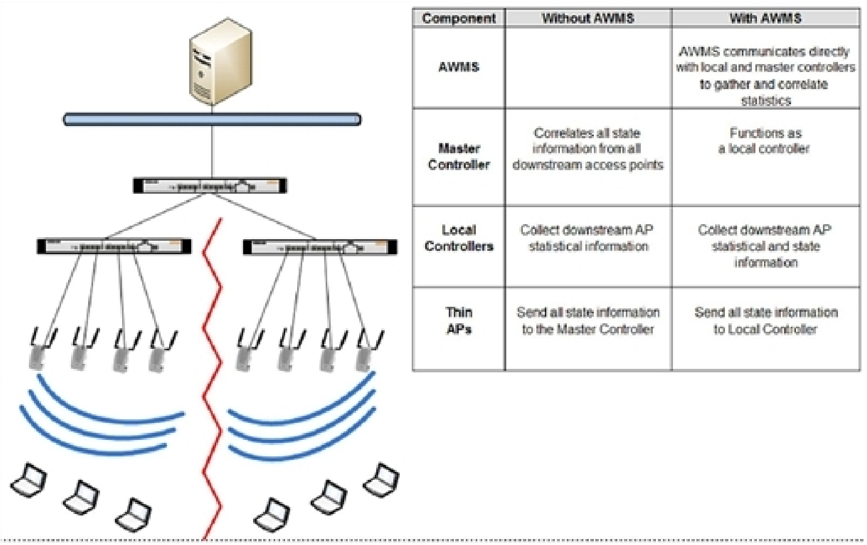
This overview chapter contains the following topics:

- "Understanding Dell Networking W-Series Topology" on page 5
- "Prerequisites for Integrating Dell Networking W-Series Infrastructure " on page 5

Understanding Dell Networking W-Series Topology

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

Figure 1 *Typical Dell Networking W-Series 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 Dell Networking W-Series Infrastructure

You will need the following information to monitor and manage your Dell Networking W-Series infrastructure:

- SNMP community string (monitoring and discovery)
- Telnet/SSH credentials (configuration only)
- **Enable** password (configuration only)

NOTE

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

- SNMPv3 credentials are required for WMS Offload:
  - Username
  - Auth password
  - Privacy password
  - Auth protocol

Chapter 2
Configuring AirWave for Global W-Series Infrastructure

This section explains how to optimally configure AirWave to globally manage your global Dell Networking W-Series infrastructure. Refer to the following topics:

- "Disabling Rate Limiting in AMP Setup > General" on page 7
- "Entering Credentials in Device Setup > Communication" on page 8
- "Setting Up Recommended Timeout and Retries" on page 9
- "Setting Up Time Synchronization" on page 9
- "Enabling Support for Channel Utilization And Statistics" on page 9

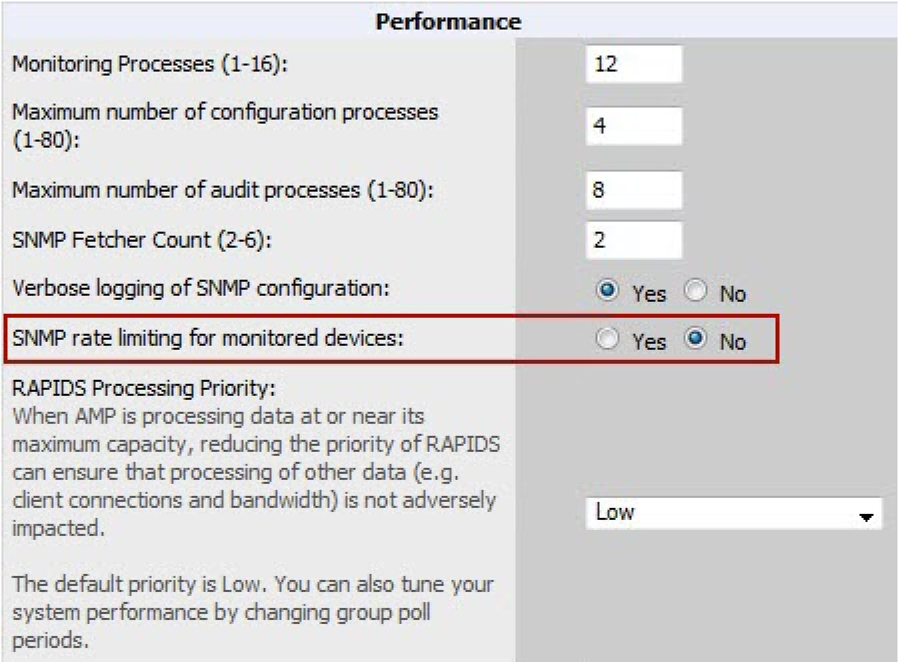
Disabling Rate Limiting in AMP Setup > General

The SNMP Rate Limiting for Monitored Devices option adds a small delay between each SNMP GET request, thus the actual polling intervals will be longer than what is configured. For example, setting a 10-minute polling interval will result in an actual 12-minute polling interval. Disabling rate limiting is recommended in most cases.

To disable rate limiting in AirWave, follow these steps:

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

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



Performance	
Monitoring Processes (1-16):	12
Maximum number of configuration processes (1-80):	4
Maximum number of audit processes (1-80):	8
SNMP Fetcher Count (2-6):	2
Verbose logging of SNMP configuration:	● Yes ○ No
SNMP rate limiting for monitored devices:	○ Yes ● No
RAPIDS Processing Priority: When AMP is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (e.g. client connections and bandwidth) is not adversely impacted. The default priority is Low. You can also tune your system performance by changing group poll periods.	Low

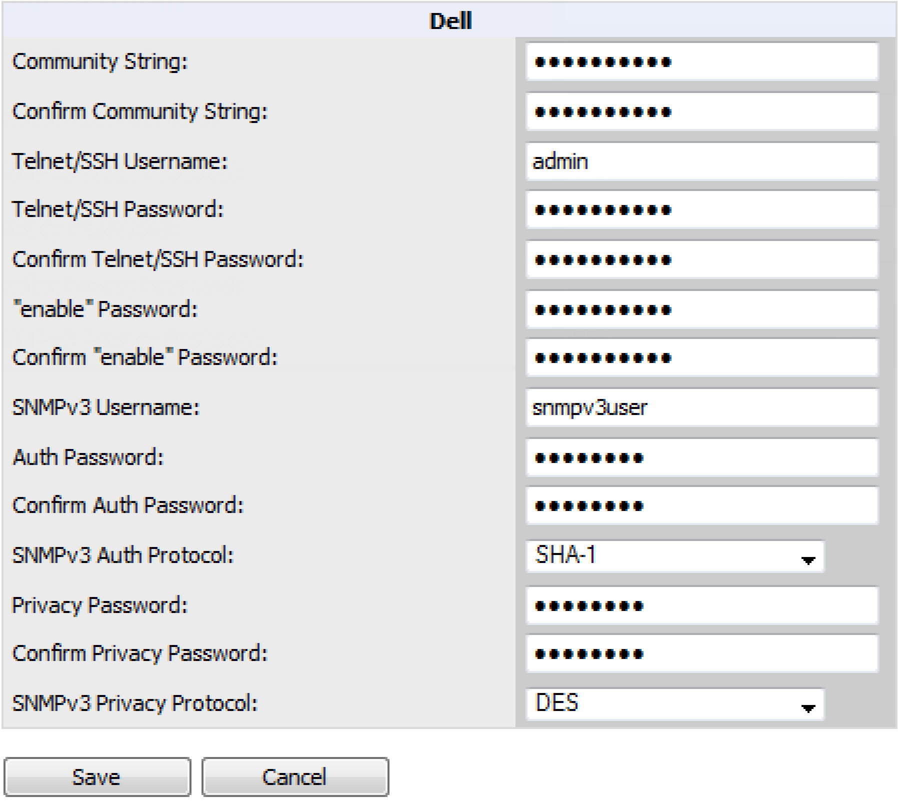
Entering Credentials in Device Setup > Communication

AirWave requires several credentials to properly interface with Dell Networking W-Series 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 Dell. 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***



Dell

Community String:	●●●●●●●●●●
Confirm Community String:	●●●●●●●●●●
Telnet/SSH Username:	admin
Telnet/SSH Password:	●●●●●●●●●●
Confirm Telnet/SSH Password:	●●●●●●●●●●
"enable" Password:	●●●●●●●●●●
Confirm "enable" Password:	●●●●●●●●●●
SNMPv3 Username:	snmpv3user
Auth Password:	●●●●●●●●
Confirm Auth Password:	●●●●●●●●
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	●●●●●●●●
Confirm Privacy Password:	●●●●●●●●
SNMPv3 Privacy Protocol:	DES

4. Enter the required fields for configuration and basic monitoring:
   - Telnet/SSH Username
   - Telnet/SSH Password
   - enable Password
5. Enter the required fields for WMS Offload:
   - SNMPv3 Username
   - Auth Password
   - SNMPv3 Auth Protocol
   - Privacy Password
   - SNMPv3 Privacy Protocol

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

6. Click **Save** when you are finished.

Setting Up Recommended Timeout and Retries

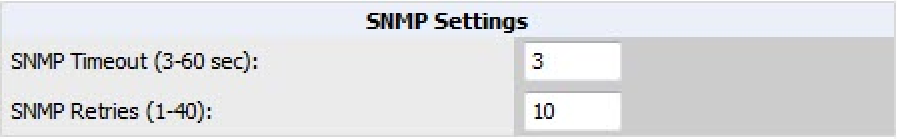
To set recommended timeout and retries settings, follow these steps:

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).

NOTE

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

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



SNMP Settings

SNMP Timeout (3-60 sec): 3

SNMP Retries (1-40): 10

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**.

Enabling Support for Channel Utilization And Statistics

In order to enable support for channel utilization statistics, you must have the following:

- Dell Networking W-AirWave 7.2 or later
- Dell Networking W-Series ArubaOS 6.0.1 or later

NOTE

Dell Networking W-Series ArubaOS 6.0.1 can report RF utilization metrics, while ArubaOS 6.1 is necessary to also obtain classified interferer information.

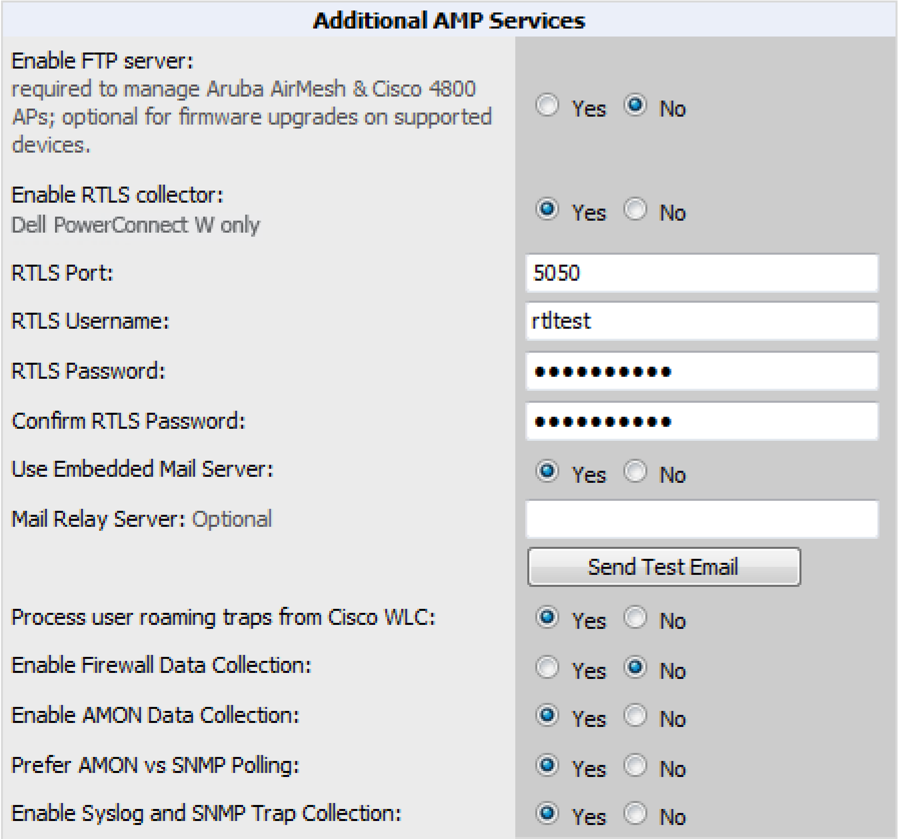
- Access points - Dell Networking W-AP92, W-AP93, W-AP105, W-AP124, W-AP125, W-AP134, W-AP135
- Controllers - Dell Networking W-600 Series, W-3000 Series, W-6000M3, or W-7200 Series

AirWave Setup

Follow these steps in AirWave:

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**.

