

OmniVista 3600 Air Manager 8.2



Copyright

© 2016 Alcatel-Lucent. All rights reserved.

Specifications in this manual are subject to change without notice.

Originated in the USA.

AOS-W, Alcatel 4302, Alcatel 4304, Alcatel 4306, Alcatel 4308, Alcatel 4324, Alcatel 4504, Alcatel 4604, Alcatel 4704, Alcatel 6000, OAW-AP41, OAW-AP68, OAW-AP60/61/65, OAW-AP70, OAW-AP80, OAW-AP92/93, OAW-AP105, OAW-AP120/121, OAW-AP124/125, OAW-AP175, OAW-IAP92/93/105, OAW-RAP2, OAW-RAP5, and Omnivista 3600 Air Manager are trademarks of Alcatel-Lucent in the United States and certain other countries.

Any other trademarks appearing in this manual are the property of their respective companies. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al.

Overview	5
Understanding Alcatel-Lucent Topology	5
Prerequisites for Integrating Alcatel-Lucent Infrastructure	5
Configuring OV3600 for Global Alcatel-Lucent Infrastructure	7
Disabling Rate Limiting in OV3600 Setup > General	7
Entering Credentials in Device Setup > Communication	7
Setting Up Recommended Timeout and Retries	9
Setting Up Time Synchronization	9
Manually Setting the Clock on a switch	9
Enabling Support for Channel Utilization And Statistics	9
OV3600 Setup	9
switch Setup (Master And Local)	10
Configuring an Alcatel-Lucent Group in OV3600	11
Basic Monitoring Configuration	11
Advanced Configuration	12
Discovering Alcatel-Lucent Infrastructure	13
Discovering or Adding Master switches	13
Local switch Discovery	15
Thin AP Discovery	15
OV3600 and Alcatel-Lucent Integration Strategies	17
Integration Goals	17
Example Use Cases	18
When to Use Enable Stats	18
When to Use WMS Offload	18
When to Use RTLS	18
When to Define OV3600 as a Trap Host	19
When to Use Channel Utilization	19
Prerequisites for Integration	19
Enable switch Statistics Using OV3600	19
WMS Offload with OV3600	20
Define OV3600 as a Trap Host Using the AOS-W CLI	21
Ensuring That IDS and Auth Traps Display in OV3600	21
Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure	23
Alcatel-Lucent Specific Capabilities in OV3600	25
Alcatel-Lucent Traps for RADIUS Auth and IDS Tracking	25
Remote AP Monitoring	26
ARM and Channel Utilization Information	27
VisualRF and Channel Utilization	28
Configuring Channel Utilization Triggers	30
Viewing Channel Utilization Alerts	30
View Channel Utilization in RF Health Reports	31
Viewing switch License Information	32
Rogue Device Classification	32
Rules-Based Controller Classification	35
Using RAPIDS Defaults for Controller Classification	35

Changing RAPIDS Based on switch Classification	35
Appendix A AOS-W and OV3600 CLI Commands	37
Enable Channel Utilization Events	37
Enable Stats With the AOS-W CLI	37
Offload WMS Using the AOS-W or OV3600 CLI	37
AOS-W CLI	37
OV3600 SNMP	38
Pushing Configs from Master to Local switches	38
Disable Debugging Utilizing the AOS-W CLI	38
Restart WMS on Local switches	39
Configure AOS-W CLI when not Offloading WMS	39
Copy and Paste to Enable Proper Traps with the AOS-W CLI	39
Appendix B OV3600 Data Acquisition Methods	43
Appendix C WMS Offload Details	46
State Correlation Process	46
Using OV3600 as a Master Device State Manager	47
Appendix D Increasing Location Accuracy	48
Understand Band Steering's Impact on Location	48
Leveraging RTLS to Increase Accuracy	48
Deployment Topology	48
Prerequisites	49
Enable RTLS Service on the OV3600 Server	49
Enable RTLS on the switch	50
Troubleshooting RTLS	51
Using the WebUI to See Status	51
Using the CLI	51
Wi-Fi Tag Setup Guidelines	52

This document provides best practices for leveraging OmniVista 3600 Air Manager to monitor and manage your Alcatel-Lucent 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 Alcatel-Lucent infrastructure.

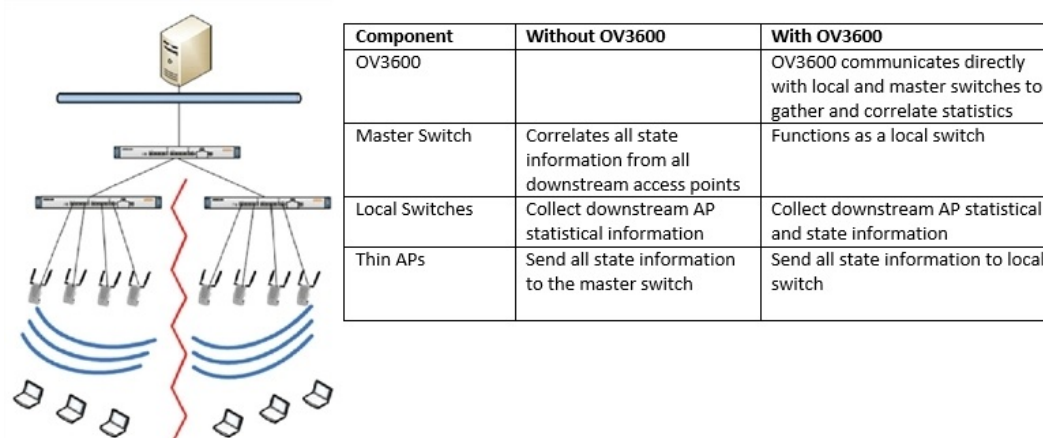
This overview chapter contains the following topics:

- "Understanding Alcatel-Lucent Topology" on page 5
- "Prerequisites for Integrating Alcatel-Lucent Infrastructure" on page 5

Understanding Alcatel-Lucent Topology

Figure 1 depicts a typical master-local deployment for OmniVista 3600 Air Manager:

Figure 1: Typical Alcatel-Lucent Deployment



There should never be a local switch managed by an OV3600 server whose master switch is also not under management.

Prerequisites for Integrating Alcatel-Lucent Infrastructure

You will need the following information to monitor and manage your Alcatel-Lucent infrastructure:

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



Without proper Telnet/SSH credentials, OV3600 will not be able to acquire license and serial information from switches.

- SNMPv3 credentials are required for Wireless LAN Management System (WMS) Offload:
 - Username

- Auth password
- Privacy password
- Auth protocol

This section explains how to configure OV3600 to globally manage your Alcatel-Lucent infrastructure.

- "Disabling Rate Limiting in OV3600 Setup > General" on page 7
- "Entering Credentials in Device Setup > Communication" on page 7
- "Setting Up Recommended Timeout and Retries" on page 9
- "Setting Up Time Synchronization" on page 9
- "Enabling Support for Channel Utilization And Statistics" on page 9

Disabling Rate Limiting in OV3600 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 OV3600, follow these steps:

1. Navigate to **OV3600 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 OV3600 Setup > General > Performance*

Performance	
Monitoring Processes (1-64):	<input type="text" value="2"/>
Maximum number of configuration processes (1-80):	<input type="text" value="5"/>
Maximum number of audit processes (1-80):	<input type="text" value="3"/>
SNMP Fetcher Count (2-6):	<input type="text" value="2"/>
Verbose logging of SNMP configuration:	<input type="radio"/> Yes <input checked="" type="radio"/> No
SNMP rate limiting for monitored devices:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Client Association Relevance Factor (0-550 days, zero disables):	<input type="text" value="0"/>
RAPIDS Processing Priority: <small>When OV3600 is processing data at or near its maximum capacity, reducing the priority of RAPIDS can ensure that processing of other data (e.g. client connections and bandwidth) is not adversely impacted.</small>	<input type="text" value="Low"/>
<small>The default priority is Low. You can also tune your system performance by changing group poll periods.</small>	

Entering Credentials in Device Setup > Communication

OV3600 requires several credentials to properly interface with Alcatel-Lucent 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 **Alcatel-Lucent**. The page illustrated in [Figure 3](#) appears.

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



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

Figure 3: Credentials in Device Setup > Communication

The screenshot shows the configuration page for an Alcatel-Lucent device. The title bar reads "Alcatel-Lucent". The form contains the following fields and values:

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

At the bottom of the form are two buttons: "Save" (blue) and "Cancel" (orange).

