Alcatel-Lucent and OmniVista 3600 Air Manager 7.4

Best Practices Guide

Legal Notice

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

Contents

Preface

This preface provides an overview of this best practices guide and contact information for Alcatel-Lucent, and includes the following sections:

Document Organization

This best practices guide includes instructions and examples of optimal ways to use and integrate the AirWave Wireless Management Suite (OV3600) with Alcatel-Lucent devices and infrastructure.

Table 1 *Document Organization and Purposes*

Chapter	Description
Chapter 1, "Overview" on page 5	This chapter explains the minimum requirements, prerequisites, topology of an Alcatel-Lucent infrastructure integrated with OV3600.
Chapter 2, "Configuring OV3600 for Global Alcatel-Lucent Infrastructure" on page 9	This chapter explains global configuration options in OV3600.
Chapter 3, "Configuring an Alcatel-Lucent Group in OV3600" on page 13	This chapter explains how to create and monitor an Alcatel-Lucent group in OV3600.
Chapter 4, "Discovering Alcatel-Lucent Infrastructure" on page 15	This chapter explains how to discover and manage your Alcatel-Lucent infrastructure.
Chapter 5, "OV3600 and Alcatel-Lucent Integration Strategies" on page 19	This chapter highlights recommended integration strategies.
Chapter 6, "Alcatel-Lucent-Specific Capabilities in OV3600" on page 27	This chapter highlights OV3600 capabilities that are specific to Alcatel-Lucent devices.
Appendix A, "CLI AOS-W & OV3600 Commands" on page 35	This appendix explains command line interface (CLI) commands.
Appendix B, "How OV3600 Acquires Data from Alcatel-Lucent Devices" on page 39	This appendix provides a table that explains how OV3600 acquires data from Alcatel-Lucent devices.
Appendix C, "WMS Offload Details" on page 41	This appendix explains WMS Offload in further detail.
Appendix D, "Increasing Location Accuracy" on page 43	This appendix explains ways to increase location accuracy in OV3600.

Note, Caution, and Warning Icons

This document uses the following notice icons to emphasize advisories for certain actions, configurations, or concepts:

Indicates helpful suggestions, pertinent information, and important things to remember.

Indicates a risk of damage to your hardware or loss of data.

Indicates a risk of personal injury or death.

Contacting Support

Table 2 *Alcatel-Lucent Contact Information*

Online Contact and Support	
Main Website	http://www.alcatel-lucent.com/enterprise
Support Website	http://service.esd.alcatel-lucent.com
Alcatel-Lucent Enterprise Service and OmniVista 3600 Email Support	Esd.support@alcatel-lucent.com

Chapter 1

Overview

This document provides best practices for leveraging OV3600 to monitor and manage your Alcatel-Lucent infrastructure. Alcatel-Lucent wireless infrastructure provides a wealth of functionality such as firewall, VPN, remote AP, IDS, IPS, and ARM, as well as an abundance of statistical information.

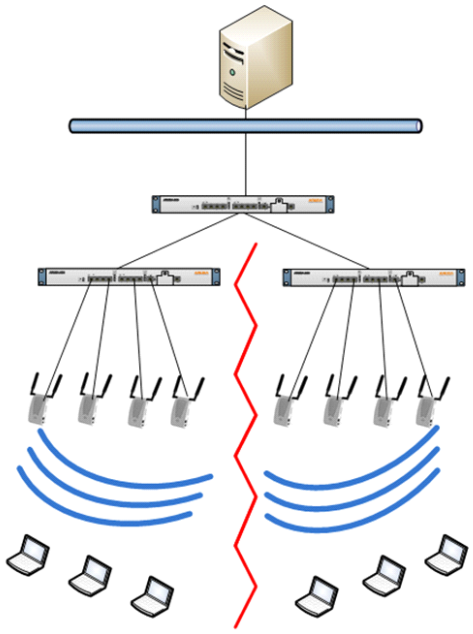
Follow the simple guidelines in this document to garner the full benefit of Alcatel-Lucent's infrastructure.

This overview chapter contains the following topics:

Understanding Alcatel-Lucent Topology

Figure 1 is a typical Master-Local deployment:

Figure 1 *Typical Alcatel-Lucent 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

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 & 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 WMS Offload:
  - Username
  - Auth password
  - Privacy password
  - Auth protocol

Feature Implementation Schedule

The following table describes the feature implementation schedule for OV3600:

Table 4 *Alcatel-Lucent Feature Implementation Schedule for OV3600*

Feature	OV3600 Implementation
Ability to filter User Session by AOS-W roles	7.0
AOS-W 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 switch specific overrides	7.0
Client dot11counter status	7.0
Added support for AP-92 and AP-93	7.1
Ability to use switch WIPS classification within RAPIDS	7.1
Use switch classification/confidence level within a RAPIDS rule	7.1
AOS-W provides Ad-Hoc rogues and encryption type	7.1
Channel Utilization	7.1
AP dot11counter statistics	7.1
Support for SNMPv3 informs	7.1
Track BW on wired users connected to RAPs	7.1
Ability to configure SNMP local configuration	7.1
Ability to track ARM power and channel changes	7.3
Ability to track Noise Floor	7.3
Ability to track Interfering Devices	7.3
Ability to store and display ARM logs	7.3

Table 4 *Alcatel-Lucent Feature Implementation Schedule for OV3600 (Continued)*

Feature	OV3600 Implementation
Ability to track user associations and roaming via SNMP traps	7.3
Ability to pull Channel Summary CLI statistics from switch	7.3
OV3600 requires a 64-bit operating system	7.3
VisualRF and RAPIDS are now standard part of the OV3600	7.3
System > Syslog & Traps page has been added to display all syslog messages and SNMP traps that OV3600 receives	7.3
Mobile Device Access Control (MDAC) secures, provisions and manages network access for Apple iOS and other employee-owned mobile devices by enabling device fingerprinting, device registration, and increased device visibility	7.3
Session-based authentication in OV3600 (login/logout)	7.3
Ability to filter on list tables (new funnel icon)	7.3
Device Type filtering on reports	7.3
Interferer location ability	7.3
Added Open switch web UI drop-down menu to the APs/Devices > Monitor and Users > User Detail pages for Alcatel-Lucent devices	7.3

This chapter explains how to optimally configure OV3600 to globally manage your Alcatel-Lucent infrastructure, and contains the following topics:

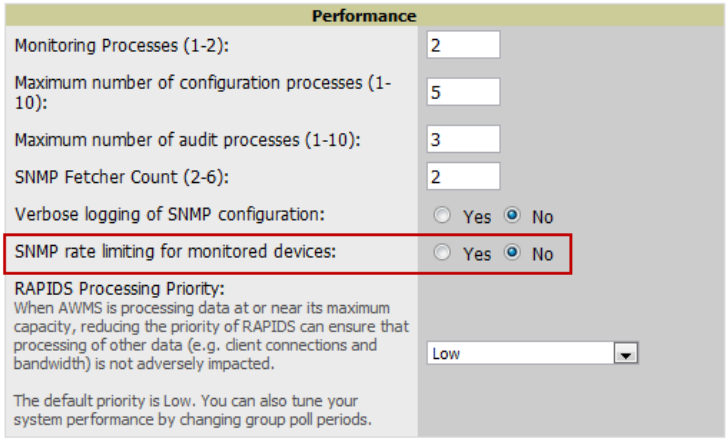
Disabling Rate Limiting in OV3600 Setup > General

The SNMP Rate Limiting for Monitored Devices option adds a small delay between each SNMP GET request, thus the actual polling intervals will be longer than what is configured. For example, setting a 10-minute polling interval will result in an actual 12-minute polling interval. Alcatel-Lucent recommends disabling rate limiting in most cases unless you are using legacy Alcatel-Lucent devices, such as M2 devices.

To disable rate limiting in OV3600, follow these steps:

1. Navigate to **OV3600 Setup > General**.
2. Locate the **Performance** section on this page.
3. In the **SNMP Rate Limiting for Monitored Devices** field, select **No**, as shown in Figure 2.
4. Select **Save**.

