Dell PowerConnect W Airwave 7.1

Best Practices Document

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:
http://www.arubanetworks.com/open_source

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.

Table of Contents

Overview

This document provides best practices for leveraging the Dell PowerConnect W AirWave Wireless Management Suite (AWMS) to monitor and manage your Dell PowerConnect infrastructure. The Dell PowerConnect W infrastructure provides a wealth of functionality (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 the Dell PowerConnect W infrastructure.

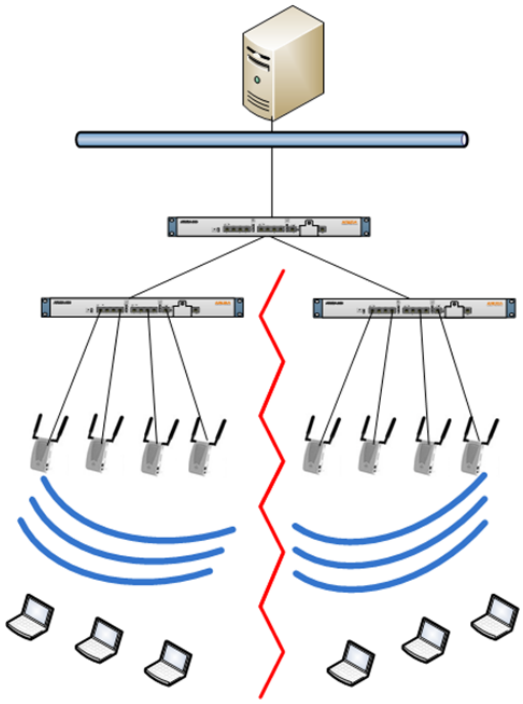
Minimum Requirements

- Dell PowerConnect W AWMS version 7.0 or higher
- Dell PowerConnect 5.0 or higher or ArubaOS 3.x or higher

Understanding Dell Topology

Here is a typical Master-Local deployment.

Figure 1 *Typical Dell PowerConnect W 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 AWMS server whose Master controller is also not under management.

Prerequisites for Integrating Dell PowerConnect W Infrastructure

You will need the following information to monitor and manage your Dell PowerConnect W infrastructure.

- SNMP community string (monitoring & discovery)
- Telnet/SSH credentials (configuration only)
- “enable” password (configuration only)

Note: Without proper Telnet/SSH credentials AWMS 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

Known and Recently Resolved Issues

AWMS Impact	Description	Resolution
7.x	AP-105s report noise floor at 20 dBm worse than actual. AMP utilizes noise floor to calculate client signal quality. Poor signal quality can reduce location accuracy.	VisualRF adds 20 dBm to client signal in order to increase location accuracy. AMP will show very low signal for all client associated with AP-105s.
7.x	The 651 controllers do not provide signal quality and BW for clients associated to the internal AP.	
7.x	wms offload does not work for APs on tagged ports. This cause client tracking issues in AMP	
7.x	Because of telnet service contention AMP device auditing fails and causes mismatches on Dell PowerConnect W controllers	7.1 will provide a more efficient method to fetching controller settings.

Dell Feature Implementation Schedule for AWMS

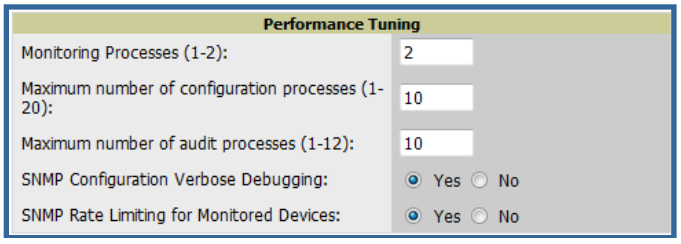
Feature	AWMS Implementation
Ability filter User Session by Dell PowerConnect ArubaOS roles	7.0
AOS 5.0 support	7.0
RAP white list management for RN 3.1	7.0
Added support for rogue containment	7.0
Added support for configuring controller specific overrides	7.0
Client dot11counter status	7.0

Configure AWMS to Optimally Manage Dell PowerConnect Infrastructure (Global)

AMP Setup General Page (Rate Limiting)

There are several SNMP tuning parameters which must be configured in order for AWMS to properly monitor Dell PowerConnect infrastructure.

Figure 2 *SNMP Rate Limiting*



- Navigate to **AMP Setup > General** page
- Locate the **Performance Tuning** section
- Enable SNMP Rate Limiting for Monitored Devices

Note : Enabling the SNMP Rate Limiting for Monitored Devices option above adds a small delay between each SNMP Get request, thus the actual polling intervals will be longer than what is configured in Section 3. For example a 10 minute polling interval will result in an actual 12 minute polling interval..

- Click **Save**.

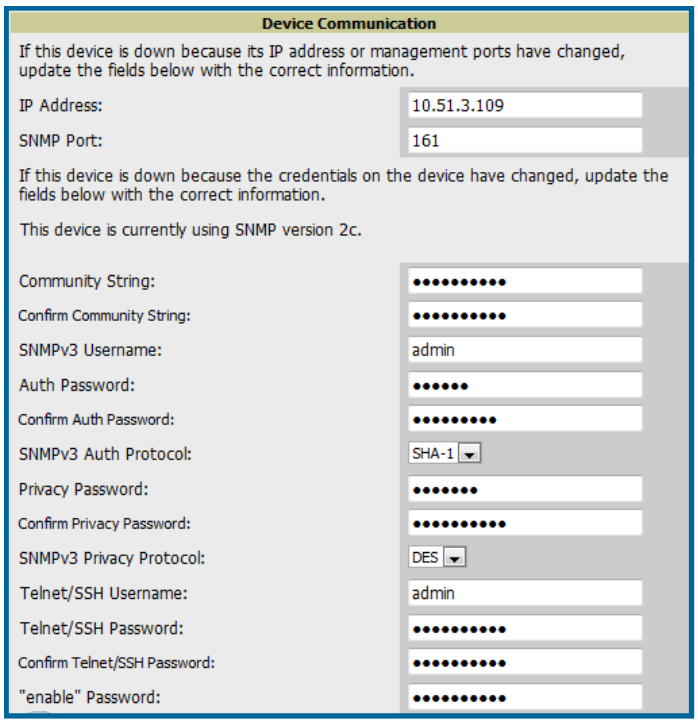
Device Setup Communication Page (Credential & Timing)

Credentials

AWMS requires several credentials to properly interface with Dell infrastructure. The Discover process detailed in Section 3 requires proper global credential configuration.

- Navigate to **Device > Setup Communication** page
- Locate the **Default Credentials** section
- Click on the Dell link

Figure 3 *Credential Setup*



Required Fields for Discovery

- Enter 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.

Required Fields for Configurations and Basic Monitoring

- Enter Telnet/SSH Username
- Enter Telnet/SSH Password
- Enter "enable" Password

Additional Required Fields for wms Offload

- Enter SNMPv3 Username
- Enter Auth Password
- Enter Privacy Password

Note : Auth and Privacy passwords must match; because the wms offload command only accepts a single password that is leveraged for both options

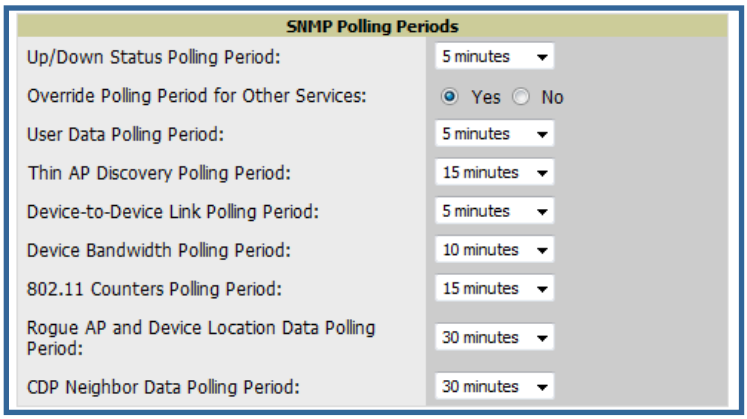
Creating an Dell PowerConnect Specific Policy (Group) in AWMS

It is prudent to establish an Dell PowerConnect Group within AWMS. During the discovery process you will move new discovered controllers into this group.

