Dell Networking
W-AirWave 8.0

Copyright

Open Source Code

Legal Notice

This document provides best practices for leveraging Dell Networking W-AirWave to monitor and manage your Dell Networking W-Series 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 Dell Networking W-Series infrastructure.
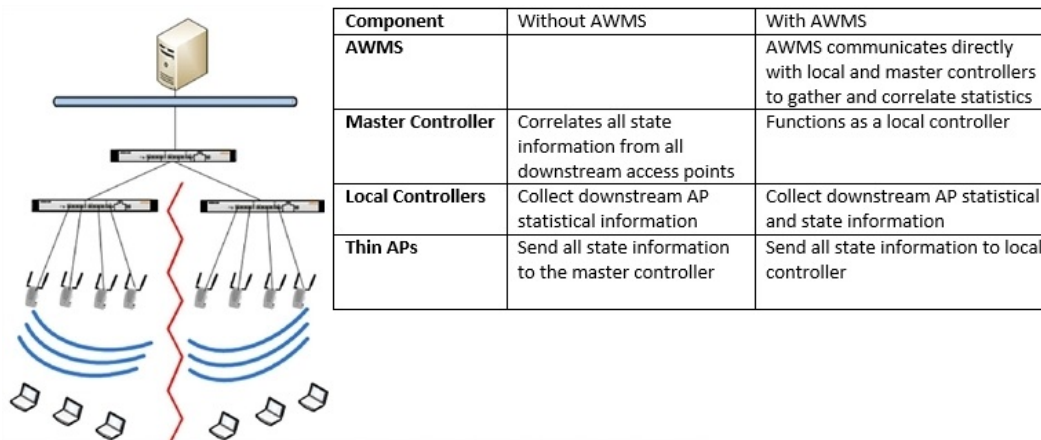
This overview chapter contains the following topics:

- "Understanding Dell Networking W-Series Topology" on page 3
- "Prerequisites for Integrating Dell Networking W-Series Infrastructure " on page 3

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 Wireless LAN Management System (WMS) Offload:

- Username
- Auth password
- Privacy password
- Auth protocol

This section explains how to configure W-AirWave to globally manage your Dell Networking W-Series infrastructure.

- "Disabling Rate Limiting in AMP Setup > General" on page 5
- "Entering Credentials in Device Setup > Communication" on page 5
- "Setting Up Recommended Timeout and Retries" on page 7
- "Setting Up Time Synchronization" on page 7
- "Enabling Support for Channel Utilization And Statistics" on page 8

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.

To disable rate limiting in W-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***

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**.

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 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

[Save] [Cancel]

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

NOTE

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

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).

> **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**.

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 W-AirWave and your network reference NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.

> **NOTE**
>
> Specifying NTP servers is optional. NTP servers synchronize the time on the 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, you must have the following versions:

- Dell Networking W-AirWave 7.6 or later
- Dell Networking W-Series AOS 6.0.1 or later
- Dell Networking W-Instant 3.3 or later

NOTE

AOS 6.0.1 can report RF utilization metrics, while AOS 6.1 is necessary to also obtain classified interferer information.

W-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)

