®

Alcatel·Lucent

Alcatel-Lucent Best Practices Guide
OV3600 6.4

www.alcatel-lucent.com/enterprise
Part Number: 0510643-01

Table of Contents

1 - Overview

This document provides best practices for leveraging the OmniVista Air Manager (OV3600) to monitor and manage your Alcatel-Lucent infrastructure. Alcatel-Lucent wireless infrastructure provides a wealth of functionality (firewall, VPN, remote AP, IDS, IPS, and ARM) as well as an abundance of statistical information. Follow the simple guidelines in this document to garner the full benefit of Alcatel-Lucent ’s infrastructure.

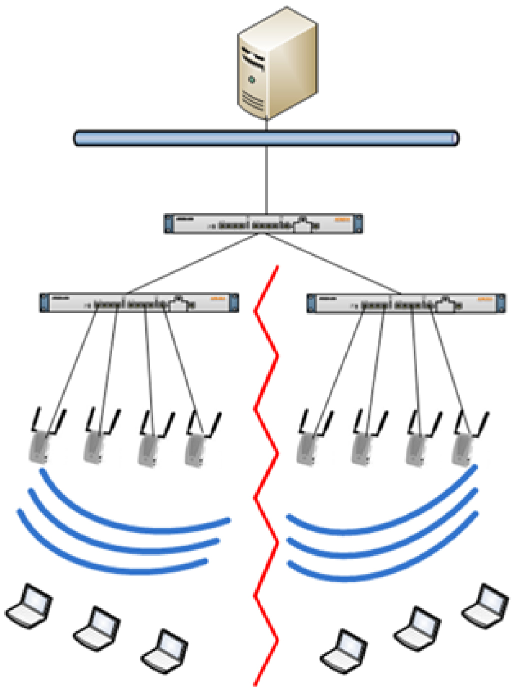
Minimum Requirements

- OV3600 version 6.0 or higher
- AOS-W 3.x or higher

Understanding Alcatel-Lucent Topology

Here is a typical Master-Local deployment.

Figure 1 – Typical Alcatel-Lucent Deployment



Component	Without OV3600	With OV3600
OV3600		OV3600 communicates directly with local and master switches to gather and correlate statistics
Master Switch	Correlates all state information from all downstream access points	Functions as a local switch
Local Switches	Collect downstream AP statistical information	Collect downstream AP statistical and state information
Alcatel-Lucent Devices	Send all state information to the Master Controller	Send all state information to Local WLAN Switch

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

1.1 - 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)

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

- SNMPv3 credentials (wms offload only)
  - Username
  - Auth password
  - Privacy password
  - Auth protocol

1.2 - Known and Recently Resolved Issues

AOS-W Impact	OV3600 Impact Ver.	Description	Resolution
3.3.x	6.x	11n client BW OIDs resetting very frequently under heavy load. This results in AMWS reporting inflated BW usage.	Fixed in AOS-W 3.3.2.17 & OV3600 6.3
3.3.x	6.x	Encryption type is not populated for wireless users.	Fixed in AOS-W 3.4 & OV3600 6.4
3.3.1		Can't create an SNMPv3 and management user with the same name on a switches.	
3.3.x		Reduced accuracy when locating clients, because of improper neighbor and client SNR values.	Fixed in AOS-W 3.3.2.6 & OV3600 6.0.9
	5.3 – 6.x	When two wireless users appear on the switch's UI with the same MAC (VMware, Parallels, or VPN) OV3600 displays only one user, but flip flops between IP addresses.	ETA 7.0
3.3.2.x	6.1 – 6.2	Switch MIB indicates radio down when the radios are actually up.	Fixed in AOS-W 3.3.2.13 & OV3600 6.1
3.3.x	All	AOS-W improperly initializes engine_id in SNMPv3 informs.	Fixed in AOS-W 3.4.x, 3.3.2 FIPS OV3600 7.0
3.3.x	All	When deleting virtual APs (SSIDs) AP's and Radios disappear when device is in Air Monitor Mode.	Fixed AOS-W 3.3.2.14 & OV3600 6.2
3.3.x	All	MIB reports incorrect switch port for APs	Removed from OV3600 UI in 6.3 AOS-W – no ETA for fix
3.3.x	6.3	wms offload caused SNMP inform queue on switch to overflow.	Fixed in AOS-W 3.3.2.14 & OV3600 6.3
3.3.x	6.x	When aggressive key caching is enabled in AOS-W users may show in OV3600 associated to wrong AP.	Fixed in AOS-W 3.3.2.17 & OV3600 6.3
3.3.x	6.x	After enabling wms offload and running the command 'show wms general' which shows wms is offloaded the local switches do not send stats to OV3600 server.	Fixed in AOS-W 3.3.2.14 & OV3600 6.2 See **Appendix A** for work around prior to 3.3.2.14 for restarting wms on local switches.
3.3.x	6.3	`show user-table` command in AOS-W reports different user totals than OV3600 displays in the UI. `show user-table` shows wired and wireless users as well as duplicative IP	ETA AOS-W fix in 4.1

AOS-W Impact	OV3600 Impact Ver.	Description	Resolution
		addresses for the same user. AMWS only shows 1 user/IP per MAC and only wireless users associated to the WLAN.	
3.3.x	6.3	If you are using OV3600 templates to configure your switches, there are some settings pushed from the Master to Local switches that are not written into startup config which causes OV3600 mismatches after pushing a change from OV3600.	Execute `write mem` on each local switch or Convert to OV3600 GUI Confg No ETA in AOS-W
3.3.2.x		Authentication failure trap “wlsx**N**UserAuthenticationFailed” only fires in AOS-W when trap “wlsxUserAuthenticationFailed” is also enabled.	Enable non “N” trap in AOS-W No ETA in AOS-W

1.3 - Alcatel-Lucent Feature Implementation Schedule for OV3600

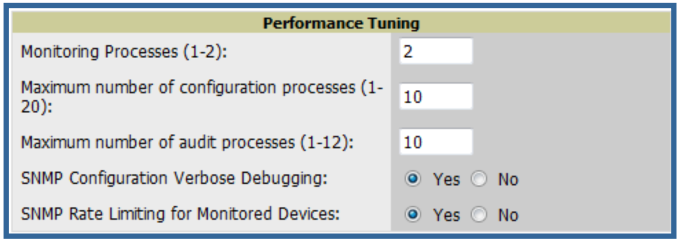
Feature	OV3600 Implementation
Automated WMS offloading	6.1
Support for monitoring Remote AP wired users	6.1
Support for Guest Provisioning (pre 3.4 settings)	6.1
Mesh monitoring and visualization support	6.1
Ability to import floor plans from Alcatel-Lucent Switches	6.1
Support device coordination amongst switches for WIPS/WIDS	6.2
Support device coordination amongst switches for ARM	6.2
Ability to provision AMs	6.2
Ability to send ARM/WIPS/WIDS classification to switches	6.2
Ability to support AP based RTLS and WiFi Tags in VisualRF	6.2
Support for AOS-W 3.3.2.x	6.2
Support for RAP-5WN & RAP-5	6.2
Auto ARM/WIPS/WIDS classification distributed to switches	6.3
Support for AP-65-WB, RAP-2WG	6.3
AOS-W GUI configuration support for Profiles and AP Groups	6.3
Show user cipher type	6.4
Support for 600 series Branch Office infrastructure	6.4
Support for AP-105	6.4
Support per radio AM monitoring	6.4
Support for AOS-W 3.3.3, 3.4, and 3.4.1	6.4
Replace RF Plan with VisualRF Plan	6.4
Standardized dashboard, navigation, and graphs with AOS-W	6.4
Support switch based RTLS and WiFi Tag history in OV3600	7.1

2 - Configure OV3600 to Optimally Manage Alcatel-Lucent Infrastructure (Global)

2.1 - OV3600 Setup General Page (Rate Limiting)

There are several SNMP tuning parameters which must be configured in order for OV3600 to properly monitor Alcatel-Lucent infrastructure

Figure 2 – SNMP Rate Limiting



Performance Tuning

Monitoring Processes (1-2):	2
Maximum number of configuration processes (1-20):	10
Maximum number of audit processes (1-12):	10
SNMP Configuration Verbose Debugging:	◉ Yes ○ No
SNMP Rate Limiting for Monitored Devices:	◉ Yes ○ No

- Navigate to **OV3600 Setup → General** page
- Locate the **Performance Tuning** section
- Enable SNMP Rate Limiting for Monitored Devices

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

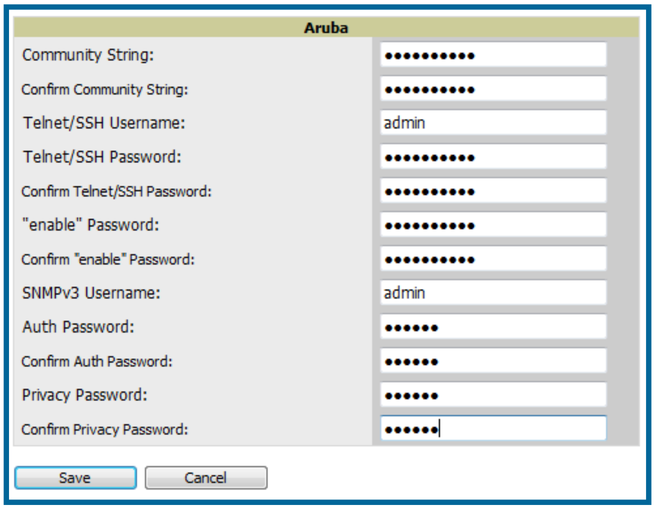
2.2 - Device Setup Communication Page (Credential & Timing)

Credentials

OV3600 requires several credentials to properly interface with Alcatel-Lucent infrastructure. The Discover process detailed in Section 3 requires proper global credential configuration.