Basic Monitoring Configuration

- Navigate to the **Groups>List** page
- Click **Add**.
- Enter a Name that represents the Dell PowerConnect W infrastructure from a security, geographical, or departmental perspective and click **Add**.
- You will be redirected to **Group > Basic** page for the Group you just created. On this page you will need to tweak a few Dell-specific settings.
- Find the **SNMP Polling Periods** section of the page
    - Change Override Poll Period for Other Services to "Yes"
    - Ensure User Data Polling Period is set to "10 minutes" Do **not** configure this interval lower than "5 minutes"

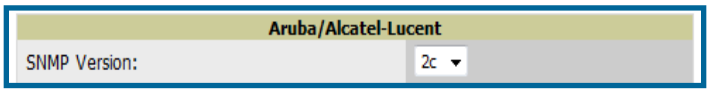
Figure 5 *Group Polling Configuration*



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

    - Change Device-to-Device Link Polling Period to "30 minutes"
    - Change Rogue AP and Device Location Data Polling Period to "30 minutes".
- Find the **Dell PowerConnect W** section of the page
    - Configure the proper SNMP version for monitoring the Dell PowerConnect W infrastructure. The other options in this section are addressed later in this document or in the Dell PowerConnect W Configuration Guide.
    - Click **Save and Apply**.

Figure 6 *Group SNMP Version for Monitoring*



Note : You should reference the Dell PowerConnect W Configuration Guide for additional information on Policy configuration.

Configuration

Reference the *Dell PowerConnect ArubaOS Configuration Guide* located on **Home > Documentation** page for detailed instructions.

Discovering Dell Infrastructure

AWMS utilizes Dell's topology to efficiently discover downstream infrastructure.

Prerequisites for discovery

- Section 2 - credentials
- Section 3 – creating Dell PowerConnect policies (Groups)

Summarized procedure for discovery and managing Dell Infrastructure

- Discover Master controllers
- Manage Master controllers which automatically discovers Local controllers affiliated with the Master controller
- Manage Local controllers which automatically discovers Thin APs affiliated to the Local controllers
- Manage Thin APs

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 AWMS 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.

Master Controller Discovery

- Scan networks containing Dell PowerConnect W Master controllers from **Device > Discover** page. This will use your Global Credentials configured in the previous section.

  - or -

- Manually enter the Master controller on the **Device > Add** page.
  - Select the controller type and click "Add" button
  - Enter IP Address

Required Fields for Discovery

- Enter 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.

Required Fields for Configurations and Basic Monitoring

- Enter Telnet/SSH Username
- Enter Telnet/SSH Password
- Enter "enable" Password

Additional Required Fields for WMS Offload

- Enter SNMPv3 Username
- Enter Auth Password
- Enter Privacy Password

Note : Auth and Privacy passwords must match; because the **wms offload** command only accepts a single password that is leveraged for both options.

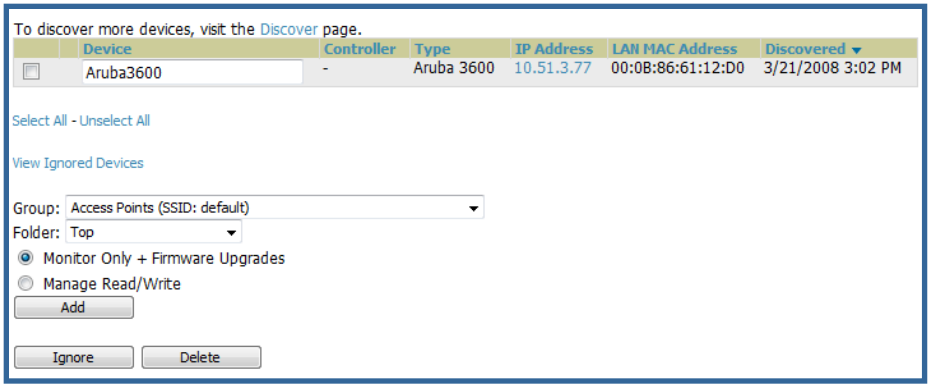
In AWMS 7.0 and later AWMS automatically configures the Auth Protocol to SHA.

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

- Assign controller to a Group & Folder
- Ensure "Monitor Only" option is selected
- Click the "Add" button

- Navigate to **APs/Devices > New** page
  - Select the Dell PowerConnect W Master controller
  - Ensure "Monitor Only" option is selected
  - Click the "Add" button

Figure 7 *Add New Controller*



Local Controller Discovery

- Local controllers are discovered via the Master controller. After waiting for the Thin AP Polling Period or executing a "Poll Now", the Local controllers will appear on the **APs//Devices > New** page. "Poll Now" button is located on the **Device > Monitoring** page.
- Add the Local controller to Group defined above. Within AWMS Local controllers can be split away from the Master controller's Group.

Thin AP Discovery

- Thin APs are discovered via the Local controller. After waiting for the Thin AP Polling Period or executing a "Poll Now", thin APs will appear on the **APs/Devices > New** page. "Poll Now" button is located on the **Device > Monitoring** page.
- Add the Thin APs to the Group defined above. Within AMWS thin APs can be split away from the controller's Group. You can split thin APs into multiple Groups if required.

AWMS and Dell PowerConnect Integration Strategies

Integration Goals	All Masters Architecture	Master Local Architecture
Rogue & Client Info		enable stats
Rogue containment only	ssh access to controllers	ssh access to controllers
Rogue & Client containment	wms offload	wms offload
Reduce Master Controller Load		wms offload debuging off
IDS & Auth Tracking	Define AWMS as trap host	Define AWMS as trap host
Track Tag Location	enable RTLS wms offload	enable RTLS wms offload

Key Integration Points

- 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

Example of When to Use Enable Stats

Customer wants to pilot AMWS and doesn't want to make major configuration changes to their infrastructure or manage configuration from AWMS. Enable Stats still pushes a small subset of commands to the controllers via SSH.

Examples of When to Use WMS Offload

- Customer has older Aruba Networks infrastructure in 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 AWMS.
- Customer is replacing MMS with AWMS and already had WMS offloaded for performance reasons.
- Customer wants to use AWMS to distribute client and rogue device classification amongst multiple Master controllers in a Master Local environment or in an all Masters environment

Examples of 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.
- A customer wants to locate items utilizing WiFi Tags.

Note : RTLS could negatively impact your AWMS server's performance

Example to Define AWMS as Trap Host

- Customer wants to track IDS events within the AWMS UI.
- Customer is in the process of converting their older 3rd Party WLAN devices to Dell PowerConnect W devices and wants a unified IDS dashboard for all WLAN infrastructure.
- Customer wants to relate Auth failures to a client device, AP, Group of APs, and controller. AWMS provides this unique correlation capability.

Prerequisites for Integration

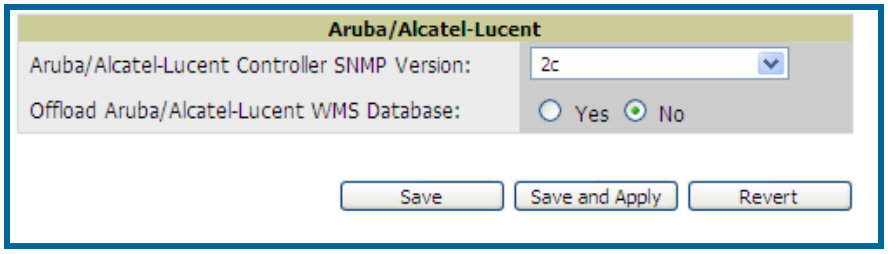
If you have not discovered the Dell infrastructure or configured credentials, proceed to Sections 3 and 4 of this document.

Enable Stats Utilizing AWMS GUI

To enable stats on the Aruba controllers:

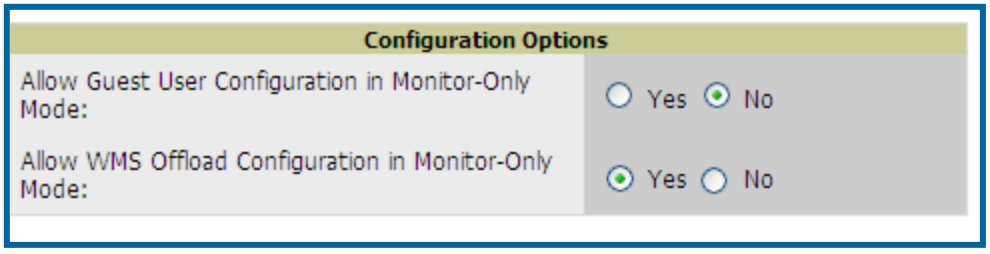
- Navigate to **Groups>Basic** page
- Locate the Dell PowerConnect W section
- Disable **Offload Dell PowerConnect WMS Database**
- Click **Save and Apply**.

Figure 8 *Enable Stats*



- Navigate to AMP Setup > General page
- Locate Configuration Options section
- Enable **Allow WMS Offload Configuration in Monitor-Only Mode**
- Click **Save**.