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

The following commands are for AOS 6.4. To get the commands for other versions of AOS, 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> profile <profile-name>
(Controller-Name) (config) # write mem
```

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

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.

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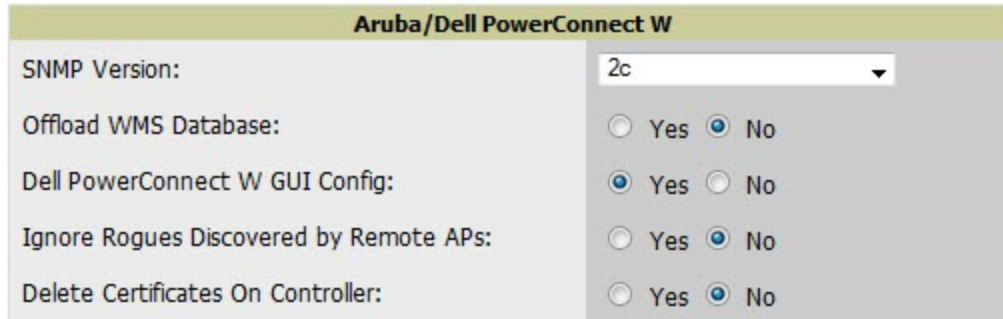
   d. Verify that the **Device-to-Device Link Polling Period** option is set to **30 minutes**.
   e. Verify that the **Rogue AP and Device Location Data Polling Period** option is set to **30 minutes**.

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

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

Figure 7: *Group SNMP Version for Monitoring*

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

Advanced Configuration

Refer to the *Dell Networking W-AirWave 8.0 Controller Configuration Guide* for detailed instructions.

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 W-AirWave for Global W-Series Infrastructure" on page 5
- "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

> **CAUTION**
>
> 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)

[Add] [Cancel]

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.

> 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 **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.

> Local Controller Discovery/monitoring may not work as expected if W-AirWave is unable to communicate directly with the target device. Be sure and update any ACL/Firewall rules to allow W-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 W-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 Dell Networking W-Series devices and contains the following topics:

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
AppRF 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

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 Statistics Utilizing AirWave" on page 19.

When to Use WMS Offload

- You have older Dell Networking W-Series 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 20
  - "Understanding WMS Offload Impact on Dell Networking W-Series Infrastructure" on page 23
  - "WMS Offload Details" on page 44

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 46.

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 AOS CLI" on page 21.

When to Use Channel Utilization

- You have a minimum version of AOS 6.1.0.0.

Prerequisites for Integration

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

- "Configuring W-AirWave for Global W-Series Infrastructure" on page 5
- "Configuring a Dell Networking W Group in AirWave" on page 11
- "Discovering Dell Networking W-Series Infrastructure" on page 13

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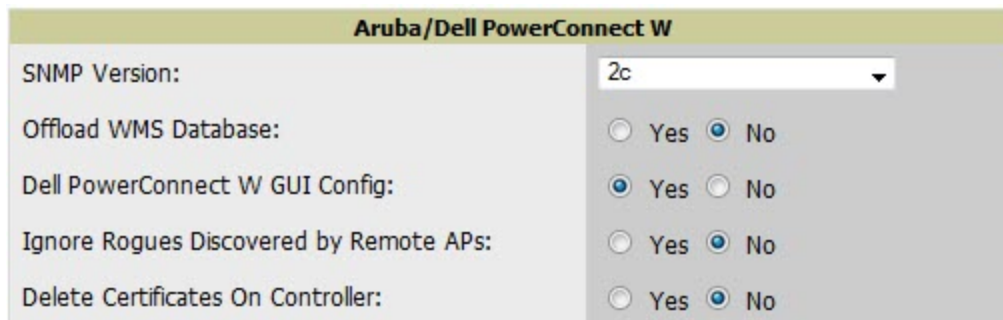
Figure 9: *WMS Offload Configuration in AMP Setup > General*

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***

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 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 "AOS CLI" on page 35 for information about how to utilize the AOS 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 "AOS CLI" on page 35 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 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**.

This process will not reboot your controllers. See "AOS and AirWave CLI Commands" on page 35 for information on how to utilize the AOS CLI to enable stats for WMS Offload.

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
```

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

Define AirWave as a Trap Host Using the AOS 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>
```

Ensure the SNMP community matches those that were configured in "Configuring W-AirWave for Global W-Series Infrastructure" on page 5.

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

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

Ensuring That IDS and Auth Traps Display in AirWave

Validate your AOS 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>
```

See "AOS CLI" on page 35 for the full command that can be copied and pasted directly into the AOS 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 **APs/Devices > Monitor** to validate the IP address in the **Device Info** section.