- Navigate to **Device → Setup Communication** page
- Locate the **Default Credentials** section
- Click on the Alcatel-Lucent link

Figure 3 – Credential Setup



Aruba

Community String:	••••••••••
Confirm Community String:	••••••••••
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••
SNMPv3 Username:	admin
Auth Password:	••••••
Confirm Auth Password:	••••••
Privacy Password:	••••••
Confirm Privacy Password:	••••••

Required Fields for Discovery

- Enter SNMP Community String

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

Required Fields for Configurations and Basic Monitoring

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

Additional Required Fields for WMS Offload

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

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

Prior to OV3600 6.3 SMNPv3 Auth Protocol was a configurable option. In OV3600 6.3 and later OV3600 automatically configures the Auth Protocol to SHA.

- SNMPv3 Auth Protocol (Applicable to OV3600 6.2 and earlier)

  *Note: Auth Protocol **must** be configured to use **SHA**.*

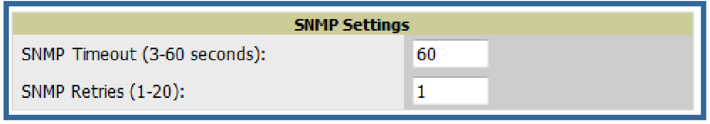
  Warning: If you are using SNMPv3 and the switch's date/time is incorrect, the SNMP agent will not respond to SNMP requests from OV3600 SNMP manager. This will result in the switch and all of its downstream access points showing down in OV3600.

  Leveraging NTP for your Alcatel-Lucent infrastructure and your OV3600 server is recommended to ensure time synchronization.

Timeout & Retries

- Locate the **SNMP Setting** settings
- Change SNMP Timeout setting to "60"
- Change SNMP Retries to "1"

Figure 4 – SNMP Time & Retries



SNMP Settings

SNMP Timeout (3-60 seconds):	60
SNMP Retries (1-20):	1

3 - Creating an Alcatel-Lucent Specific Policy (Group) in OV3600

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

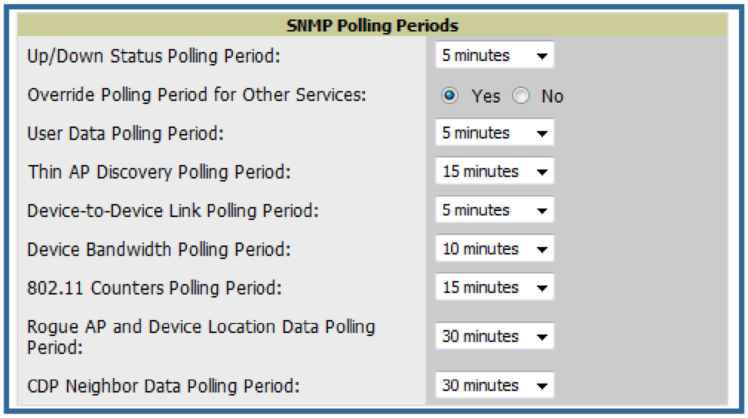
3.1 – Basic Monitoring Configuration

- Navigate to **Groups → List** page
- Click the “Add” button
- Enter a Name that represents the Alcatel-Lucent infrastructure from a security, geographical, or departmental perspective and click the “Add” button
- You will be redirected to **Group → Basic** page for the Group you just created. On this page you will need to tweak a few Alcatel-Lucent -specific settings.
- Find the **SNMP Polling Periods** section of the page
    - Change Override Poll Period for Other Services to “Yes”
    - Ensure User Data Polling Period is set to “10 minutes”

      Do not configure this interval lower tha

      Note: Enabling the SNMP Rate Limiting for Monitored Devices option above adds a small delay between each SNMP Get request, thus the actual polling interval is 12 minutes for 10 minute polling interval.
    - Change Device-to-Device Link Polling Period to “30 minutes”
    - Change Rogue AP and Device Location Data Polling Period to “30 minutes”.

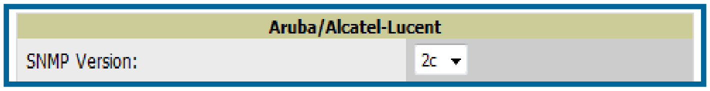
Figure 5 – Group Polling Configuration



SNMP Polling Periods	
Up/Down Status Polling Period:	5 minutes
Override Polling Period for Other Services:	● Yes ○ No
User Data Polling Period:	5 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	5 minutes
Device Bandwidth Polling Period:	10 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

- Find the **Alcatel-Lucent /Alcatel-Lucent** section of page
    - Configure the proper SNMP version for monitoring the Alcatel-Lucent infrastructure.
    - The other options in this section are addressed later in this document or in the AOS-W Configuration Guide.
- Click the “Save and Apply” button

Figure 6 – Group SNMP Version for Monitoring



Aruba/Alcatel-Lucent	
SNMP Version:	2c

Note: You should reference the Alcatel-Lucent Configuration Guide for additional information on Policy configuration.

3.2 – Configuration

Reference the AOS-W Configuration Guide for detailed instructions.

4 - Discovering Alcatel-Lucent Infrastructure

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

Prerequisites for discovery:

- Section 2 - credentials
- Section 3 – creating Alcatel-Lucent policies (Groups)

Summarized procedure for discovery and managing Alcatel-Lucent Infrastructure:

- Discover Master switches
- Manage Master switches which automatically discovers Local switches affiliated with the Master switch
- Manage Local switches which automatically discovers Thin APs affiliated to the Local switches
- Manage Thin APs

Note: 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.*

4.1 - Master Switch Discovery

- Scan networks containing Alcatel-Lucent Master switches from **Device → Discover** page. This will use your Global Credentials configured in the previous section.

  - or -

- Manually enter the Master switch on the **Device → Add** page.
  - Select the switch type and click “Add” button
  - Enter IP Address

  Required Fields for Discovery

  - Enter SNMP Community String

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

  Required Fields for Configurations and Basic Monitoring

  - Enter Telnet/SSH Username
  - Enter Telnet/SSH Password
  - Enter “enable” Password

  Additional Required Fields for WMS Offload

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

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

Prior to OV3600 6.3 SMNPv3 Auth Protocol was a configurable option. In OV3600 6.3 and later OV3600 automatically configureS the Auth Protocol to **SHA**.

- SNMPv3 Auth Protocol (Applicable to OV3600 6.2 and earlier)

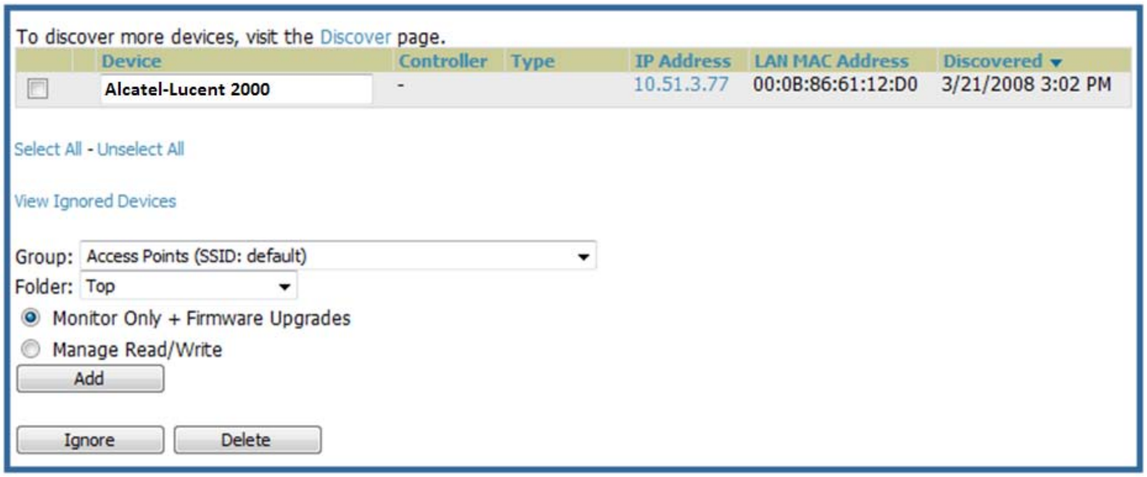
  *Note: Auth Protocol **must** be configured to use **SHA**.*

  Warning: 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 down in OV3600.

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

- Navigate to **APs/Devices → New** page
  - Select the Alcatel-Lucent master switch
  - Ensure "Monitor Only" option is selected
  - Click the "Add" button

Figure 7 – Add New Switch



To discover more devices, visit the Discover page.