Figure 5 *AMON Data Collection setting in* ***AMP Setup > General***



Additional AMP Services

Enable FTP server: required to manage Aruba AirMesh & Cisco 4800 APs; optional for firmware upgrades on supported devices.	○ Yes ● No
Enable RTLS collector: Dell PowerConnect W only	● Yes ○ No
RTLS Port:	5050
RTLS Username:	rtltest
RTLS Password:	••••••••••
Confirm RTLS Password:	••••••••••
Use Embedded Mail Server:	● Yes ○ No
Mail Relay Server: Optional	
	Send Test Email
Process user roaming traps from Cisco WLC:	● Yes ○ No
Enable Firewall Data Collection:	○ Yes ● No
Enable AMON Data Collection:	● Yes ○ No
Prefer AMON vs SNMP Polling:	● Yes ○ No
Enable Syslog and SNMP Trap Collection:	● Yes ○ No

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

Controller Setup (Master And Local)

CAUTION

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.

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) # write mem
```

CAUTION

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

Chapter 3

Configuring a Dell Networking W Group in AirWave

It is prudent to establish one or more Dell Networking W 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 11
- "Advanced Configuration " on page 12

Basic Monitoring Configuration

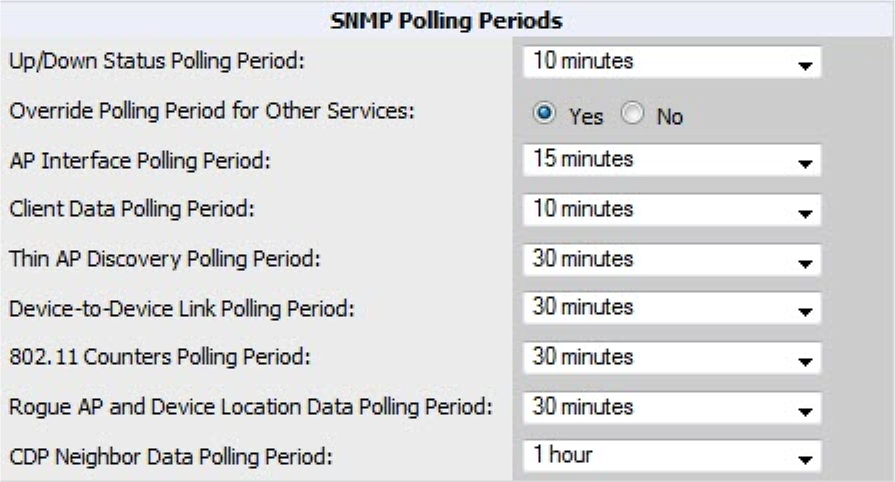
1. Navigate to **Groups** > **List**.
2. Select **Add**.
3. Enter a **Name** that represents the Dell Networking W-Series device infrastructure from a security, geographical, or departmental perspective and select **Add**.
4. You will be redirected to the **Groups** > **Basic** page for the Group you just created. On this page you will need to verify and/or change the following Dell-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.

NOTE

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**.

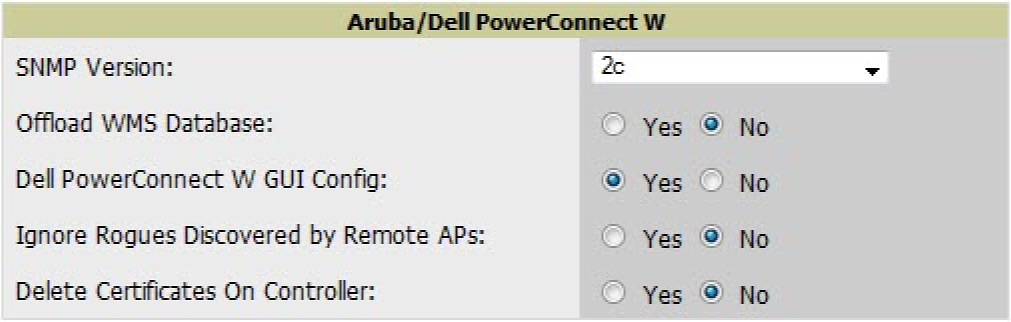
Figure 6 *SNMP Polling Periods section of **Groups > Basic***



SNMP Polling Periods	
Up/Down Status Polling Period:	10 minutes
Override Polling Period for Other Services:	● Yes ○ No
AP Interface Polling Period:	15 minutes
Client Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	30 minutes
Device-to-Device Link Polling Period:	30 minutes
802.11 Counters Polling Period:	30 minutes
Rogue AP and Device Location Data Polling Period:	30 minutes
CDP Neighbor Data Polling Period:	1 hour

5. Locate the Aruba/Dell Networking W section of this page, as illustrated in Figure 7.
6. Configure the proper **SNMP Version** for monitoring the Dell Networking W-Series infrastructure.

Figure 7 *Group SNMP Version for Monitoring*



Aruba/Dell PowerConnect W

SNMP Version:	2c
Offload WMS Database:	○ Yes ● No
Dell PowerConnect W GUI Config:	● Yes ○ No
Ignore Rogues Discovered by Remote APs:	○ Yes ● No
Delete Certificates On Controller:	○ Yes ● No

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

Advanced Configuration

Refer to the *Dell Networking W-AirWave Controller Configuration Guide* at **dell.com/support/manuals** for detailed instructions.

Chapter 4
Discovering Dell Networking W-Series Infrastructure

AirWave utilizes the Dell Networking W-Series topology to efficiently discover downstream infrastructure. This section guides you through the process of discovering and managing your Dell Networking W-Series device infrastructure.

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

- "Configuring AirWave for Global W-Series Infrastructure" on page 7
- "Configuring a Dell Networking W Group in AirWave" on page 11

The following topics in this chapter walk through the basic procedure for discovering and managing Dell Networking W-Series infrastructure:

- "Discovering or Adding Master Controllers" on page 13
- "Local Controller Discovery" on page 15
- "Thin AP Discovery" on page 15

NOTE

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 Dell Networking W-Series master controllers from **Device Setup** > **Discover.**

- or -

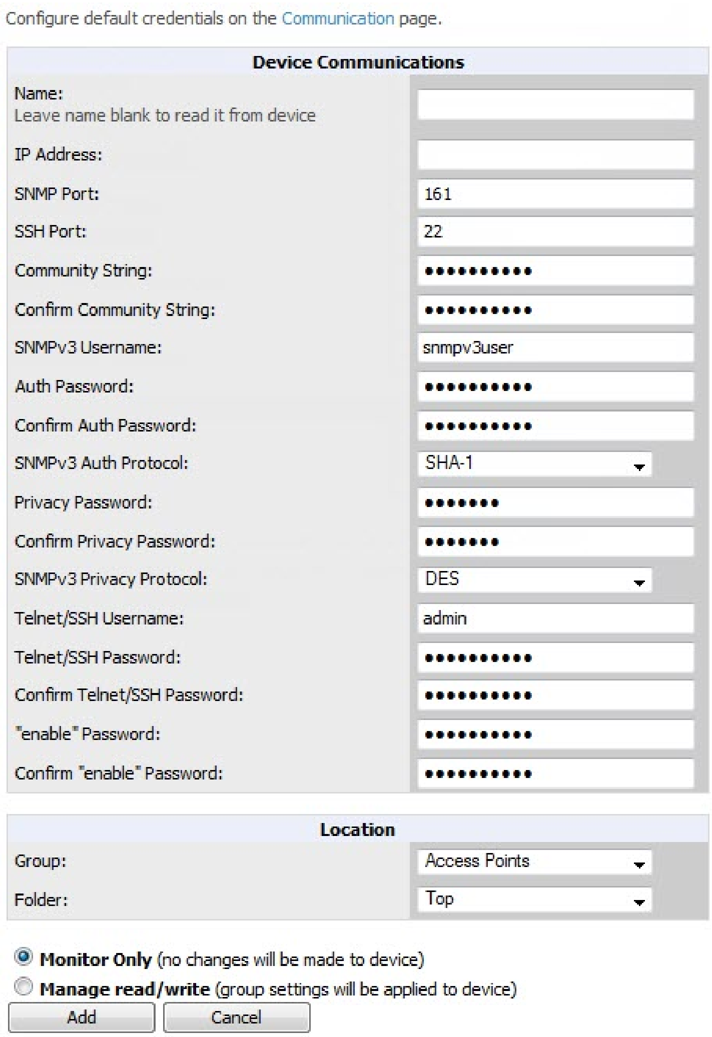
Manually enter the master controller by following these steps in the **Device Setup** > **Add** page:

1. Select the **Dell** Controller 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.

NOTE

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 *Dell Networking W Credentials in **Device Setup > Add***



Configure default credentials on the Communication page.

Device Communications

Name: Leave name blank to read it from device	
IP Address:	
SNMP Port:	161
SSH Port:	22
Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	snmpv3user
Auth Password:	••••••••••
Confirm Auth Password:	••••••••••
SNMPv3 Auth Protocol:	SHA-1
Privacy Password:	•••••••
Confirm Privacy Password:	•••••••
SNMPv3 Privacy Protocol:	DES
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••

Location

Group:	Access Points
Folder:	Top

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

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

4. Enter the required fields for configuration and basic monitoring:
   - Telnet/SSH Username
   - Telnet/SSH password
   - enable password
5. Enter the required fields for WMS Offload
   - SNMPv3 Auth Protocol
   - SNMPv3 Privacy Protocol
   - SNMPv3 Username
   - Auth Password
   - Privacy Password

NOTE

The protocols for SNMPv3 Auth and SNMPv3 Privacy should 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.

NOTE

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

8. Select **Add**.
9. Navigate to the **APs/Devices** > **New** page.
10. Select the Dell Networking W-Series 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 **APs/Devices** > **Monitor** page, the local controllers will appear on the **APs/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 **APs/Devices** > **Monitor** page, thin APs will appear on the **APs/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.

AirWave and Dell Networking W-Series Integration Strategies

This section describes strategies for integrating AirWave and Dell Networking W-Series devices and contains the following topics:

Integration Goals

The following table summarizes the types of integration goals and strategies for meeting them in certain architectural contexts:

Table 1: *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 RTLS WMS Offload	enable RTLS WMS Offload
Channel Utilization	enable AMON	enable AMON
Spectrum	enable AMON	enable AMON
Policy Enforcement Firewall (PEF) visibility	enable AMON	enable AMON
Health Information	enable 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 18
- "When to Use WMS Offload" on page 18
- "When to Use RTLS" on page 18
- "When to Define AirWave as a Trap Host" on page 18
- "When to Use Channel Utilization" on page 19

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.

NOTE

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

See "Enable Stats Utilizing AirWave" on page 19.

When to Use WMS Offload

- You have older Dell Networking W-Series infrastructure in a master/local environment and their master controller is fully taxed. Offloading WMS will increase the capacity of the master controller by offloading statistic 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 20
  - "Understanding WMS Offload Impact on Dell Networking W-Series Infrastructure" on page 24
  - "WMS Offload Details" on page 43

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 WiFi Tags.

NOTE

RTLS can negatively impact your AirWave server's performance.

- See "Leveraging RTLS to Increase Accuracy" on page 45.

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 Dell Networking W-Series 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 21.

When to Use Channel Utilization

- You have a minimum version of ArubaOS 6.1.0.0 and W-AP105 or W-AP135.

Prerequisites for Integration

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

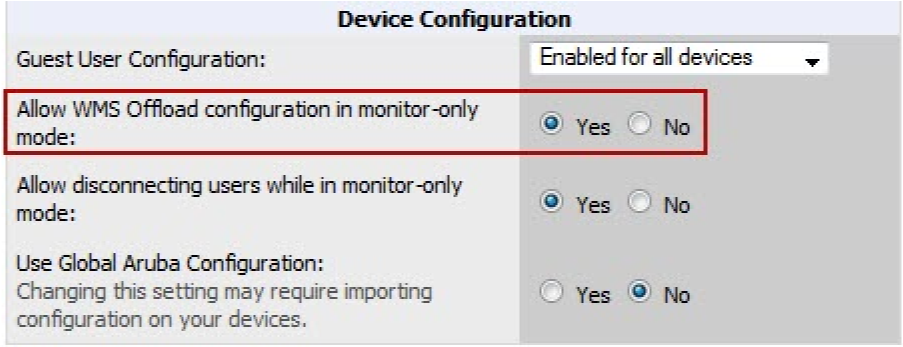
- "Configuring AirWave for Global W-Series Infrastructure" on page 7
- "Configuring a Dell Networking W Group in AirWave" on page 11
- "Discovering Dell Networking W-Series Infrastructure" on page 13

Enable Stats Utilizing AirWave

To enable stats on the Dell Networking W-Series 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:

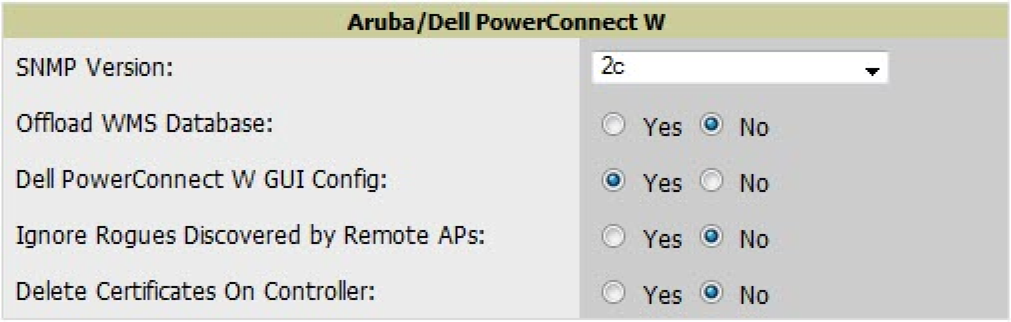
Figure 9 *WMS Offload Configuration in* ***AMP Setup > General***



Device Configuration	
Guest User Configuration:	Enabled for all devices ▾
Allow WMS Offload configuration in monitor-only mode:	● Yes ○ No
Allow disconnecting users while in monitor-only mode:	● Yes ○ No
Use Global Aruba Configuration: Changing this setting may require importing configuration on your devices.	○ Yes ● No

3. Navigate to **Groups** > **Basic** for the group that contains your Dell Networking W-Series controllers.
4. Locate the Dell Networking W 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***



Aruba/Dell PowerConnect W	
SNMP Version:	2c
Offload WMS Database:	○ Yes ● No
Dell PowerConnect W GUI Config:	● Yes ○ No
Ignore Rogues Discovered by Remote APs:	○ Yes ● No
Delete Certificates On Controller:	○ Yes ● No

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

This will push a set of commands via SSH to all Dell Networking W-Series 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 don't 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 37 for information on how to utilize the ArubaOS CLI to enable stats on Dell Networking W-Series infrastructure.

If your credentials are invalid or the changes are not applied to the controller, error messages will display on the controller's **APs/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 37 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 Dell Networking W-Series 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 Dell Networking W-Series 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 in order to push these commands
3. Navigate to **Groups** > **Basic** and locate the **Dell Networking W** section.
4. Set the **Offload WMS Database** field to **Yes**.

NOTE

This process will not reboot your controllers. See "ArubaOS and AirWave CLI Commands" on page 37 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 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 W-Series Infrastructure" on page 7.