Figure 9 *WMS Offload Configuration Options (enable stats)*



This will push a set of commands via SSH to all Dell PowerConnect local Controllers. AWMS must have read/write access to the controllers in order to push these commands. See **Device Setup Communication Section** below for help configuring your device credentials.

Note : This process will not reboot your controllers

Warning : If you don't follow the above steps local controllers will not be configured to populate statistics. This decreases AWMS' capability to trend client signal information and to properly locate devices. See Appendix A on how to utilize the Dell PowerConnect W AirWave CLI to enable stats on Dell PowerConnect W infrastructure.

Note : If your credentials are invalid or the changes are not applied to the controller, error messages will display on the controller's Device > Monitoring page under the Recent Events section. If the change fail, AWMS does not audit these setting (display mismatches) and you will need to apply to the controller by hand, see Appendix A for detailed instructions.

Commands Pushed by AWMS during Enable Stats

(Do not enter these commands)

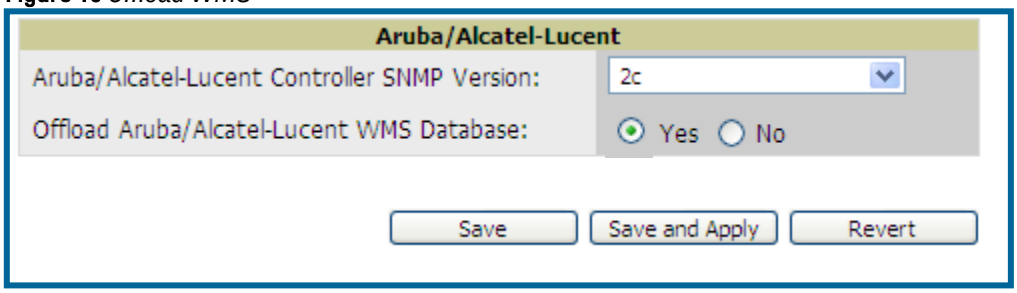
```
configure terminal
no mobility-manager <Active WMS IP Address>
wms
general collect-stats enable
stats-update-interval 120
show wms general
write mem
```

WMS Offload Utilizing AWMS GUI

To Offload WMS on the Dell PowerConnect W controllers:

- Navigate to **Groups>Basic** page
- Locate the Dell PowerConnect W section
- Enable **Offload Dell PowerConnect W WMS Database**
- Locate the Configuration section
- Enable or Disable **Allow WMS Offload Configuration in Monitor-Only Mode**
- Click **Save and Apply**

Figure 10 *Offload WMS*



This will push a set of commands via SSH to all Dell PowerConnect W Master Controllers. If the controller does not have an SNMPv3 user that matches AWMS' database it will automatically create a new SNMPv3 user. AWMS must have read/write access to the controllers in order to push these commands.

Note : This process will not reboot your controllers. See Appendix A on how to utilize the Dell PowerConnect W CLI to enable stats or wms offload.

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

Note : Auth Protocol **must** be configured to **SHA**. Privacy Protocol **must** be configured to **DES**

Commands Pushed by AWMS during WMS Offload

(Do not enter these commands)

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

Note : When you use Dell PowerConnect W AWMS 7.0 with Dell PowerConnect W , Dell PowerConnect W AWMS AWMS will configure SNMPv2 traps with the mobile manager command.

Other Processes for wms offload

AWMS will issue an SNMPGet on table (wlsxSysExtHostname) to complete the offload process (OID=.1.3.6.1.4.1.14823.2.2.1.2.1.2.0.)

Define AWMS as Trap Host using Dell PowerConnect ArubaOS CLI

To ensure the AWMS server is defined a trap host, SSH into 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 <AWMS IP ADDR> version 2c <SNMP
community string of conroller>
```

Note : Ensure the SNMP community matches what was configured in Section 2

```
(Controller-Name) (config) # snmp-server trap source <CONTROLLER'S IP>

(Controller-Name) (config) # write mem

Saving Configuration...

Saved Configuration
```

Warning : Do not configure the SNMP version to v3, because AWMS does not support SNMPv3 traps/informs.

- Dell PowerConnect ArubaOS Traps utilized by AWMS

  Auth Traps Utilized by AWMS

  - wlsxNUserAuthenticationFailed
  - wlsxUserAuthenticationFailed (AMP does not use this trap)
  - wlsxNAuthServerReqTimedOut

  IDS Traps Utilized by AWMS

  - wlsxSignatureMatchAP
  - 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

Diagnostic Steps to Ensure IDS & Auth Traps Display in AWMS

- Validate your Dell PowerConnect ArubaOS configuration by exiting the "configure terminal" mode and issue the following command:

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

If any of the traps below don't show as enabled enter configure terminal mode and issue the following command:

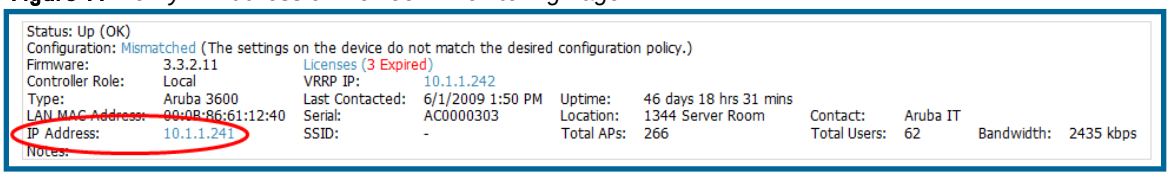
```
(Controller-Name) (config) # snmp-server trap enable <TRAPS FROM LIST ABOVE>
```

Note : See Appendix A for the full command that can be copied and pasted directly into the Dell PowerConnect W CLI.

```
(Controller-Name) (config) # write mem
Saving Configuration...
Saved Configuration
```

- Ensure the source IP of the traps match the IP that AWMS utilizes to manage the controller. Navigate to **Device > Monitoring** page to validate the IP address.

Figure 11 *Verify IP Address on Device > Monitoring 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 firewall port 162 (default) is open between AWMS and the controller.
- Validate traps are making it into AWMS by issuing the following commands from AWMS command line.

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

[root@AWMS ~]# 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:
"aruba-ap"SNMPv2-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: "aruba-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:d
0"
```

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

Ensure you disable qlogging after testing as it could negatively impact AWMS performance if let turned on.

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

Understanding WMS Offload Impact on Dell Infrastructure

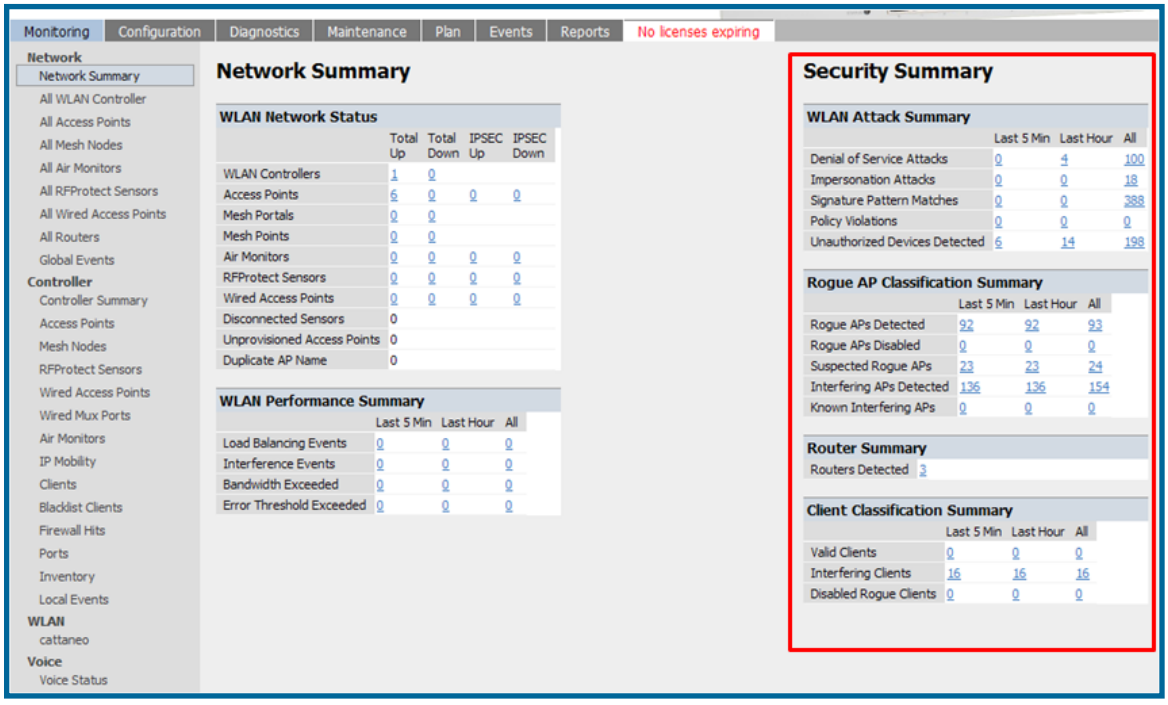
When offloading WMS it is important to understand what functionality is migrated to AWMS and what functionality is deprecated.