	Device	Controller	Type	IP Address	LAN MAC Address	Discovered ▾
□	Alcatel-Lucent 2000	-		10.51.3.77	00:0B:86:61:12:D0	3/21/2008 3:02 PM

Select All - Unselect All

View Ignored Devices

Group: Access Points (SSID: default)

Folder: Top

● Monitor Only + Firmware Upgrades

○ Manage Read/Write

4.2 – Local Switch Discovery

- Local switches are discovered via the Master switch. After waiting for the Thin AP Polling Period or executing a "Poll Now", the Local switches will appear on the **APs//Devices → New** page. "Poll Now" button is located on the **Device → Monitoring** page.
- Add the Local switch to Group defined above. Within OV3600 Local switches can be split away from the Master switch's Group.

4.3 - Thin AP Discovery

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

5 - OV3600 and Alcatel-Lucent Integration Strategies

Integration Goals	All Masters Architecture	Master Local Architecture
Rogue & Client Info		enable stats
Rogue & Client Mitigation	wms offload	wms offload
Reduce Master Switch Load		wms offload debuging 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

Key Integration Points:

- IDS Tracking does **not** require "wms offoad" 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.

5.1 - Example Use Cases

Example of When to Use Enable Stats

- Customer wants to pilot AMWS and doesn't want to make major configuration changes to their infrastructure or manage configuration from OV3600.

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

Examples of When to Use WMS Offload

- Customer has older Alcatel-Lucent infrastructure in 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.
- Customer is replacing MMS with OV3600 and already had WMS offloaded for performance reasons.
- Customer wants 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

Examples of When to Use RTLS

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

Note: RTLS could negatively impact your OV3600 server's performance.

Example to Define OV3600 as Trap Host

- Customer wants to track IDS events within the OV3600 UI.
- Customer is in the process of converting their older 3rd Party WLAN devices to Alcatel-Lucent and wants a unified IDS dashboard for all WLAN infrastructure.
- Customer wants to relate Auth failures to a client device, AP, Group of APs, and switch. OV3600 provides this unique correlation capability.

5.2 - Prerequisites for Integration

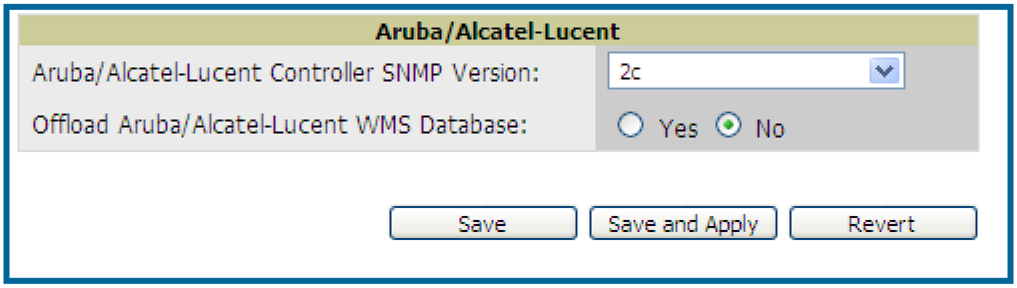
If you have not discovered the Alcatel-Lucent infrastructure or configured credentials, proceed to Sections 3 and 4 of this document.

5.3 - Enable Stats Utilizing OV3600 GUI

To enable stats on the Alcatel-Lucent switches:

- Navigate to **Groups→Basic** page
- Locate the Aruba/Alcatel Lucent section
- Disable "Offload Aruba/Alcatel-Lucent WMS Database
- Click "Save and Apply" button

Figure 8 – Enable Stats



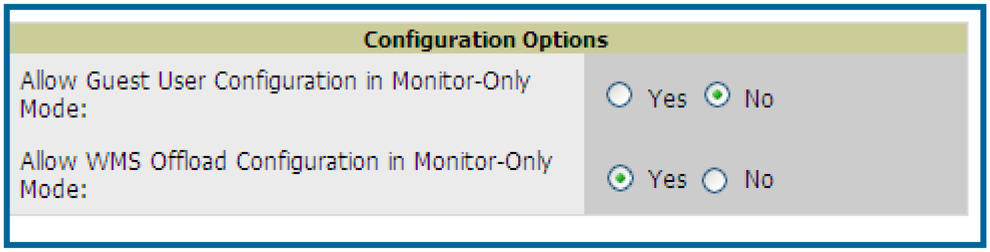
Aruba/Alcatel-Lucent

Aruba/Alcatel-Lucent Controller SNMP Version: 2c

Offload Aruba/Alcatel-Lucent WMS Database: ○ Yes ● No

- Navigate to **OV3600 Setup → General** page
- Locate Configuration Options section
- Enable "Allow WMS Offload Configuration in Monitor-Only Mode"
- Click the "Save" button

Figure 9 – WMS Offload Configuration Options (enable stats)



Configuration Options

Allow Guest User Configuration in Monitor-Only Mode: ○ Yes ● No

Allow WMS Offload Configuration in Monitor-Only Mode: ● Yes ○ No

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. See **Device Setup Communication Section** below for help configuring your device credentials.

Note: This process will not reboot your switches.

Warning: 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 on how to utilize AOS-W CLI to enable stats on Alcatel-Lucent infrastructure.

*Note: If your credentials are invalid or the changes are not applied to the switch, error messages will display on the switch's **Device → Monitoring page** under the **Recent Events** section. If the change fail, OV3600 does not audit these setting (display mismatches) and you will need to apply to the switch by hand, see Appendix A for detailed instructions.*

Commands Pushed by OV3600 during Enable Stats **(Do not enter these commands)**

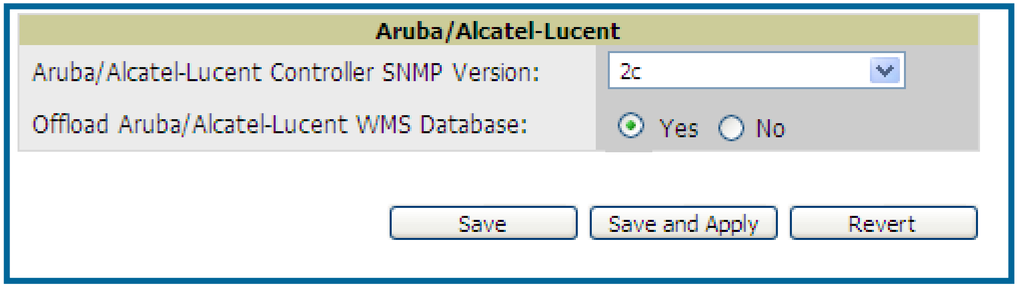
```
configure terminal
no mobility-manager <Active WMS IP Address>
wms
general collect-stats enable
stats-update-interval 120
show wms general
write mem
```

5.4 - WMS Offload Utilizing OV3600 GUI

To Offload WMS on the Alcatel-Lucent switches:

- Navigate to **Groups→Basic** page
- Locate the Aruba/Alcatel Lucent section
- Enable "Offload Aruba/Alcatel-Lucent WMS Database
- Locate the Configuration section
- Enable or Disable "Allow WMS Offload Configuration in Monitor-Only Mode"
- Click "Save and Apply" button

Figure 10 – Offload WMS



Aruba/Alcatel-Lucent

Aruba/Alcatel-Lucent Controller SNMP Version: 2c

Offload Aruba/Alcatel-Lucent WMS Database: ● Yes ○ No

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 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.

Note: This process will not reboot your switches. See Appendix A on how to utilize AOS-W CLI to enable stats or wms offload.

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

*Note: Auth Protocol **must** be configured to use **SHA**.*

Commands Pushed by OV3600 during WMS Offload **(Do not enter these commands)**

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

Note: In AOS-W 3.3.2.14 and later versions OV3600 will configure SNMPv2 traps with the mobile manager command.

Other Processes for wms offload

OV3600 will issue an SNMPGet on table (wlsxSysExtHostname) to complete the offload process (OID=.1.3.6.1.4.1.14823.2.2.1.2.1.2.0.)

Diagnostic Steps if you are not seeing Rogue devices appear in OV3600 in AOS-W versions prior to 3.3.2.14

- If you are able, upgrade to latest 3.3.x or 3.4 AOS-W version and it will automatically resolve this issue.

- or -

- Ensure “Is Master” flag is not enabled on local switches, SSH into each local switch, enter “enable” mode, and issue the following commands:

```
(Switch-Name) # show wms general

General Attributes
------------------
Key                            Value
---                            -----
poll-interval                  60000
poll-retries                   3
ap-ageout-interval             30
sta-ageout-interval            30
learn-ap                       disable
persistent-known-interfering   enable
propagate-wired-macs           enable
stat-update                    enable
collect-stats                  enable
classification-server-ip       10.2.32.3
rtls-port                      8000
wms-on-master                  disable
use-db                         disable
calc-poll-interval             60000
Switch IP                      10.51.5.109
Is Master                      enable
```

If the “Is Master” flag is enabled as shown above and you are not able to upgrade your AOS-W, use the following instructions to resolve the issue.

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

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

Note: This command will need to be reissued after each configuration change from the Master Switch.

5.5 - 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:

```
(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>
```

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

```
(Switch-Name) (config) # snmp-server trap source <SWITCH’S IP>

(Switch-Name) (config) # write mem

Saving Configuration...

Saved Configuration
```

Warning: Do not configure the SNMP version to v3. OV3600 does not support SNMPv3 traps/informs because of an outstanding issue on AOS-W firmware related to the initialization of engine_id. This will cause SNMP Inform queue on switch to overflow in AOS-W versions prior to AOS-W 3.4.