4. Enter the required information for configuration and basic monitoring:

- Telnet/SSH username
- Telnet/SSH password
- Enable mode password

5. Enter the required data for WMS Offload:

- SNMPv3 username
- Authentication password
- SNMPv3 authentication protocol (must be **SHA-1**)
- Privacy password
- SNMPv3 privacy protocol (must be **DES**)



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

6. Click **Save**.

Setting Up Recommended Timeout and Retries

1. In the **Device Setup > Communication** page, locate the **SNMP Setting** section.
2. Change the **SNMP Timeout** setting to a value of either **3**, **4**, or **5**. This is the number of seconds that OV3600 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 OV3600 tries to poll a device when it does not receive a response within the SNMP Timeout Period or the Group's Missed SNMP Poll Threshold setting (1-100).



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

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

SNMP Settings	
SNMP Timeout (3-60 sec):	<input type="text" value="3"/>
SNMP Retries (1-40):	<input type="text" value="3"/>

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

Setting Up Time Synchronization

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

Manually Setting the Clock on a switch

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

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

Enabling Support for Channel Utilization And Statistics

To enable support for channel utilization statistics, your OV3600 server and Alcatel-Lucent AOS-W and Alcatel-Lucent Instant devices must be running the following versions of software:

- OmniVista 3600 Air Manager 7.6 or later
- Alcatel-Lucent AOS-W 6.0.1 or later
- Alcatel-Lucent Instant 3.3 or later



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

OV3600 Setup

1. Navigate to **OV3600 Setup > General**.

- In the **Additional OV3600 Services** section, set **Enable AMON Data Collection** to **Yes**, and set **Prefer AMON vs SNMP Polling** to **Yes**.
- Click **Save**.

Figure 5: AMON Data Collection Setting in OV3600 Setup > General

Additional OV3600 Services	
Enable FTP server: <small>required to manage Alcatel-Lucent AirMesh & Cisco 4800 APs; optional for firmware upgrades on supported devices.</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable RTLS collector: <small>Aruba/Alcatel-Lucent only</small>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Embedded Mail Server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Mail Relay Server: <small>Optional</small>	<input type="text" value="Enter a Value"/>
	<input type="button" value="Send Test Email"/>
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AMON Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Clarity Data Collection: <small>Requires AOS-W Version 6.4.3 and Above</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AppRF Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
AppRF Storage Allocated (GiB): <small>Greater than or equal to 2 GiB</small>	<input type="text" value="25"/>
Enable UCC Data Collection: <small>Requires AOS-W Version 6.4 and Above</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UCC Calls Stitching (Heuristics):	<input checked="" type="radio"/> Yes <input type="radio"/> No
Prefer AMON vs SNMP Polling:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Syslog and SNMP Trap Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Require SSH host key verification:	<input type="radio"/> Yes <input checked="" type="radio"/> No

switch Setup (Master And Local)



CAUTION

Enabling these commands on AOS-W versions prior to 6.0.1.0 can result in performance issues on the switch. If you are running previous firmware versions such as AOS-W 6.0.0.0, you should upgrade to AOS-W 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-W versions 6.3.1 and later. To get the commands for other versions of AOS-W, refer to the *Command-Line Interface Reference Guide* for that version.

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

```
(switch-Name) # configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(switch-Name) (config) # mgmt-server type ov3600 primary-server <OV3600-IP>
(switch-Name) (config) # mgmt-server profile <profile-name>
(switch-Name) (config) # write mem
```



NOTE

You can add up to four <OV3600-IP> addresses.

It is prudent to establish one or more Alcatel-Lucent Groups within OV3600. During the discovery process you will move new discovered switches 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 Alcatel-Lucent 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 Alcatel-Lucent-specific settings.
 - a. Find the **SNMP Polling Periods** section of the page, as illustrated in [Figure 6](#).
 - b. Verify that the **Override Polling Period for Other Services** option is set to **Yes**.
 - c. Verify that **Client Data Polling Period** is set to 10 minutes. Do not configure this interval lower than 5 minutes.



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

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

Figure 6: SNMP Polling Periods section of Groups > Basic

SNMP Polling Periods	
Up/Down Status Polling Period:	5 minutes ▾
Override Polling Period for Other Services:	<input type="radio"/> Yes <input checked="" type="radio"/> No
AP Interface Polling Period:	10 minutes ▾
Client Data Polling Period:	10 minutes ▾
Thin AP Discovery Polling Period:	15 minutes ▾
Device-to-Device Link Polling Period:	5 minutes ▾
802.11 Counters Polling Period:	15 minutes ▾
Rogue AP and Device Location Data Polling Period:	30 minutes ▾
CDP Neighbor Data Polling Period:	30 minutes ▾
Mesh Discovery Polling Period:	15 minutes ▾

5. Locate the Aruba/Alcatel-Lucent section of this page. See [Figure 7](#).
6. Configure the proper **SNMP Version** for monitoring the Alcatel-Lucent infrastructure.

Figure 7: Group SNMP Version for Monitoring

Aruba / Alcatel-Lucent	
SNMP Version:	2c ▾
Offload WMS Database:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Aruba GUI Config:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Manage local configuration on controllers: <small>This option enables/disables the management of local configuration including audit, push and import operations</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Ignore Rogues Discovered by Remote APs:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Delete Certificates On Controller:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Archive Controller/Switch Backups:	<input checked="" type="radio"/> Yes <input type="radio"/> No

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

Advanced Configuration

Refer to the *OmniVista 3600 Air Manager 8.2 Controller Configuration Guide* for detailed instructions.

OV3600 utilizes the Alcatel-Lucent topology to efficiently discover downstream infrastructure. This section guides you through the process of discovering and managing your Alcatel-Lucent device infrastructure.

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

- "Configuring OV3600 for Global Alcatel-Lucent Infrastructure" on page 7
- "Configuring an Alcatel-Lucent Group in OV3600" on page 11

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

- "Discovering or Adding Master switches" on page 13
- "Local switch Discovery" on page 15
- "Thin AP Discovery" on page 15



Always add one switch 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 OV3600 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 switches

Scan networks containing Alcatel-Lucent master switches from the **Device Setup > Discover** page, or manually enter the master switch by following these steps in the **Device Setup > Add** page:

1. Select the **Alcatel-Lucent** OmniSwitch type and select **Add**. The page illustrated on [Figure 8](#) appears.
2. Enter the **Name** and the **IP Address** for the switch.
3. Enter **SNMP Community String**, which is required field for device discovery.



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

Figure 8: Alcatel-Lucent Credentials in Device Setup > Add

Configure default credentials on the [Communication](#) page.

Device Communications	
Name: <small>Leave name blank to read it from device</small>	<input type="text" value="Enter a Value"/>
IP Address:	<input type="text" value="Enter a Value"/>
SNMP Port:	<input type="text" value="161"/>
SSH Port:	<input type="text" value="22"/>
Community String:	<input type="password" value="....."/>
Confirm Community String:	<input type="password" value="....."/>
SNMPv3 Username:	<input type="text" value="Enter a Value"/>
Auth Password:	<input type="password"/>
Confirm Auth Password:	<input type="password"/>
SNMPv3 Auth Protocol:	<input type="text" value="SHA-1"/>
Privacy Password:	<input type="password"/>
Confirm Privacy Password:	<input type="password"/>
SNMPv3 Privacy Protocol:	<input type="text" value="DES"/>
Telnet/SSH Username:	<input type="text" value="admin"/>
Telnet/SSH Password:	<input type="password" value="....."/>
Confirm Telnet/SSH Password:	<input type="password" value="....."/>
"enable" Password:	<input type="password" value="....."/>
Confirm "enable" Password:	<input type="password" value="....."/>

Location	
Group:	<input type="text" value="APs"/>
Folder:	<input type="text" value="Top"/>

Update group settings based on this device's current configuration

Monitor Only (no changes will be made to device)

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

4. Enter the required fields for configuration and basic monitoring:

- Telnet/SSH Username
- Telnet/SSH password
- enable password

5. Enter the required fields for WMS Offload

- SNMPv3 Authentication Protocol (must be **SHA-1**)
- SNMPv3 Privacy Protocol (must be **DES**)
- SNMPv3 Username
- Authentication Password
- Privacy Password



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



If you are using SNMPv3, and the switch's date/time is incorrect, the SNMP agent will not respond to SNMP requests from the OV3600 SNMP manager. This will result in the switch and all of its downstream access points showing as Down in OV3600.

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



If you select Manage read/write, OV3600 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 Alcatel-Lucent master switch you just added from the list of new devices.
11. Ensure **Monitor Only** option is selected.
12. Select **Add**.

Local switch Discovery

Local switches are added to OV3600 via the master switch 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 switches will appear on the **APs/Devices > New** page.