The following Tabs and sections are deprecated after offload wms

- Plan Tab - where floor plans are stored and heatmaps are generated. Prior to offloading wms ensure that you have exported floor plans from the Dell PowerConnect ArubaOS and imported into AWMS. All functionality within the Plan Tab is incorporated with the VisaulRF module in AWMS.
- Report Tab – All reports are incorporate within AWMS.
- Events Tab – the majority of functionality within this Tab is incorporate within AWMS Reports and Alerts sections with the exception of:
    - Interference Detected
    - Rogue AP
    - Station Failed
    - Suspected Rogue AP

One important area to note is the Security Summary display disappears after offloading WMS. The data is still being processed by the Master Controller, but the summary information is not available. AWMS does provide ability to view some of this information in detail and summary form.

Figure 12 *Security Summary on Master Controller*



WLAN Attack Summary

- DOS Attacks – no summary data available in AWMS
- Impersonation Attacks – no summary data available in AWMS
- Signature Pattern Matches – partial summary data available on **Home** and **RAPIDS > Overview** pages

- Policy Violations – no summary data available in AWMS
- Unauthorized Devices Detected – no summary data available in AWMS

Rogue AP_Classification Summary

- Rogue APs Detected – summary data available on **RAPIDS > Overview** page
- Rogue APs Disabled – no summary data available in AWMS
- Suspected Rogue APs – partial data is available in AWMS on each AP's **Device > Management** page
- Interfering APs Detected – partial data is available in AWMS on each AP's **Device > Management** page
- Known Interfering APs – partial data is available in AWMS on each AP's **Device > Management** page

Router Summary

- Routers Detected – no summary data available in AWMS

Client Classification Summary

- Valid Clients – summary data available on all pages in the dashboard
- Interfering clients – no summary data available in AWMS
- Disabled Clients – no summary data available in AWMS

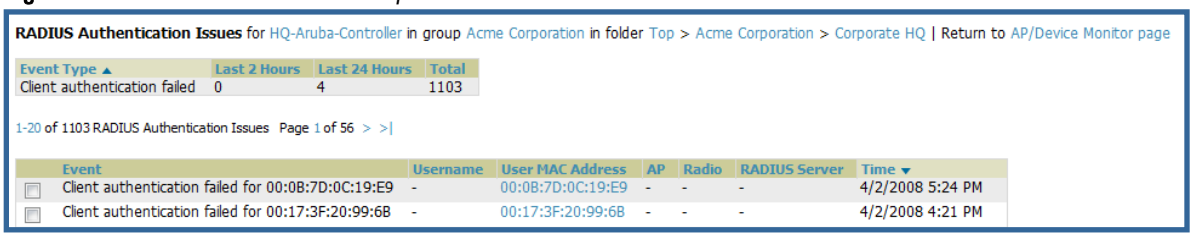
See "Device Classification" for more information on Security, IDS, WIPS, WIDS, classification, and RAPIDS.

Dell-Specific Capabilities within AWMS

Dell PowerConnect Traps for RADIUS Auth & IDS Tracking

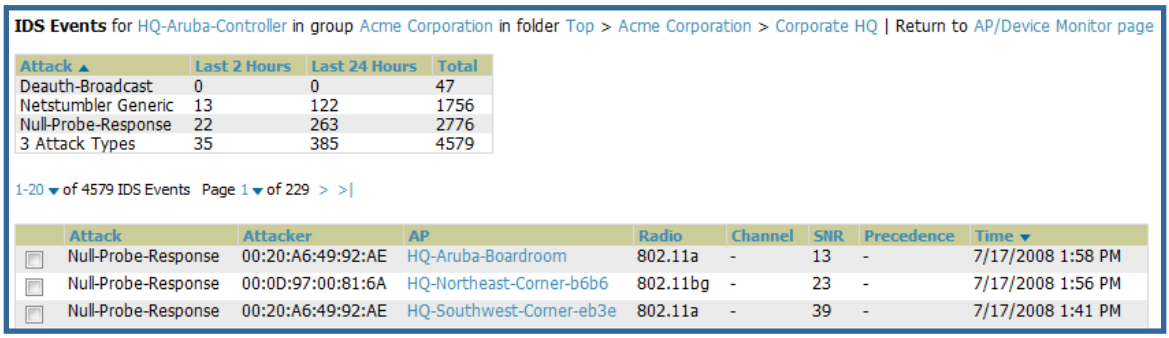
The authentication failure traps are received by the AWMS server and correlated to the proper controller, AP, and user. See Figure below showing all authentication failures related to a controller.

Figure 13 *RADIUS Authentication Traps as Seen in AWMS*



The IDS traps are received by the AWMS server and correlated to the proper controller, AP, and user. See Figure below showing all IDS traps related to a controller.

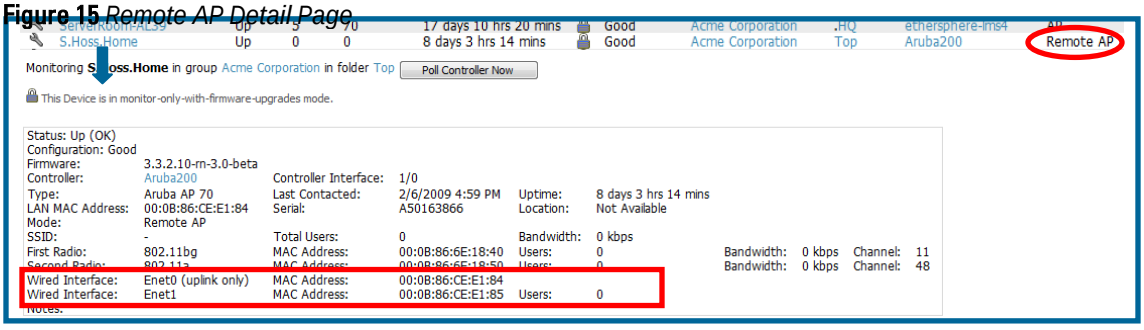
Figure 14 *IDS Traps as Seen in AWMS*



Remote AP & Wired Networking Monitoring

- From the Device > List page you can distinguish and sort on Mode "Remote"
- To view detailed information on the remote device click on the device name. You can see if there are users plugged into the wired interfaces.

Figure 15 *Remote AP Detail Page*

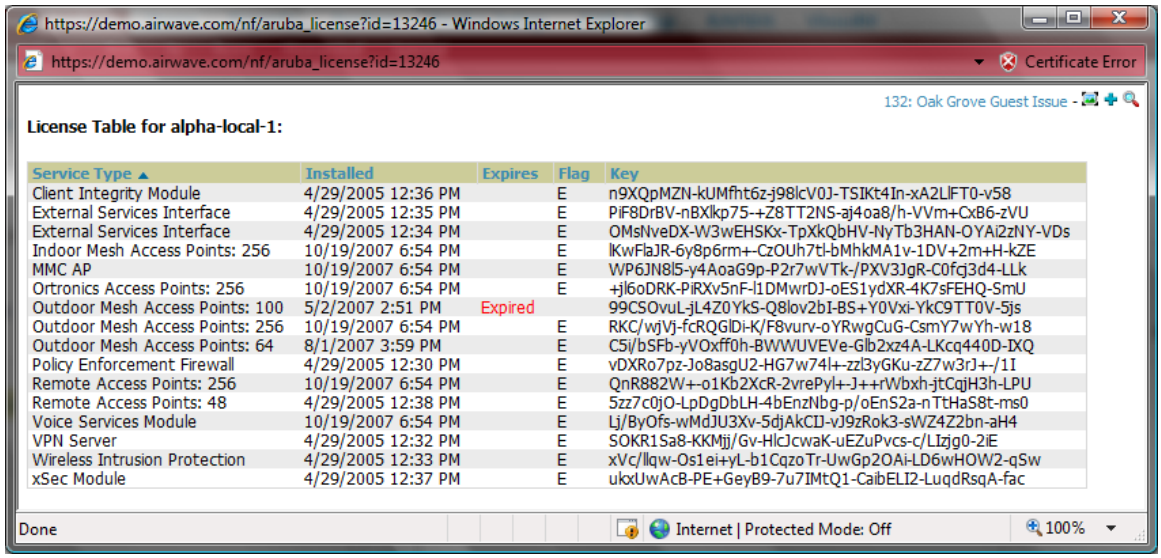


Note : This feature is only available when the remote APs are in split tunnel and tunnel modes.