- AOS-W Traps utilized by OV3600

Auth Traps Utilized by OV3600

- wlsxNUserAuthenticationFailed
- wlsxUserAuthenticationFailed

  OV3600 does not use this trap, but in AOS-W 3.3.2.x wlsx**N**UserAuthenticationFailed will not fire unless wlsxUserAuthenticationFailed (no “**N**”) is enabled
- wlsxNAuthServerReqTimedOut

IDS Traps Utilized by OV3600

- wlsxSignatureMatchAP
- wlsxSignatureMatchSta
- wlsxSignAPNetstumbler
- wlsxSignStaNetstumbler
- wlsxSignAPAsleap
- wlsxSignStaAsleap
- wlsxSignAPAirjack
- wlsxSignStaAirjack
- wlsxSignAPNullProbeResp
- wlsxSignStaNullProbeResp
- wlsxSignAPDeauthBcast
- wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
- wlsxChannelFrameFragmentationRateExceeded
- wlsxChannelFrameRetryRateExceeded
- wlsxNIpSpoofingDetected
- wlsxStaImpersonation
- wlsxReservedChannelViolation
- wlsxValidSSIDViolation
- wlsxStaPolicyViolation
- wlsxRepeatWEPIVViolation
- wlsxWeakWEPIVViolation
- wlsxFrameRetryRateExceeded

- wlsxFrameReceiveErrorRateExceeded
- wlsxFrameFragmentationRateExceeded
- wlsxFrameBandWidthRateExceeded
- wlsxFrameLowSpeedRateExceeded
- wlsxFrameNonUnicastRateExceeded
- wlsxChannelRateAnomaly
- wlsxNodeRateAnomalyAP
- wlsxNodeRateAnomalySta
- wlsxEAPRateAnomaly
- wlsxSignalAnomaly
- wlsxSequenceNumberAnomalyAP
- wlsxSequenceNumberAnomalySta
- wlsxApFloodAttack
- wlsxInvalidMacOUIAP
- wlsxInvalidMacOUISta
- wlsxStaRepeatWEPIVViolation
- wlsxStaWeakWEPIVViolation
- wlsxStaAssociatedToUnsecureAP
- wlsxStaUnAssociatedFromUnsecureAP
- wlsxAPImpersonation
- wlsxDisconnectStationAttackAP
- wlsxDisconnectStationAttackSta

Diagnostic Steps to Ensure IDS & Auth Traps Display in 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 below don't show as enabled enter configure terminal mode and issue the following command:

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

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

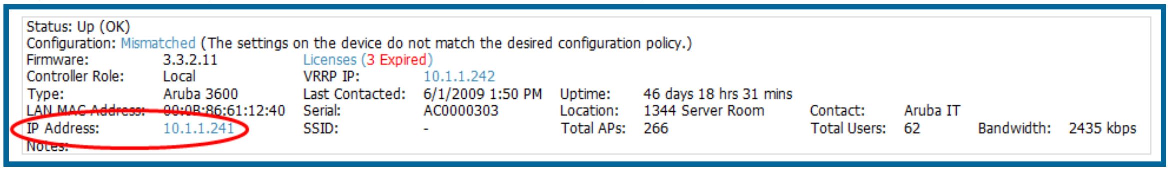
  ```
  (Switch-Name) (config) # write mem

  Saving Configuration...

  Saved Configuration
  ```

- Ensure the source IP of the traps match the IP that OV3600 utilizes to manage the switch. Navigate to **Device → Monitoring** page to validate the IP address.

Figure 11 – Verify IP Address on Device → Monitoring Page



```
Status: Up (OK)
Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)
Firmware:          3.3.2.11           Licenses (3 Expired)
Controller Role:   Local              VRRP IP:          10.1.1.242
Type:              Aruba 3600         Last Contacted:   6/1/2009 1:50 PM   Uptime:      46 days 18 hrs 31 mins
LAN MAC Address:   00:0B:86:61:12:40  Serial:           AC0000303          Location:    1344 Server Room       Contact:      Aruba IT
IP Address:        10.1.1.241         SSID:             -                  Total APs:   266                    Total Users:  62         Bandwidth:   2435 kbps
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 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/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-ap"SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.1.0 = Hex-
STRING: 00 1A 1E C0 2B 32  SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.56.0 =
INTEGER: 2    SNMPv2-SMI::enterprises.14823.2.3.1.11.1.1.17.0 = STRING:
"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:d
0"
```

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

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

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

5.6 - Understanding WMS Offload Impact on Alcatel-Lucent Infrastructure

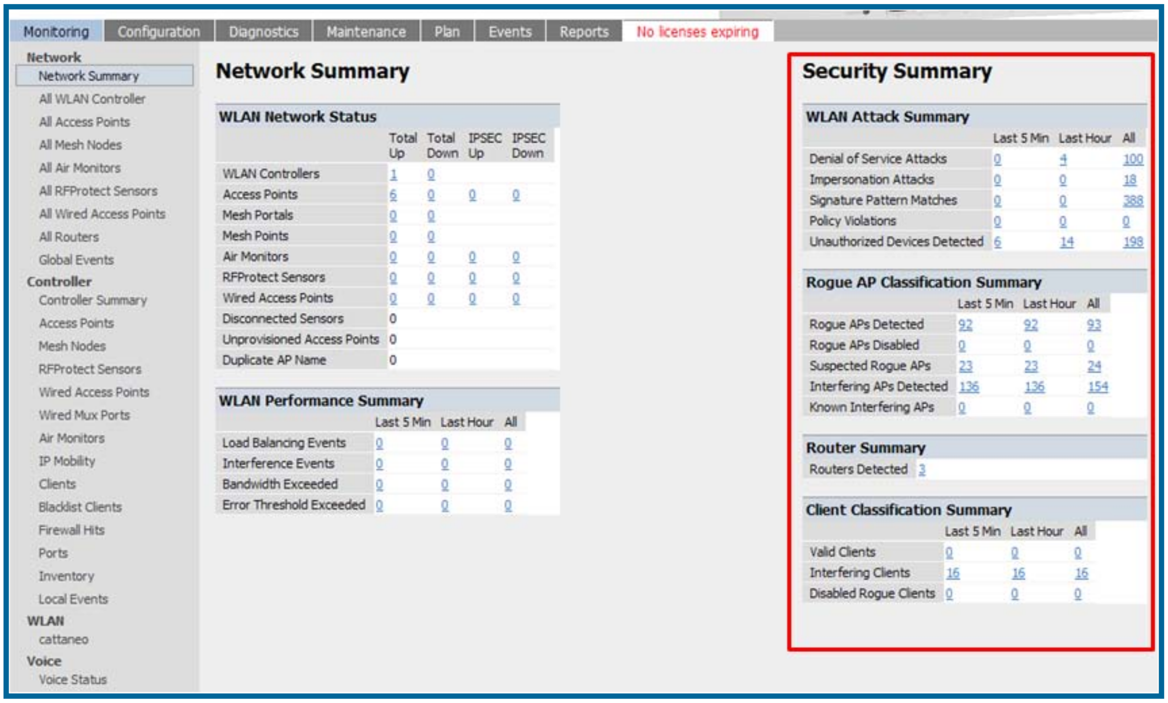
When offloading WMS it is important to understand what functionality is migrated to OV3600 and what functionality is deprecated.

The following Tabs and sections are deprecated after offload wms

- Plan Tab - where floor plans are stored and heatmaps are generated. Prior to offloading wms ensure that you have exported floor plans from the AOS-W and imported into OV3600. All functionality within the Plan Tab is incorporated with the VisaulRF 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

One important area to note is the Security Summary display disappears after offloading WMS. The data is still being processed by the Master Switch, but the summary information is not available. OV3600 does provide ability to view some of this information in detail and summary form.

Figure 12 – Security Summary on Master Switch



Network Summary

WLAN Network Status

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Controllers	1	0		
Access Points	6	0	0	0
Mesh Portals	0	0		
Mesh Points	0	0		
Air Monitors	0	0	0	0
RFProtect Sensors	0	0	0	0
Wired Access Points	0	0	0	0
Disconnected Sensors	0			
Unprovisioned Access Points	0			
Duplicate AP Name	0			

WLAN Performance Summary

	Last 5 Min	Last Hour	All
Load Balancing Events	0	0	0
Interference Events	0	0	0
Bandwidth Exceeded	0	0	0
Error Threshold Exceeded	0	0	0

Security Summary

WLAN Attack Summary

	Last 5 Min	Last Hour	All
Denial of Service Attacks	0	4	100
Impersonation Attacks	0	0	18
Signature Pattern Matches	0	0	388
Policy Violations	0	0	0
Unauthorized Devices Detected	6	14	198

Rogue AP Classification Summary

	Last 5 Min	Last Hour	All
Rogue APs Detected	92	92	93
Rogue APs Disabled	0	0	0
Suspected Rogue APs	23	23	24
Interfering APs Detected	136	136	154
Known Interfering APs	0	0	0

Router Summary

Routers Detected	3

Client Classification Summary

	Last 5 Min	Last Hour	All
Valid Clients	0	0	0
Interfering Clients	16	16	16
Disabled Rogue Clients	0	0	0