Figure 2 *SNMP Rate Limiting in OV3600 Setup > General*



Entering Credentials in Device Setup > Communication

OV3600 requires several credentials to properly interface with Alcatel-Lucent infrastructure. To enter these credentials, follow these steps:

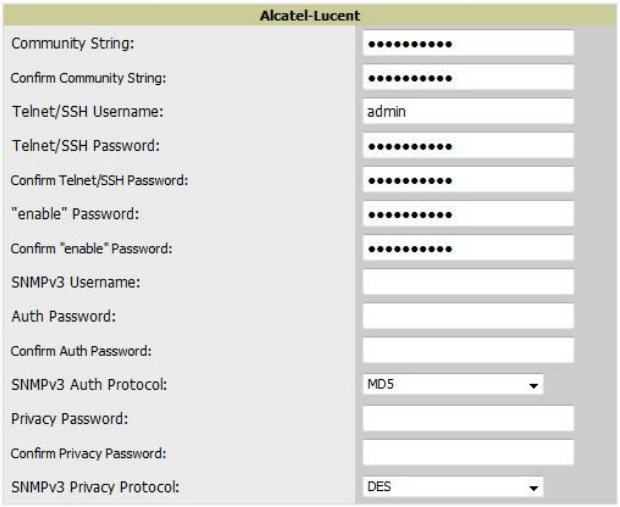
1. Navigate to **Device Setup > Communication**.

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**.

NOTE

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

Figure 3 *Alcatel-Lucent Credentials in* ***Device Setup > Communication***



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

NOTE

The protocols should be SHA and DES in order for WMS Offload to work.

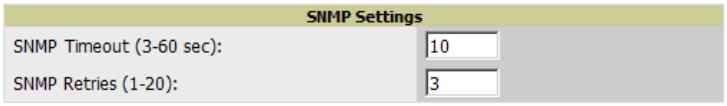
6. When finished, select **Save**.

Setting Up Recommended Timeout and Retries

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

1. In the **Device Setup > Communication** page, locate the **SNMP Setting** section.
2. Change **SNMP Timeout** setting to **10**.
3. Change **SNMP Retries** to **1**.

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



4. Select **Save**.

Setting Up Time Synchronization

Setting up NTP on OV3600

On the **OV3600 Setup > Network** page, locate the **Network Time Protocol (NTP)** section. The Network Time Protocol is used to synchronize the time between OV3600 and your network reference NTP server. NTP servers synchronize with external reference time sources, such as satellites, radios, or modems.

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

To disable NTP services, clear both the **Primary** and **Secondary** NTP server fields. Any problem related to communication between AWMS and the NTP servers creates an entry in the event log. For more information on ensuring that OV3600 servers have the correct time, please see http://support.ntp.org/bin/view/Servers/NTPPoolServers.

Table 5 ***OV3600 Setup > Network > Secondary Network*** *Fields and Default Values*

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

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

Manually Setting the Clock on a Controller

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

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

Enabling Support for Channel Utilization & Statistics

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

- OV3600 7.3 or later
- AOS-W 6.0.1 or later

NOTE

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

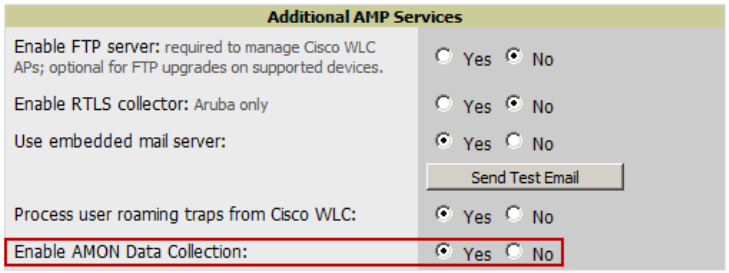
- Access points - Alcatel-Lucent AP-105, AP-92, AP-93, AP-125, AP-124, AP-134, AP-135
- Controllers - Alcatel-Lucent 6xx, 3xxx, or 6000 Controller Series

OV3600 Setup

Follow these steps in OV3600:

1. Navigate to **OV3600 Setup > General.**
2. In the **Additional OV3600 Services** section, set **Enable AMON Data Collection** to **Yes**, as shown in Figure 5:

Figure 5 *AMON Data Collection setting in* ***OV3600 Setup > General***



3. Select **Save**.

Controller Setup (Master & 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.

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

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

It is prudent to establish an Alcatel-Lucent Group within OV3600. During the discovery process you will move new discovered switches into this group.

This chapter contains the following topics:

Basic Monitoring Configuration

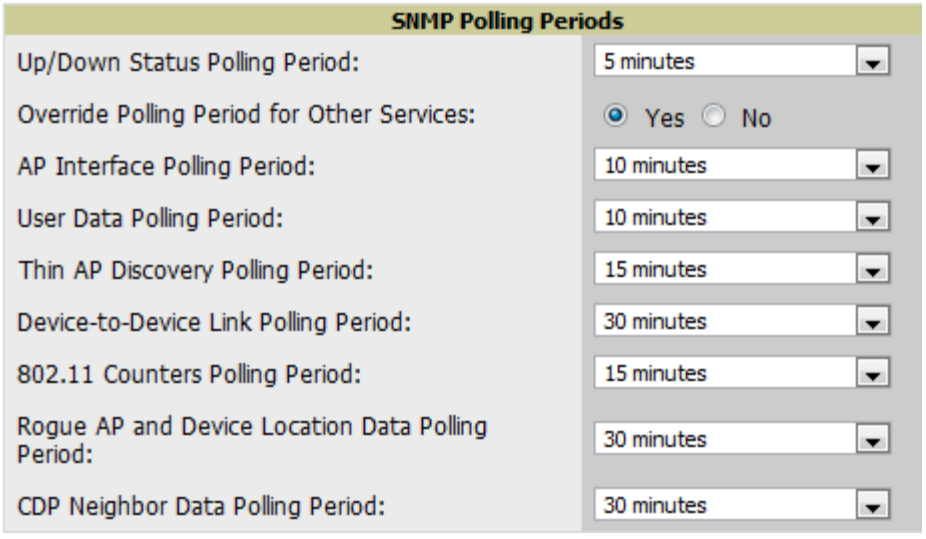
1. Navigate to **Groups > List.**
2. Select **Add**.
3. Enter a **Name** that represents the Alcatel-Lucent infrastructure from a security, geographical, or departmental perspective and select **Add**.
4. You will be redirected to the **Groups > Basic** page for the Group you just created. On this page you will need to tweak a few Alcatel-Lucent-specific settings.
5. Find the **SNMP Polling Periods** section of the page, as illustrated in Figure 6.
6. Change **Override Polling Period for Other Services** to **Yes.**
7. Ensure **User Data Polling Period** is set to 10 minutes. Do not configure this interval lower than 5 minutes.

NOTE

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

8. Change **Device-to-Device Link Polling Period** to **30 minutes.**
9. Change **Rogue AP and Device Location Data Polling Period** to **30 minutes.**

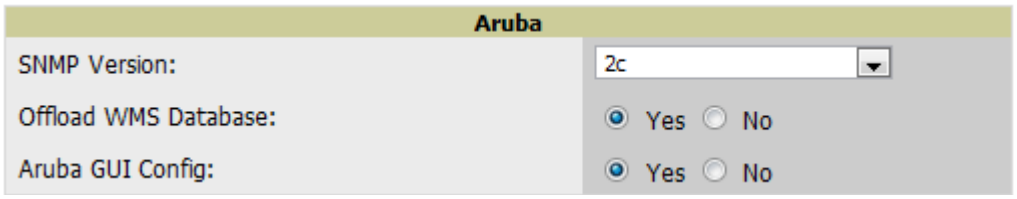
Figure 6 *SNMP Polling Periods section of* ***Groups > Basic***



10. Locate the **Alcatel-Lucent** section of this page, as illustrated in Figure 7.

11. Configure the proper **SNMP Version** for monitoring the Alcatel-Lucent infrastructure.

Figure 7 *Group SNMP Version for Monitoring*



12. Select **Save and Apply.**

Advanced Configuration

Refer to the *OV3600 7.3 Alcatel-Lucent Configuration Guide* located in **Home > Documentation** for detailed instructions.