Add the local switch to the Group defined previously. Within OV3600, local switches can be split away from the master switch's Group.



Local switch Discovery/monitoring may not work as expected if OV3600 is unable to communicate directly with the target device. Be sure and update any ACL/Firewall rules to allow OV3600 to communicate with your network equipment.

Thin AP Discovery

Thin APs are discovered via the local switch. 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 OV3600, thin APs can be split away from the switch's Group. You can split thin APs into multiple Groups if required.

This section describes strategies for integrating OV3600 and Alcatel-Lucent devices and contains the following topics:

- "Integration Goals" on page 17
- "Example Use Cases" on page 18
- "Prerequisites for Integration" on page 19
- "Enable switch Statistics Using OV3600" on page 19
- "WMS Offload with OV3600" on page 20
- "Define OV3600 as a Trap Host Using the AOS-W CLI" on page 21
- "Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure" on page 23

Integration Goals

Table 1 summarizes the types of integration goals and strategies for meeting them in certain architectural contexts:

Table 1: *Integration Goals in All Masters or Master/Local Architectures*

Integration Goals	All Masters Architecture	Master/Local Architecture
Rogue And Client Info		enable stats
Rogue containment only	ssh access to switches	ssh access to switches
Rogue And Client containment	WMS Offload	WMS Offload
Reduce Master switch Load		WMS Offload debugging off
IDS And Auth Tracking	Define OV3600 as a trap host	Define OV3600 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 Visibility	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 switch's web interface.
- WMS Offload encompasses enable stats or enable stats is a subset of WMS Offload.
- Unless you enable stats on the local switches in a master/local environment, the local switches 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 switch.

Example Use Cases

The following are example use cases of integration strategies:

- ["When to Use Enable Stats" on page 18](#)
- ["When to Use WMS Offload" on page 18](#)
- ["When to Use RTLS" on page 18](#)
- ["When to Define OV3600 as a Trap Host" on page 19](#)
- ["When to Use Channel Utilization" on page 19](#)

When to Use Enable Stats

You want to pilot OV3600, and you do not want to make major configuration changes to their infrastructure or manage configuration from OV3600.



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

See ["Enable switch Statistics Using OV3600" on page 19](#).

When to Use WMS Offload

- You have older Alcatel-Lucent infrastructure in a master/local environment and the master switch is fully taxed. Offloading WMS will increase the capacity of the master switch by offloading statistics gathering requirements and device classification coordination to OV3600.
- You want to use OV3600 to distribute client and rogue device classification amongst multiple master switches in a master/local environment or in an All-Masters environment.
- See the following topics:
 - ["WMS Offload with OV3600" on page 20](#)
 - ["Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure" on page 23](#)
 - ["WMS Offload Details" on page 46](#)

When to Use RTLS

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



RTLS can negatively impact your OV3600 server's performance.

- See ["Leveraging RTLS to Increase Accuracy" on page 48](#).

When to Define OV3600 as a Trap Host

- You want to track IDS events within the OV3600 UI.
- You are in the process of converting their older third-party WLAN devices to Alcatel-Lucent 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 switch. OV3600 provides this unique correlation capability.

See ["Define OV3600 as a Trap Host Using the AOS-W CLI"](#) on page 21.

When to Use Channel Utilization

- You have a minimum version of AOS-W 6.1.0.0.

Prerequisites for Integration

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

- ["Configuring OV3600 for Global Alcatel-Lucent Infrastructure"](#) on page 7
- ["Configuring an Alcatel-Lucent Group in OV3600"](#) on page 11
- ["Discovering Alcatel-Lucent Infrastructure"](#) on page 13

Enable switch Statistics Using OV3600

To enable stats on the Alcatel-Lucent switches, follow these steps:

1. Navigate to **OV3600 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 **OV3600 Setup > General**

Device Configuration	
Guest User Configuration:	Enabled for device <input type="button" value="v"/>
Allow WMS Offload configuration in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Allow disconnecting users while in monitor-only mode:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Global Alcatel Lucent Configuration: <small>Changing this setting may require importing configuration on your devices.</small>	<input type="radio"/> Yes <input checked="" type="radio"/> No

3. Navigate to **Groups > Basic** for the group that contains your Alcatel-Lucent switches.
4. Locate the Alcatel-Lucent section on the page.
5. Set the **Offload WMS Database** field to **No**, as shown in [Figure 10](#):

Figure 10: Offload WMS Database field in Groups > Basic

Aruba / Alcatel-Lucent	
SNMP Version:	<input type="text" value="2c"/>
Offload WMS Database:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Aruba GUI Config:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Manage local configuration on controllers: <small>This option enables/disables the management of local configuration including audit, push and import operations</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Ignore Rogues Discovered by Remote APs:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Delete Certificates On Controller:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Archive Controller/Switch Backups:	<input checked="" type="radio"/> Yes <input type="radio"/> No

6. Select **Save and Apply**.

7. Select **Save**.

This will push a set of commands via SSH to all Alcatel-Lucent local switches. OV3600 must have read/write access to the switches in order to push these commands.



This process will not reboot your switches.



If you do not follow the above steps, local switches will not be configured to populate statistics. This decreases OV3600's capability to trend client signal information and to properly locate devices. See "AOS-W CLI" on page 37 for information about how to utilize the AOS-W CLI to enable stats on Alcatel-Lucent infrastructure.

If your credentials are invalid or the changes are not applied to the switch, error messages will display on the switch's **APs/Devices > Monitor** page under the **Recent Events** section. If the change fails, OV3600 does not audit these setting (display mismatches) and you will need to apply to the switch by hand. See "AOS-W CLI" on page 37 for detailed instructions.

These are the commands pushed by OV3600 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 OV3600

To offload WMS on the Alcatel-Lucent switches using OV3600:

1. In **OV3600 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 Alcatel-Lucent master switches. If the switch does not have an SNMPv3 user that matches the OV3600 database it will automatically create a new SNMPv3 user. OV3600 must have read/write access to the switches to push these commands
3. Navigate to **Groups > Basic** and locate the **Alcatel-Lucent** section.
4. Set the **Offload WMS Database** field to **Yes**.



This process will not reboot your switches. See ["AOS-W and OV3600 CLI Commands"](#) on page 37 for information on how to utilize the AOS-W 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 OV3600 while enabling WMS Offload.

```
configure terminal
mobility-manager <OV3600 IP> user <OV3600 SNMPv3 User Name> <OV3600 Auth/Priv PW>
stats-update-interval 120
write mem
```



OV3600 will configure SNMPv2 traps with the **mobile manager** command.

Define OV3600 as a Trap Host Using the AOS-W CLI

To ensure the OV3600 server is defined as a trap host, access the command line interface of each switch (master and local), enter enable mode, and issue the following commands:

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

```
(switch-Name) (config) # snmp-server host <OV3600 IP ADDR> version 2c <SNMP Community String of switch>
```



Ensure the SNMP community matches those that were configured in ["Configuring OV3600 for Global Alcatel-Lucent Infrastructure"](#) on page 7.

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



OV3600 supports SNMP v2 traps and SNMP v3 informs in AOS-W 3.4 and higher. SNMP v3 traps are not supported.

Ensuring That IDS and Auth Traps Display in OV3600

Validate your AOS-W configuration by exiting the configure terminal mode and issue the following command:

```
(switch-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:

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



See "AOS-W CLI" on page 37 for the full command that can be copied and pasted directly into the AOS-W CLI.

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

Ensure the source IP of the traps match the IP that OV3600 uses to manage the switch, 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

Device Info					
Status: Up (OK)					
Configuration: Good					
Firmware:	6.4.4.3	Licenses			
Upstream Device:	-	Upstream Port:	-		
Controller Role:	Master				
Type:	Aruba 7220	Last Contacted:	1/22/2016 12:33 PM PST	Uptime:	33 days 12 hrs 27 mins
LAN MAC Address:	00:1A:1E:00:0E:28	Serial:	BB0000118		
Location:	1344-1 Rack 28	Contact:	-		
IP Address:	10.11.0.11	APs:	38	Clients:	115
VPN Sessions:	0	VPN Usage:	-		
Quick Links:	Open controller web UI...	Run command...			
Notes:					

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

```
(switch-Name) # show snmp community
```

```
SNMP COMMUNITIES
```

```
-----
```

```
COMMUNITY ACCESS      VERSION
```

```
-----
```

```
public      READ_ONLY V1, V2c
```

```
(switch-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 OV3600 and the switch.