```
(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.

ArubaOS Traps Utilized by AirWave

The following are Auth, IDS, and ARM traps utilized by AirWave:

- "Auth Traps " on page 21
- "IDS Traps " on page 22
- "ARM Traps" on page 23

Auth Traps

- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimedOut

IDS Traps

- wlsxwlsxSignatureMatchAP
- wlsxSignatureMatchSta
- wlsxSignAPNetstumbler
- wlsxSignStaNetstumbler
- wlsxSignAPAsleap
- wlsxSignStaAsleap
- wlsxSignAPAirjack
- wlsxSignStaAirjack
- wlsxSignAPNullProbeResp
- wlsxSignStaNullProbeResp
- wlsxSignAPDeauthBcast
- wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
- wlsxChannelFrameFragmentationRateExceeded
- wlsxChannelFrameRetryRateExceeded
- wlsxNIpSpoofingDetected
- wlsxStaImpersonation
- wlsxReservedChannelViolation
- wlsxValidSSIDViolation
- wlsxStaPolicyViolation
- wlsxRepeatWEPIVViolation
- wlsxWeakWEPIVViolation
- wlsxFrameRetryRateExceeded
- wlsxFrameReceiveErrorRateExceeded
- wlsxFrameFragmentationRateExceeded
- wlsxFrameBandWidthRateExceeded
- wlsxFrameLowSpeedRateExceeded
- wlsxFrameNonUnicastRateExceeded
- wlsxChannelRateAnomaly
- wlsxNodeRateAnomalyAP
- wlsxNodeRateAnomalySta
- wlsxEAPRateAnomaly
- wlsxSignalAnomaly
- wlsxSequenceNumberAnomalyAP
- wlsxSequenceNumberAnomalySta
- wlsxApFloodAttack
- wlsxInvalidMacOUIAP
- wlsxInvalidMacOUISta
- wlsxStaRepeatWEPIVViolation
- wlsxStaWeakWEPIVViolation
- wlsxStaAssociatedToUnsecureAP
- wlsxStaUnAssociatedFromUnsecureAP

- wlsxAPImpersonation
- wlsxDisconnectStationAttackAP
- wlsxDisconnectStationAttackSta

ARM Traps

- AP Power Change
- AP Mode Change
- AP Channel Change

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>
```

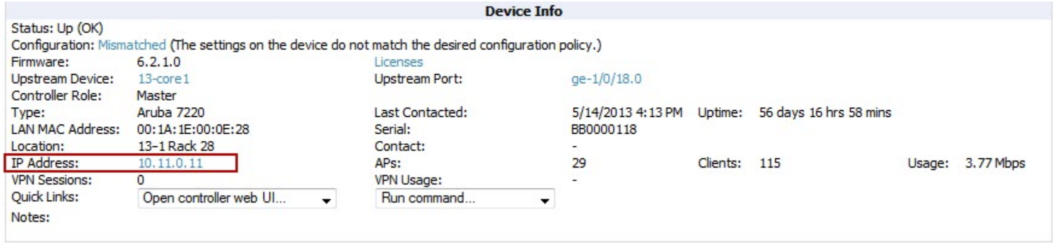
NOTE

See "ArubaOS CLI" on page 37 for the full command that can be copied and pasted directly into the ArubaOSCLI.

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

Ensure the source IP of the traps match the IP that AirWave utilizes to manage the controller, as shown in Figure 11. Navigate to **APs/Devices** > **Monitor** to validate the IP address in the **Device Info** section.

Figure 11 *Verify IP Address on* ***APs/Devices > Monitor*** *Page*



Device Info

Status: Up (OK)

Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)

Firmware:	6.2.1.0	Licenses					
Upstream Device:	13-core1	Upstream Port:	ge-1/0/18.0				
Controller Role:	Master						
Type:	Aruba 7220	Last Contacted:	5/14/2013 4:13 PM	Uptime:	56 days 16 hrs 58 mins		
LAN MAC Address:	00:1A:1E:00:0E:28	Serial:	BB0000118				
Location:	13-1 Rack 28	Contact:	-				
IP Address:	10.11.0.11	APs:	29	Clients:	115	Usage:	3.77 Mbps
VPN Sessions:	0	VPN Usage:	-				
Quick Links:	Open controller web UI...	Run command...					
Notes:							

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
```

Verify that firewall port **162** (default) is **open** between AirWave and the controller.

Validate that traps are making it into AirWave by issuing the following commands from AirWave command line.

```
[root@AMP ~]# qlog enable snmp_traps

[root@AMP ~]# tail -f /var/log/amp_diag/snmp_traps

1241627740.392536 handle_trap|2009-05-06 09:35:40 UDP: [10.2.32.65]->[10.51.5.118]:-32737 sends
trap: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (127227800) 14 days, 17:24:38.00 SNMPv2-
MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.14823.2.3.1.11.1.2.1106 SNMPv2-SMI::enterpris
es.14823.2.3.1.11.1.1.60 = Hex-STRING: 07 D9 05 06 09 16 0F 00 2D 08 00    SNMPv2-SMI::enterpri
ses.14823.2.3.1.11.1.1.5.0 = Hex-STRING: 00 1A 1E 6F 82 D0 SNMPv2-SMI::enterprises.14823.2.3.1.
11.1.1.6.0 = STRING: dell-apSNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.1.0 = Hex-STRING: 00 1A
1E C0 2B 32 SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.56.0 = INTEGER: 2    SNMPv2-SMI::enterpr
ises.14823.2.3.1.11.1.1.17.0 = STRING: dell-124-c0:2b:32 SNMPv2-SMI::enterprises.14823.2.3.1.11
.1.1.18.0 = INTEGER: 11   SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.58.0 = STRING: http://10.5
1.5.118/screens/wmsi/reports.html?mode=ap&bssid=00:1a:1e:6f:82:d0
```

NOTE

You will see many IDS and Auth Traps from this command. AirWave only processes a small subset of these traps which display within AirWave. The traps that AirWave does process are listed above.

We recommend that you disable qlogging after testing. Leaving it turned on can negatively impact AirWave performance:

```
[root@AMP ~]# qlog enable snmp_traps
```

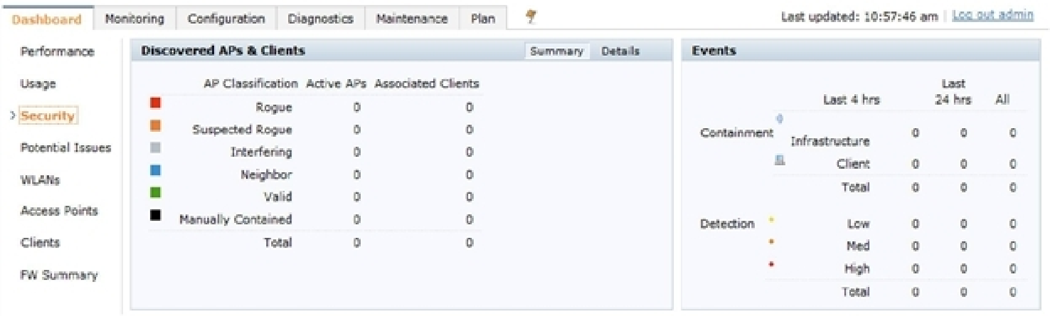
Understanding WMS Offload Impact on Dell Networking W-Series Infrastructure

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. Prior to 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 **APs/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*



Last updated: 10:57:46 am

Discovered APs & Clients

	AP Classification	Active APs	Associated Clients
🟥	Rogue	0	0
🟧	Suspected Rogue	0	0
⬜	Interfering	0	0
🟦	Neighbor	0	0
🟩	Valid	0	0
■	Manually Contained	0	0
	Total	0	0

Events

		Last 4 hrs	Last 24 hrs	All
Containment	Infrastructure	0	0	0
	Client	0	0	0
	Total	0	0	0
Detection	Low	0	0	0
	Med	0	0	0
	High	0	0	0
	Total	0	0	0

See "Rogue Device Classification" on page 33 for more information on security, IDS, WIPS, WIDS, classification, and RAPIDS.

Dell Networking W-Series Specific Capabilities in AirWave

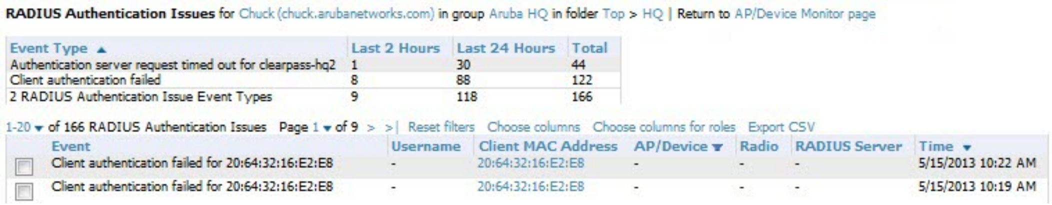
This section discusses Dell Networking W-Series specific capabilities in AirWave and contains the following topics:

Dell Networking W-Series 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. See Figure 13 showing all authentication failures related to a controller.