View Controller License Information

- Navigate to the **Device > Detail** page of a controller under AWMS management
- Click on the License link

Figure 16 *License Popup*



6.4 - Device Classification

Only utilize this section if you have completed WMS offload procedure above. After offloading WMS, AWMS maintains the primary (ARM, WIPS, and WIDS) state classification for all devices discovered over-the-air.

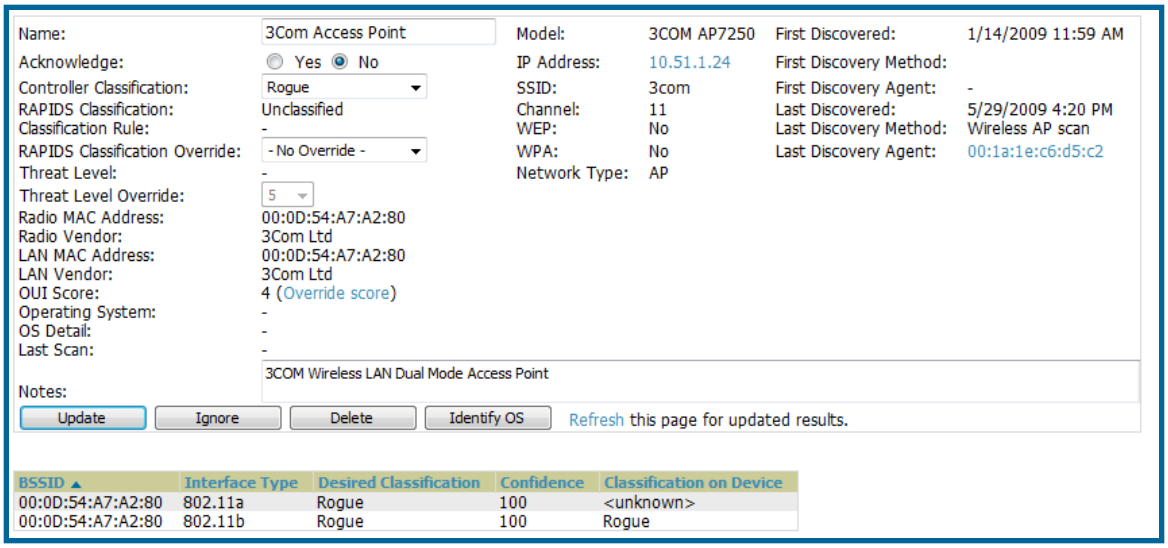
WIPS/WIDS to AWMS Controller Classification Matrix

AWMS 'Controller Classification'	AOS (WIPS/WIDS)
Unclassified (default state)	Unknown
Valid	Valid
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Suspected Rogue	Suspected Rogue
Rogue	Rogue
Contained Rogue	DOS

To check and reclassify rogue devices

- Navigate to **the Rogue > Detail** page for the device
- Select the proper classification from the Controller Classification Pull Down

Figure 17 *Rogue Detail*



Warning : Changing the controller's classification within the Dell PowerConnect W AWMS UI will push a reclassification message to all controllers managed by the AWMS server that are in Groups with the **Offloading the WMS database** parameter set to **Yes**. To reset the controller classification of a rogue device on AWMS, change the controller classification on the AWMS UI to "unclassified".

Controller classification can also be updated from **RAPIDS > List** page via the modify-these-devices mechanism.

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 Dell PowerConnect W as "valid" will also be classified within Dell PowerConnect W AWMS as "valid" for their controller classification as well. As APs report subsequent classification information about rogues, this classification will be reflected within AWMS UI and propagated to controllers that AWMS manages. It is probable that the device classification reflected in the controller's UI and in AWMS' UI will not match, because the controller/APs do not reclassify rogue devices frequently.

To update a group of devices' controller classification to match the Dell PowerConnect ArubaOS device classification navigate to **RAPIDS > List** page and utilize the modify-these-devices mechanism combined with the multiple sorting a filtering features.

ARM to AWMS Classification Matrix

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

- Navigate to the **User > Detail** page for the user

- Select the proper classification from the Classification Pull Down

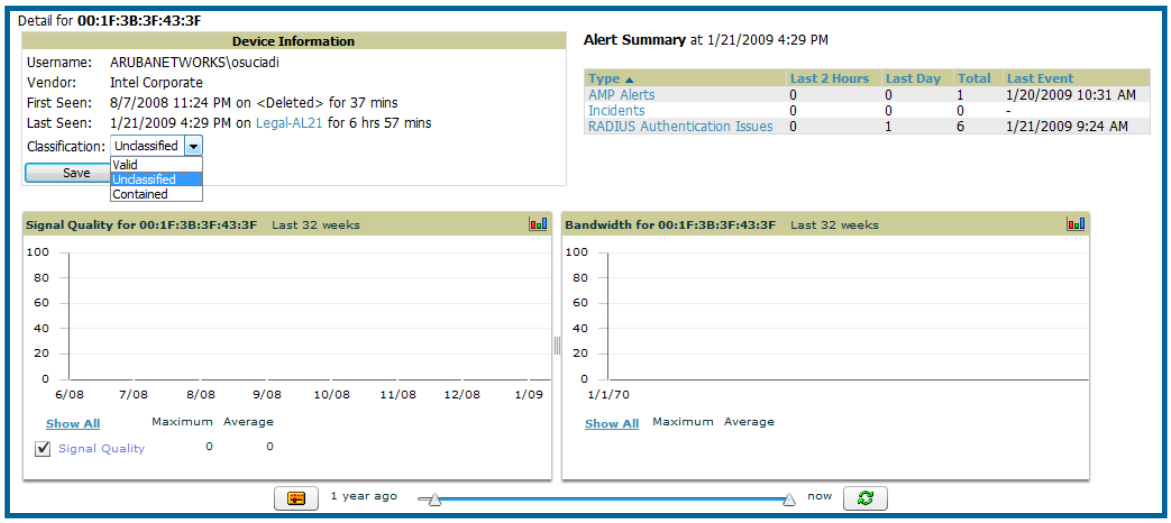


Figure 18 *User Classification*

Warning : Changing User Classification within the Dell PowerConnect W AWMS UI will push a user reclassification message to all controllers managed by the AWMS server that are in groups with the **Offloading the WMS database parameter** 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 AWMS UI and propagated to controllers that AWMS manages. It is probable that the user's classification reflected in the Controller's UI and in AWMS' UI will not match, because the Controller/APs do not reclassify users frequently.

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

Appendix A - Dell PowerConnect ArubaOS & AWMS CLI Commands

Enable Stats Utilizing the Dell PowerConnect W CLI (Local Controller in Master Local Environment)

Note : Do not use these commands if using the Dell PowerConnect W AWMS WebUI to set these commands.

SSH into the controller, 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) # wms general collect-stats enable
(Controller-Name) (config) # write mem
Saving Configuration...
Saved Configuration
```

Offload WMS Utilizing Dell PowerConnect ArubaOS CLI and AWMS CLI (SNMP Walk)

Note : Do not use these commands if using the Dell PowerConnect W AWMS WebUI.

Dell PowerConnect W 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> trap-version 2c (trap-version was added in 3.3.2.14 to prevent
the SNMPv3 inform queue overflow on the controller)
```

This command creates an SNMPv3 user on the controller with 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 Dell PowerConnect W AWMS adheres to this IETF recommendation. DellPowerConnect W automatically creates Auth and Privacy passwords from this single password. If mobility-manager is already using a preconfigured SNMPv3 user ensure the Privacy & Authentication passwords are the same. This command also creates the AWMS server as an SNMPv3 Trap Host in the controller's running configuration

```
Sample: mobility-manager 10.2.32.1 user airwave123 airwave123
(Controller-Name) (config) # write mem
Saving Configuration...
Saved Configuration
```

Dell PowerConnect W AWMS SNMP

Login into the AMWS server with proper administrative access and issue the following command for all controllers (master and locals):

Note : Do not use these commands if using the Dell PowerConnect W AWMS WebUI.