Figure 11: *Verify IP Address on **APs/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
```

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::enterprises.14823.2.3.1.11.1.1.60 = Hex-STRING: 07 D9 05 06 09 16 0F 00 2D 08 00     SNMPv2-
SMI::enterprises.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::enterprises.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://10.51.5.118/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 AOS 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 AOS 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*
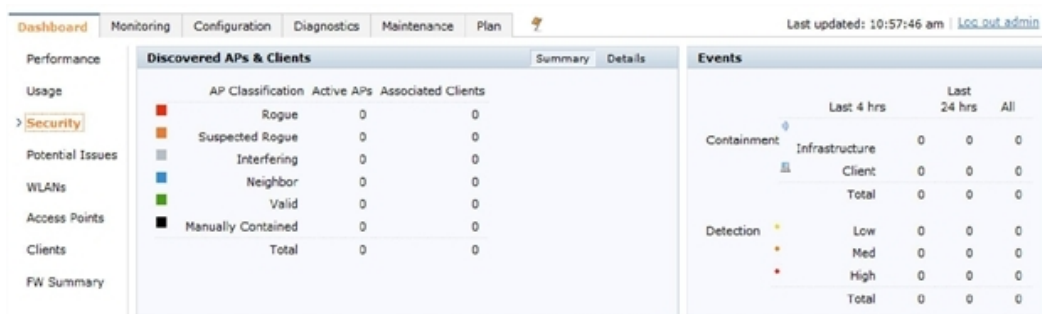
See "Rogue Device Classification" on page 31 for more information about security, IDS, WIPS, WIDS, classification, and RAPIDS.

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" on page 25
- "Remote AP Monitoring" on page 26
- "ARM and Channel Utilization Information" on page 26
- "Viewing Controller License Information" on page 30
- "Rogue Device Classification" on page 31
- "Rules-Based Controller Classification" on page 33

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. Figure 13 shows all authentication failures related to RADIUS data.

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*

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

Figure 14: *IDS Events in AirWave*

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 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.

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 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*
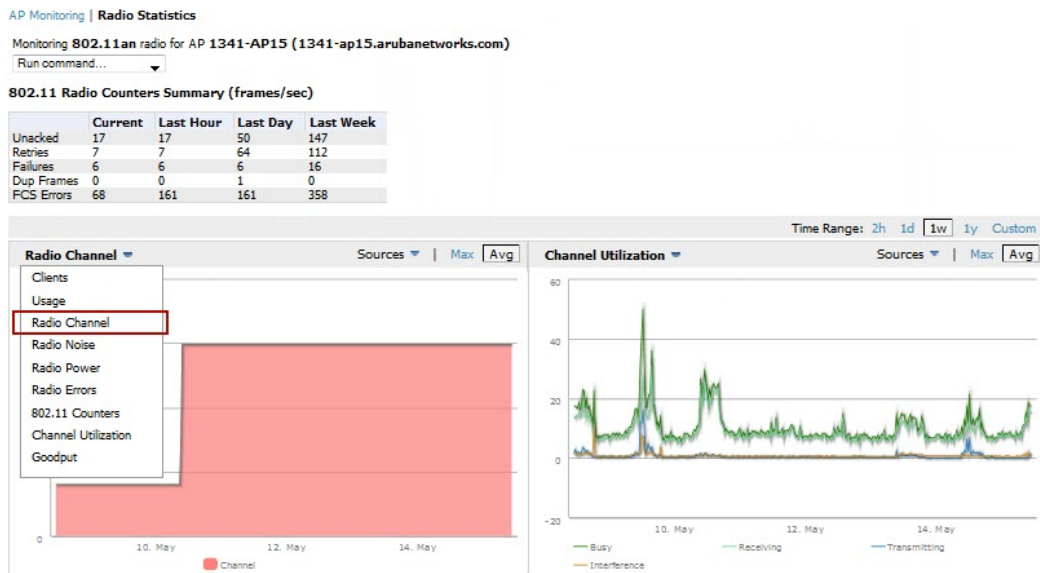
See the *Dell Networking W-AirWave 8.0 User Guide* more information about the data that displays in the **Radio Statistics** page for these devices.

VisualRF and Channel Utilization

1. Navigate to a floor plan by clicking on the thumbnail on a device's **APs/Devices > Monitor** page or navigating to **VisualRF > Floor Plans** page.