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

<u>Rogue AP Classification Summary</u>

- Rogue APs Detected – summary data available on **RAPIDS → Overview** page
- Rogue APs Disabled – no summary data available in OV3600
- Suspected Rogue APs – partial data is available in OV3600 on each AP's **Device → Management** page
- Interfering APs Detected – partial data is available in OV3600 on each AP's **Device → Management** page
- Known Interfering APs – partial data is available in OV3600 on each AP's **Device → Management** page

<u>Router Summary</u>

- Routers Detected – no summary data available in OV3600

<u>Client Classification Summary</u>

- 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

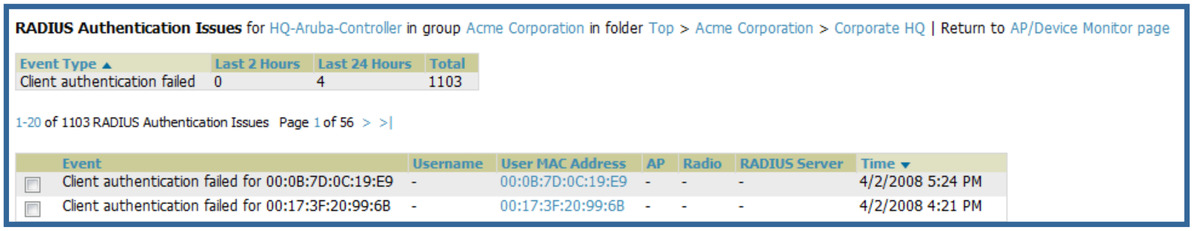
See section 6.4 for more information on Security, IDS, WIPS, WIDS, classification, and RAPIDS.

6 - Alcatel-Lucent Specific Capabilities within OV3600

6.1 - 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 below showing all authentication failures related to a switch.

Figure 13 – RADIUS Authentication Traps as Seen 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

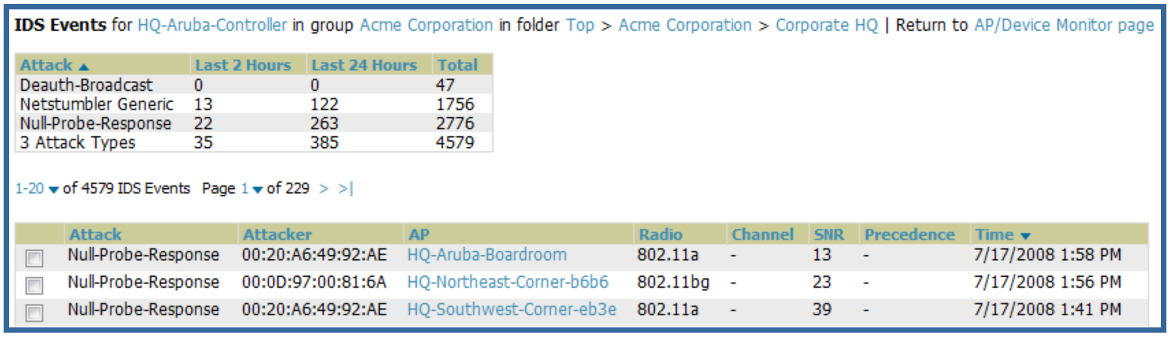
Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Client authentication failed	0	4	1103

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 below showing all IDS traps related to a switch.

Figure 14 – IDS Traps as Seen in OV3600



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

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 > >|

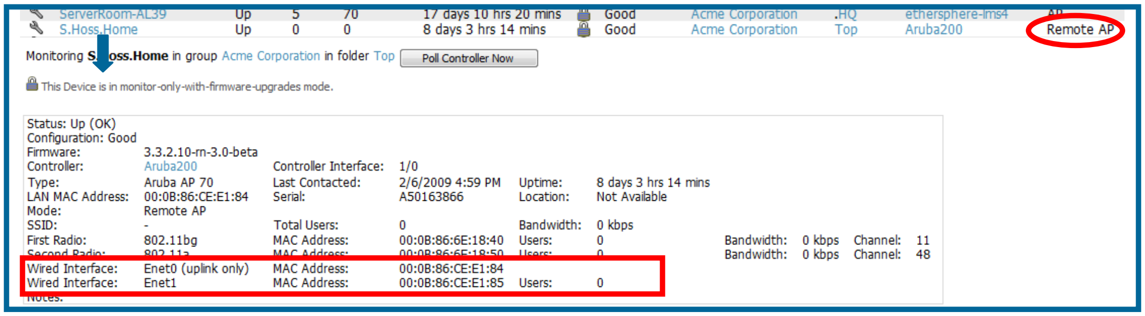
	Attack	Attacker	AP	Radio	Channel	SNR	Precedence	Time ▼
□	Null-Probe-Response	00:20:A6:49:92:AE	HQ-Aruba-Boardroom	802.11a	-	13	-	7/17/2008 1:58 PM
□	Null-Probe-Response	00:0D:97:00:81:6A	HQ-Northeast-Corner-b6b6	802.11bg	-	23	-	7/17/2008 1:56 PM
□	Null-Probe-Response	00:20:A6:49:92:AE	HQ-Southwest-Corner-eb3e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

6.2 - Remote AP & Wired Networking Monitoring

- From the Device → List page you can distinguish and sort on Mode "Remote"
- To view detailed information on the remote device click on the device name.

Figure 15 – Remote AP Detail Page

- You can see if there are users plugged into the wired interfaces.



ServerRoom-AL39	Up	5	70	17 days 10 hrs 20 mins	Good	Acme Corporation	.HQ	ethersphere-lms4	AP
S.Hoss.Home	Up	0	0	8 days 3 hrs 14 mins	Good	Acme Corporation	Top	Aruba200	Remote AP

Monitoring **S.Hoss.Home** in group Acme Corporation in folder Top Poll Controller Now

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

Status: Up (OK)
Configuration: Good

Firmware:	3.3.2.10-rn-3.0-beta								
Controller:	Aruba200	Controller Interface:	1/0						
Type:	Aruba AP 70	Last Contacted:	2/6/2009 4:59 PM	Uptime:	8 days 3 hrs 14 mins				
LAN MAC Address:	00:0B:86:CE:E1:84	Serial:	A50163866	Location:	Not Available				
Mode:	Remote AP								
SSID:	-	Total Users:	0	Bandwidth:	0 kbps				
First Radio:	802.11bg	MAC Address:	00:0B:86:6E:18:40	Users:	0	Bandwidth:	0 kbps	Channel:	11
Second Radio:	802.11a	MAC Address:	00:0B:86:6E:18:50	Users:	0	Bandwidth:	0 kbps	Channel:	48
Wired Interface:	Enet0 (uplink only)	MAC Address:	00:0B:86:CE:E1:84						
Wired Interface:	Enet1	MAC Address:	00:0B:86:CE:E1:85	Users:	0				

Notes:

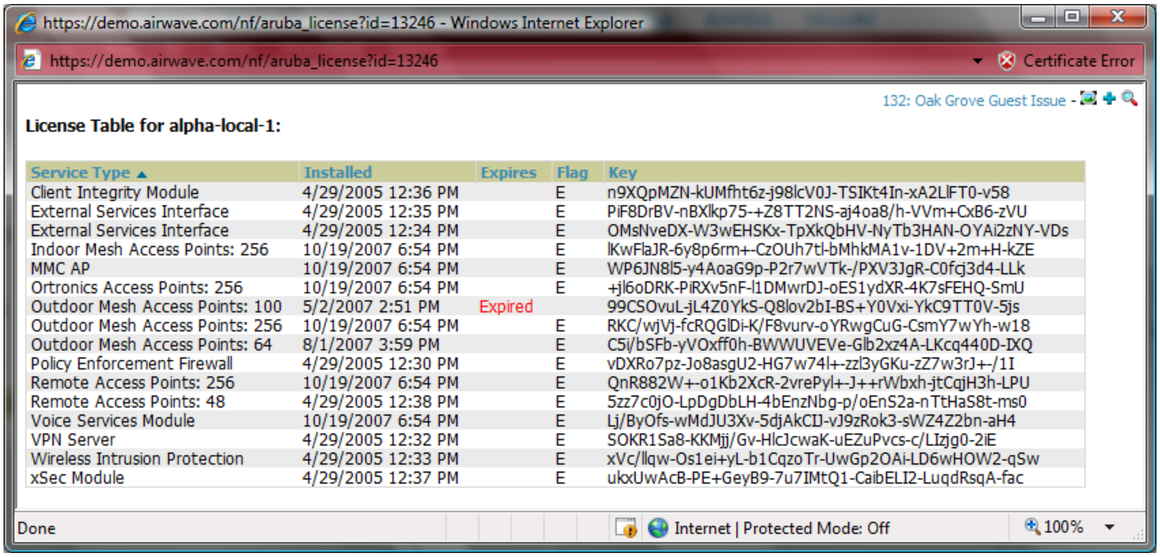
Note: This feature is only available in OV3600 version 6.2 or greater and AOS-W 3.3.2.10 or greater when the remote APs are in split tunnel and tunnel modes.

6.3 - View Switch License Information

- Navigate to the Device → Detail page of a switch under OV3600 management

- Click on the License link

Figure 16 – License Popup


https://demo.airwave.com/nf/aruba_license?id=13246 - Windows Internet Explorer
https://demo.airwave.com/nf/aruba_license?id=13246
Certificate Error
132: Oak Grove Guest Issue -
Done
Internet | Protected Mode: Off
100%

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-VDs
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

6.4 - Device Classification

Only utilize 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.