Validate that traps are making it into OV3600 by issuing the following commands from OV3600 command line.

```
[root@OV3600 ~]# qlog enable snmp_traps
```

```
[root@OV3600 ~]# tail -f /var/log/ov3600_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: Alcatel-Lucent-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: Alcatel-Lucent-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
```



You will see many IDS and Auth Traps from this command. OV3600 only processes a small subset of these traps which display within OV3600. The traps that OV3600 does process are listed above.

We recommend that you disable qlogging after testing. Leaving it turned on can negatively impact OV3600 performance:

```
[root@OV3600 ~]# qlog enable snmp_traps
```

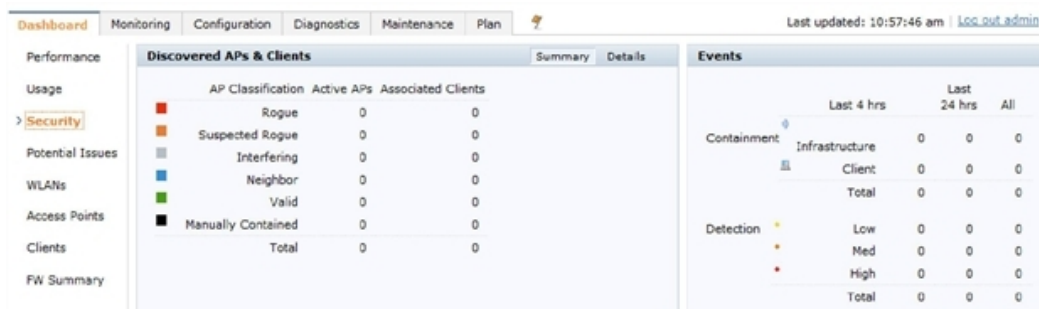
Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure

When offloading WMS, it is important to understand what functionality is migrated to OV3600 and what functionality is deprecated.

The following AOS-W 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-W and imported them into OV3600. All functionality within the Plan Tab is incorporated with the VisualRF module in OV3600.
- **Dashboard > Security Summary** - The **Security Summary** section (Figure 12) disappears after offloading WMS. The data is still being processed by the master switch, but the summary information is not available. You must use OV3600 to view data for APs, clients and events in detail and summary from.
 - OV3600 displays information on Rogue APs in the **RAPIDS > Overview** pages.
 - Information on Suspected Rogue, Interfering and known interfering APs is available in OV3600 on each **APs/Devices > Manage** page.
 - IDS events data and reports appear on OV3600's **Reports > Generated > IDS Events** page.

Figure 12: Security Summary on the Master switch



See "Rogue Device Classification" on page 32 for more information about security, IDS, WIPS, WIDS, classification, and RAPIDS.

This section discusses Alcatel-Lucent specific capabilities in OV3600 and contains the following topics:

- "Alcatel-Lucent Traps for RADIUS Auth and IDS Tracking" on page 25
- "Remote AP Monitoring" on page 26
- "ARM and Channel Utilization Information" on page 27
- "Viewing switch License Information" on page 32
- "Rogue Device Classification" on page 32
- "Rules-Based Controller Classification" on page 35

Alcatel-Lucent Traps for RADIUS Auth and IDS Tracking

The authentication failure traps are received by the OV3600 server and correlated to the proper switch, AP, and user.

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

Figure 13: RADIUS Issues Summary

RADIUS Issues for devices in folder [Top](#) and subfolders | [Return to Home Overview](#)

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

1-20 of 12,121 RADIUS Issues Page 1 of 606 > > Reset filters Choose columns Export CSV							
Event	Username	Client MAC Address	Client IP	AP/Device	BSSID	Radio	C
<input type="checkbox"/> Client authentication failed for F8:95:C7:FF:B2:94	xjma	F8:95:C7:FF:B2:94	0.0.0.0	1310-325	AC:A3:1E:53:B3:F0	802.11ac	et
<input type="checkbox"/> Client authentication failed for 00:00:00:00:00:00	-	00:00:00:00:00:00	10.69.2.253	-	-	-	af
<input type="checkbox"/> Client authentication failed for 00:24:D7:EB:22:68	kenc	00:24:D7:EB:22:68	0.0.0.0	1341-AP123	AC:A3:1E:55:91:B0	802.11ac	Cl
<input type="checkbox"/> Client authentication failed for 00:00:00:00:00:00	-	00:00:00:00:00:00	10.69.2.253	-	-	-	af

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

Figure 14: IDS Events in OV3600

IDS Events for devices in folder [Top](#) and subfolders | [View all IDS Events](#)

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

1-20 ▼ of 20,625 IDS Events Page 1 ▼ of 1,032 > > | [Reset filters](#) [Choose columns](#) [Export CSV](#)

	Severity ▼	Category ▼	Scope ▼	Attack ▼	Detail
<input type="checkbox"/>	Highest	Rogue Activity	Client	Station Associated to Rogue AP	Station Associated to Rogue AP
<input type="checkbox"/>	Highest	Rogue Activity	Client	Station Associated to Rogue AP	Station Associated to Rogue AP

Remote AP Monitoring

To monitor remote APs, follow these steps:

1. From the **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

Monitoring ss-155 in group APs in folder Top Help

This Device is in monitor-only mode. Poll Controller Now

Device Info

Status: Up
Configuration: Good

Controller:	7210-alpha-1	Aruba AP Group:	India-raps	Upstream Device:	-
Type:	Aruba RAP-155P	Remote Device:	Yes	Last Contacted:	1/21/2016 10:21 PM PST
LAN MAC Address:	00:0B:86:8F:68:12	Serial:	CC0003393		
IP Address:	1.1.1.20	Clients:	26	Usage:	232 Kbps
Outer IP:	27.251.187.226	Remote LAN IP:	192.168.10.167	Active Uplink:	Ethernet

Quick Links: Open controller web UI...

Notes:

Radios

INDEX	NAME	MAC ADDRESS	CLIENTS	USAGE (KBPS)	CHANNEL	TX POWER	ANTENNA TYPE	ROLE	SSID
1	802.11bgn	6C:F3:7F:78:E3:80	26	232 Kbps	11.	20 dBm	External	Access	alpha-voip, alp
2	802.11an	6C:F3:7F:78:E3:90	-	-	-	23 dBm	External	Access	alpha-voip, alp

USB Interfaces

INDEX	NETWORK SERVICE LEVEL	STATUS	OPERATIONAL STATUS	RSSI	USAGE
1	-	Not Plugged	Down	-	0 bps

Wired Interfaces

INTERFACE NAME	MAC ADDRESS	CLIENTS	ADMIN STATUS	OPERATIONAL STATUS	TYPE	DUPLEX	ARUBA PORT MO
Enet0	00:0B:86:8F:68:12	0	Up	Up	gigabitEthernet	Full	N/A
Enet1	00:0B:86:8F:68:13	0	Up	Up	gigabitEthernet	Half	Split
Enet2	00:0B:86:8F:68:14	0	Up	Up	gigabitEthernet	Half	Split
Enet3	00:0B:86:8F:68:15	0	Up	Down	gigabitEthernet	Half	Split
Enet4	00:0B:86:8F:68:16	0	Up	Down	gigabitEthernet	Half	Split

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



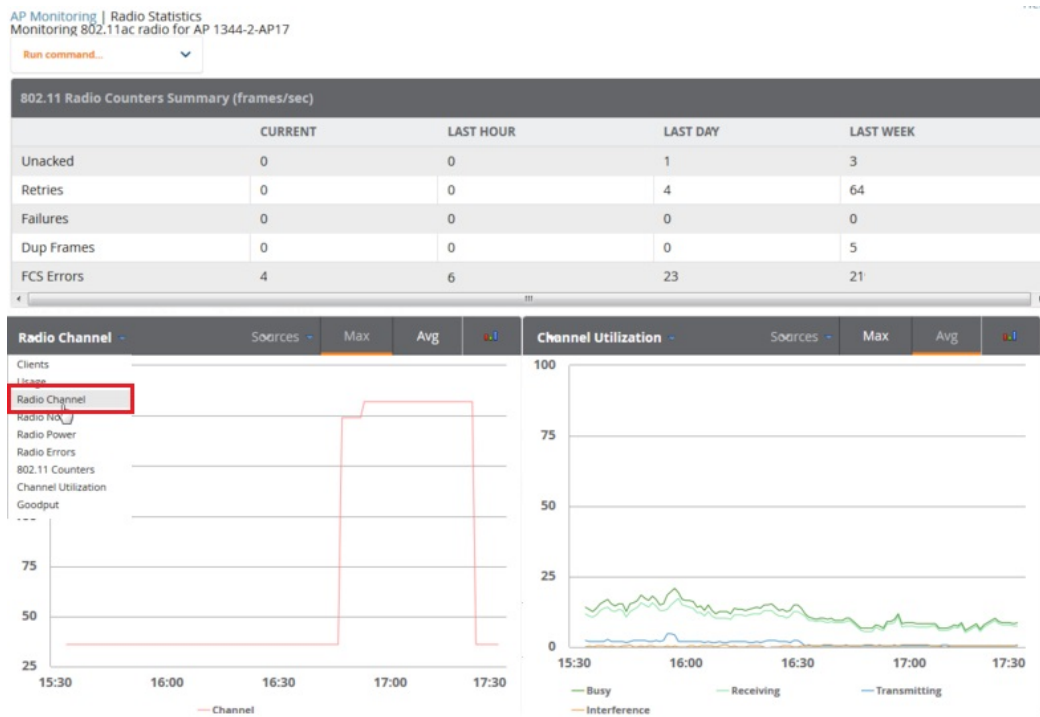
This feature is only available when the remote APs are in split tunnel and tunnel modes.