Chapter 4

Discovering Alcatel-Lucent Infrastructure

This chapter guides you through the process of discovering and managing your Alcatel-Lucent infrastructure.

OV3600 utilizes Alcatel-Lucent's topology to efficiently discover downstream infrastructure.

Refer to the following earlier chapters in this book before attempting discovery:

- Chapter 2, “Configuring OV3600 for Global Alcatel-Lucent Infrastructure” on page 9
- Chapter 3, “Configuring an Alcatel-Lucent Group in OV3600” on page 13

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

- “Discovering Master Switches” on page 15
- “Local Controller Discovery” on page 17
- “Thin AP Discovery” on page 17

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 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 Master Switches

Scan networks containing Alcatel-Lucent Master switches from **Device Setup > Discover.**

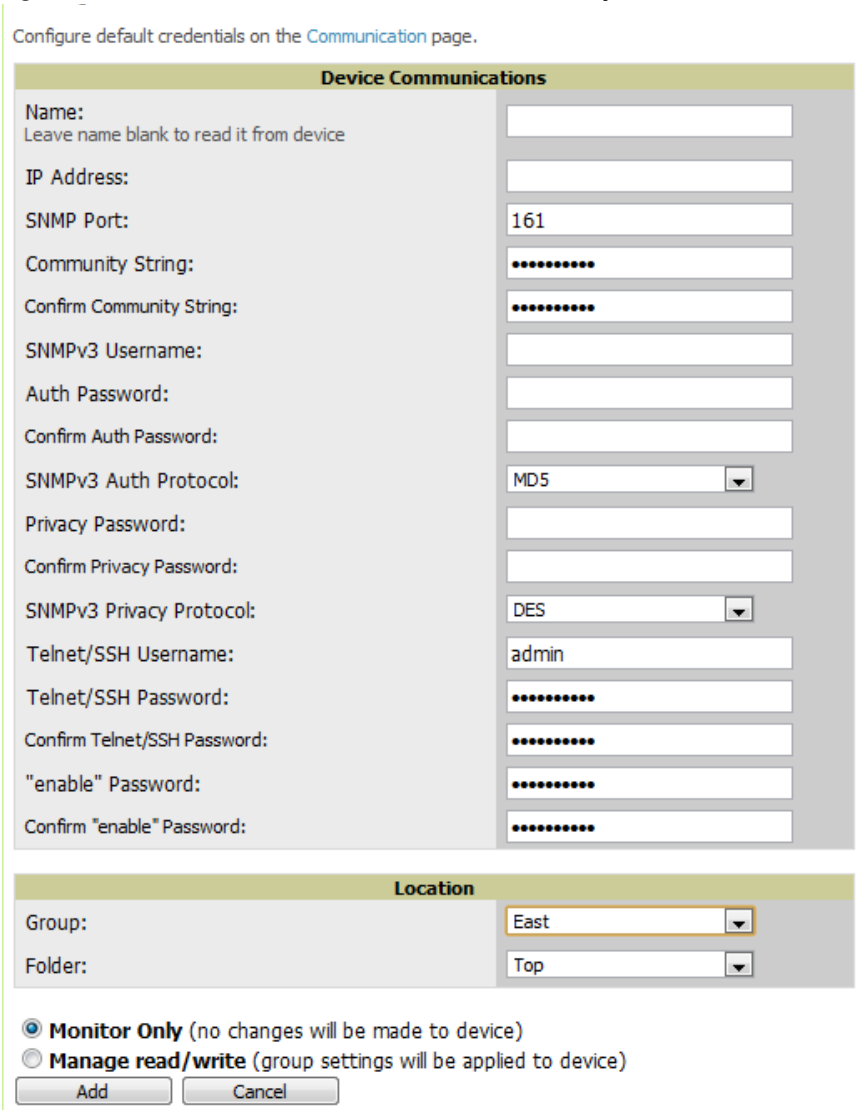
- or -

Manually enter the Master switch by following these steps in the **Device Setup > Add** page:

1. Select the **Alcatel-Lucent Controller** 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***



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

NOTE

The protocols should be SHA and DES in order for WMS Offload to work.

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

6. Assign switch to a Group & Folder.
7. Ensure **Monitor Only** option is selected.
8. Select **Add.**
9. Navigate to **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 Controller 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 Group defined previously. Within OV3600, Local switches can be split away from the Master switch's Group.

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

Chapter 5

OV3600 and Alcatel-Lucent Integration Strategies

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

Integration Goals

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

Table 6 *Integration Goals in All Masters or Master/Local Architectures*

Integration Goals	All Masters Architecture	Master/ Local Architecture
Rogue & Client Info		enable stats
Rogue containment only	ssh access to switches	ssh access to switches
Rogue & Client containment	WMS Offload	WMS Offload
Reduce Master Switch Load		WMS Offload debugging off
IDS & Auth Tracking	Define OV3600 as trap host	Define OV3600 as trap host
Track Tag Location	enable RTLS WMS Offload	enable RTLS WMS Offload
Channel Utilization	enable AMON	enable AMON
Spectrum	enable AMON	enable AMON

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 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 Switch.

Example Use Cases

The following are example use cases of integration strategies:

When to Use Enable Stats

You want to pilot OV3600 and doesn't 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 Stats Utilizing OV3600" on page 21.

When to Use WMS Offload

- You have older Alcatel-Lucent infrastructure in a Master/Local environment and their Master switch is fully taxed. Offloading WMS will increase the capacity of the Master Switch by offloading statistic 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 Utilizing OV3600" on page 22
  - "Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure" on page 25
  - "WMS Offload Details" on page 41

When to Use RTLS

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

RTLS could negatively impact your OV3600 server's performance.

- See "Leveraging RTLS to Increase Accuracy" on page 43.

When to Define OV3600 as 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 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 Trap Host using AOS-W CLI" on page 22.

When to use Channel Utilization

- You have a minimum version of AOS-W 6.1.0.0 and AP-105, AP-135

Prerequisites for Integration

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

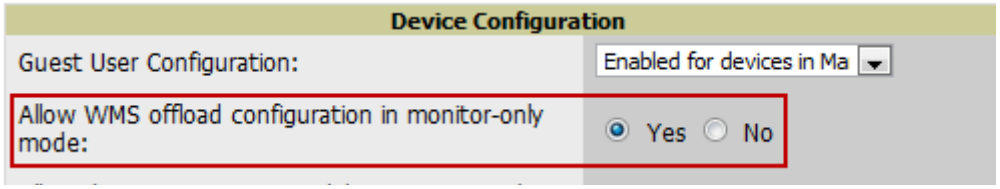
- Chapter 2, “Configuring OV3600 for Global Alcatel-Lucent Infrastructure” on page 9
- Chapter 3, “Configuring an Alcatel-Lucent Group in OV3600” on page 13
- Chapter 4, “Discovering Alcatel-Lucent Infrastructure” on page 15

Enable Stats Utilizing 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***



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***

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 don't follow the above steps, local switches will not be configured to populate statistics. This decreases OV3600' capability to trend client signal information and to properly locate devices. See Appendix A, “CLI AOS-W & OV3600 Commands” on page 35 on how to utilize 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 Appendix A, “CLI AOS-W & OV3600 Commands” on page 35 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 Utilizing 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 in order to push these commands
3. Navigate to **Groups > Basic** and locate the Alcatel-Lucent section.
4. Set the **Offload WMS Database** field to **Yes**, as shown previously in Figure 10.

NOTE

This process will not reboot your switches. See Appendix A, “CLI AOS-W & OV3600 Commands” on page 35on how to utilize AOS-W CLI to enable stats or WMS Offload.

CAUTION

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

Do not enter these commands; these are pushed by 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
```

NOTE

OV3600 will configure SNMPv2 traps with the mobile manager command.

Define OV3600 as Trap Host using AOS-W CLI

To ensure the OV3600 server is defined a trap host, SSH into each switch (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 <OV3600 IP ADDR> version 2c <SNMP
COMMUNITY STRING OF CONTROLLER>
```

NOTE

Ensure the SNMP community matches those that were configured in Chapter 2, “Configuring OV3600 for Global Alcatel-Lucent Infrastructure” .