You can view RADIUS authentication issues by selecting the RADIUS Authentication Issues link in the Alert Summary table.

Figure 13 *RADIUS Authentication Traps in AirWave*



RADIUS Authentication Issues for Chuck (chuck.arubanetworks.com) in group Aruba HQ in folder Top > HQ | Return to AP/Device Monitor page

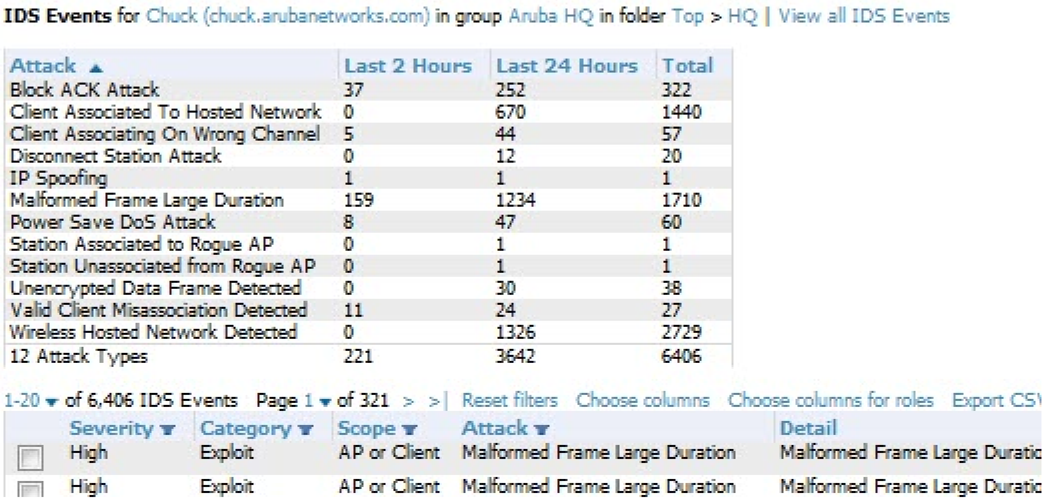
Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Authentication server request timed out for clearpass-hq2	1	30	44
Client authentication failed	8	88	122
2 RADIUS Authentication Issue Event Types	9	118	166

1-20 ▾ of 166 RADIUS Authentication Issues Page 1 ▾ of 9 > >| Reset filters Choose columns Choose columns for roles Export CSV

	Event	Username	Client MAC Address	AP/Device ▾	Radio	RADIUS Server	Time ▾
□	Client authentication failed for 20:64:32:16:E2:E8	-	20:64:32:16:E2:E8	-	-	-	5/15/2013 10:22 AM
□	Client authentication failed for 20:64:32:16:E2:E8	-	20:64:32:16:E2:E8	-	-	-	5/15/2013 10:19 AM

The IDS traps are received by the AirWave server and correlated to the proper controller, AP, and user. See Figure 14 showing all IDS traps related to a controller. You can view IDS events by selecting the IDS Events link in the Alert Summary table.

Figure 14 *IDS Events in AirWave*



IDS Events for Chuck (chuck.arubanetworks.com) in group Aruba HQ in folder Top > HQ | View all IDS Events

Attack ▲	Last 2 Hours	Last 24 Hours	Total
Block ACK Attack	37	252	322
Client Associated To Hosted Network	0	670	1440
Client Associating On Wrong Channel	5	44	57
Disconnect Station Attack	0	12	20
IP Spoofing	1	1	1
Malformed Frame Large Duration	159	1234	1710
Power Save DoS Attack	8	47	60
Station Associated to Rogue AP	0	1	1
Station Unassociated from Rogue AP	0	1	1
Unencrypted Data Frame Detected	0	30	38
Valid Client Misassociation Detected	11	24	27
Wireless Hosted Network Detected	0	1326	2729
12 Attack Types	221	3642	6406

1-20 ▾ of 6,406 IDS Events Page 1 ▾ of 321 > >| Reset filters Choose columns Choose columns for roles Export CS\

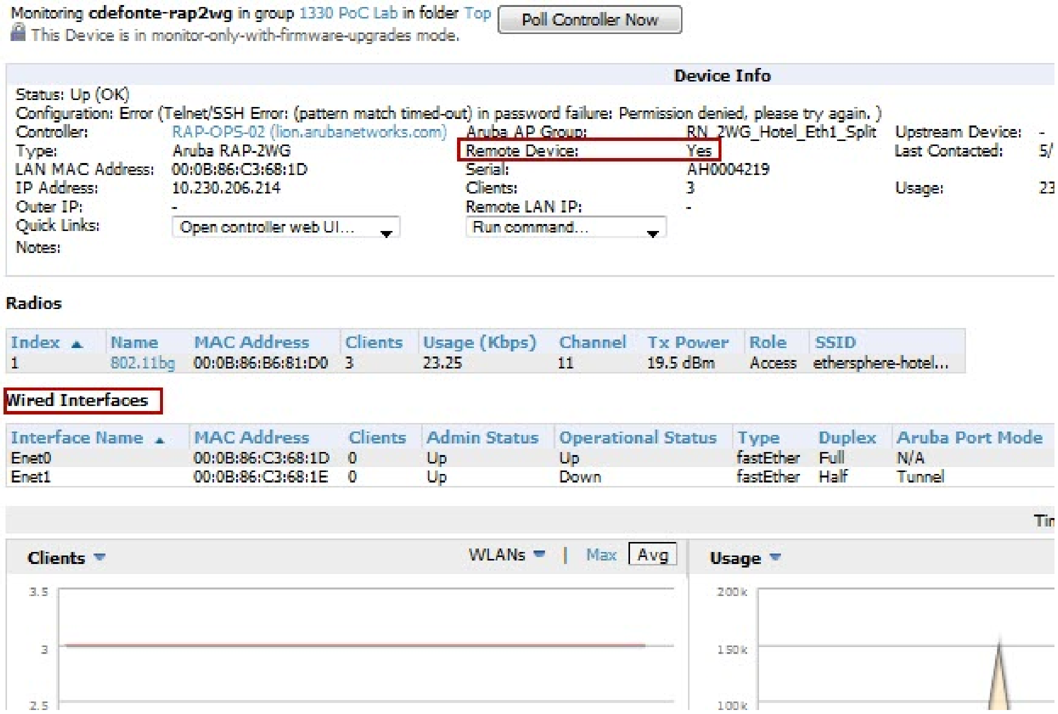
	Severity ▾	Category ▾	Scope ▾	Attack ▾	Detail
□	High	Exploit	AP or Client	Malformed Frame Large Duration	Malformed Frame Large Duratic
□	High	Exploit	AP or Client	Malformed Frame Large Duration	Malformed Frame Large Duratic

Remote AP Monitoring

To monitor remote APs, follow these steps:

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

Figure 15 *Remote AP Detail Page*



Monitoring **cdefonte-rap2wg** in group 1330 PoC Lab in folder Top

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

Device Info

Status: Up (OK)

Configuration: Error (Telnet/SSH Error: (pattern match timed-out) in password failure: Permission denied, please try again.)

Controller:	RAP-OPS-02 (lion.arubanetworks.com)	Aruba AP Group:	RN_2WG_Hotel_Eth1_Split	Upstream Device:	-
Type:	Aruba RAP-2WG	Remote Device:	Yes	Last Contacted:	5/
LAN MAC Address:	00:0B:86:C3:68:1D	Serial:	AH0004219		
IP Address:	10.230.206.214	Clients:	3	Usage:	23
Outer IP:	-	Remote LAN IP:	-		
Quick Links:	Open controller web UI...	Run command...			
Notes:					

Radios

Index ▲	Name	MAC Address	Clients	Usage (Kbps)	Channel	Tx Power	Role	SSID
1	802.11bg	00:0B:86:B6:81:D0	3	23.25	11	19.5 dBm	Access	ethersphere-hotel...

Wired Interfaces

Interface Name ▲	MAC Address	Clients	Admin Status	Operational Status	Type	Duplex	Aruba Port Mode
Enet0	00:0B:86:C3:68:1D	0	Up	Up	fastEther	Full	N/A
Enet1	00:0B:86:C3:68:1E	0	Up	Down	fastEther	Half	Tunnel

3. You can also see if there are users plugged into the wired interfaces in the Connected Clients list below the Clients and Usage graphs.

NOTE

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 **APs/Devices > Monitor** page for any of the following: Dell Networking W-AP105, W-AP92, W-AP93, W-AP124, W-AP125, W-AP134, or W-AP135.
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 the drop down icon for each to change these to Radio Channel and Channel Utilization.

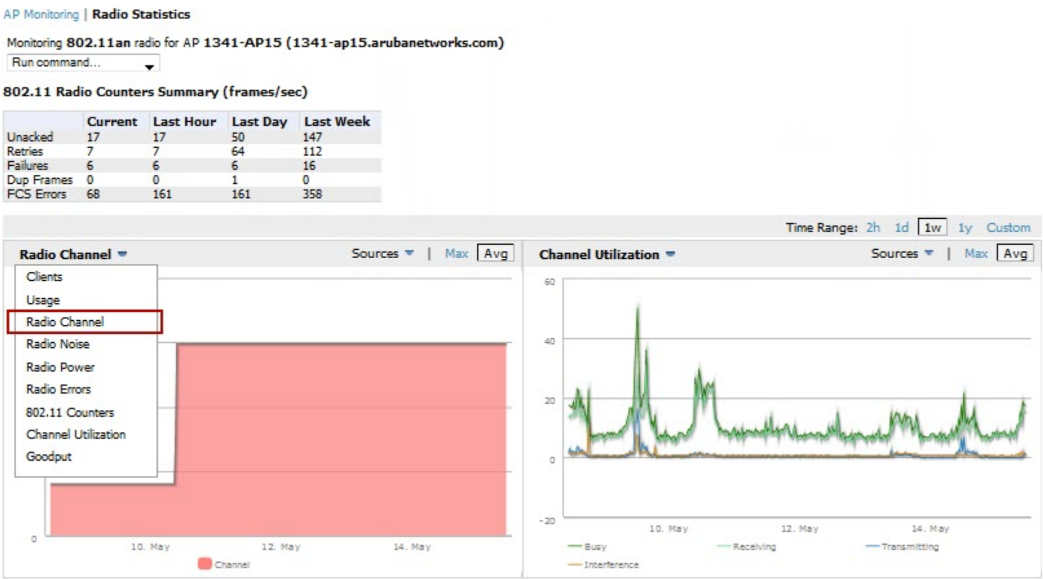


Figure 16 *ARM and Channel Utilization Graphs*

AP Monitoring | Radio Statistics

Monitoring 802.11an radio for AP 1341-AP15 (1341-ap15.arubanetworks.com)

802.11 Radio Counters Summary (frames/sec)

	Current	Last Hour	Last Day	Last Week
Unacked	17	17	50	147
Retries	7	7	64	112
Failures	6	6	6	16
Dup Frames	0	0	1	0
FCS Errors	68	161	161	358