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

WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchIp.0 = IpAddress: 10.51.5.222
WLSX-SYSTEMEXT-MIB::wlsxSysExtHostname.0 = STRING: aruba-3600-2
.
.
.
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchLastReload.0 = STRING: User reboot.
WLSX-SYSTEMEXT-MIB::wlsxSysExtLastStatsReset.0 = Timeticks: (0) 0:00:00.00
esponse

[root@AWMS ~]#
```

If this SNMP walk command is not 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.

Sample: snmpwalk -v3 -a SHA -l AuthPriv -u airwave123 -A airwave123 -X airwave123 10.51.3.222 wlsxSystemExtGroup

Because the MIB walk/touch does not persist through a controller reboot, you must add a cronjob on the AWMS server to ensure continue statistical population.

Ensuring Master Controller Pushes Config to Local Controllers Utilizing Dell PowerConnect ArubaOS CLI

This command ensures configuration changes made on the master controller will propagate to all local controllers.

Note : Do not use these commands if using the Dell PowerConnect W AWMS WebUI.

```
(Controller-Name) (config) # cfgm mms config disable
(Controller-Name) (config) # write mem
Saving Configuration...
Saved Configuration
```

Disable Debugging Utilizing Dell PowerConnect ArubaOS CLI

If you are experiencing performance issues on the Master Controller, you want to ensure debugging is disabled. It should be disabled by default. Debugging coupled with gathering the enhanced statistics can put a strain on the controllers 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
Saving Configuration...
Saved Configuration
```

Restart WMS on Local Controllers Utilizing Dell PowerConnect ArubaOS CLI

To ensure local controllers are populating rogue information properly, SSH into 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
```

Note : You will need to wait until the next Rogue Poll Period on execute a "Poll Now" for each local controller to see rogue devices begin to appear in AWMS after doing a "restart wms" in Dell PowerConnect W.

Copy & Paste to Enable Proper Traps Utilizing Dell PowerConnect ArubaOS CLI

To ensure the proper traps are configured on Dell PowerConnect W controllers copy and paste the following command after entering "enable" mode and issuing the "configure terminal command":

Copy and Paste the Text Below

```
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
```

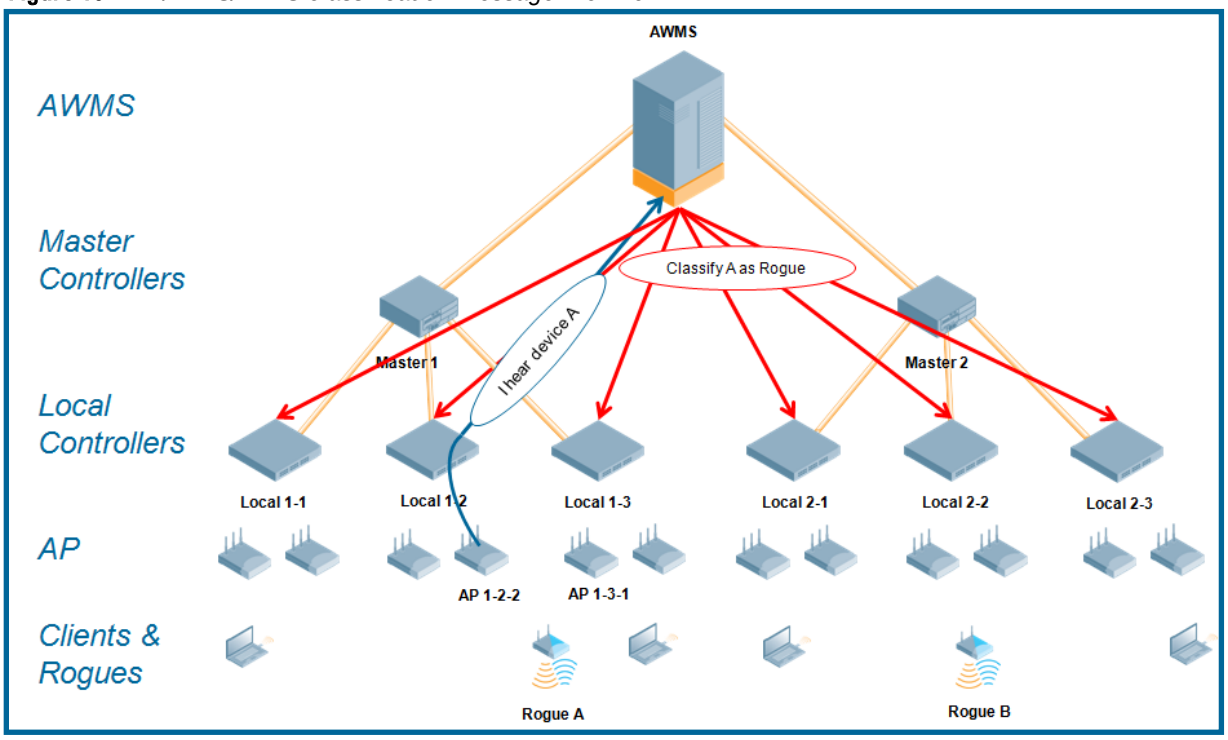
```
snmp-server trap enable wlsxFrameRetryRateExceeded
snmp-server trap enable wlsxFrameReceiveErrorRateExceeded
snmp-server trap enable wlsxFrameFragmentationRateExceeded
snmp-server trap enable wlsxFrameBandWidthRateExceeded
snmp-server trap enable wlsxFrameLowSpeedRateExceeded
snmp-server trap enable 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 to save your changes

Appendix B – WMS Offload Details

WMS offload instructs the Master controller to stop correlating ARM, WIPS, and WIDS state information amongst its Local controllers, because AWMS will assume this responsibility. Figure 4 below depicts how Dell PowerConnect W AMWS communicates state information with Local controllers.

Figure 19 *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 the AWMS
3. AWMS receives message and re-classifies the device if necessary and reflects this within AWMS GUI and via SNMP traps, if configured.
4. AWMS sends a classification message back to all Local controllers managed by Master controller 1, (1-1, 1-2, and 1-3)
5. AWMS sends a classification message back to all additional Local controllers managed by the AMWS 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 AWMS user manually overrides the classification, then AWMS will send a re-classification message to all applicable local controllers.
7. AWMS periodically polls each Local controller's MIB to ensure state parity with AWMS' database. If the Local controller's device state does not comply with AWMS' database, AWMS will send a re-classification message to bring it back into compliance.

Important notes:

- Customers upgrading to AWMS 6.2 or later will have all their rogue devices set to a default controller classification of "unclassified". Customers will need to classify these devices manually from the AWMS UI. AWMS updates the classification of a rogue device based on SNMP polling only if the controller classification defined on AWMS is set to "unclassified".
- The **Rogue Detail Page** displays a BSSID table for each rogue that displays the desired classification and the classification on the device.

Benefits of using AWMS as Master Device State Manager:

- Ability to correlate state amongst 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 3rd party access points with ARM. This will ensure Dell infrastructure interoperates more efficient in a mixed infrastructure environment.
- Ability to better classify devices based on AWMS wire-line information not currently available in Dell PowerConnect ArubaOS.
- AWMS provides a near real-time event notification and classification of new devices entering air space.
- RAPIDS gains additional wire-line discovery data from Dell PowerConnect W controllers.

Appendix C – Converting from MMS to Dell PowerConnect W AWMS

The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into MMS or Dell PowerConnect W into Dell PowerConnect W AWMS.

Pre conversion checklist

- The conversion tool is only supported for **IE6** and later.
- Ensure you increase VisualRF memory prior to beginning the MMS export option. Navigate to **VisualRF > Setup** and use the pull-down menu for Memory Allocation

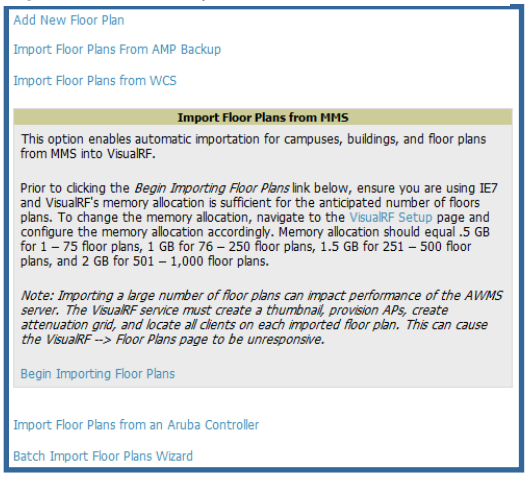
Number of Floor Plans	Memory in GB
1 – 75	.5
76 – 250	1
251 – 500	1.5
501 – 1,000	2

Migrating Floor Plans from MMS to AWMS

Process

- Navigate to VisualRF > Import Page
- Select the "Import floor plans from MMS" link
- Detailed instructions will appear on the screen
- Select the "Begin Importing Floor Plans" link

Figure 20 *MMS Export Instructions*

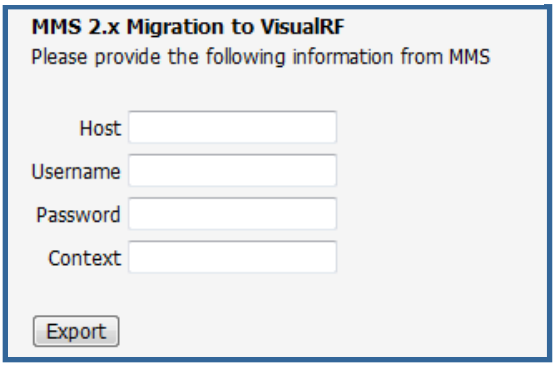


Input the following information:

- Host – enter the hostname or IP address of the MMS server
- Username – enter the MMS administrative user account.