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

CAUTION

Do not configure the SNMP version to v3 because OV3600 does not support SNMPv3 traps/informs.

AOS-W Traps Utilized by OV3600

The following are Auth, IDS, and ARM traps utilized by OV3600:

Auth Traps

- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimedOut

IDS Traps

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

- wlsxSequenceNumberAnomalySta
- wlsxApFloodAttack
- wlsxInvalidMacOUIAP
- wlsxInvalidMacOUISta
- wlsxStaRepeatWEPIVViolation
- wlsxStaWeakWEPIVViolation
- wlsxStaAssociatedToUnsecureAP
- wlsxStaUnAssociatedFromUnsecureAP
- wlsxAPImpersonation
- wlsxDisconnectStationAttackAP
- wlsxDisconnectStationAttackSta

ARM Traps

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

Ensuring That IDS & Auth Traps Display in OV3600 Using CLI

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

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

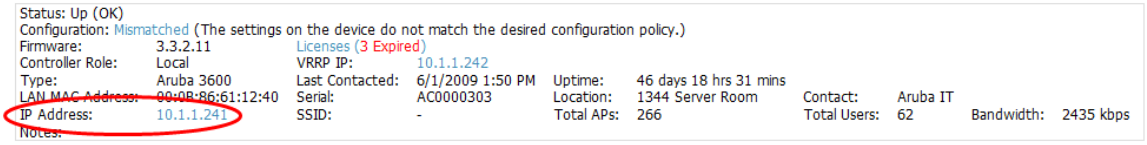
If any of the traps below don't show as enabled enter `configure terminal` mode and issue the following command:

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

See Appendix A, “CLI AOS-W & OV3600 Commands” on page 35 for the full command that can be copied and pasted directly into the AOS-W CLI.

Ensure the source IP of the traps match the IP that OV3600 utilizes to manage the switch, as shown in Figure 11. Navigate to **APs/Devices > Monitor** to validate the IP address in the **Device Info** section.