ARM and Channel Utilization Information

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

1. Navigate to an **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 *OmniVista 3600 Air Manager 8.2 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 navigating to **VisualRF > Floor Plans** page.
2. Click the **list** link at the top of the Floor Plans page, and select a floor plan from the list.
3. Click the **View** tab
4. Select the **Overlays** menu.
5. Select the **Ch. Utilization** overlay.
6. Select **Current** or **Maximum** (over last 24 hours).
7. Use the Data Set drop-down list to display **Total**, **Receive (Rx)**, **Transmit (Tx)**, or **Interference** utilization data.
8. Select the option to view information for the current floor only, or to include information about the floor above, and/or the floor below.
9. Select a frequency (**5 GHz** and/or **2.4 GHz**).

Figure 17: Overlays

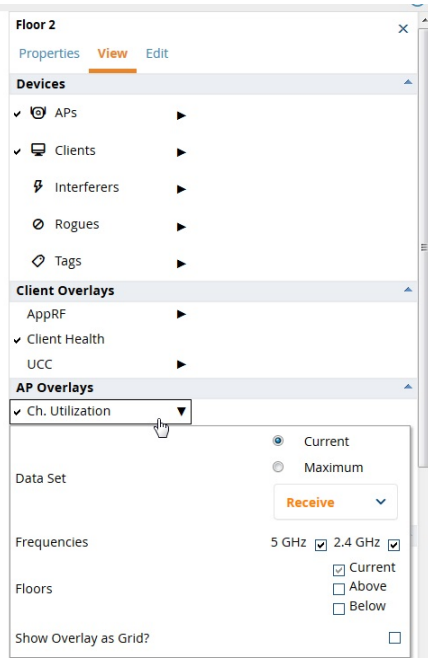
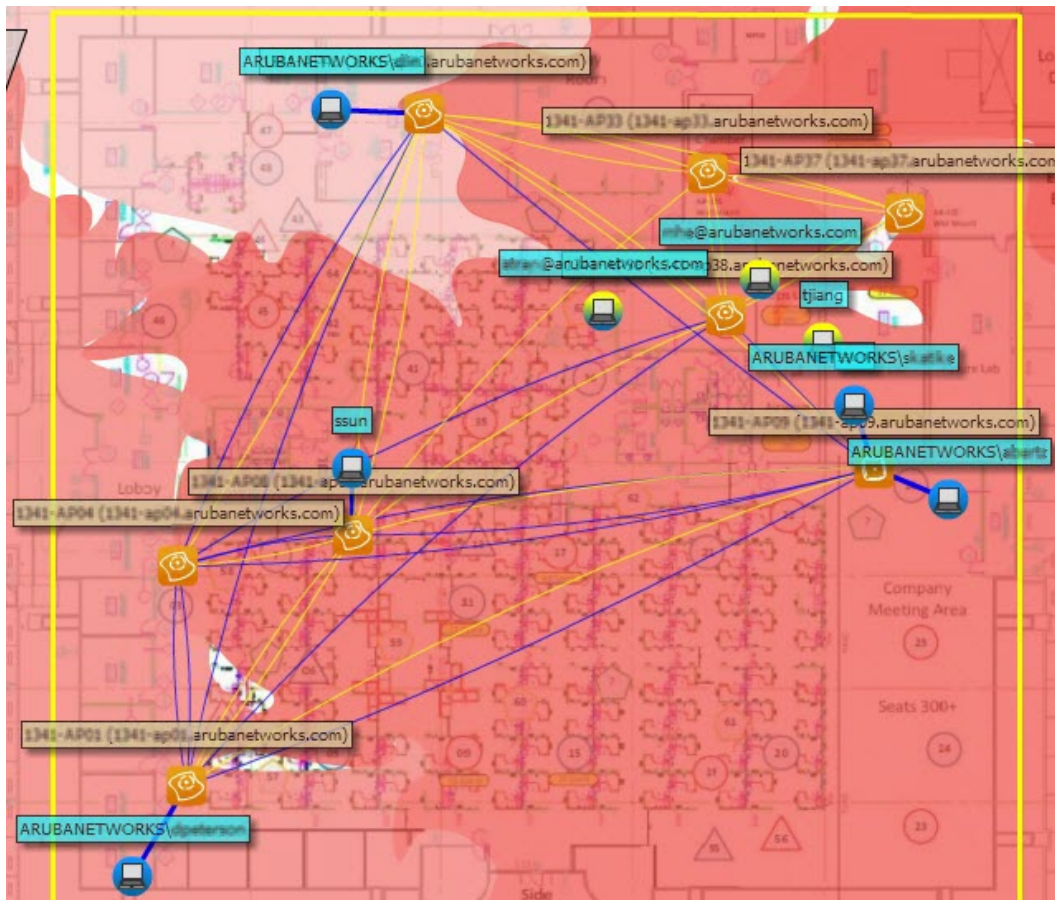


Figure 18: Channel Utilization in VisualRF (Interference/2.4 GHz)



Configuring Channel Utilization Triggers

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

Figure 19: Channel Utilization Trigger

The screenshot shows the 'Trigger' configuration page. At the top, the 'Type' is set to 'Channel Utilization', 'Severity' is 'Warning', and 'Duration' is '5 Minutes'. Below this is the 'Conditions' section, where 'Matching conditions' are set to 'All'. A list of 'Available Conditions' includes 'Interference (%)', 'Radio Type', 'Time Busy (%)', 'Time Receiving (%)', and 'Time Transmitting (%)'. An 'Add New Trigger Condition' button is present. Below this is a table with columns 'OPTION', 'CONDITION', and 'VALUE'. Two conditions are listed: 'Interference (%)' with a condition of '>=' and a value of '50', and 'Time Busy (%)' with a condition of '>=' and a value of '70'. Below the table is the 'Trigger Restrictions' section, with 'Folder' set to 'Top', 'Include Subfolders' set to 'Yes', and 'Group' set to 'ProVision Switches'. At the bottom is the 'Alert Notifications' section with a 'Notes' text area.

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 *OmniVista 3600 Air Manager 8.2 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.

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

1. Navigate to the **APs/Devices > list** page and select a device.
2. Navigate to the **APs/Devices > Monitor** page for that device.
3. Scroll down to the **Alert Summary** table and select **OV3600 Alerts**.

Figure 20: Channel Utilization alerts

Alerts for ITC in group Ethersphere-Ims in folder Top > Sunnyvale HQ | Return to AP/Device Monitor Page

Summary			
Attack ▲	Last 2 Hours	Last 24 Hours	Total
Channel Utilization Interference (%) >= 20% for 5 minutes	0	2	4

1-1 ▼ of 1 Alerts Page 1 ▼ of 1 >| Choose columns Export CSV

Alerts					
<input type="checkbox"/>	Trigger Type ▲	Trigger Summary	Triggering Agent	Time	Severity
<input type="checkbox"/>	Channel Utilization	Interference (%) >= 20% for 5 minutes	1341-AP116 (radio 802.11bgn)	1/21/2016 8:03 PM PST	Normal

1-1 ▼ of 1 Alerts Page 1 ▼ of 1
[Select All - Unselect All](#)
[Acknowledge](#) [Delete](#)