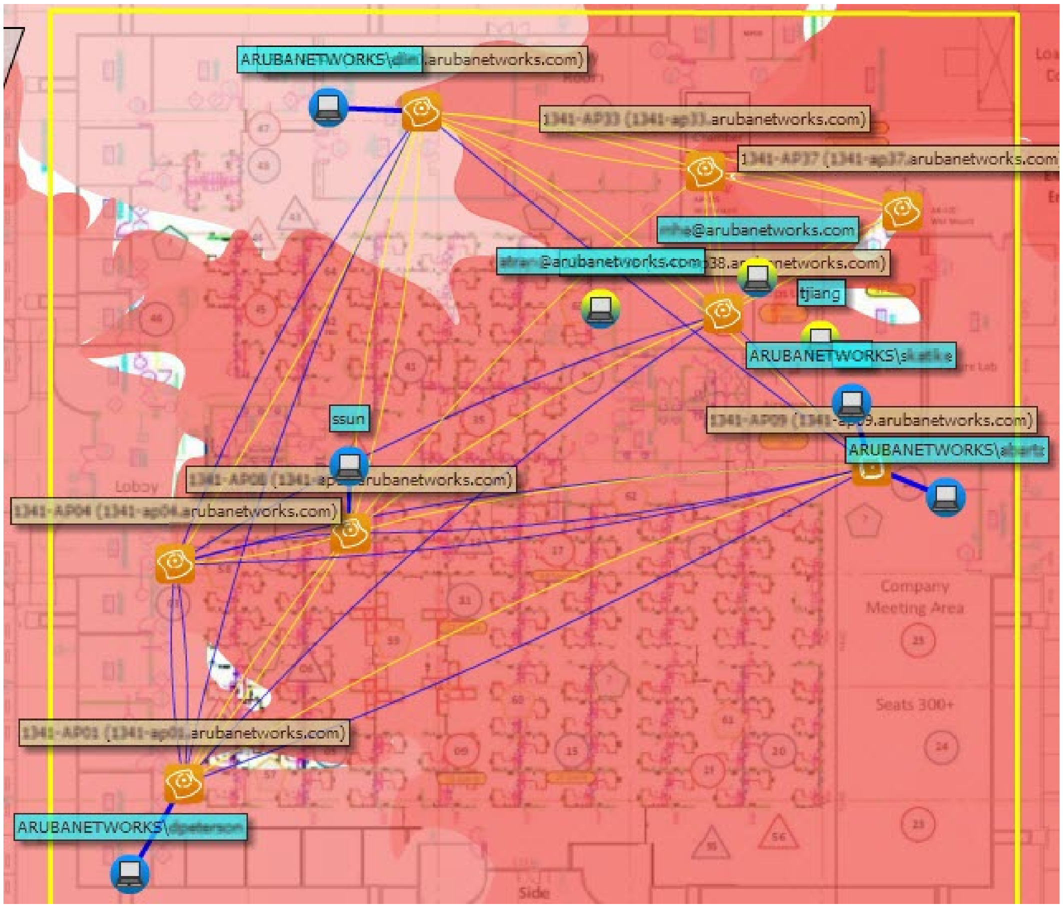
See the *Dell Networking W-AirWave 7.7 User Guide* at **dell.com/support/manuals** for more information on the data that displays in the **Radio Statistics** page for these devices.

VisualRF and Channel Utilization

To view how channel utilization is impacting an area within a building, follow these steps:

1. Navigate to a floor plan by clicking on the thumbnail on a device's **APs/Devices > Monitor** page or navigating to **VisualRF > Floor Plans** page.
2. Select the **Overlays** menu.
3. Select the **Ch. Utilization** overlay.
4. Select **Current** or **Maximum** (over last 24 hours).
   - If Maximum is selected, then use the drop down menu to select total (default), receive (RX), transmit (TX), or interference (Int.).
5. Select to view information for the current floor, the floor above, and/or the floor below.
6. Select a frequency of 5 GHz and/or 2.4 GHz.

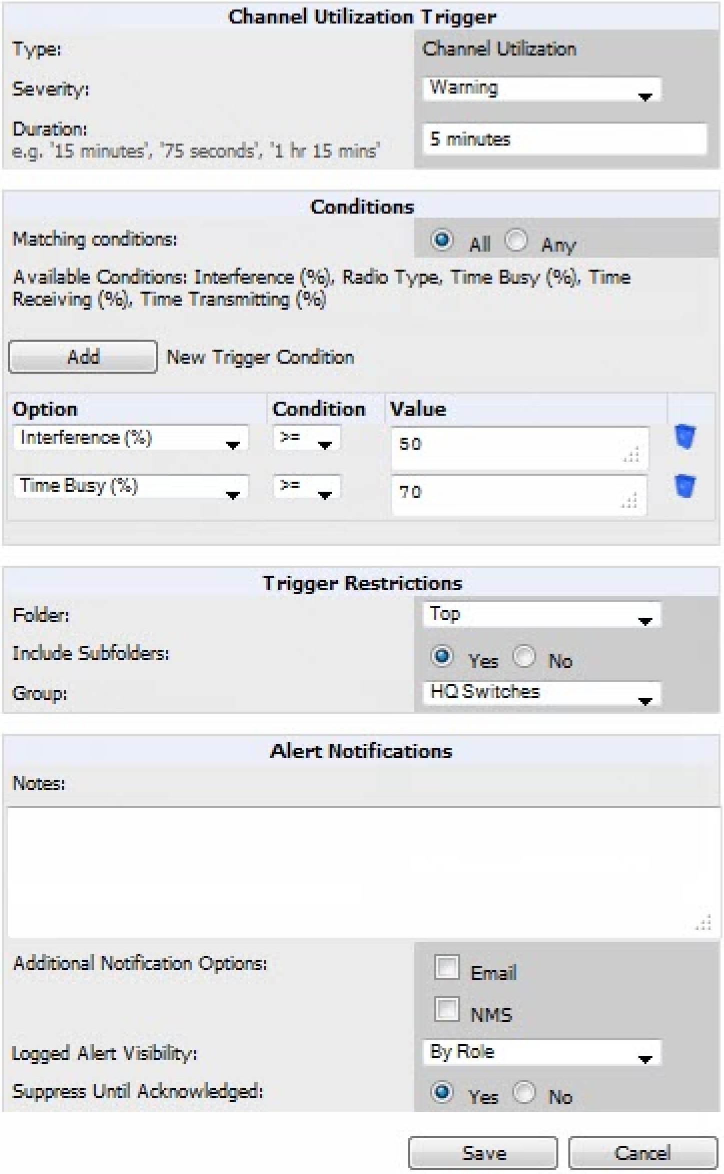
Figure 17 *Channel Utilization in VisualRF (Interference/2.4 GHz)*


ARUBANETWORKS\[redacted].arubanetworks.com)
1341-AP33 (1341-ap33.arubanetworks.com)
1341-AP37 (1341-ap37.arubanetworks.com
[redacted]@arubanetworks.com
[redacted]@arubanetworks.com
38.ar[redacted]networks.com)
tjiang
ARUBANETWORKS\[redacted]
1341-AP09 (1341-ap09.arubanetworks.com)
ARUBANETWORKS\[redacted]
ssun
1341-AP08 (1341-ap[redacted]rubanetworks.com)
Lobby
1341-AP04 (1341-ap04.arubanetworks.com)
Company
Meeting Area
Seats 300+
1341-AP01 (1341-ap01.arubanetworks.com)
ARUBANETWORKS\[redacted]
Side

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 18:

Figure 18 *Channel Utilization Trigger*



Channel Utilization Trigger

Type:	Channel Utilization
Severity:	Warning
Duration: e.g. '15 minutes', '75 seconds', '1 hr 15 mins'	5 minutes

Conditions

Matching conditions: ● All ○ Any

Available Conditions: Interference (%), Radio Type, Time Busy (%), Time Receiving (%), Time Transmitting (%)

New Trigger Condition

Option	Condition	Value
Interference (%)	>=	50
Time Busy (%)	>=	70

Trigger Restrictions

Folder:	Top
Include Subfolders:	● Yes ○ No
Group:	HQ Switches

Alert Notifications

Notes:

Additional Notification Options:	□ Email □ NMS
Logged Alert Visibility:	By Role
Suppress Until Acknowledged:	● Yes ○ No

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 *Dell Networking W-AirWave 7.7 User Guide* at **dell.com/support/manuals** for more details.)
8. When you are finished, click **Add**.

Viewing Channel Utilization Alerts

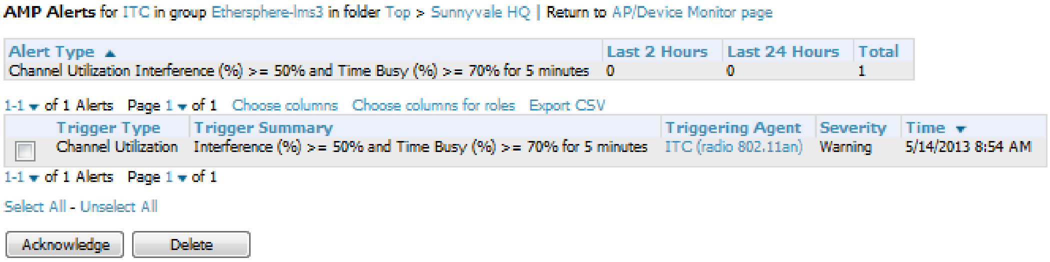
You can view Channel Utilization alerts from the APs/Devices > Monitor page and on the System > Alerts page.

Channel Utilization Alerts on the APs/Devices > Monitor Page

1. Navigate to **APs/Devices > Monitor** page for a selected device.

2. Scroll down to the Alert Summary page and select AMP Alerts.

Figure 19 *Channel Utilization alerts*



AMP Alerts for ITC in group Ethersphere-lms3 in folder Top > Sunnyvale HQ | Return to AP/Device Monitor page

Alert Type ▲	Last 2 Hours	Last 24 Hours	Total
Channel Utilization Interference (%) >= 50% and Time Busy (%) >= 70% for 5 minutes	0	0	1

1-1 ▾ of 1 Alerts Page 1 ▾ of 1 Choose columns Choose columns for roles Export CSV

	Trigger Type	Trigger Summary	Triggering Agent	Severity	Time ▾
☐	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 minutes	ITC (radio 802.11an)	Warning	5/14/2013 8:54 AM

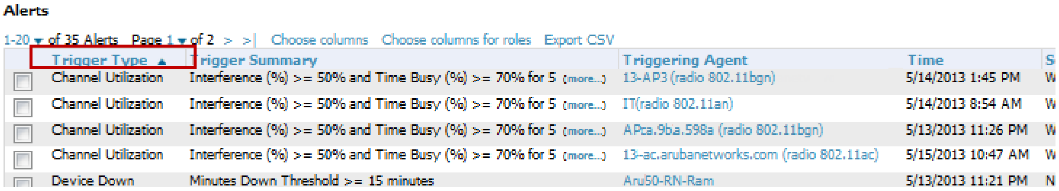
1-1 ▾ of 1 Alerts Page 1 ▾ of 1

Select All - Unselect All

Channel Utilization Alerts on the System > Alerts Page

1. Navigate to the **System** > **Alerts** page.
2. Sort the **Trigger Type** column and find **Channel Utilization** alerts.

Figure 20 *Channel Utilization alerts on the System > Alerts page*



Alerts

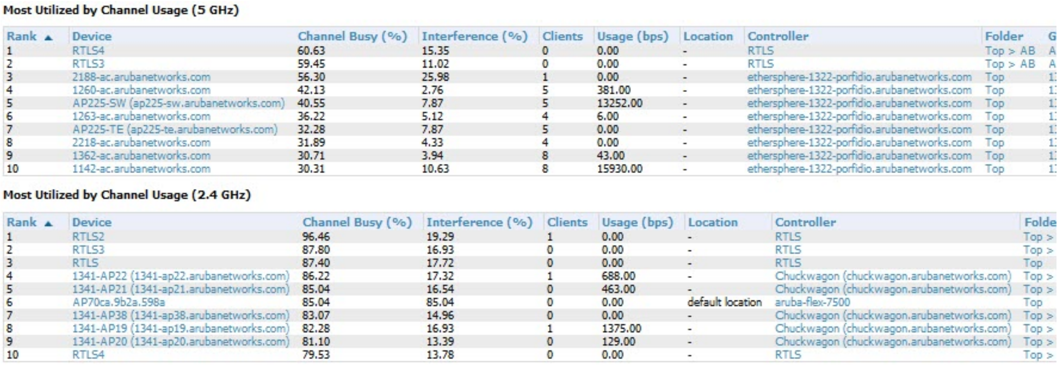
1-20 ▾ of 35 Alerts Page 1 ▾ of 2 > >| Choose columns Choose columns for roles Export CSV

	Trigger Type ▲	Trigger Summary	Triggering Agent	Time	S
☐	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	13-AP3 (radio 802.11bgn)	5/14/2013 1:45 PM	W
☐	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	IT(radio 802.11an)	5/14/2013 8:54 AM	W
☐	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	APca.9ba.598a (radio 802.11bgn)	5/13/2013 11:26 PM	W
☐	Channel Utilization	Interference (%) >= 50% and Time Busy (%) >= 70% for 5 (more...)	13-ac.arubanetworks.com (radio 802.11ac)	5/15/2013 10:47 AM	W
☐	Device Down	Minutes Down Threshold >= 15 minutes	Aru50-RN-Ram	5/13/2013 11:21 PM	N

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 most and least utilized 2.4 and 5 channel usage information.