2. Select the **Overlays** menu.

Figure 17: *Overlays*
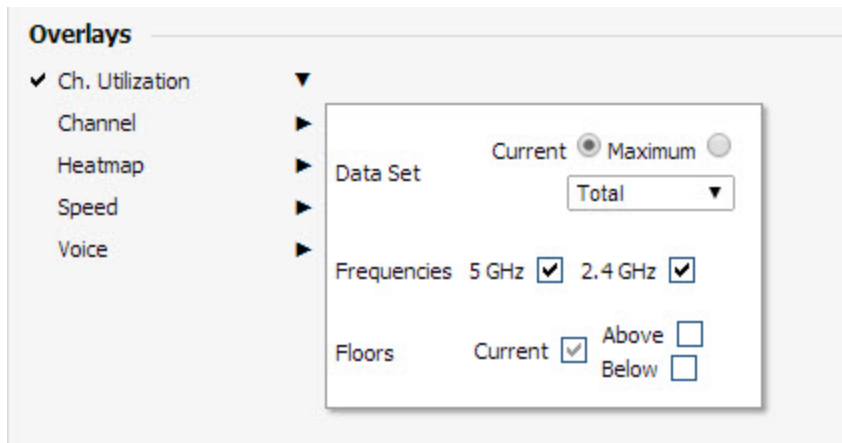
3. Select the **Ch. Utilization** overlay.

4. Select **Current** or **Maximum** (over last 24 hours).

   - If Maximum is selected, then use the drop-down list 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 18: *Channel Utilization in VisualRF (Interference/2.4 GHz)*
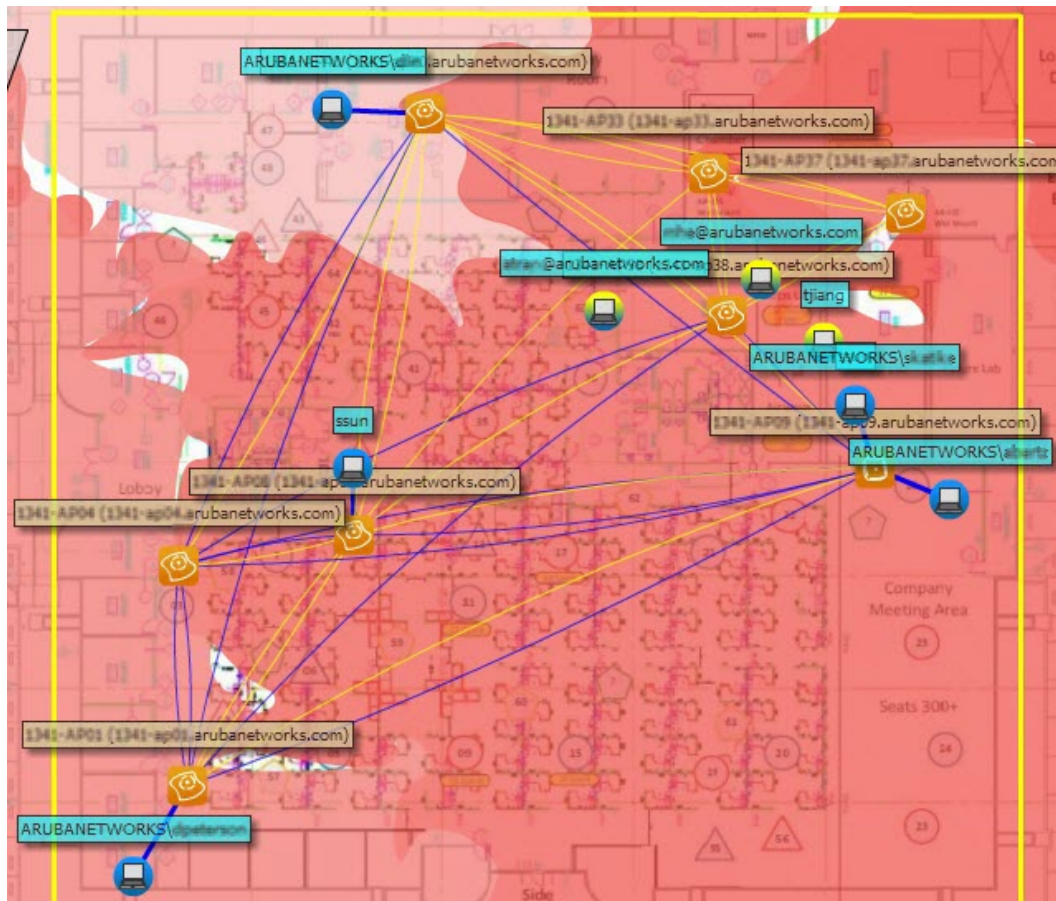
Configuring Channel Utilization Triggers

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 *Dell Networking W-AirWave 8.0 User Guide* 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 AirWave Alerts.

Figure 20: *Channel Utilization alerts*

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 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 most and least utilized 2.4 and 5 channel usage information.

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

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 23: *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	AITUcIWKj-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 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	AOS (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 from the **RAPIDS Classification Override** drop-down list.

Figure 24: *Rogue Detail Page Illustration*

Name:	Aruba-21:38:30	Model:	-	First Discovered:	5/13/2013 12:19 PM
Acknowledge:	Yes / No	IP Address:	-	First Discovery Method:	Wireless AP scan
Controller Classification:	Suspected Rogue	Confidence:	20		
SSID:	CampusF-secure	First Discovery Agent:	AP-224-11ac-VRF		
RAPIDS Classification:	Suspected Rogue	Channel:	1	Last Discovered:	5/15/2013 1:39 PM
Classification Rule:	Signal strength > -75 dBm	WEP:	Yes	Last Discovery Method:	Wireless AP scan
RAPIDS Classification Override:	- No Override -	WPA:	Yes	Last Discovery Agent:	00:24:6c:c8:6e:e0
Threat Level:	- No Override -	Network Type:	AP		
Threat Level Override:	Valid				