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

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

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

1-50 ▼ of 64 Alerts Page 1 ▼ of 2 > >| Choose columns Export CSV

Alerts							
<input type="checkbox"/>	Trigger Type ▲	Trigger Summary	Triggering Agent	Time	Severity	Details	Notes
<input type="checkbox"/>	Channel Utilization	Interference (%) >= 20% for 5 minutes	1341-AP116 (radio 802.11bgn)	1/21/2016 8:03 PM PST	Normal	-	don't edit
<input type="checkbox"/>	Channel Utilization	Interference (%) >= 20% for 5 minutes	AP7c0e.cef5.ae14 (radio 802.11bgn)	1/21/2016 6:55 PM PST	Normal	-	don't edit
<input type="checkbox"/>	Channel Utilization	Time Busy (%) >= 80% for 10 minute	1341-AP112 (radio 802.11bgn)	1/21/2016 11:16 PM PST	Normal	-	
<input type="checkbox"/>	Channel Utilization	Radio Type is 2.4Ghz (802.11 b/g/n) and Time Busy (%) >= (more...)	1341-AP115 (radio 802.11bgn)	1/22/2016 2:24 PM PST	Normal	-	
<input type="checkbox"/>	Channel Utilization	Interference (%) >= 20% for 5 minutes	1341-AP115 (radio 802.11bgn)	1/22/2016 1:37 PM PST	Normal	-	don't edit

View Channel Utilization in RF Health Reports

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

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

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

Most Utilized by Channel Usage (2.4 GHz)									
Rank ▲	Device	Channel Busy (%)	Interference (%)	Clients	Usage	Location	Controller	Folder	Group
1	1341-AP125	77.95	17.32	0	17.48 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
2	AP7c0e.ccf5.ae14	76.77	76.77	0	11.98 Kbps	default location	Cisco8510	Top	Cisco Gear
3	1341-AP127	74.02	14.96	0	8.08 Kbps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
4	APd072.dce0.225c	73.23	73.23	0	6.21 Kbps	default location	Cisco7500	Top	Cisco Gear
5	1341-X-AP09	72.83	26.77	0	4.13 Kbps	-	alpo	Top > Sunnyvale HQ	Aruba HQ
6	1341-AP114	70.08	10.63	0	68 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
7	1341-AP124	69.29	9.84	0	47 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
8	1341-AP132	68.50	9.06	0	2 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
9	1341-AP117	67.32	10.24	0	0 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ
10	1341-AP116	66.54	8.27	0	0 bps	-	Chuckwagon	Top > Sunnyvale HQ	Aruba HQ

Viewing switch License Information

Follow these steps to view your switch's license information in OV3600:

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

Figure 23: switch License Popup from the APs/Devices > Monitor page

License Table for Chuck:

Service Type ▲	Installed	Expires	Flag	Key
Access Points: 512	10/21/2012		E	F/luldyB-tPp9X7q5-SRXPUdRJ-gKmr5CPP-j2D
Internal Test Functions	10/16/2015		E	nbq1fJtt-Eq44rroM-06zsbiXT-9Ht8WFPV-3AxrZ
Next Generation Policy Enforcement Firewall Module: 512	10/21/2012		E	XxD6a4uH-BGWea+XP-DPRYRrg7-eut+IoHA
Policy Enforcement Firewall for VPN users	10/21/2012		E	Eb/n2d02-9AeE6coJ-3J0Orfj-iaBu7tpX-Bi8sw6J
RF Protect: 512	10/21/2012		E	859Gc/BG-nQnXrvjb-WMmHOVDT-dCjJOOv-Q
Voice Service Module: 8192	10/20/2012		E	YNIGZ88x-UrVfvPlv-WKSX1LzM-564tsWH8-x

Rogue Device Classification

Complete the steps in this section if you have completed the WMS Offload procedure. After offloading WMS, OV3600 maintains the primary ARM, WIPS, and WIDS state classification for all devices discovered over-the-air. See [Table 2](#) below for details.

Table 2: WIPS/WIDS to OV3600 switch Classification Matrix

OV3600 switch Classification	AOS-W (WIPS/WIDS)
Unclassified (default state)	Unknown

Table 2: WIPS/WIDS to OV3600 switch Classification Matrix (Continued)

OV3600 switch Classification	AOS-W (WIPS/WIDS)
Valid	Valid
Suspected Valid	Suspected Valid
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Suspected Rogue	Suspected Rogue
Rogue	Rogue
Contained Rogue	DOS

To check and reclassify rogue devices, follow these steps:

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

Figure 24: Rogue Detail Page Illustration

Name:	Aruba Netw-D3:F9:00	Model:	-	First Discovered:	9/2/2015 2:36 PM PDT
Acknowledge:	<input type="radio"/> Yes <input checked="" type="radio"/> No	IP Address:	-	First Discovery Method:	Wireless AP scan
Controller Classification:	Suspected Rogue	Confidence:	20		
Match Type:	-	Match Method:	-	Match MAC:	-
Match IP Address:					
SSID:	mcell1341	First Discovery Agent:	-		
RAPIDS Classification:	Suspected Rogue	Channel:	1	Last Discovered:	1/22/2016 2:24 PM PST
Classification Rule:	Signal strength > -75 dBm	WEP:	No	Last Discovery Method:	Wireless AP scan
RAPIDS Classification Override:	- No Override -	WPA:	Yes	Last Discovery Agent:	1341-X-AP11
Threat Level:	Valid	Network Type:	AP	Signal:	-20
Threat Level Override:	Suspected Valid				
	Neighbor				
	Suspected Neighbor				
	Suspected Rogue				
	Rogue				
Radio MAC Address:	Aruba Networks				
Radio Vendor:	Aruba Networks	Current Associations:	0		
LAN MAC Address:	-	Max Associations:	0		
LAN Vendor:	-				
OUI Score:	-				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				



Changing the switch's classification within the OV3600 WebUI will push a reclassification message to all switches managed by the OV3600 server that are in Groups with Offloading the WMS database set to **Yes**. To reset the switch classification of a rogue device on OV3600, change the switch classification on the OV3600 WebUI to unclassified.

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

All rogue devices will be set to a default switch classification of **unclassified** when WMS is first offloaded except for devices classified as valid. Rogue devices classified in AOS-W as valid will also be classified within OV3600 as valid for their switch classification as well. As APs report subsequent classification information about rogues, this classification will be reflected within OV3600 WebUI and propagated to switches that OV3600 manages. The

device classification reflected in the switch's WebUI and in the OV3600 WebUI will probably not match, because the switch/APs do not reclassify rogue devices frequently.

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

Table 3: ARM to OV3600 Classification Matrix

OV3600	AOS-W (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

Detail for F4:AF:93:5C:89:89

Device Info

Last Username:	kartee
First Seen:	12/21/2015 11: AM PST on 1341-AP98 for 20 mins
Last Seen:	1/15/2016 2:00 PM PST on 1341-AP115 for 50 mins
Device Type:	<input type="checkbox"/> OS X
Network Interface Vendor:	Unknown
AOS Device Type:	OS X
Aruba HTTP Fingerprint:	-
Classification:	<div style="border: 1px solid #ccc; padding: 2px;"> Unclassified ▾ <ul style="list-style-type: none"> <li style="background-color: #007bff; color: white; padding: 2px;">Valid <li style="padding: 2px;">Unclassified <li style="padding: 2px;">Contained </div>
Watched Client:	
Notes:	



Changing User Classification within the OV3600 WebUI will push a user reclassification message to all switches managed by the OV3600 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 OV3600 WebUI and propagated to switches that OV3600 manages. It is probable that the user's classification reflected in the switch's WebUI and in the OV3600 WebUI will not match, because the switches/APs do not reclassify users frequently.

There is no method in the OV3600 WebUI to update user classification before bulk to match the switch's classification. Each client must be updated individually within the OV3600 WebUI .

Rules-Based Controller Classification

This section contains the following topics:

- "Using RAPIDS Defaults for Controller Classification" on page 35
- "Changing RAPIDS Based on switch Classification" on page 35

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

The screenshot shows the 'RAPIDS Classification Rule' configuration page. The 'Rule name' is 'Detected Wirelessly and On LAN'. The 'Classification' dropdown is open, showing a list of options under 'RAPIDS Classification' and 'Device Classification'. The 'Use Controller Classification' option is highlighted. Below the dropdown, there is a 'Detected on WLAN' dropdown and an 'Add' button. At the bottom, there are 'Save' and 'Cancel' buttons.

Rule name:	Detected Wirelessly and On LAN
Classification:	Suspected Neighbor
Threat Level:	
Enabled:	
	Detected on WLAN
	Add
Device has been detected wirelessly:	(remove condition)
	Save
	Cancel

Changing RAPIDS Based on switch 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

RAPIDS Classification Rule

Rule name: Detected Wirelessly and on LAN

Classification: Rogue

Threat Level: 5

Enabled: Yes No

Detected on WLAN **Add**

Yes No
(remove condition)

Save **Cancel**

- Detected on WLAN
- Detected AP count
- Encryption
- Network type
- Signal strength
- SSID
- Channel
- Detected Client Count
- Wireline Properties**
 - Detected on LAN
 - Fingerprint scan
 - IP address
 - OUI score
 - Operating system
- Wireless/Wireline Properties**
 - Manufacturer
 - MAC Address
- Alcatel Lucent Controller Properties**
 - Controller Classification**
 - Confidence

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

Enable Channel Utilization Events



Enabling these commands on AOS-W versions prior to 6.1 can result in performance issues on the switch.