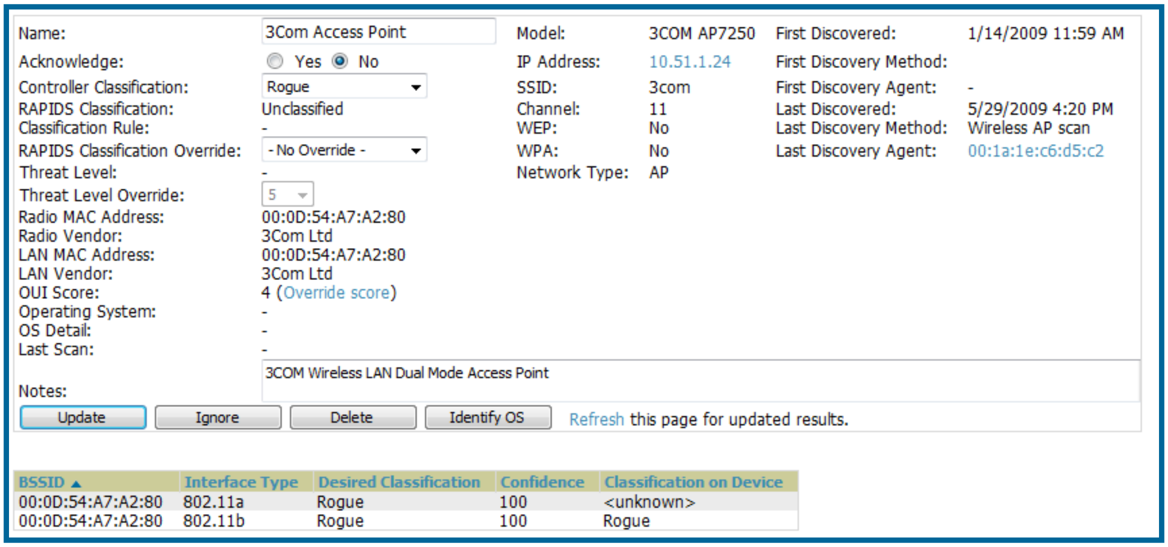
WIPS/WIDS to OV3600 Switch Classification Matrix

OV3600 'Switch Classification'	AOS-W (WIPS/WIDS)
Unclassified (default state)	Unknown
Valid	Valid
Suspected Neighbor	Interfering
Neighbor	Known Interfering
Suspected Rogue	Suspected Rogue
Rogue	Rogue
Contained	DOS

To check and reclassify rogue devices

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

Figure 17 – Rogue Detail



Name:	3Com Access Point	Model:	3COM AP7250	First Discovered:	1/14/2009 11:59 AM
Acknowledge:	○ Yes ● No	IP Address:	10.51.1.24	First Discovery Method:	
Controller Classification:	Rogue	SSID:	3com	First Discovery Agent:	-
RAPIDS Classification:	Unclassified	Channel:	11	Last Discovered:	5/29/2009 4:20 PM
Classification Rule:	-	WEP:	No	Last Discovery Method:	Wireless AP scan
RAPIDS Classification Override:	- No Override -	WPA:	No	Last Discovery Agent:	00:1a:1e:c6:d5:c2
Threat Level:	-	Network Type:	AP		
Threat Level Override:	5				
Radio MAC Address:	00:0D:54:A7:A2:80				
Radio Vendor:	3Com Ltd				
LAN MAC Address:	00:0D:54:A7:A2:80				
LAN Vendor:	3Com Ltd				
OUI Score:	4 (Override score)				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				
Notes:	3COM Wireless LAN Dual Mode Access Point				

Refresh this page for updated results.

BSSID ▲	Interface Type	Desired Classification	Confidence	Classification on Device
00:0D:54:A7:A2:80	802.11a	Rogue	100	<unknown>
00:0D:54:A7:A2:80	802.11b	Rogue	100	Rogue

Warning: *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".*

Switch classification can also be updated from **RAPIDS → Rogue APs** page via the modify-these-devices mechanism.

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. It is probable that the device classification reflected in the Switch's UI and in OV3600' UI will not match, because the Switch/APs do not reclassify rogue devices frequently.

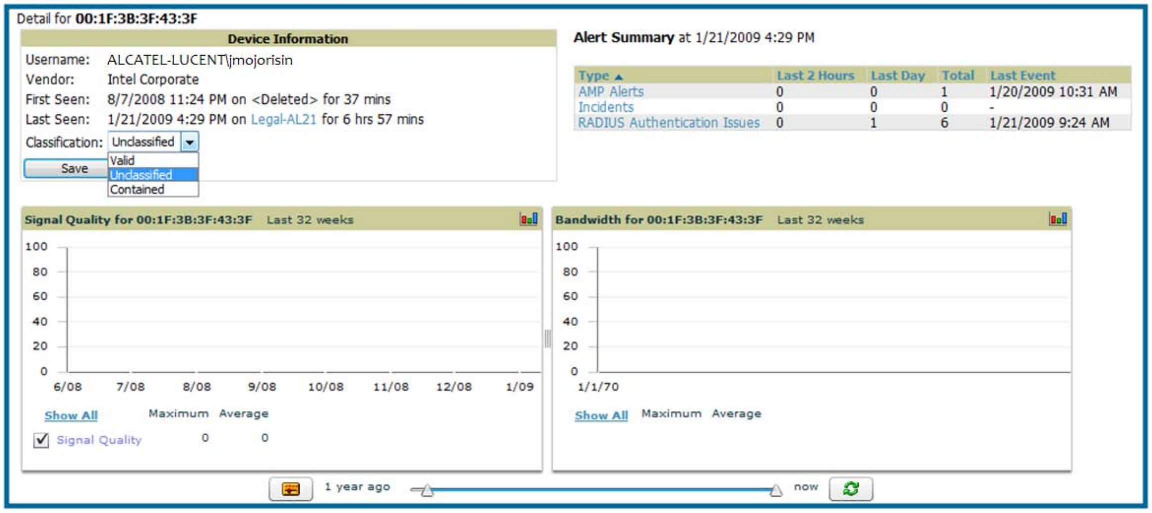
To update a group of devices' switch classification to match the AOS-W device classification navigate to **RAPIDS → Rogue APs** page and utilize the modify-these-devices mechanism combined with the multiple sorting a filtering features.

ARM to OV3600 Classification Matrix

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

- Navigate to the **User → Detail** page for the user
- Select the proper classification from the Classification Pull Down

Figure 18 – User Classification



Detail for **00:1F:3B:3F:43:3F**

Device Information

Username: ALCATEL-LUCENT\jmojorisin
Vendor: Intel Corporate
First Seen: 8/7/2008 11:24 PM on <Deleted> for 37 mins
Last Seen: 1/21/2009 4:29 PM on Legal-AL21 for 6 hrs 57 mins
Classification: Unclassified

Alert Summary at 1/21/2009 4:29 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	1	1/20/2009 10:31 AM
Incidents	0	0	0	-
RADIUS Authentication Issues	0	1	6	1/21/2009 9:24 AM

Warning: 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 Switch's UI and in OV3600' UI will not match, because the Switch/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.

Appendix A - CLI AOS-W & OV3600 Commands

A.1 - Enable Stats Utilizing AOS-W CLI (Local Switch in Master Local Environment)

Note: Do not use these commands if using OV3600 GUI to set these commands.

SSH into the switch, 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) # wms general collect-stats enable


(Switch-Name) (config) # write mem
Saving Configuration...

Saved Configuration
```

A.2 - Offload WMS Utilizing AOS-W CLI and OV3600 CLI (SNMP Walk)

Note: Do not use these commands if using OV3600 GUI to set these commands.

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

> **Note:** 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.
>
> Note: 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 ov3600123 ov3600123`

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

Saving Configuration...

Saved Configuration
```

OV3600 SNMP

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

Note: 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  SWITCH 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
esponse

[root@OV3600 ~]#
```

Note: 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 OV3600123 -A OV3600123 -X OV3600123
10.51.3.222 wlsxSystemExtGroup
```

Because the MIB walk/touch does not persist through a switch reboot, you must add a cronjob on the OV3600 server to ensure continue statistical population.

A.3 - Ensuring Master Switch Pushes Config to Local Switches Utilizing AOS-W CLI

Note: Do not use these commands if using OV3600 GUI.

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

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

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

Saved Configuration
```

A.4 - Disable Debugging Utilizing AOS-W CLI

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

```
(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
   Saving Configuration...