Figure 21 *Channel Utilization in an RF Health Report (partial view)*



Most Utilized by Channel Usage (5 GHz)

Rank ▲	Device	Channel Busy (%)	Interference (%)	Clients	Usage (bps)	Location	Controller	Folder	G
1	RTLS4	60.63	15.35	0	0.00	-	RTLS	Top > AB	A
2	RTLS3	59.45	11.02	0	0.00	-	RTLS	Top > AB	A
3	2188-ac.arubanetworks.com	56.30	25.98	1	0.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
4	1260-ac.arubanetworks.com	42.13	2.76	5	381.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
5	AP225-SW (ap225-sw.arubanetworks.com)	40.55	7.87	5	13252.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
6	1263-ac.arubanetworks.com	36.22	5.12	4	6.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
7	AP225-TE (ap225-te.arubanetworks.com)	32.28	7.87	5	0.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
8	2218-ac.arubanetworks.com	31.89	4.33	4	0.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
9	1362-ac.arubanetworks.com	30.71	3.94	8	43.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1
10	1142-ac.arubanetworks.com	30.31	10.63	8	15930.00	-	ethersphere-1322-porfidio.arubanetworks.com	Top	1

Most Utilized by Channel Usage (2.4 GHz)

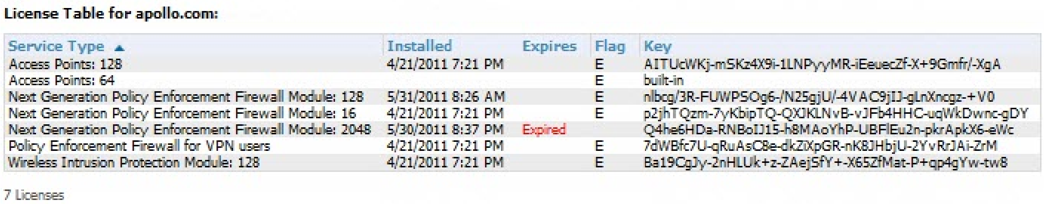
Rank ▲	Device	Channel Busy (%)	Interference (%)	Clients	Usage (bps)	Location	Controller	Folde
1	RTLS2	96.46	19.29	1	0.00	-	RTLS	Top >
2	RTLS3	87.80	16.93	0	0.00	-	RTLS	Top >
3	RTLS	87.40	17.72	0	0.00	-	RTLS	Top
4	1341-AP22 (1341-ap22.arubanetworks.com)	86.22	17.32	1	688.00	-	Chuckwagon (chuckwagon.arubanetworks.com)	Top >
5	1341-AP21 (1341-ap21.arubanetworks.com)	85.04	16.54	0	463.00	-	Chuckwagon (chuckwagon.arubanetworks.com)	Top >
6	AP70ca.9b2a.598a	85.04	85.04	0	0.00	default location	aruba-flex-7500	Top
7	1341-AP38 (1341-ap38.arubanetworks.com)	83.07	14.96	0	0.00	-	Chuckwagon (chuckwagon.arubanetworks.com)	Top >
8	1341-AP19 (1341-ap19.arubanetworks.com)	82.28	16.93	1	1375.00	-	Chuckwagon (chuckwagon.arubanetworks.com)	Top >
9	1341-AP20 (1341-ap20.arubanetworks.com)	81.10	13.39	0	129.00	-	Chuckwagon (chuckwagon.arubanetworks.com)	Top >
10	RTLS4	79.53	13.78	0	0.00	-	RTLS	Top >

Viewing Controller License Information

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

1. Navigate to the **APs/Devices** > **Monitor** page of a controller.
2. Select the **Licenses** link in the **Device Info** section. A pop-up window appears listing all licenses.

Figure 22 *License Popup from **APs/Devices > Monitor** page a controller*



License Table for apollo.com:

Service Type ▲	Installed	Expires	Flag	Key
Access Points: 128	4/21/2011 7:21 PM		E	AITUcWKj-mSKz4X9i-1LNPyyMR-iEeuecZf-X+9Gmfr/-XgA
Access Points: 64			E	built-in
Next Generation Policy Enforcement Firewall Module: 128	5/31/2011 8:26 AM		E	nlbcg/3R-FUWPSOg6-/N25gjU/-4VAC9jIJ-gLnXncgz-+V0
Next Generation Policy Enforcement Firewall Module: 16	4/21/2011 7:21 PM		E	p2jhTQzm-7yKbipTQ-QXJKLNvB-vJFb4HHC-uqWkDwnc-gDY
Next Generation Policy Enforcement Firewall Module: 2048	5/30/2011 8:37 PM	Expired		Q4he6HDa-RNBoIJ15-h8MAoYhP-UBFlEu2n-pkrApkX6-eWc
Policy Enforcement Firewall for VPN users	4/21/2011 7:21 PM		E	7dWBfc7U-qRuAsC8e-dkZiXpGR-nK8JHbjU-2YvRrJAi-ZrM
Wireless Intrusion Protection Module: 128	4/21/2011 7:21 PM		E	Ba19CgJy-2nHLUk+z-ZAejSfY+-X65ZfMat-P+qp4gYw-tw8

7 Licenses

Rogue Device Classification

Complete this section if you have completed WMS Offload procedure above. After offloading WMS, AirWave maintains the primary ARM, WIPS, and WIDS state classification for all devices discovered over-the-air.

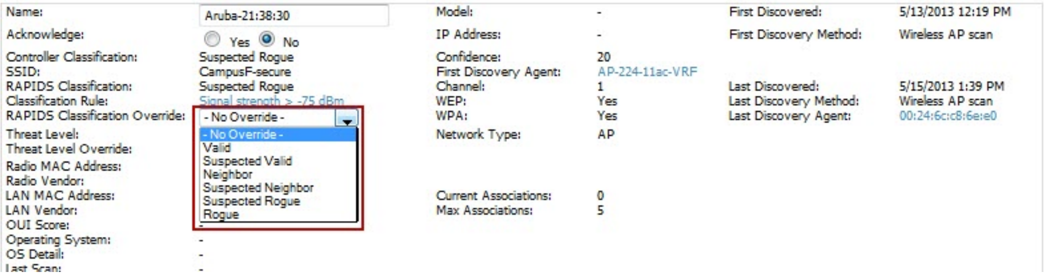
Table 2: *WIPS/WIDS to AirWave ControllerClassification Matrix*

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, as shown in the following figure.
2. Select the proper classification from the **RAPIDS Classification Override** drop-down menu.

Figure 23 *Rogue Detail Page Illustration*



Name: Aruba-21:38:30
Acknowledge: ○ Yes ● No
Controller Classification: Suspected Rogue
SSID: CampusF-secure
RAPIDS Classification: Suspected Rogue
Classification Rule: Signal strength > -75 dBm
RAPIDS Classification Override: - No Override -
Threat Level:
Threat Level Override:
Radio MAC Address:
Radio Vendor:
LAN MAC Address:
LAN Vendor:
OUI Score: -
Operating System: -
OS Detail: -
Last Scan: -

Model: -
IP Address: -
Confidence: 20
First Discovery Agent: AP-224-11ac-VRF
Channel: 1
WEP: Yes
WPA: Yes
Network Type: AP
Current Associations: 0
Max Associations: 5

First Discovered: 5/13/2013 12:19 PM
First Discovery Method: Wireless AP scan
Last Discovered: 5/15/2013 1:39 PM
Last Discovery Method: Wireless AP scan
Last Discovery Agent: 00:24:6c:c8:6e:e0

CAUTION

Changing the controller's classification within the AirWave UI 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 UI 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 UI and propagated to controllers that AirWave manages. The device classification reflected in the controller's UI and in the AirWave UI will probably not match, because the controller/APs do not reclassify rogue devices frequently.

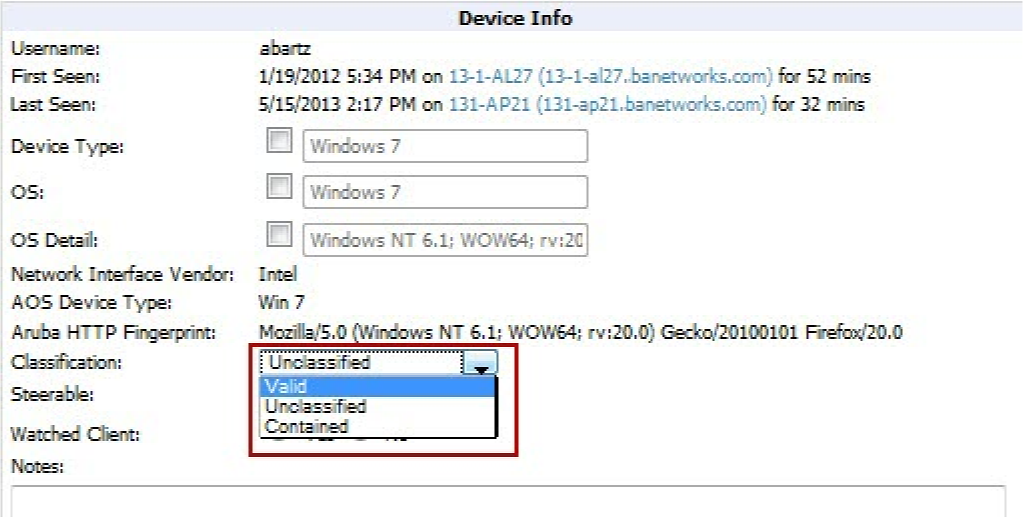
To update a group of devices' controller classification to match the ArubaOS device classification, navigate to **RAPIDS > List** and utilize the **Modify Devices** checkbox combined with the multiple sorting a filtering features.

Table 3: *ARM to AMP Classification Matrix*

AMP	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 menu as seen in Figure 24:

Figure 24 *User Classification*



Device Info

Username: abartz
First Seen: 1/19/2012 5:34 PM on 13-1-AL27 (13-1-al27.banetworks.com) for 52 mins
Last Seen: 5/15/2013 2:17 PM on 131-AP21 (131-ap21.banetworks.com) for 32 mins
Device Type: □ Windows 7
OS: □ Windows 7
OS Detail: □ Windows NT 6.1; WOW64; rv:20
Network Interface Vendor: Intel
AOS Device Type: Win 7
Aruba HTTP Fingerprint: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0
Classification: Unclassified
Steerable:
Watched Client:
Notes:

CAUTION

Changing User Classification within the AirWave UI 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 UI and propagated to controllers that AirWave manages. It is probable that the user's classification reflected in the controller's UI and in the AirWave UI will not match, because the controllers/APs do not reclassify users frequently.

There is no method in the AirWave UI to update user classification on mass to match the controller's classification. Each client must be updated individually within the AirWave UI.

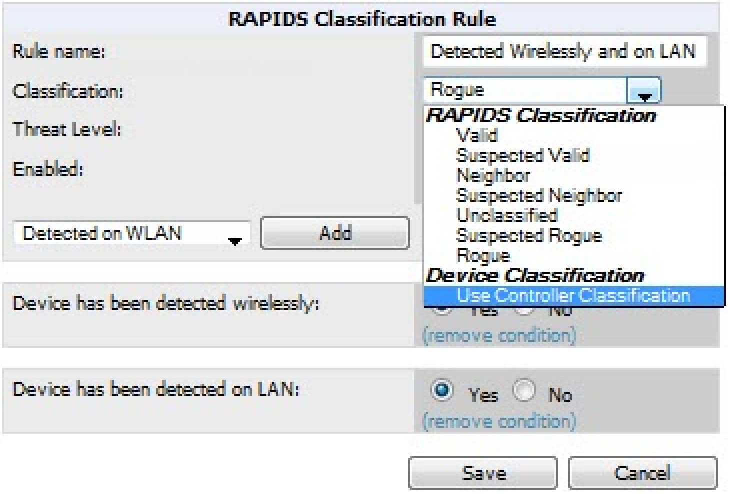
Rules-Based Controller Classification

Using RAPIDS Defaults for Controller Classification

To use the controller's classification as RAPIDS classification, follow these steps:

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 menu, select **Use Controller Classification** as seen in Figure 25.