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

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

(switch-Name) (config) # mgmt-server type ov3600 primary-server <OV3600 IP> profile <profile-name>
(switch-Name) (config) # write mem
```

Enable Stats With the AOS-W CLI

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



Do not use these commands if you use the OV3600 WebUI to monitor APs and Clients. Enabling these commands on AOS-W versions prior to 6.1 can result in performance issues on the switch.

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

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

(switch-Name) (config) # ids wms-general-profile collect-stats enable
(switch-Name) (config-ids-wms-general-profile) # collect-stats
(switch-Name) (config-ids-wms-general-profile) # exit
(switch-Name) (config) # write mem
```

Offload WMS Using the AOS-W or OV3600 CLI



Do not use these commands if you use the OV3600 WebUI to monitor APs and clients.

Additional commands can be used to offload WMS using the AOS-W command-line interface or the OV3600 SNMP Walk.

Refer to:

["AOS-W CLI" on page 37](#)

["OV3600 SNMP " on page 38](#)

AOS-W CLI

SSH into all switches (local and master), and enter enable mode, and issue the following commands:

```
(switch-Name) # configure terminal
```

```
Enter Configuration commands, one per line. End with CNTL/Z
(switch-Name) (config) # mobility-manager <OV3600 IP> user <MMS-USER> <MMS-SNMP-PASSWORD>
(switch-Name) (config) # write mem
```

This command creates an SNMPv3 user on the switch 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 OV3600 adheres to this IETF recommendation. AOS-W 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 ov3600123 ov3600123
```

OV3600 SNMP

Log in into the OV3600 server with proper administrative access and issue the following command for all switches (master and locals):

```
[root@OV3600 ~]# snmpwalk -v3 -a SHA -l AuthPriv -u <MMS-USER> -A <MMS-SNMP-PASSWORD> -X <MMS-SNMP-PASSWORD> <switch-IP> wlsxSystemExtGroup
```

```
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchIp.0 = IPAddress: 10.51.5.222
WLSX-SYSTEMEXT-MIB::wlsxSysExtHostname.0 = STRING: Alcatel-Lucent-3600-2
.
..
WLSX-SYSTEMEXT-MIB::wlsxSysExtSwitchLastReload.0 = STRING: User reboot.
WLSX-SYSTEMEXT-MIB::wlsxSysExtLastStatsReset.0 = Timeticks: (0) 0:00:00.00 response
[root@OV3600 ~]#
```

Unless this SNMP walk command is issued properly on all of the switches, 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 ov3600123 -A ov3600123 -X ov3600123 10.51.3.222
wlsxSystemExtGroup
```

If you do not use the OV3600 WebUI to offload WMS, you must add a cronjob on the OV3600 server to ensure continued statistical population. Because the MIB walk/touch does not persist through a switch reboot, a cronjob is required to continually walk and touch the MIB.

Pushing Configs from Master to Local switches

Use the following AOS-W CLI commands to ensure that the master switch is properly pushing configuration settings from the master switch to local switches. This command ensures configuration changes made on the master switch will propagate to all local switches.



Do not use these commands if you use the OV3600 WebUI to monitor APs and clients.

```
(switch-Name) (config) # cfm mms config disable
(switch-Name) (config) # write mem
```

Disable Debugging Utilizing the AOS-W CLI

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

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

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

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

```
(switch-Name) # configure terminal
```

Enter Configuration commands, one per line. End with CNTL/Z

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

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

Restart WMS on Local switches

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

```
(switch-Name) # configure terminal
```

Enter Configuration commands, one per line. End with CNTL/Z

```
(switch-Name) (config) # process restart wms
```

After executing the `restart wms` command in Alcatel-Lucent AOS-W, you will need to wait until the next Rogue Poll Period on OV3600 and execute a **Poll Now** operation for each local switch on the **APs/Devices > List page** before rogue devices begin to appear in OV3600.

Configure AOS-W CLI when not Offloading WMS

To ensure proper event correlation for IDS events when WMS is not offloaded to OV3600, access the command line interface of each switch (master and local), enter enable mode, and issue the following commands:

```
(switch-Name) # configure terminal
```

Enter Configuration commands, one per line. End with CNTL/Z

```
(switch-Name) (config) # ids management-profile
```

```
(switch-Name) (config) # ids general-profile <name>
```

```
(switch-Name) (config) # ids-events logs-and-traps
```