   Saved Configuration
```

A.5 - Restart WMS on Local Switches 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:

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

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

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

A.6 – Copy & Paste to Enable Proper Traps Utilizing 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”:

Copy & Paste the Text Below

```
snmp-server trap enable wlsxNUserAuthenticationFailed
snmp-server trap enable wlsxUserAuthenticationFailed
snmp-server trap enable wlsxNAuthServerReqTimedOut
snmp-server trap enable wlsxSignatureMatchAP
snmp-server trap enable wlsxSignatureMatchSta
snmp-server trap enable wlsxSignAPNetstumbler
snmp-server trap enable wlsxSignStaNetstumbler
snmp-server trap enable wlsxSignAPAsleap
snmp-server trap enable wlsxSignStaAsleap
snmp-server trap enable wlsxSignAPAirjack
snmp-server trap enable wlsxSignStaAirjack
snmp-server trap enable wlsxSignAPNullProbeResp
snmp-server trap enable wlsxSignStaNullProbeResp
snmp-server trap enable wlsxSignAPDeauthBcast
snmp-server trap enable wlsxSignStaDeauthBcastwlsxChannelFrameErrorRateExceeded
snmp-server trap enable wlsxChannelFrameFragmentationRateExceeded
snmp-server trap enable wlsxChannelFrameRetryRateExceeded
snmp-server trap enable wlsxNIpSpoofingDetected
snmp-server trap enable wlsxStaImpersonation
snmp-server trap enable wlsxReservedChannelViolation
snmp-server trap enable wlsxValidSSIDViolation
snmp-server trap enable wlsxStaPolicyViolation
snmp-server trap enable wlsxRepeatWEPIVViolation
```

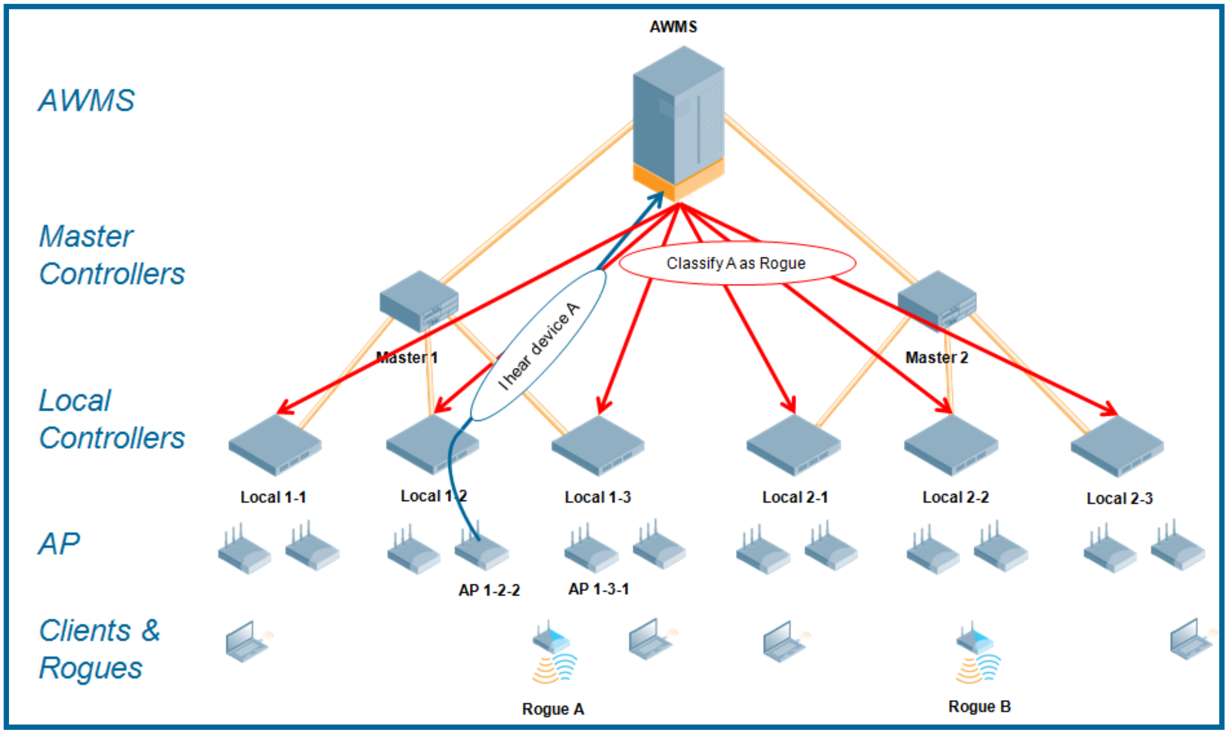
```
snmp-server trap enable wlsxWeakWEPIVViolation
snmp-server trap enable wlsxFrameRetryRateExceeded
snmp-server trap enable wlsxFrameReceiveErrorRateExceeded
snmp-server trap enable wlsxFrameFragmentationRateExceeded
snmp-server trap enable wlsxFrameBandWidthRateExceeded
snmp-server trap enable wlsxFrameLowSpeedRateExceeded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

Note: You will need to issue the “write mem” command.

Appendix B – WMS Offload Details

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 4 below depicts how AMWS communicates state information with Local switches.

Figure 19 – ARM/WIPS/WIDS Classification Message Workflow



B.1 - 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 AMWS 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 OV3600' database. If the Local switch's device state does not comply with OV3600' database, OV3600 will send a re-classification message to bring it back into compliance.

Important notes:

- Customers upgrading to OV3600 6.2 or later will have all their rogue devices set to a default switch classification of “unclassified”. Customers will need to classify these devices manually from the OV3600 UI. OV3600 updates the classification of a rogue device based on SNMP polling only if the switch classification defined on OV3600 is set to “unclassified”.
- The **Rogue Detail Page** displays a BSSID table for each rogue that displays the desired classification and the classification on the device.

Benefits of using OV3600 as Master Device State Manager:

- Ability to correlate state amongst multiple Master switches. This will reduce delays in mitigating a rogue device or authorizing a valid device when devices roam across a large campus.
- Ability to correlate state of 3rd party access points with ARM. This will ensure Alcatel-Lucent infrastructure interoperates more efficient 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 wire-line discovery data from Alcatel-Lucent switches.

Appendix C – Converting from MMS to OV3600

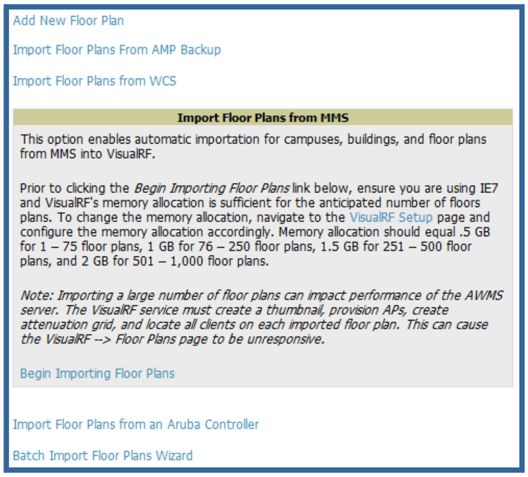
The instructions below will enable you to seamlessly migrate all building, campus, and floor plan information previously entered into MMS or AOS-W into OV3600.

Pre conversion checklist

- The conversion tool is only supported for **IE6** and **E7**.
- Ensure you increase VisualRF memory prior to beginning the MMS export option. Navigate to **VisualRF → Setup** and use the pull-down menu for Memory Allocation

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

Figure 20 – MMS Export Instructions


Add New Floor Plan
Import Floor Plans From AMP Backup
Import Floor Plans from WCS

Import Floor Plans from MMS

This option enables automatic importation for campuses, buildings, and floor plans from MMS into VisualRF.

Prior to clicking the *Begin Importing Floor Plans* link below, ensure you are using IE7 and VisualRF's memory allocation is sufficient for the anticipated number of floors plans. To change the memory allocation, navigate to the VisualRF Setup page and configure the memory allocation accordingly. Memory allocation should equal .5 GB for 1 – 75 floor plans, 1 GB for 76 – 250 floor plans, 1.5 GB for 251 – 500 floor plans, and 2 GB for 501 – 1,000 floor plans.

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

Begin Importing Floor Plans
Import Floor Plans from an Aruba Controller
Batch Import Floor Plans Wizard

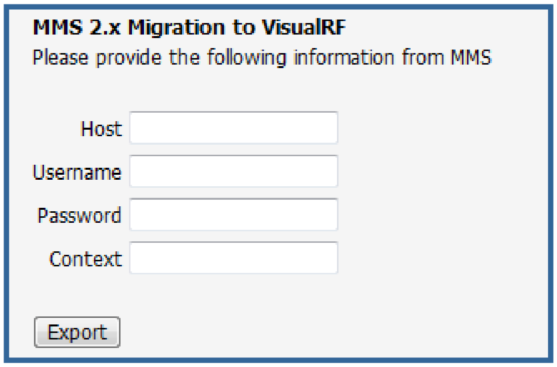
C.1 - Migrating Floor Plans from MMS to OV3600

Process

- **Navigate to VisualRF → Import Page**
- Select the "Import floor plans from MMS" link
- Detailed instructions will appear on the screen
- Select the "Begin Importing Floor Plans" link
- Input the following information:
  - Host – enter the hostname or IP address of the MMS server
  - Username – enter the MMS administrative user account.
  - Password
  - Context (optional) – leave this blank unless you have enabled context on you MMS. Most customers do not utilize context.

    Note: If you are using context, then you will have to enter a different user for each context defined within MMS.
- Click on the "Export" button and the program will automatically redirect to the page below detailing the status of the export.