Figure 25 *Using Controller Classification*



RAPIDS Classification Rule

Rule name: Detected Wirelessly and on LAN

Classification: Rogue

Threat Level:

Enabled:

Detected on WLAN

Device has been detected wirelessly: ○ Yes ○ No

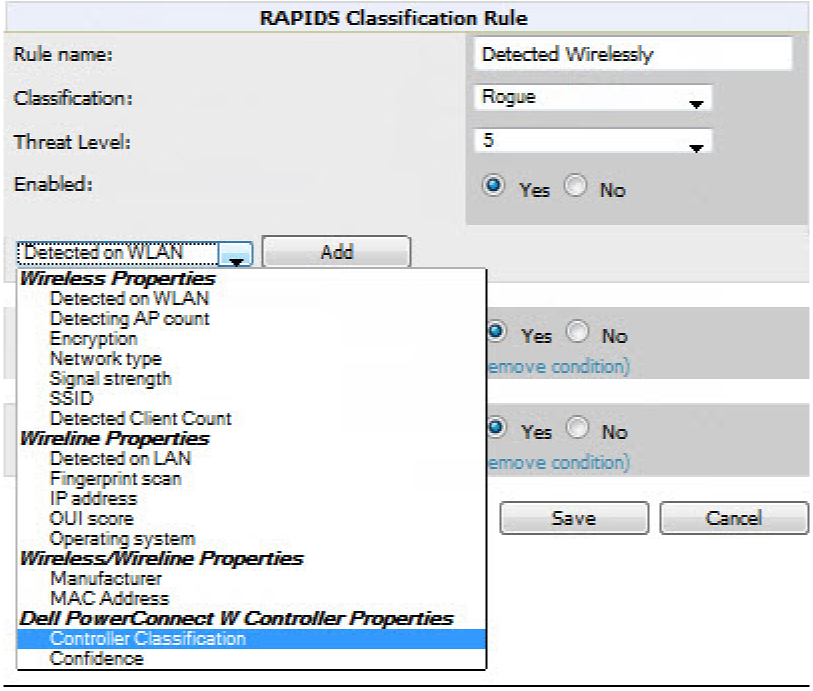
Device has been detected on LAN: ● Yes ○ No

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

Changing RAPIDS based on Controller Classification

1. Navigate to **RAPIDS > Rules** and select the desired rule.
2. In the **Classification** drop-down menu, select desired RAPIDS classification.
3. Select **Controller Classification** from the drop-down menu, as shown in Figure 26.

Figure 26 *Configure Rules for Classification*



RAPIDS Classification Rule

Rule name: Detected Wirelessly

Classification: Rogue

Threat Level: 5

Enabled: ● Yes ○ No

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

Appendix A
ArubaOS and AirWave CLI Commands

Enable Channel Utilization Events

CAUTION

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 Dell Networking W-Series 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>
(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.

NOTE

Do not use these commands if you use the AirWave GUI 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 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) # ids wms-general-profile collect-stats enable
(Controller-Name) (config-ids-wms-general-profile) # collect-stats
(Controller-Name) (config-ids-wms-general-profile) # exit
(Controller-Name) (config) # write mem
```

Offload WMS Using the ArubaOS or AirWave CLI

NOTE

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

Additional commands can be used to offload WMS using the ArubaOS command-line interface or the AirWave SNMP Walk.

Refer to:

"ArubaOS CLI" on page 37

"AirWave SNMP " on page 38

ArubaOS CLI

SSH into all controllers (local and master), and 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 creates an SNMPv3 user on the controller with the 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.

Example:

```
mobility-manager 10.2.32.1 user airwave123 airwave123
```

AirWave SNMP

Log in into the AirWave server with proper administrative access and issue the following command for all controllers (master and locals):

```
[root@AMP ~]# snmpwalk -v3 -a SHA -l AuthPriv -u <MMS-USER> -A <MMS-SNMP-PASSWORD> -X <MMS-SNMP-
PASSWORD> <Controller-IP> wlsxSystemExtGroup

WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchIp.0 = IpAddress: 10.51.5.222
WLSX-SYSTEMEXT-MIB::wlsxSysExtHostname.0 = STRING: dell-3600-2
.
..
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchLastReload.0 = STRING: User reboot.
WLSX-SYSTEMEXT-MIB::wlsxSysExtLastStatsReset.0 = Timeticks: (0) 0:00:00.00 response
[root@AMP ~]#
```

Unless this SNMP walk command is issued properly on all of the controllers, they will not properly populate client and rogue statistics. Ensure the user and passwords match exactly to those entered in above sections.

Example:

```
snmpwalk -v3 -a SHA -l AuthPriv -u airwave123 -A airwave123 -X airwave123 10.51.3.222 wlsxSyste
mExtGroup
```

If you do not use the AirWave WebUI to offload WMS, you must add a cronjob on the AirWave server to ensure continued statistical population. Because the MIB walk/touch does not persist through a controller reboot, a cronjob is required to continually walk and touch the MIB.

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.

NOTE

Do not use these commands if you use the AirWave GUI 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, 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) # process restart wms
```

After executing the `restart wms` command in Dell Networking W-Series ArubaOS, you will need to wait until the next Rogue Poll Period on AirWave and execute a **Poll Now** operation for each local controller on the **APs/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 Dell Networking W-Series controllers, copy and paste the following command in config mode:

```
snmp-server trap enable wlsxNUserAuthenticationFailed
snmp-server trap enable wlsxUserAuthenticationFailed
snmp-server trap enable wlsxNAuthServerReqTimedOut
snmp-server trap enable wlsxSignatureMatchAP
snmp-server trap enable wlsxSignatureMatchSta
snmp-server trap enable wlsxSignAPNetstumbler
snmp-server trap enable wlsxSignStaNetstumbler
snmp-server trap enable wlsxSignAPAsleap
snmp-server trap enable wlsxSignStaAsleap
snmp-server trap enable wlsxSignAPAirjack
snmp-server trap enable wlsxSignStaAirjack
snmp-server trap enable wlsxSignAPNullProbeResp
snmp-server trap enable wlsxSignStaNullProbeResp
snmp-server trap enable wlsxSignAPDeauthBcast
snmp-server trap enable wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
snmp-server trap enable wlsxChannelFrameFragmentationRateExceeded
```

```
snmp-server trap enable wlsxChannelFrameRetryRateExceeded
snmp-server trap enable wlsxNIpSpoofingDetected
snmp-server trap enable wlsxStaImpersonation
snmp-server trap enable wlsxReservedChannelViolation
snmp-server trap enable wlsxValidSSIDViolation
snmp-server trap enable wlsxStaPolicyViolation
snmp-server trap enable wlsxRepeatWEPIVViolation
snmp-server trap enable wlsxWeakWEPIVViolation
snmp-server trap enable wlsxFrameRetryRateExceeded
snmp-server trap enable wlsxFrameReceiveErrorRateExceeded
snmp-server trap enable wlsxFrameFragmentationRateExceeded
snmp-server trap enable wlsxFrameBandWidthRateExceeded
snmp-server trap enable wlsxFrameLowSpeedRateExceeded
snmp-server trap enable wlsxFrameNonUnicastRateExceeded
snmp-server trap enable wlsxChannelRateAnomaly
snmp-server trap enable wlsxNodeRateAnomalyAP
snmp-server trap enable wlsxNodeRateAnomalySta
snmp-server trap enable wlsxEAPRateAnomaly
snmp-server trap enable wlsxSignalAnomaly
snmp-server trap enable wlsxSequenceNumberAnomalyAP
snmp-server trap enable wlsxSequenceNumberAnomalySta
snmp-server trap enable wlsxApFloodAttack
snmp-server trap enable wlsxInvalidMacOUIAP
snmp-server trap enable wlsxInvalidMacOUISta
snmp-server trap enable wlsxStaRepeatWEPIVViolation
snmp-server trap enable wlsxStaWeakWEPIVViolation
snmp-server trap enable wlsxStaAssociatedToUnsecureAP
snmp-server trap enable wlsxStaUnAssociatedFromUnsecureAP
snmp-server trap enable wlsxAPImpersonation
snmp-server trap enable wlsxDisconnectStationAttackAP
snmp-server trap enable wlsxDisconnectStationAttackSta
```

NOTE

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

Appendix B
AirWave Data Acquisition Methods

The following table describes the different methods through which AirWave acquires data from Dell Networking W-Series devices on the network.

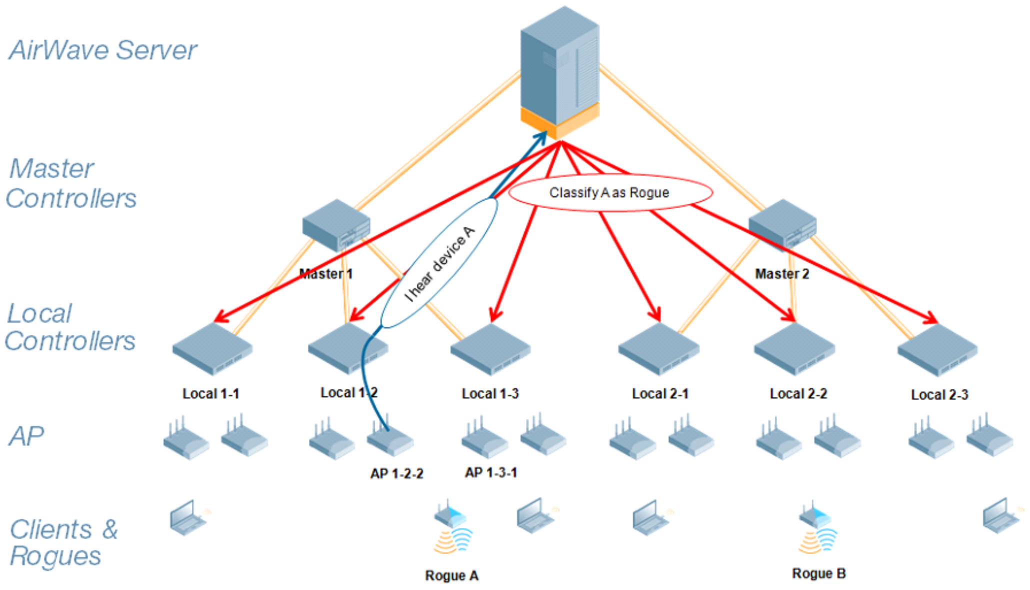
Table 4: *Methods by which AirWave Acquires Data from Dell Networking W-Series Devices*

Data Elements	Controller/Thin AP						Dell Networking W-Instant
	SNMP MIB	SNMP Traps	AMON	CLI/SSH	WMS Offload	RTLS	HTTPS
Configuration interface							
Device configuration/audit				X			X
User and client interfaces							
Assoc/auth/roam	X	X					X
Bandwidth	X						X
Signal quality	X					X	X
Auth failures		X					*N/A*
AP/radio interfaces							
CPU And memory utilization	<--------------------------------*N/A*-->						X
Bandwidth	X						X
Transmit Power	X						X
Channel utilization			X				X
Noise floor	X						
Frame rates	X						X
Error counters	X						X
Channel summary				X			*N/A*
ARM events		X					*N/A*
Active interferers			X				*N/A*

Data Elements	Controller/Thin AP						Dell Networking W-Instant
Active BSSIDs/SSIDs	X						X
Security							
IDS events		X					*N/A*
Neighbors/rogues	X				X		X
Neighbor re-classification				X	X		*N/A*
Client classification					X		*N/A*
User deauthorization				X			*N/A*

WMS Offload instructs the master controller to stop correlating ARM, WIPS, and WIDS state information amongst its local controllers because AirWave will assume this responsibility. Figure 27 depicts how AirWave communicates state information with local controllers.

Figure 27 *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 re-classifies the device if necessary and reflects this within the AirWave GUI 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 theAirWave 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 Dell Networking W-Series 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 Dell Networking W-Series controllers.