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



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

```
(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 OV3600 and the switch.

Validate 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/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: 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.

Ensure you disable qlogging after testing as it could negatively impact OV3600 performance if left turned on:

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

Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure

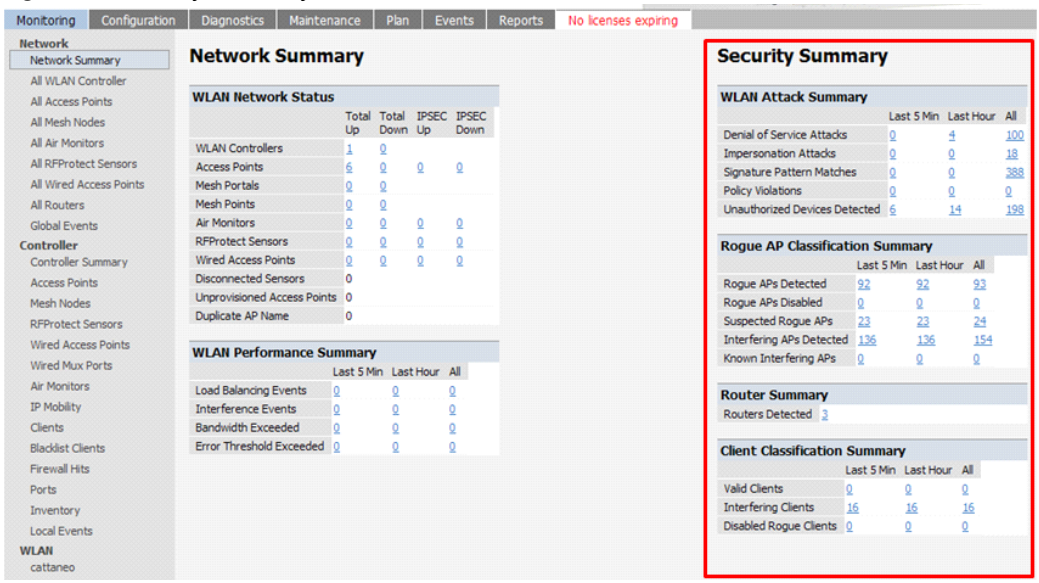
When offloading WMS, it is important to understand what functionality is migrated to OV3600 and what functionality is deprecated.

The following AOS-W tabs and sections are deprecated after offloading WMS:

- **Plan Tab -** where floor plans are stored and heatmaps are generated. Prior to offloading WMS, ensure that you have exported floor plans from AOS-W and imported into OV3600. All functionality within the Plan Tab is incorporated with the VisualRF module in OV3600.
- **Report Tab** - All reports are incorporate within OV3600.
- **Events Tab** - the majority of functionality within this Tab is incorporate within OV3600 Reports and Alerts sections with the exception of:
  - Interference Detected
  - Rogue AP
  - Station Failed
  - Suspected Rogue AP

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. OV3600 does provide the ability to view some of this information in detail and summary form.

Figure 12 *Security Summary on Master Switch*



WLAN Attack Summary

- DOS Attacks - no summary data available in OV3600
- Impersonation Attacks - no summary data available in OV3600
- Signature Pattern Matches - partial summary data available on Home and RAPIDS > Overview pages
- Policy Violations - no summary data available in OV3600
- Unauthorized Devices Detected - no summary data available in OV3600

Rogue AP Classification Summary

- Rogue APs Detected - summary data available on **RAPIDS > Overview**
- Rogue APs Disabled - no summary data available in OV3600
- Suspected Rogue APs - partial data is available in OV3600 on each APs/Devices > Manage page
- Interfering APs Detected - partial data is available in OV3600 on each APs/Devices > Manage page
- Known Interfering APs - partial data is available in OV3600 on each APs/Devices > Manage page

Router Summary

- Routers Detected - no summary data available in OV3600

Client Classification Summary

- Valid Clients - summary data available on all pages in the dashboard
- Interfering clients - no summary data available in OV3600
- Disabled Clients - no summary data available in OV3600

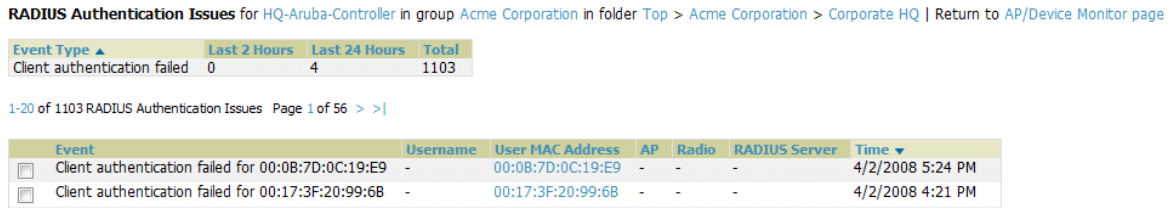
See "Rogue Device Classification" on page 31 for more information on security, IDS, WIPS, WIDS, classification, and RAPIDS.

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

Alcatel-Lucent Traps for RADIUS Auth & IDS Tracking

The authentication failure traps are received by the OV3600 server and correlated to the proper switch, AP, and user. See Figure 13 showing all authentication failures related to a switch.

Figure 13 *RADIUS Authentication Traps in OV3600*



RADIUS Authentication Issues for HQ-Aruba-Controller in group Acme Corporation in folder Top > Acme Corporation > Corporate HQ | Return to AP/Device Monitor page

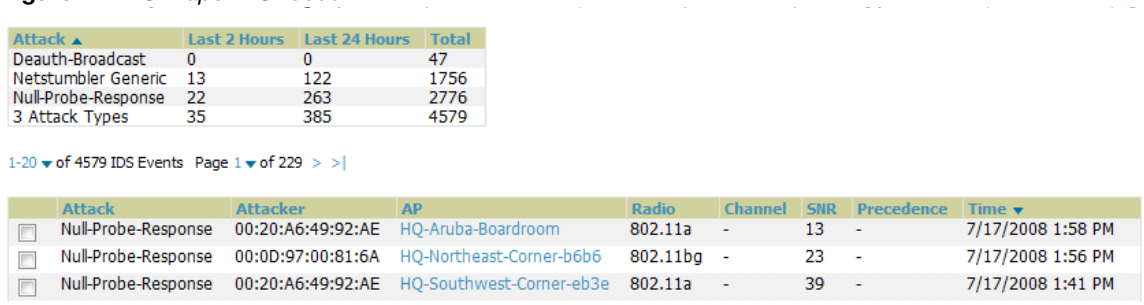
Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Client authentication failed	0	4	1103

1-20 of 1103 RADIUS Authentication Issues Page 1 of 56 > >|

Event	Username	User MAC Address	AP	Radio	RADIUS Server	Time ▼
Client authentication failed for 00:0B:7D:0C:19:E9	-	00:0B:7D:0C:19:E9	-	-	-	4/2/2008 5:24 PM
Client authentication failed for 00:17:3F:20:99:6B	-	00:17:3F:20:99:6B	-	-	-	4/2/2008 4:21 PM

The IDS traps are received by the OV3600 server and correlated to the proper switch, AP, and user. See Figure 14 showing all IDS traps related to a switch.

Figure 14 *IDS Traps in OV3600*



Attack ▲	Last 2 Hours	Last 24 Hours	Total
Deauth-Broadcast	0	0	47
Netstumbler Generic	13	122	1756
Null-Probe-Response	22	263	2776
3 Attack Types	35	385	4579

1-20 ▼ of 4579 IDS Events Page 1 ▼ of 229 > >|

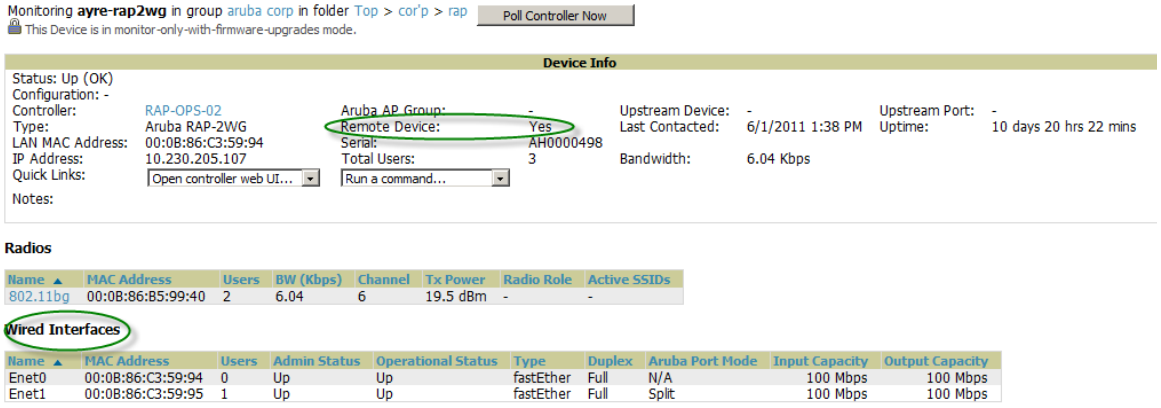
Attack	Attacker	AP	Radio	Channel	SNR	Precedence	Time ▼
Null-Probe-Response	00:20:A6:49:92:AE	HQ-Aruba-Boardroom	802.11a	-	13	-	7/17/2008 1:58 PM
Null-Probe-Response	00:0D:97:00:81:6A	HQ-Northeast-Corner-b6b6	802.11bg	-	23	-	7/17/2008 1:56 PM
Null-Probe-Response	00:20:A6:49:92:AE	HQ-Southwest-Corner-eb3e	802.11a	-	39	-	7/17/2008 1:41 PM

Remote AP Monitoring

To monitor remote APs, follow these steps:

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

Figure 15 *Remote AP Detail Page*



3. You can also see if there are users plugged into the wired interfaces in the Connected Users list.

NOTE

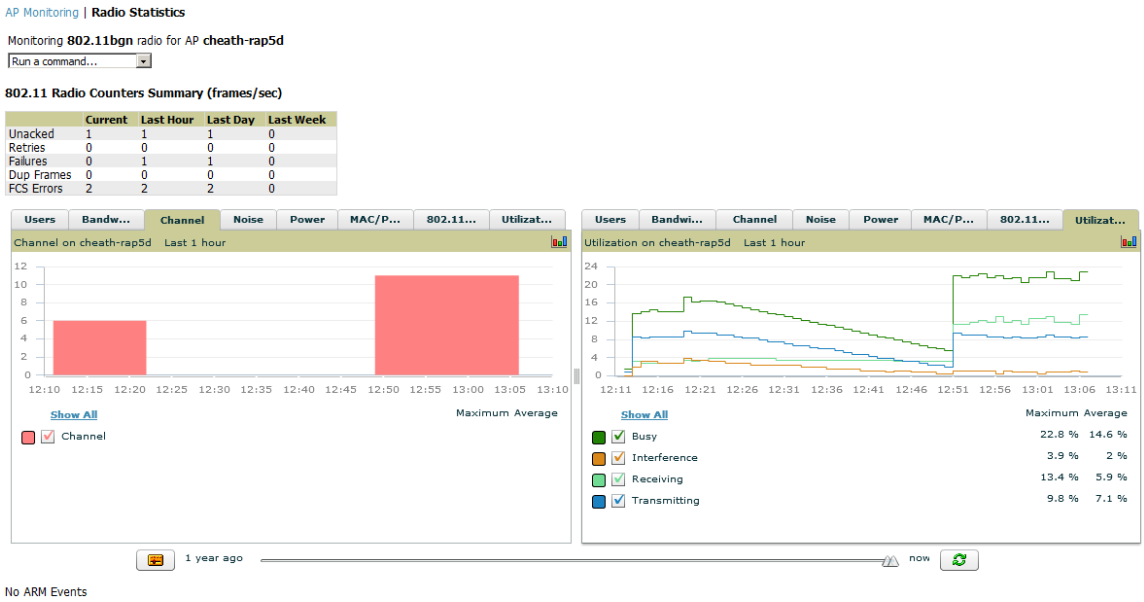
This feature is only available when the remote APs are in split tunnel and tunnel modes.

ARM & Channel Utilization Information

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

1. Navigate to an **APs/Devices > Monitor** page for any of the following Alcatel-Lucent models: AP-105, AP-92, AP-93, AP-124, AP-125, or AP-135.
2. In the **Radios** table, select a radio link under the **Name** column for a radio.

Figure 16 *ARM and Channel Utilization Graphs*



See the *OV3600 7.3 User Guide* in **Home > Documentation** for more information on the data displayed in the **Radio Statistics** page for these devices.

VisualRF and Channel Utilization

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

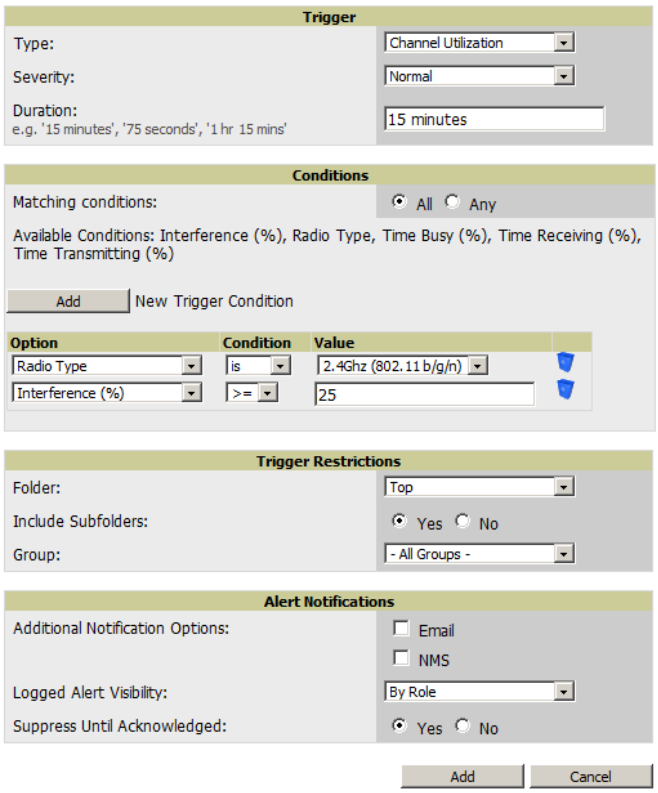
1. Navigate to a floor plan by clicking on the thumbnail on a device's **APs/Devices > Monitor** page or navigating to **VisualRF > Floor Plans** page.
2. Select the **Overlays** menu.
3. Select **Utilization** overlay.
4. Select **Current** or **Maximum** (over last 24 hours).
5. Select total (default), receive, transmit, or interference (see Figure 17).

Figure 17 *Channel Utilization in VisualRF (Interference)*

Configuring Channel Utilization Triggers

1. Navigate to **System > Triggers** and select **Add**.
2. Select **Channel Utilization** from the **Type** drop-down menu as seen on Figure 18:

Figure 18 *Channel Utilization Trigger*



3. Enter the duration evaluation period.
4. Select **Add New Trigger Condition**.
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 *OV3600 7.3 User Guide* in **Home > Documentation** for more details)
8. When finished, select **Add**.

Viewing Channel Utilization Alerts

1. Navigate to **APs/Devices > Monitor** or **System > Alerts**.
2. Sort the **Trigger Type** column and find **Channel Utilization** alerts.

View Channel Utilization in RF Health Reports

1. Navigate to **Reports > Generated**.
2. Find and select a Device Summary or RF Health report.

Figure 19 *Channel Utilization in an RF Health Report*

Most Utilized by Channel Usage (2.4 GHz)

Rank ▲	Device	Channel Busy (%)	Interference (%)	Number of Users	Bandwidth (bps)	Location	Controller
1	AP0018.19bd.b1d0	85.43	83.86	0	14.00	ap lab	wlc 5500
2	AP001d.a1fc.ca7a	85.04	83.86	0	32.00	default location	wlc 5500
3	Cisco-13:21:1E	67.72	59.45	0	4.00	default location	wlc 5500
4	AP10	64.57	63.39	0	24.00	Sales Office-helloX	Cisco4400

Viewing Controller License Information

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

1. Navigate to the **APs/Devices > Monitor** page of a switch under OV3600 management.
2. Select the **License** link in the **Device Info** section. A pop-up window appears listing all licenses.

Figure 20 *License Popup from **APs/Devices > Monitor***

132: Oak Grove Guest Iss

License Table for alpha-local-1:

Service Type ▲	Installed	Expires	Flag	Key
Client Integrity Module	4/29/2005 12:36 PM		E	n9XQpMZN-kUMfht6z-j98lcV0J-TSIKt4In-xA2LlFT0-v58
External Services Interface	4/29/2005 12:35 PM		E	PiF8DrBV-nBXlkp75-+Z8TT2NS-aj4oa8/h-VVm+CxB6-zVU
External Services Interface	4/29/2005 12:34 PM		E	OMsNveDX-W3wEHSKx-TpXkQbHV-NyTb3HAN-OYAi2zNY-V
Indoor Mesh Access Points: 256	10/19/2007 6:54 PM		E	lKwFlaJR-6y8p6rm+-CzOUh7tl-bMhkMA1v-1DV+2m+H-kZE
MMC AP	10/19/2007 6:54 PM		E	WP6JN8l5-y4AoaG9p-P2r7wVTk-/PXV3JgR-C0fcj3d4-LLk
Ortronics Access Points: 256	10/19/2007 6:54 PM		E	+jl6oDRK-PiRXv5nF-l1DMwrDJ-oES1ydXR-4K7sFEHQ-SmU
Outdoor Mesh Access Points: 100	5/2/2007 2:51 PM	Expired		99CSOvuL-jL4Z0YkS-Q8lov2bI-BS+Y0Vxi-YkC9TT0V-5js
Outdoor Mesh Access Points: 256	10/19/2007 6:54 PM		E	RKC/wjVj-fcRQGlDi-K/F8vurv-oYRwgCuG-CsmY7wYh-w18
Outdoor Mesh Access Points: 64	8/1/2007 3:59 PM		E	C5i/bSFb-yVOxff0h-BWWUVEVe-Glb2xz4A-LKcq440D-IXQ
Policy Enforcement Firewall	4/29/2005 12:30 PM		E	vDXRo7pz-Jo8asgU2-HG7w74l+-zzl3yGKu-zZ7w3rJ+-/1I
Remote Access Points: 256	10/19/2007 6:54 PM		E	QnR882W+-o1Kb2XcR-2vrePyl+-J++rWbxh-jtCqjH3h-LPU
Remote Access Points: 48	4/29/2005 12:38 PM		E	5zz7c0jO-LpDgDbLH-4bEnzNbg-p/oEnS2a-nTtHaS8t-ms0
Voice Services Module	10/19/2007 6:54 PM		E	Lj/ByOfs-wMdJU3Xv-5djAkCIJ-vJ9zRok3-sWZ4Z2bn-aH4
VPN Server	4/29/2005 12:32 PM		E	SOKR1Sa8-KKMjj/Gv-HlcJcwaK-uEZuPvcs-c/LIzjg0-2iE
Wireless Intrusion Protection	4/29/2005 12:33 PM		E	xVc/llqw-Os1ei+yL-b1CqzoTr-UwGp2OAi-LD6wHOW2-qSw
xSec Module	4/29/2005 12:37 PM		E	ukxUwAcB-PE+GeyB9-7u7IMtQ1-CaibELI2-LuqdRsqA-fac

Rogue Device Classification

Only complete this section if you have completed WMS Offload procedure above. After offloading WMS, OV3600 maintains the primary ARM, WIPS, and WIDS state classification for all devices discovered over-the-air.

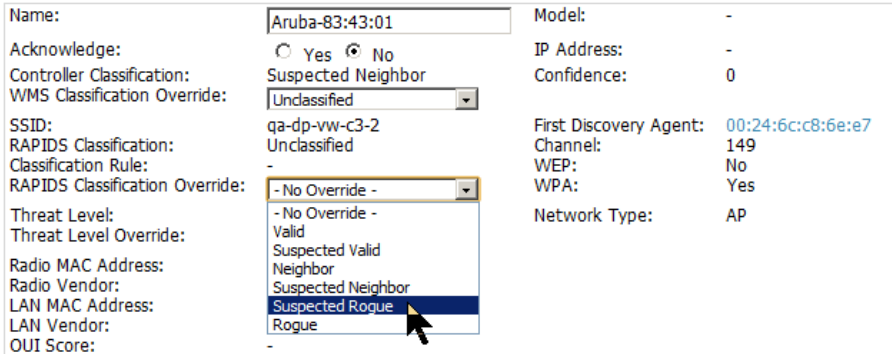
Table 7 *WIPS/WIDS to OV3600 Controller Classification Matrix*

OV3600 Controller Classification	AOS-W (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, follow these steps:

1. Navigate to the **Rogue > Detail** page for the rogue device, as shown in Figure 21.

Figure 21 *Rogue Detail Page Illustration*



2. Select the proper classification from the **RAPIDS Classification Override** drop-down menu.

Caution: Changing the switch's classification within the OV3600 UI 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 UI to unclassified.

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

All rogue devices will be set to a default 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 UI and propagated to switches that OV3600 manages. The device classification reflected in the Controller's UI and in the OV3600 UI will probably not match, because the Controller/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 8 *ARM to OV3600 Classification Matrix*

OV3600	AOS-W (ARM)
Unclassified (default state)	Unknown
Valid	Valid
Contained	DOS

1. Navigate to the **Users > User Detail** page for the user.
2. Select the proper classification from the **Classification** drop-down menu as seen in Figure 22:

Figure 22 *User Classification*

CAUTION

Caution: Changing User Classification within the OV3600 UI 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 OV3600 UI and propagated to switches that OV3600 manages. It is probable that the user's classification reflected in the Controller's UI and in the OV3600 UI will not match, because the Controller/APs do not reclassify users frequently.

There is no method in the OV3600 UI to update user classification on mass to match the switch's classification. Each client must be updated individually within the OV3600 UI.

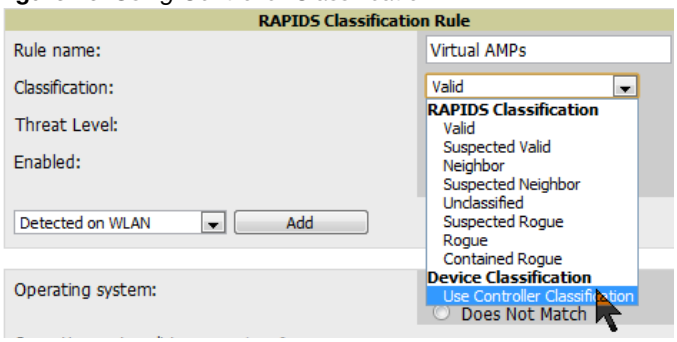
Rules-Based Controller Classification

Using RAPIDS Defaults for Controller Classification

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

1. Navigate to **RAPIDS > Rules** and select the pencil icon for a rule.
2. In the **Classification** drop-down menu, select **Use Controller Classification** as seen in Figure 23.
3. Select **Save**.

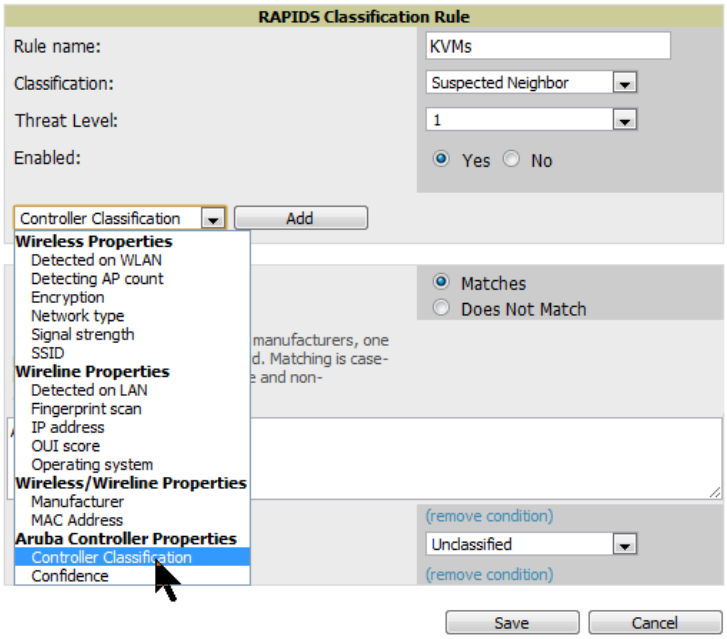
Figure 23 *Using Controller Classification*



Changing RAPIDS based on Controller Classification

1. Navigate to **RAPIDS > Rules**.
2. In the **Classification** drop-down menu, select desired RAPIDS classification.
3. Select **Controller Classification** from drop-down menu, as shown in Figure 24.

Figure 24 *Configure Rules for Classification*



4. Select **Add**.
5. Select desired switch classification to use as an evaluation in RAPIDS.
6. Select **Save**.

Enable Channel Utilization Events Utilizing AOS-W CLI (Local and Master Switches)

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

SSH into the switch, 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) # mgmt-server type amp primary-server <OV3600 IP>
(Controller-Name) (config) # write mem
```