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

Copy and Paste to Enable Proper Traps with the AOS-W CLI

To ensure the proper traps are configured on Alcatel-Lucent switches, 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
```

wlsxClietFloodAttack
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
wlsxSignStaAsleep
wlsxSignStaDeauthBcast
wlsxSignStaNetstumbler
wlsxSignStaNullProbeResp
wlsxStaAssociatedToUnsecureAP
wlsxStaImpersonation
wlsxStaPolicyViolation
wlsxStaRepeatWEPIVViolation
wlsxStaUnAssociatedFromUnsecureAP
wlsxStaWeakWEPIVViolation
wlsxTKIPReplayAttack
wlsxUserEntryAttributesChanged
wlsxValidClientMisassociation
wlsxValidClientNotUsingEncryption
wlsxValidSSIDViolation
wlsxWeakWEPIVViolation
wlsxWEPMisconfiguration
wlsxWindowsBridgeDetected
wlsxWindowsBridgeDetectedAP
wlsxWindowsBridgeDetectedSta
wlsxWirelessBridge
wlsxWirelessHostedNetworkContainment
wlsxWirelessHostedNetworkDetected



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

Table 4: Data Flow between Controllers and OV3600 (Continued)

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Enabling of WMS Offload			←									
Exec UI							→					When AMON is used for client monitoring, OV3600 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 OV3600 via HTTPS.
IDS Events		→										
Interface Monitoring	←											
Lync/UCC/Voice				→								Available in OV3600 8.0 and later.
Neighbor Clients	←			→								
Network Derivations			←									
RADIUS Auth Issues		→										
RAPIDS	←											
RF Capacity				→								
RF Health				→								
Rogue AP OS									↑			

Table 4: Data Flow between Controllers and OV3600 (Continued)

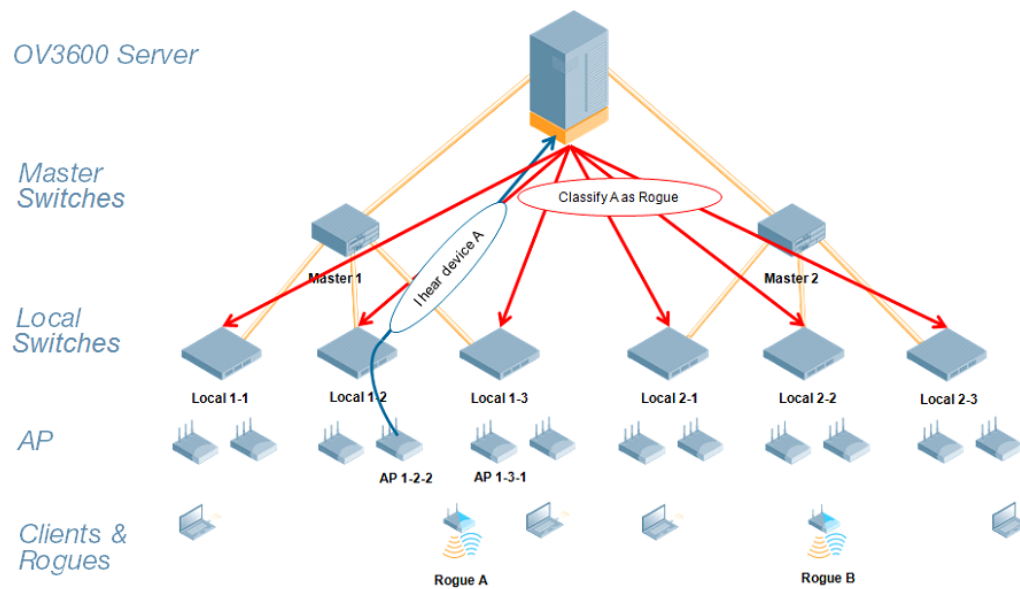
Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
Rogue Classification	←				←							If WMS Offload enabled, OmniVista 3600 Air Manager updates rogue classifications on a controller using PAPI; otherwise it's done with SNMP.
Rogue Clients	←											
Syslog						→						
VisualRF	←			→								VisualRF's client data comes from OV3600, which gets its data from SNMP + AMON.

Table 5: Data Flow between Instant Devices and OV3600

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
All Monitoring Data							→					VC sends data to OV3600 every minute in an HTTP POST.
Configuration Commands							→					When OV3600 needs to send data to a VC, it sends it in the HTTPS response.
Diagnostic Commands							→					
Firmware Images							→					

WMS Offload instructs the master switch to stop correlating ARM, WIPS, and WIDS state information among its local switches because OV3600 will assume this responsibility. Figure 28 depicts how OV3600 communicates state information with local switches.

Figure 28: ARM/WIPS/WIDS Classification Message Workflow



State Correlation Process

1. AP-1-3-1 hears rogue device A.
2. Local switch 1-3 evaluates devices and does initial classification and sends a classification request to OV3600.
3. OV3600 receives message and reclassifies the device if necessary and reflects this within the OV3600 WebUI and via SNMP traps, if configured.
4. OV3600 sends a classification message back to all local switches managed by master switch 1, (1-1, 1-2, and 1-3).
5. OV3600 sends a classification message back to all additional local switches managed by the OV3600 server. In this example all local switches under master switch 2, (2-1, 2-2, and 2-3) would receive the classification messages.
6. If an administrative OV3600 user manually overrides the classification, then OV3600 will send a re-classification message to all applicable local switches.
7. OV3600 periodically polls each local switch's MIB to ensure state parity with the OV3600 database. If the local switch's device state does not comply with the OV3600 database, OV3600 will send a re-classification message to bring it back into compliance.



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

Using OV3600 as a Master Device State Manager

OV3600 offers the following benefits as a master device state manager:

- Ability to correlate state among multiple master switches. 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 Alcatel-Lucent infrastructure inter-operates more efficiently in a mixed infrastructure environment.
- Ability to better classify devices based on OV3600 wire-line information not currently available in AOS-W.
- OV3600 provides a near real-time event notification and classification of new devices entering air space.
- RAPIDS gains additional wire-line discovery data from Alcatel-Lucent switches.

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 6: 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 OV3600 and Alcatel-Lucent WLAN infrastructure with Alcatel-Lucent's RTLS feed to more accurately locate wireless clients and Wi-Fi Tags.

Deployment Topology

Figure 29: Typical Client Location

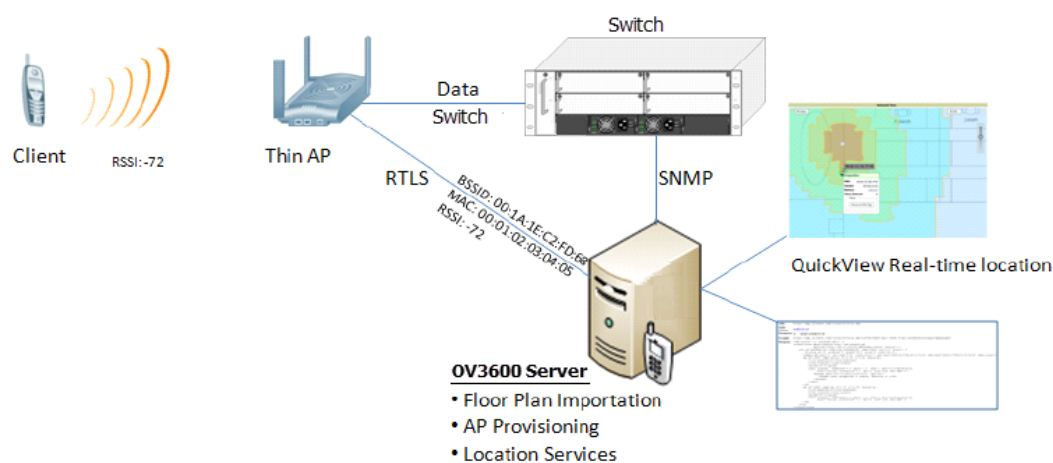
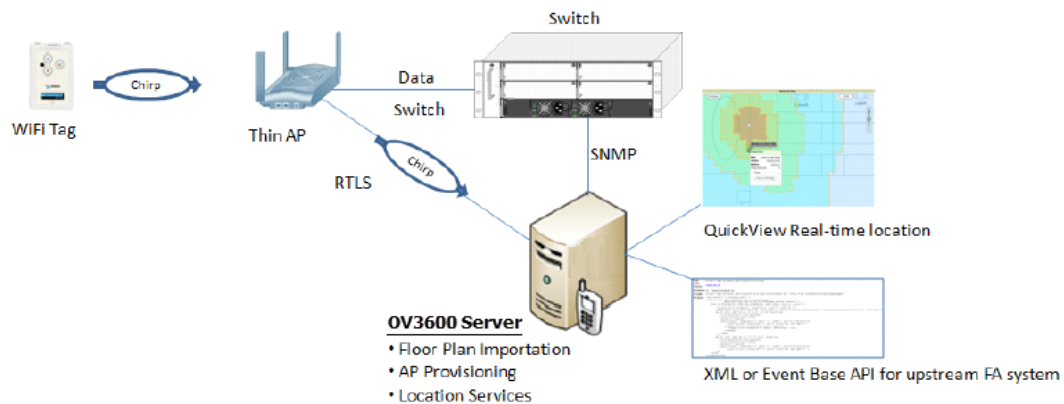


Figure 30: Typical Tag Deployment



Prerequisites

You will need the following information to monitor and manage your Alcatel-Lucent infrastructure.

- Ensure that the OV3600 server is already monitoring Alcatel-Lucent 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 OV3600 server's IP address and each access point's IP address.

Enable RTLS Service on the OV3600 Server

1. Navigate to **OV3600 Setup > General** and locate the **Additional OV3600 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 switch default is 5050.
 - **RTLS Username**—This must match the SNMPv3 MMS username configured on the switch.
 - **RTLS Password**—This must match the SNMPv3 MMS password configured on the switch.
4. Click **Save**.

Figure 31: RTLS Fields in OV3600 Setup > General > Additional OV3600 Services

Additional OV3600 Services	
Enable FTP server: <small>required to manage Alcatel-Lucent AirMesh & Cisco 4800 APs; optional for firmware upgrades on supported devices.</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable RTLS collector: <small>Aruba/Alcatel-Lucent only</small>	<input type="radio"/> Yes <input checked="" type="radio"/> No
Use Embedded Mail Server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Mail Relay Server: <small>Optional</small>	<input type="text" value="Enter a Value"/>
	<input type="button" value="Send Test Email"/>
Process user roaming traps from Cisco WLC:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AMON Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Clarity Data Collection: <small>Requires AOS-W Version 6.4.3 and Above</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable AppRF Data Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
AppRF Storage Allocated (GiB): <small>Greater than or equal to 2 GiB</small>	<input type="text" value="25"/>
Enable UCC Data Collection: <small>Requires AOS-W Version 6.4 and Above</small>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UCC Calls Stitching (Heuristics):	<input checked="" type="radio"/> Yes <input type="radio"/> No
Prefer AMON vs SNMP Polling:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Syslog and SNMP Trap Collection:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Require SSH host key verification:	<input type="radio"/> Yes <input checked="" type="radio"/> No

Enable RTLS on the switch



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

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

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

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

(switch-Name) (AP system profile default) # rtls-server ip-addr <IP of OV3600 Server> port 5050
key <switch-SNMPv3-MMS-Password>

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

To validate exit configuration mode:

```
(switch-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 OV3600 server.

Using the WebUI to See Status

1. In the OV3600 WebUI, navigate to the **System > Status** page.
2. Scroll down through the Services list to locate the RTLS service, as shown below.

Figure 32: RTLS System Status

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

Using the CLI

Use SSH to access the command-line interface of your OV3600 server, and issue the following commands:

```
[root@OV3600Server]# 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 OV3600 server.

```
[root@OV3600Server]# logs
```

```
[root@OV3600Server]# tail rtls
```

```
payload:
00147aaf01000020001a1ec02b320000001000000137aae0100000c001a1ec02b320000001a1e82b322590006ddf
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:
0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec05078000000d54a7a280540001ddf
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:
0014c9c90100003c001a1ec05078000000200000013c9c70100000c001a1ec05078000000d54a7a280540001ddf
f020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
```

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

```
[root@OV3600Server]# 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 Wi-Fi Tag information by running the Tag XML API:

```
https://<OV3600-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.