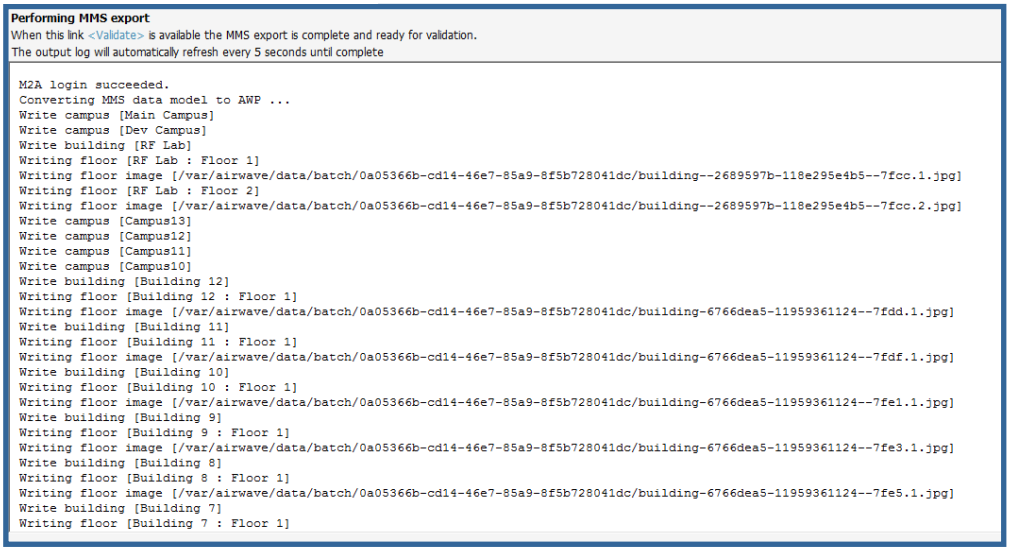
- Password
- Context (optional) – leave this blank unless you have enabled context on you MMS. Most customers do not utilize context. If you are using context, then you will have to enter a different user for each context defined within MMS.

Figure 21 *MMS Export to AWMS window*



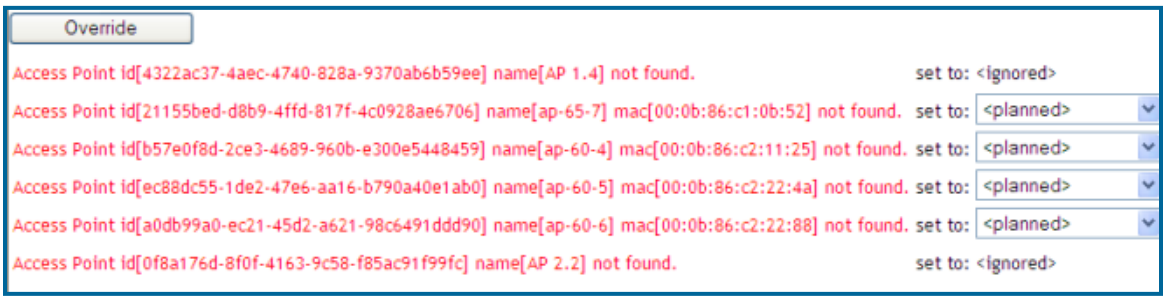
- Click on the "Export" button and the program will automatically redirect to the page below detailing the status of the export.

Figure 22 *MMS export status*



- Once the exportation process is complete the <Validate> tag will change to a clickable link.
- Click the "Validate" link to validate the XML exported from MMS. This will automatically redirect you to the Bulk Importation Wizard to import the exported floor plans into AWMS.
- If APs in the XML that are not in AWMS, the following screen will be displayed. Set the APs to be ignored or identify them as planned, and click the "Override" button to continue.

Figure 23 *Override options*



- If there are no new APs, click the “Next” button to complete the process.

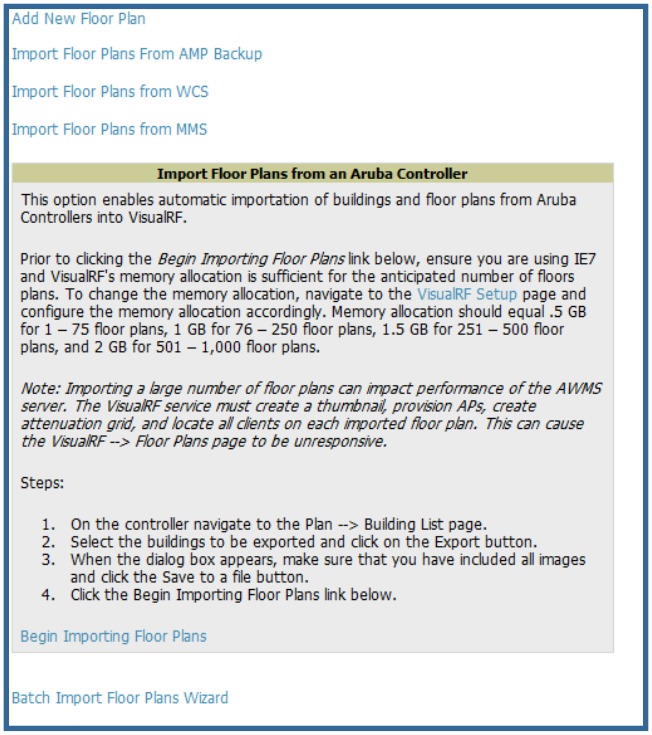
Importing a large number of floor plans can impact performance on the AMWS server; once the batch process is initiated, it can take up to 30 minutes to complete the import process. The VisualRF service must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. The can cause the **VisualRF > Floor Plans** page to be unresponsive.

Migrating Floor Plans from Dell PowerConnect ArubaOS (Controller) to AWMS

Process on Dell PowerConnect W Controller

- Login into the Dell PowerConnect W controller’s Web UI
- Navigate to the **Plan > Building List** page.
- Select the buildings to be exported and click on the “Export” button.
- When the dialog box appears, make sure that you have included all images and click the “Save to a file” button.

Figure 24 *Import Floor Plans from a Dell PowerConnect ArubaOS (Controller)*

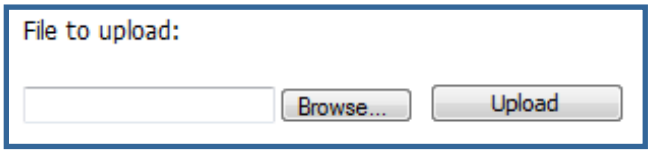


Process to Import within AWMS

- Navigate to **VisualRF > Import** page
- Select the “Import floor plans from an Dell PowerConnect W Controller ” link
- A detailed set of directions will appear.
- Click on the “Begin Importing Floor Plans” link at the bottom of the instructions and it will automatically redirect to the file upload explorer.

- Browse for the file that was saved during the controller export process above.
- Click the "Upload" button to validate the XML exported from the controller.
- If there are errors in the XML you will see errors on screen.

Figure 25 *File Upload Explorer*



Importing a large number of floor plans can impact performance on the AMWS server. The VisualRF service must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. The can cause the **VisualRF > Floor Plans** page to be unresponsive.

Migrating Floor Plans from RF Plan to AWMS

Process with RF Plan

- Navigate to the **File > Export** page.
- From Export drop down select "**Controller WebUI Format 3.0**" or "**VisualRF Format**"
- Within the dialog box, name the export file
- From the Campus Building tree, select the Campuses and Buildings you want to export
- Click the **Next** button

Process to Import within AWMS

- Navigate to **VisualRF > Import** page
- Select the "Import floor plans from an RF Plan " link
- A detailed set of directions will appear.
- Click on the "Begin Importing Floor Plans" link at the bottom of the instructions and it will automatically redirect to the file upload explorer.
- Browse for the file that was saved during the RF Plan export process above.
- Click the "Upload" button to validate the XML exported from the controller.
- If there are errors in the XML you will see errors on screen.