Enable Stats With the AOS-W CLI (Local Controller in Master Local Environment)

Do not use these commands if using OV3600 GUI.

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

SSH into the switch, 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
```

Offload WMS Utilizing AOS-W CLI and OV3600 CLI (SNMP Walk)

Do not use these commands if using OV3600 GUI.

AOS-W CLI

SSH into all switches (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 <OV3600 IP> user <MMS-USER> <MMS-SNMP-
PASSWORD> trap-version 2c
```

This command creates an SNMPv3 user on the switch 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 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 & Authentication passwords are the same.

This command also creates the OV3600 server as an SNMPv3 Trap Host in the switch's running configuration.

Sample: `mobility-manager 10.2.32.1 user airwave123 airwave123`

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

OV3600 SNMP

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

Do not use these commands if using OV3600 GUI.

```
[root@OV3600 ~]# snmpwalk -v3 -a SHA -l AuthPriv -u <MMS-USER> -A <MMS-SNMP-PASSWORD> -
X <MMS-SNMP-PASSWORD> <Alcatel-Lucent CONTROLLER IP ADDRESS> 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.

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

If you do not use OV3600 GUI 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.

Ensuring Master Switch Pushes Config to Local Controllers Utilizing AOS-W CLI

Do not use these commands if using OV3600 GUI.

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

This command ensures configuration changes made on the master switch will propagate to all local switches.

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

Disable Debugging Utilizing 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 switches CPU, so it is highly recommended to disable debugging.

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

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

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

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

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

Restart WMS on Local Controllers Utilizing AOS-W CLI

To ensure local switches are populating rogue information properly, SSH into each local switch, 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
```

You will need to wait until the next Rogue Poll Period to execute a Poll Now for each local switch to see rogue devices begin to appear in OV3600 after executing `restart wms` in AOS-W.

Configure AOS-W CLI when not Offloading WMS to OV3600 (AOS-W 6.0 & GT)

To ensure proper event correlation for IDS events when WMS if not offloaded to OV3600, SSH into each switch (Master and Local), enter "enable" mode, and issue the following commands:

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

Copy & 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 after entering “enable” mode and issuing the configure terminal command:

```
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

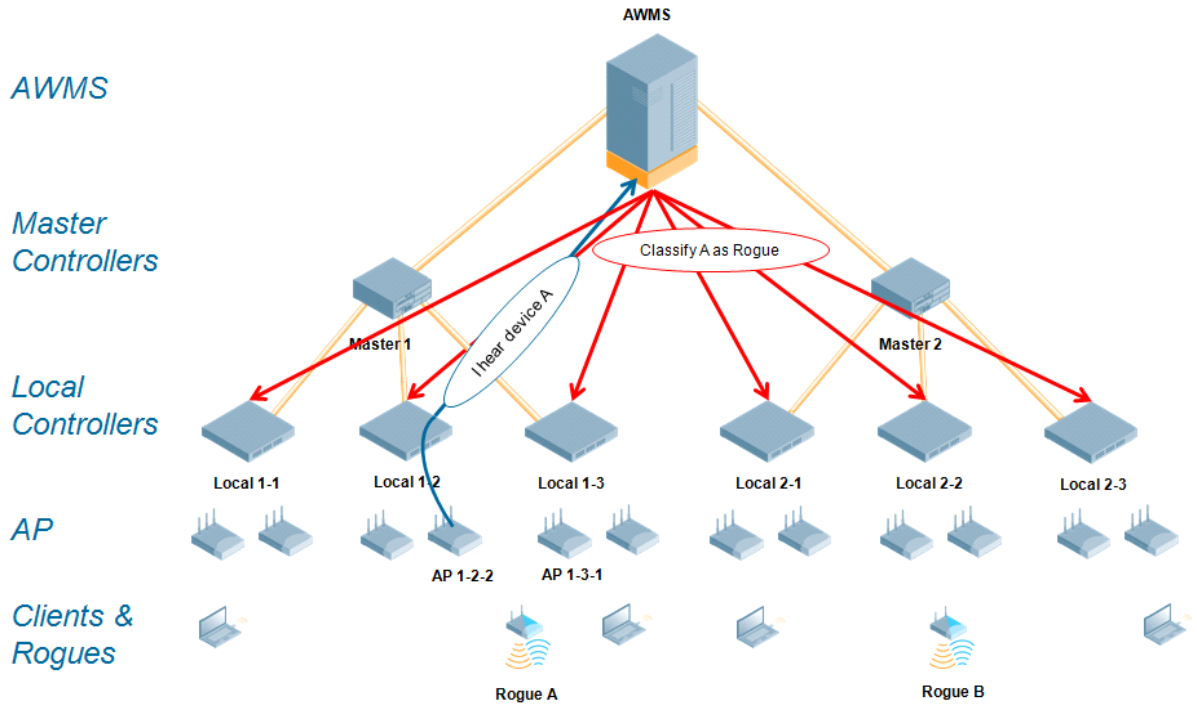
You will need to issue the **`write mem`** command.

Table 9 *How OV3600 Acquires Data from Alcatel-Lucent Devices*

Data Elements	Controller/Thin AP						Alcatel-Lucent Instant
	SNMP MIB	SNMP Traps	AMON	CLI/SSH	WMS Offload	RTLS	HTTPS
Configuration interface							
Device configuration/audit				X			X
User and client interfaces							
Assoc/auth/roam	X	X					X
Bandwidth	X						X
Signal quality	X					X	X
Auth failures		X					*N/A*
AP/radio interfaces							
CPU & memory utilization	<----------N/A---------->						X
Bandwidth	X						X
Transmit Power	X						X
Channel utilization			X				X
Noise floor	X						X
Frame rates	X						X
Error counters	X						X
Channel summary				X			*N/A*
ARM events		X					*N/A*
Active interferers			X				*N/A*
Active BSSIDs/SSIDs	X						X
Security							
IDS events		X					*N/A*
Neighbors/rogues	X				X		X
Neighbor re-classification				X	X		*N/A*
Client classification					X		*N/A*
User de-auth				X			*N/A*

WMS Offload instructs the Master switch to stop correlating ARM, WIPS, and WIDS state information amongst its Local switches, because OV3600 will assume this responsibility. Figure 25 depicts how OV3600 communicates state information with Local switches.

Figure 25 *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 the OV3600.
3. OV3600 receives message and re-classifies the device if necessary and reflects this within OV3600 GUI 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 displays a BSSID table for each rogue that displays the desired classification and the classification on the device.

Benefits of using OV3600 as 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 Alcatel-Lucent infrastructure interoperates 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.

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.

Table 10 *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, Alcatel-Lucent WLAN infrastructure and Alcatel-Lucent's RTLS feed for more accurately locating wireless clients and WiFi Tags.

Deployment Topology

Figure 26 *Typical Client Location*

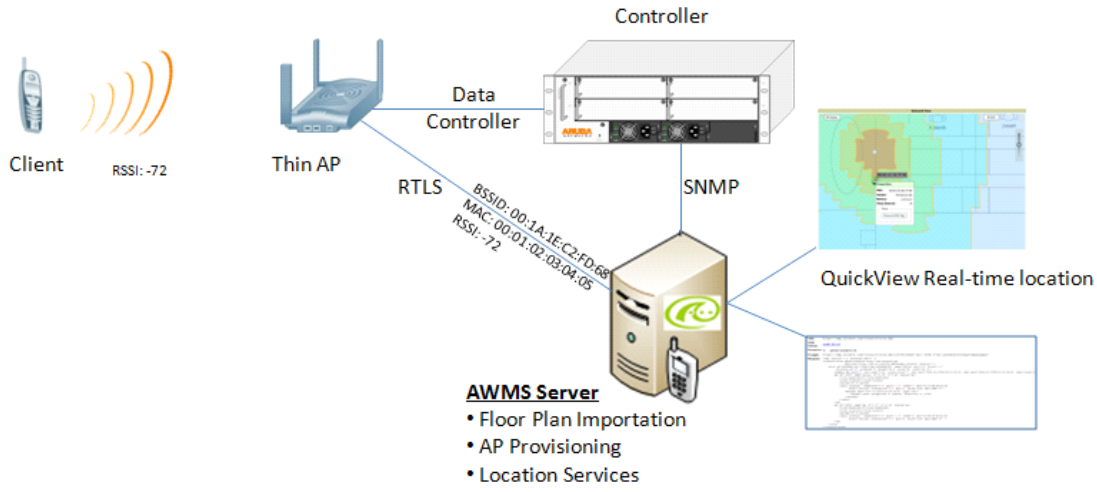
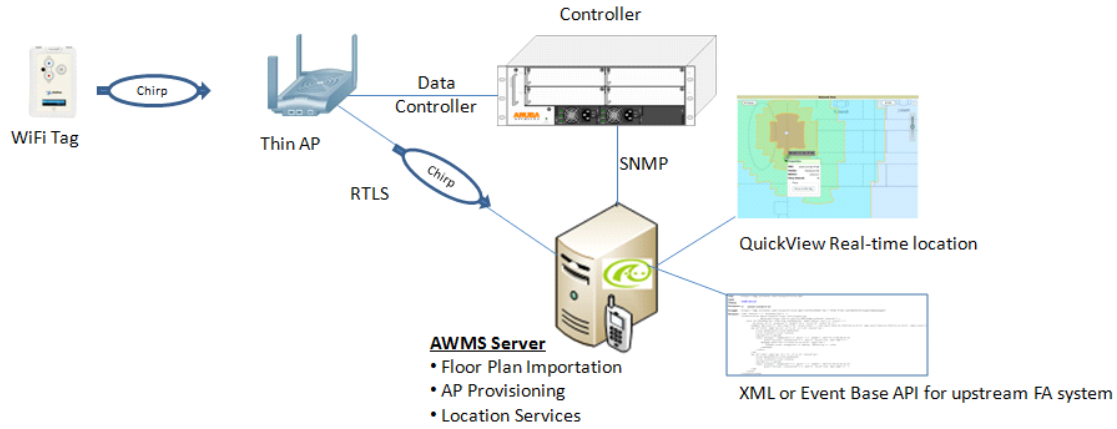


Figure 27 *Typical Tag Deployment*



Prerequisites

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

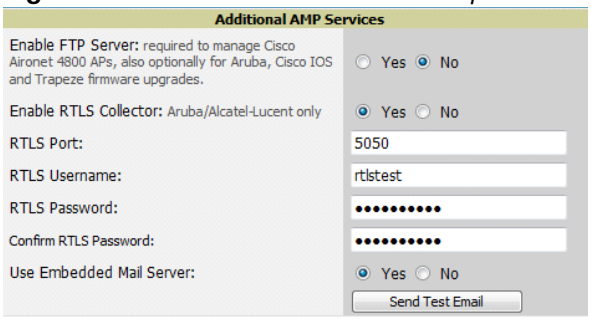
- Ensure OV3600 server is already monitoring Alcatel-Lucent infrastructure
- Ensure WMS Offload process is complete
- Ensure firewall configuration for port 5050 (default port) supports bidirectional UDP communication between the OV3600 server's IP address and each access point's IP address

Enable RTLS service on the OV3600 server

To enable RTLS service on the OV3600 server, follow these steps:

1. Navigate to **OV3600 Setup > General** and locate the **OV3600 Additional Services** section
2. Select **Yes** to Enable RTLS Collector.
3. A new section will automatically appear with the following settings:
   - **RTLS Port** - match switch default is 5050
   - **RTLS Username** - match the SNMPv3 MMS username configured on switch
   - **RTLS Password** - match the SNMPv3 MMS password configured on switch

Figure 28 *RTLS Fields in OV3600 Setup > General*



4. Select **Save** at the bottom of the page.

Enable RTLS on Switch

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

SSH into master switch, 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 OV3600
SERVER> port 5050 key <SNMPv3 MMS PASSWORD CONFIGURED ON CONTROLLER>

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

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 OV3600 server. SSH into your OV3600 server.

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

or

Navigate to **System > Status** and look for the RTLS service, as shown in

Figure 29 *RTLS System Status*

RFprotect Detection	OK	/var/log/sensor_rf_detection
Rogue Filter	OK	/var/log/rogue_filter
RTLS Collector	OK	/var/log/rtls
Sensor Discovery	OK	/var/log/sensor_discovery

Check the RTLS log file to ensure Tag chirps are making it to the OV3600 server. SSH into your OV3600 server.

```
[root@AMPServer]# logs

[root@AMPServer]# tail rtls

payload:
00147aaf01000020001a1ec02b320000000100000137aae0100000c001a1ec02b320000001a1e82b32259
0006ddff02

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:
0014c9c90100003c001a1ec0507800000002000000013c9c70100000c001a1ec050780000000d54a7a28054
0001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02

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:
0014c9c90100003c001a1ec0507800000002000000013c9c70100000c001a1ec050780000000d54a7a28054
0001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006c4ff02
```

Ensure chirps are published to Airbus by snooping on proper topics

```
[root@OV3600 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://<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 (3) access points from any given location. The recommended setting is 4 for best results.
- Ensure that the tags chirp on all regulatory channels.