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

Leveraging RTLS to Increase Accuracy

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

Deployment Topology

Figure 28 *Typical Client Location*

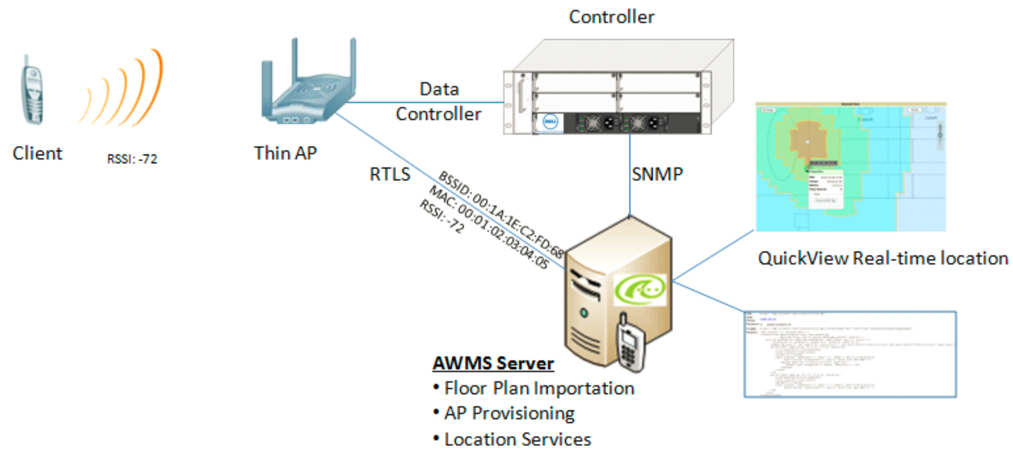
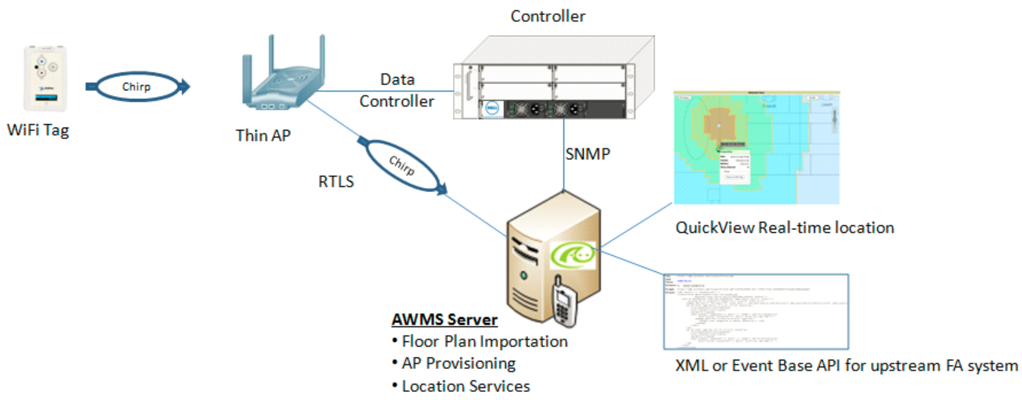


Figure 29 *Typical Tag Deployment*



Prerequisites

You will need the following information to monitor and manage your Dell Networking W-Series infrastructure.

- Ensure that the AirWave server is already monitoring Dell Networking W-Series infrastructure.
- Ensure that the WMS Offload process is complete.

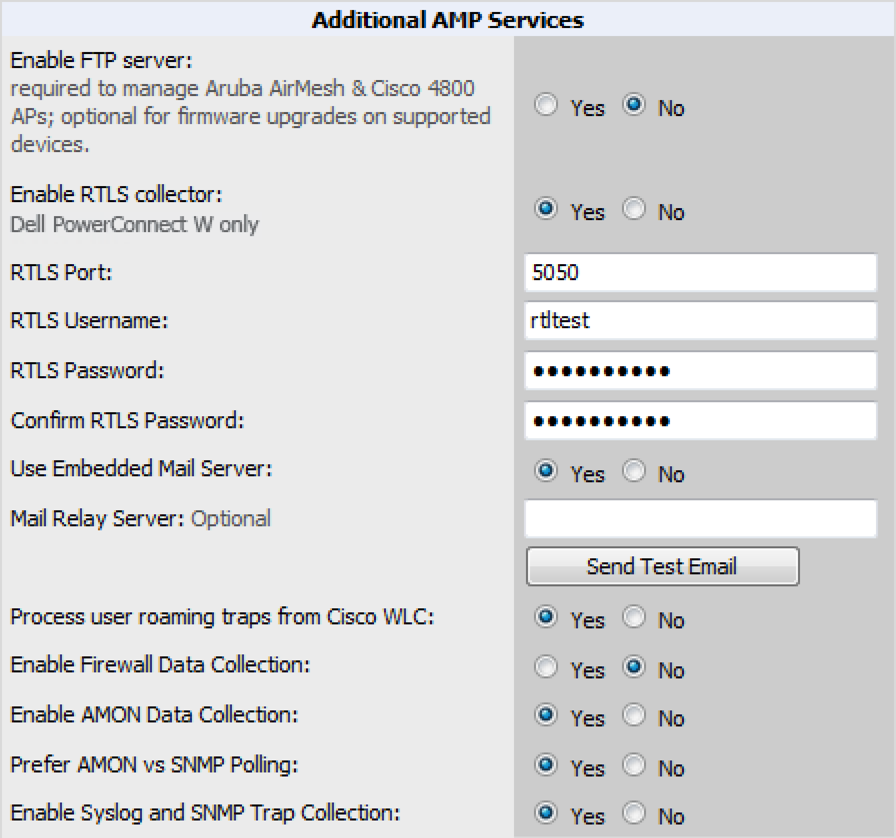
- Ensure that the firewall configuration for port 5050 (default port) supports bidirectional UDP communication between the AirWave server's IP address and each access point's IP address.

Enable RTLS Service on the AirWave Server

To enable RTLS service on the AirWave server, follow these steps:

1. Navigate to **AMP Setup > General** and locate the **Additional AMP Services** section
2. Select **Yes** for the **Enable RTLS Collector** option.
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 username configured on the controller.
   - **RTLS Password** - This must match the SNMPv3 MMS password configured on the controller.

Figure 30 *RTLS Fields in **AMP Setup> General***



Additional AMP Services

Enable FTP server: required to manage Aruba AirMesh & Cisco 4800 APs; optional for firmware upgrades on supported devices.	○ Yes ● No
Enable RTLS collector: Dell PowerConnect W only	● Yes ○ No
RTLS Port:	5050
RTLS Username:	rtltest
RTLS Password:	●●●●●●●●●●●
Confirm RTLS Password:	●●●●●●●●●●●
Use Embedded Mail Server:	● Yes ○ No
Mail Relay Server: Optional	
	Send Test Email
Process user roaming traps from Cisco WLC:	● Yes ○ No
Enable Firewall Data Collection:	○ Yes ● No
Enable AMON Data Collection:	● Yes ○ No
Prefer AMON vs SNMP Polling:	● Yes ○ No
Enable Syslog and SNMP Trap Collection:	● Yes ○ No

4. Click **Save** at the bottom of the page when you are done.

Enable RTLS on the Controller

NOTE

RTLS can only be enabled on the master controller and it will automatically propagate 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

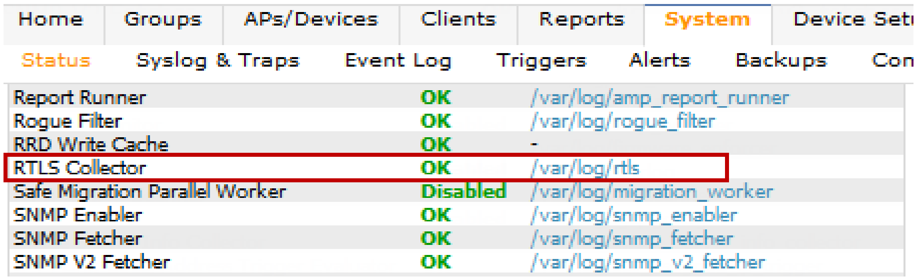
You can use either the WebUI or CLI to ensure the RTLS service is running on your AirWave server.

Using the WebUI

In the AirWave WebUI, navigate to the **System** > **Status** page.

Scroll down through the Services list to locate the RTLS service, as shown below.

Figure 31 *RTLS System Status*



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

Using the CLI

Use SSH to access the command-line interface of your AirWave server, and issue the following commands:

```
[root@AMPServer]# daemons | grep RTLS
   root     17859 12809 0 10:35 ?        00:00:00 Daemon::RTLS
```

Issue the **logs** and **tail rtls** commands to check the RTLS log file and verify that Tag chirps are making it to the AirWave server.

```
[root@AMPServer]# logs
```

```
[root@AMPServer]# tail rtls
```

```
   payload: 00147aaf01000020001a1ec02b320000000001000000137aae0100000c001a1ec02b320000001a1e82b322
   590006ddff02
   1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050
   Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from 10.51.1.39 on port 5050
   payload: 0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec050780000000d54a7a280
   540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
   1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050
```

```
Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from 10.51.1.39 on port 5050
payload: 0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec050780000000d54a7a280
540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
```

Ensure chirps are published to Airbus by snooping on RTLS tag reports.

```
[root@AMPServer]# airbus_snoop rtls_tag_report

Snooping on rtls_tag_report:
Mon Oct 20 13:49:03 2008 (1224535743.54077)
%
    ap_mac => 00:1A:1E:C0:50:78
    battery => 0
    bssid => 00:1A:1E:85:07:80
    channel => 1
    data_rate => 2
    noise_floor => 85
    payload =>
    rssi => -64
    tag_mac => 00:14:7E:00:4C:E4
    timestamp => 303139810
    tx_power => 19
```

Verify external applications can see WiFi Tag information by exercising the Tag XML API:

```
https://<AMP-Server-IP>/visualrf/rfid.xml
```

You should see the following XML output:

```
<visualrf:rfids version=1>
 <rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4C:E0
    vendor=>
    <radio phy=g xmit-dbm=10.0/>
    <discovering-radio ap=SC-MB-03-AP10 dBm=-91 id=811 index=1
      timestamp=2008-10-21T12:23:30-04:00/>
    <discovering-radio ap=SC-MB-03-AP06 dBm=-81 id=769 index=1
      timestamp=2008-10-21T12:23:31-04:00/>
    <discovering-radio ap=SC-MB-01-AP06 dBm=-63 id=708 index=1
      timestamp=2008-10-21T12:23:31-04:00/>
    <discovering-radio ap=SC-MB-02-AP04 dBm=-88 id=806 index=1
    timestamp=2008-10-21T12:22:34-04:00/>
 </rfid>
 <rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4B:5C
    vendor=>
    <radio phy=g xmit-dbm=10.0/>
    <discovering-radio ap=SC-MB-03-AP06 dBm=-74 id=769 index=1
      timestamp=2008-10-21T12:23:20-04:00/>
    <discovering-radio ap=SC-MB-01-AP06 dBm=-58 id=708 index=1
      timestamp=2008-10-21T12:23:20-04:00/>
    <discovering-radio ap=SC-MB-03-AP02 dBm=-91 id=734 index=1
      timestamp=2008-10-21T12:23:20-04:00/>
 </rfid>
 <rfid battery-level=0 chirp-interval= radio-mac=00:14:7E:00:4D:06
    vendor=>
    <radio phy=g xmit-dbm=10.0/>
    <discovering-radio ap=SC-SB-GR-AP04 dBm=-91 id=837 index=1
      timestamp=2008-10-21T12:21:08-04:00/>
    <discovering-radio ap=SC-MB-03-AP06 dBm=-79 id=769 index=1
      timestamp=2008-10-21T12:22:08-04:00/>
    <discovering-radio ap=SC-MB-01-AP06 dBm=-59 id=708 index=1
      timestamp=2008-10-21T12:23:08-04:00/>
    <discovering-radio ap=SC-MB-02-AP04 dBm=-90 id=806 index=1
      timestamp=2008-10-21T12:22:08-04:00/>
 </rfid>
</visualrf:rfids>
```

Wi-Fi Tag Setup Guidelines

- Ensure that the tags can be heard by at least three (3) access points from any given location. The recommended value is is 4 APs.
- Ensure that the tags chirp on all regulatory channels.