Appendix D – Increasing Location Accuracy

Understand Band Steering's Impact on Location

Band steering can negatively impact location accuracy when testing in highly mobile environment. The biggest hurdle is scanning times in 5 GHz frequency

Operating Frequency	Total Channels	Scanninn 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

Overview

This section provides instructions for integrating the AWMS, Dell WLAN infrastructure and Dell's RTLS feed for more accurately locating wireless clients and WiFi Tags.

Minimum Requirements

- AWMS version 7.0 or higher
- Dell PowerConnect ArubaOS (AOS) 6.x or higher

Deployment Topology

Figure 26 *Typical Client Location*

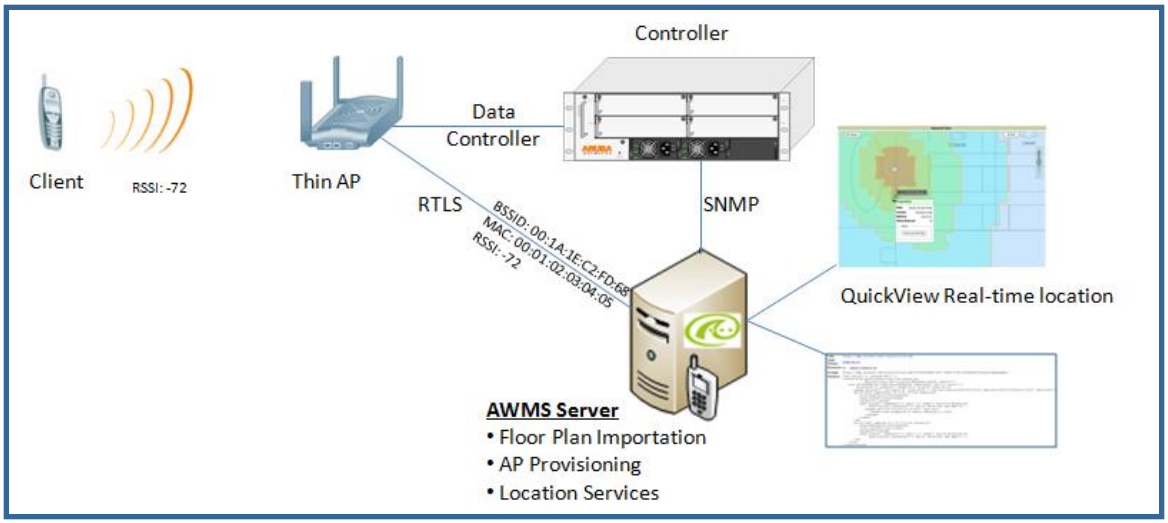
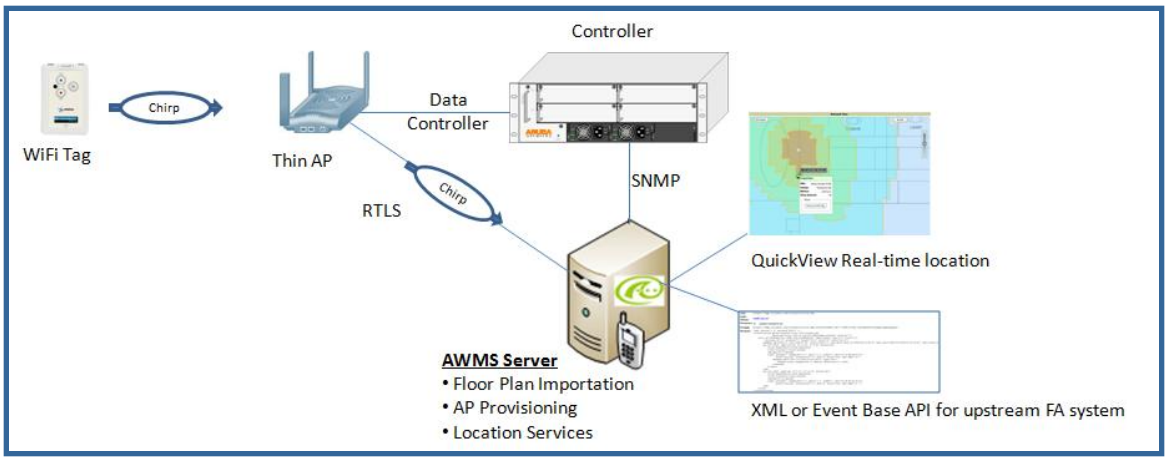


Figure 27 *Typical Tag Deployment*



Prerequisites

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

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

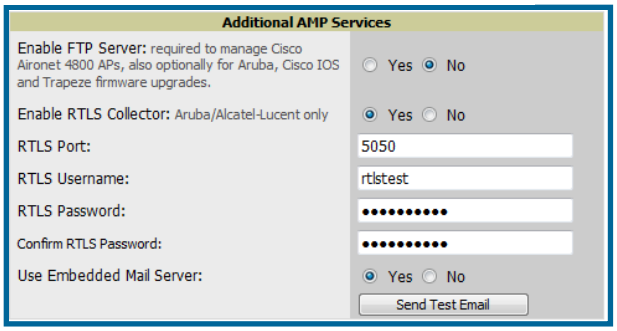
Known Issues

Aruba OS	Dell PowerConnect W AWMS	Description	Resolution
3.x	7.x	Wi-Fi Tags will only display in VisualRF. Wi-Fi Tags will not display within AWMS' UI or the controller's UI.	AWMS 7.1

Enable RTLS service on the AWMS server

- Navigate to **AMP Setup > General** page
- Locate the **AMP Additional Services** section
- Select "Yes" to Enable RTLS Collector

Figure 28 *RTLS Setup*



- A new section will automatically appear with the following settings
  - RTLS Port – match controller default is 5050
  - RTLS Username – match the SNMPv3 "MMS" username configured on controller
  - RTLS Password – match the SNMPv3 "MMS" password configured on controller
- Click **Save** at the bottom of the page.

Enable RTLS on 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 <PROFILE USED BY THIN APs>
(Controller-Name) (AP system profile "default") # rtls-server ip-addr <IP OF AWMS SERVER> port 5050 key <SNMPv3 "MMS" PASSWORD CONFIGURED ON CONTROLLER>
(Controller-Name) (AP system profile "default") # write mem
Saving Configuration...
Saved Configuration
```

- To validate exit configuration mode

```
(Controller-Name) # show ap monitor debug status ip-addr <IP ADDRESS OF ANY THIN ACCESS POINTS>
...
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         *
```

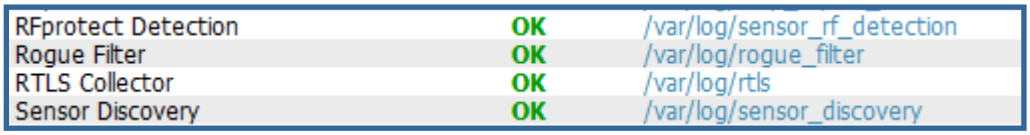
TroubleShooting RTLS

- Ensure the RTLS service is running on your AWMS server. SSH into your AWMS server.

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

or navigate to System > Status page and look for the RTLS service

Figure 26 *RTLS Service Status*



- Check the RTLS log file to ensure Tag chirps are making it to the AWMS server. SSH into your AWMS server.

```
[root@AWMSServer]# logs
[root@AWMSServer]# tail rtls

payload:
00147aaf01000020001a1ec02b320000001000000137aae0100000c001a1ec02b3
20000001a1e82b322590006ddff02

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:
0014c9c90100003c001a1ec0507800000000200000013c9c70100000c001a1ec0507
80000000d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb
8ae9a9000006c4ff02

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:
0014c9c90100003c001a1ec0507800000000200000013c9c70100000c001a1ec0507
80000000d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb
8ae9a9000006c4ff02
```

- Ensure chirps are published to Airbus by snooping on proper topics

```
[root@AWMS server]# 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://<AWMS 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 tags can be heard by at least 3 access points from any given location. The recommended is 4 for best results.
- Ensure tags chirp on all regulatory channels.

Component	Description
Autonomous AP	Standalone device which performs radio and authentication functions
Thin AP	Radio-only device coupled with WLAN Controller to perform authentication
WLAN Controller	Used in conjunction with thin APs to coordinate authentication and roaming
NMS	Network Management Systems and Event Correlation (OpenView, Tivoli, and so forth)
RADIUS Auth.	RADIUS Authentication servers (Funk, FreeRADIUS, ACS, or IAS)
RADIUS Accounting	AWMS itself serves as a RADIUS accounting client
Wireless Gateways	Provide HTML redirect and/or wireless VPNs
TACACS+	Used to authenticated AWMS administrative users
Routers/Switches	Provide AWMS with data for user information and AP and Rogue discovery
Help Desk Systems	Remedy EPICOR
Rogue APs	Unauthorized APs not registered in the AWMS database of managed APs