Radio MAC Address:	Suspected Valid				
Radio Vendor:	Neighbor				
LAN MAC Address:	Suspected Neighbor	Current Associations:	0		
LAN Vendor:	Suspected Rogue	Max Associations:	5		
OUI Score:	Rogue				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				

⚠️ **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 AOS 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 AOS device classification, navigate to **RAPIDS > List** and utilize the **Modify Devices** checkbox combined with the multiple sorting a filtering features.

Table 4: *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 list (see Figure 25):

Figure 25: *User Classification*

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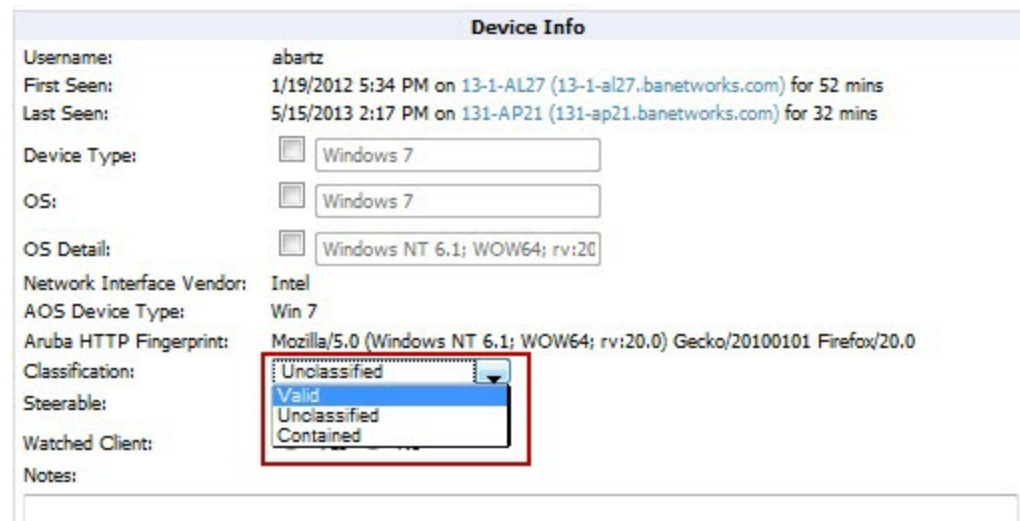
Changing User Classification within the AirWave UI will push a user reclassification message to all controllers managed by the AirWave server that are in Groups with Offloading the WMS database set to **Yes**.

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 before bulk to match the controller's classification. Each client must be updated individually within the AirWave UI.

Rules-Based Controller Classification

This section contains the following topics:

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

> **CAUTION**
>
> Enabling these commands on AOS versions prior to 6.1 can result in performance issues on the controller.

To enable channel utilization events utilizing the Dell Networking W-Series AOS 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 AOS 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 AOS 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 AOS 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 AOS command-line interface or the AirWave SNMP Walk.

Refer to:

AOS 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. AOS 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
wlsxSystemExtGroup
```

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 AOS 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 AOS 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 AOS, 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 AOS 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 AOS 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
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
```

NOTE

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

The tables below describe the different methods through which AirWave acquires data from Dell Networking W-Series devices on the network.

The tables use the following symbols:

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

Table 5: *Data Flow between Controllers and W-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 Dell Networking W-Series AOS 6.3 or later and AirWave 7.7.7 or later.
Configuration Audit			←									
Configuration Push			←									
Controller Up/Down Status	←							←				
Device CPU/Memory	←											
Enabling of WMS Offload			←									

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

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Exec UI							→					When AMON is used for client monitoring, W-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 W-AirWave via HTTPS.
IDS Events		→										
Interface Monitoring	←											
Lync/UCC/Voice				→								Available in W-AirWave 8.0 and beyond.
Neighbor Clients	←			→								
Network Derivations			←									
RADIUS Auth Issues		→										
RAPIDS	←											
RF Capacity				→								
RF Health				→								
Rogue AP OS									↑			
Rogue Classification	←				←							If WMS Offload enabled, Dell Networking W-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 W-AirWave*

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

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*
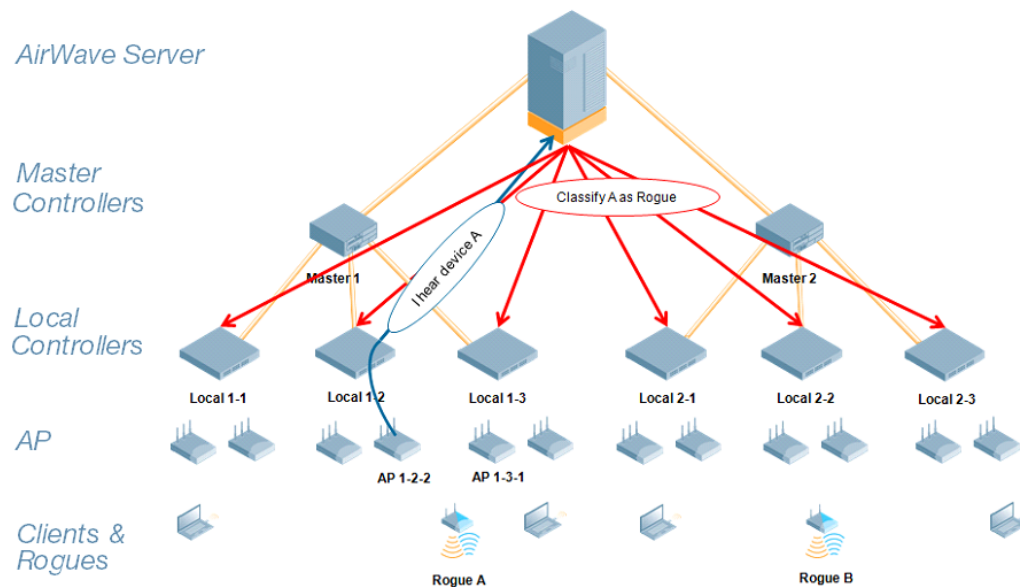
State Correlation Process

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 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 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 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 AOS.

- 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 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 7: *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 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

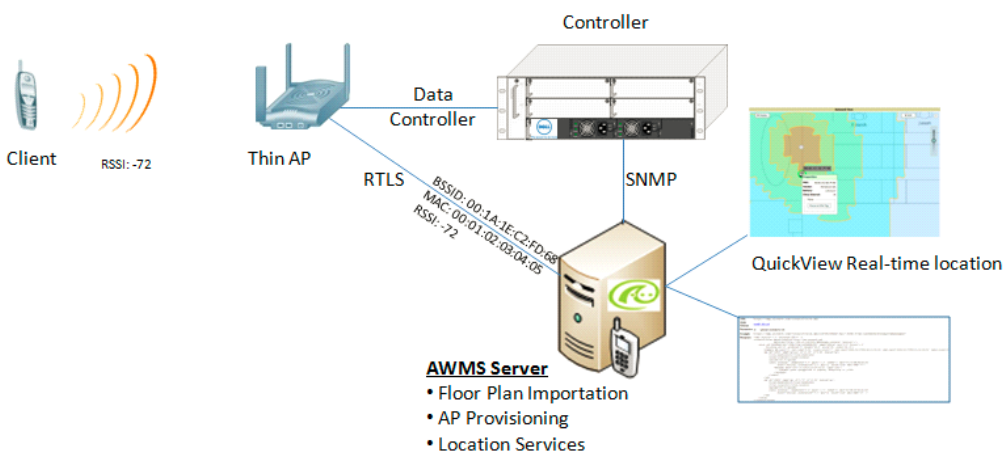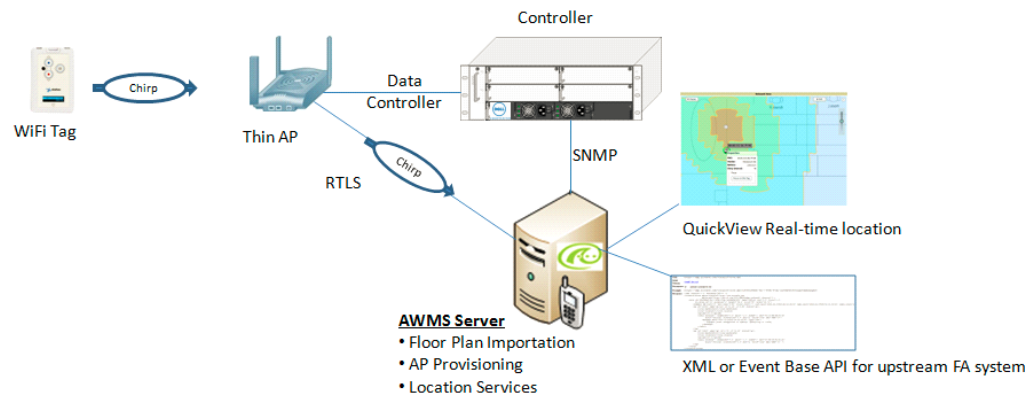**Figure 29:** *Typical Client Location*

Figure 30: *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

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 username 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 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

Enable RTLS on the Controller

> **NOTE:** 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*

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:
    00147aaf01000020001a1ec02b3200000001000000137aae0100000c001a1ec02b320000001a1e82b322590006ddf
    f02
    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:
    0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec050780000000d54a7a280540001ddf
    f020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
    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:
    0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec050780000000d54a7a280540001ddf
    f020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
```

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 running 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 access points from any given location. The recommended value is four APs.
- Ensure that the tags chirp on all regulatory channels.

This appendix describes the feature implementation schedule for AirWave.

Table 8: *Feature Implementation Schedule for AirWave*

Feature	AirWave Implementation
HTML5-based UI for VisualRF	8.0
VisualRF Floor Upload Wizard	8.0
VisualRF Navigation Improvements	8.0
AppRF Overlay	8.0
AppRF Reports	8.0
UCC Visability	8.0
Additive Licensing	8.0
Client Health Graph	8.0
New Supported Devices	8.0