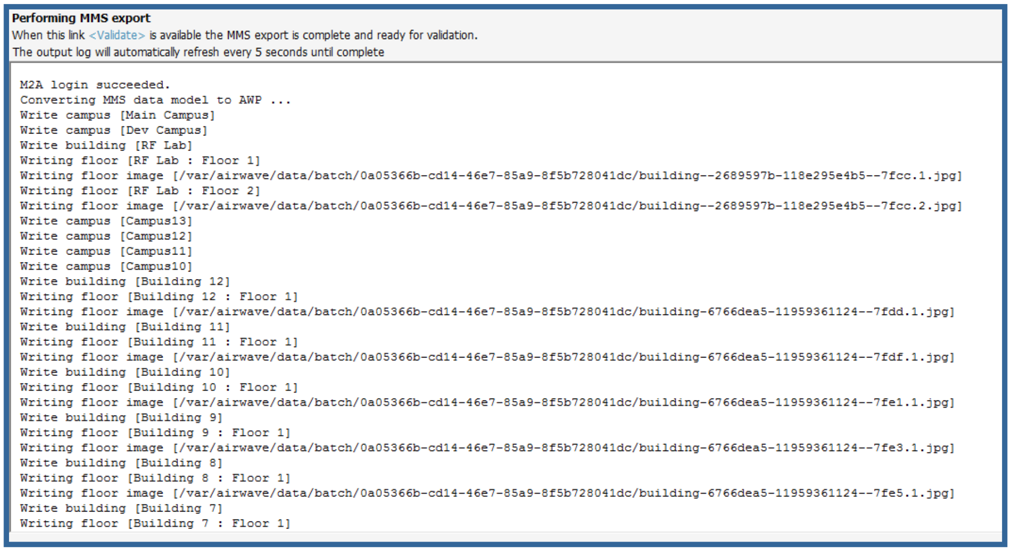
Figure 21 – MMS Export to OV3600 window



MMS 2.x Migration to VisualRF

Please provide the following information from MMS

Figure 22 – MMS export



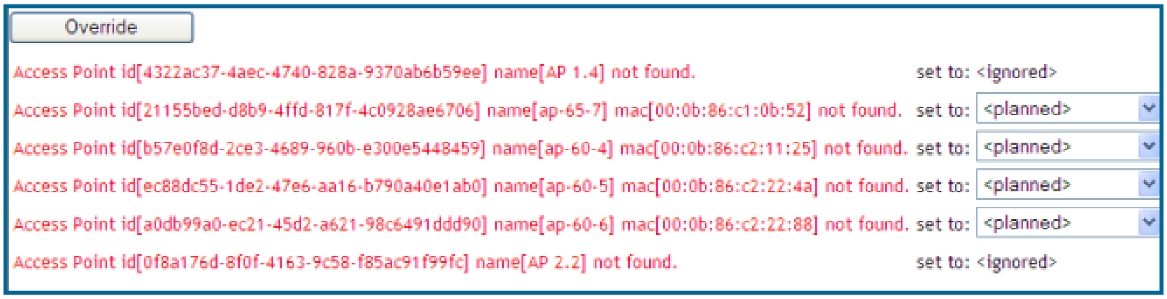
Performing MMS export

When this link <Validate> is available the MMS export is complete and ready for validation.
The output log will automatically refresh every 5 seconds until complete

```
M2A login succeeded.
Converting MMS data model to AWP ...
Write campus [Main Campus]
Write campus [Dev Campus]
Write building [RF Lab]
Writing floor [RF Lab : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building--2689597b-118e295e4b5--7fcc.1.jpg]
Writing floor [RF Lab : Floor 2]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building--2689597b-118e295e4b5--7fcc.2.jpg]
Write campus [Campus13]
Write campus [Campus12]
Write campus [Campus11]
Write campus [Campus10]
Write building [Building 12]
Writing floor [Building 12 : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building-6766dea5-11959361124--7fdd.1.jpg]
Write building [Building 11]
Writing floor [Building 11 : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building-6766dea5-11959361124--7fdf.1.jpg]
Write building [Building 10]
Writing floor [Building 10 : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building-6766dea5-11959361124--7fe1.1.jpg]
Write building [Building 9]
Writing floor [Building 9 : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building-6766dea5-11959361124--7fe3.1.jpg]
Write building [Building 8]
Writing floor [Building 8 : Floor 1]
Writing floor image [/var/airwave/data/batch/0a05366b-cd14-46e7-85a9-8f5b728041dc/building-6766dea5-11959361124--7fe5.1.jpg]
Write building [Building 7]
Writing floor [Building 7 : Floor 1]
```

- Once the exportation process is complete the <Validate> tag will change to a clickable link.
- Click the “Validate” link to validate the XML exported from MMS. This will automatically redirect you to the Bulk Importation Wizard to import the exported floor plans into OV3600.
- If APs in the XML that are not in OV3600, the following screen will be displayed. Set the APs to be ignored or identify them as planned, and click the “Override” button to continue.

Figure 23 – Override



Access Point id[4322ac37-4aec-4740-828a-9370ab6b59ee] name[AP 1.4] not found. set to: <ignored>
Access Point id[21155bed-d8b9-4ffd-817f-4c0928ae6706] name[ap-65-7] mac[00:0b:86:c1:0b:52] not found. set to: <planned>
Access Point id[b57e0f8d-2ce3-4689-960b-e300e5448459] name[ap-60-4] mac[00:0b:86:c2:11:25] not found. set to: <planned>
Access Point id[ec88dc55-1de2-47e6-aa16-b790a40e1ab0] name[ap-60-5] mac[00:0b:86:c2:22:4a] not found. set to: <planned>
Access Point id[a0db99a0-ec21-45d2-a621-98c6491ddd90] name[ap-60-6] mac[00:0b:86:c2:22:88] not found. set to: <planned>
Access Point id[0f8a176d-8f0f-4163-9c58-f85ac91f99fc] name[AP 2.2] not found. set to: <ignored>

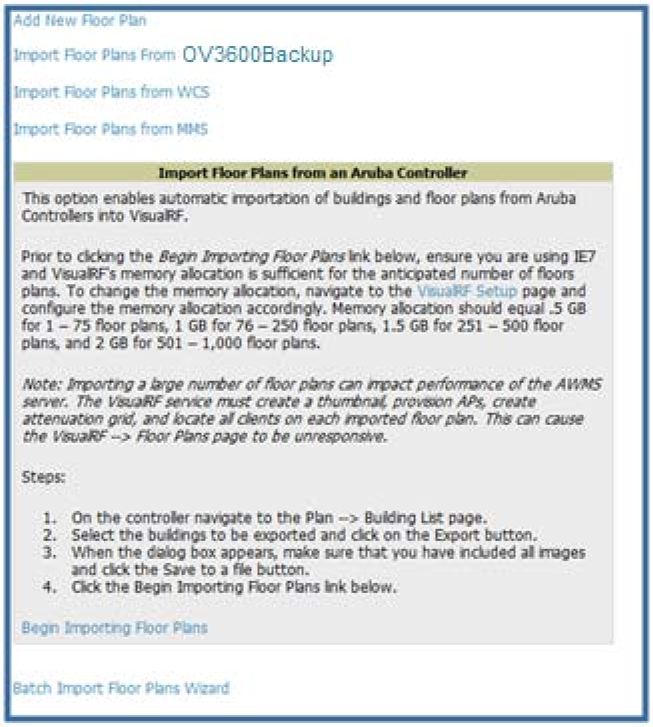
- If there are no new APs, click the “Next” button to complete the process.

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

C.2 - Migrating Floor Plans from AOS-W (Switch) to OV3600

Process on Aruba Controller

Figure 24 – Import Floor Plans from an Aruba Controller



Add New Floor Plan
Import Floor Plans From OV3600Backup
Import Floor Plans from WCS
Import Floor Plans from MMS

Import Floor Plans from an Aruba Controller

This option enables automatic importation of buildings and floor plans from Aruba Controllers into VisualRF.

Prior to clicking the *Begin Importing Floor Plans* link below, ensure you are using IE7 and VisualRF's memory allocation is sufficient for the anticipated number of floors plans. To change the memory allocation, navigate to the VisualRF Setup page and configure the memory allocation accordingly. Memory allocation should equal .5 GB for 1 – 75 floor plans, 1 GB for 76 – 250 floor plans, 1.5 GB for 251 – 500 floor plans, and 2 GB for 501 – 1,000 floor plans.

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

Steps:

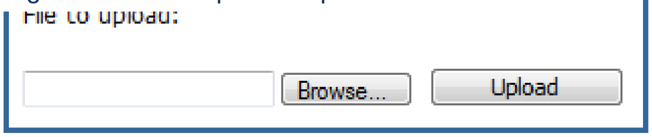
1. On the controller navigate to the Plan --> Building List page.
2. Select the buildings to be exported and click on the Export button.
3. When the dialog box appears, make sure that you have included all images and click the Save to a file button.
4. Click the Begin Importing Floor Plans link below.

- Login into the Alcatel-Lucent switch's Web UI
- Navigate to the **Plan → Building List** page.
- Select the buildings to be exported and click on the "Export" button.
- When the dialog box appears, make sure that you have included all images and click the "Save to a file" button.

Process to Import within OV3600

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

Figure 25 – File Upload Explorer



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

C.3 - Migrating Floor Plans from RF Plan to OV3600

Process with RF Plan

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

Process to Import within OV3600

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

Appendix D – Increasing Location Accuracy

D.1 – Understand Band Steering's Impact on Location

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

Operating Frequency	Total Channels	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

D.2 – Leveraging RTLS to Increase Accuracy

Overview

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.

Minimum Requirements

- OV3600 version 6.2 or higher
- AOS-W-W 3.1.x or higher

Deployment Topology

Figure 26 – Typical Client Location

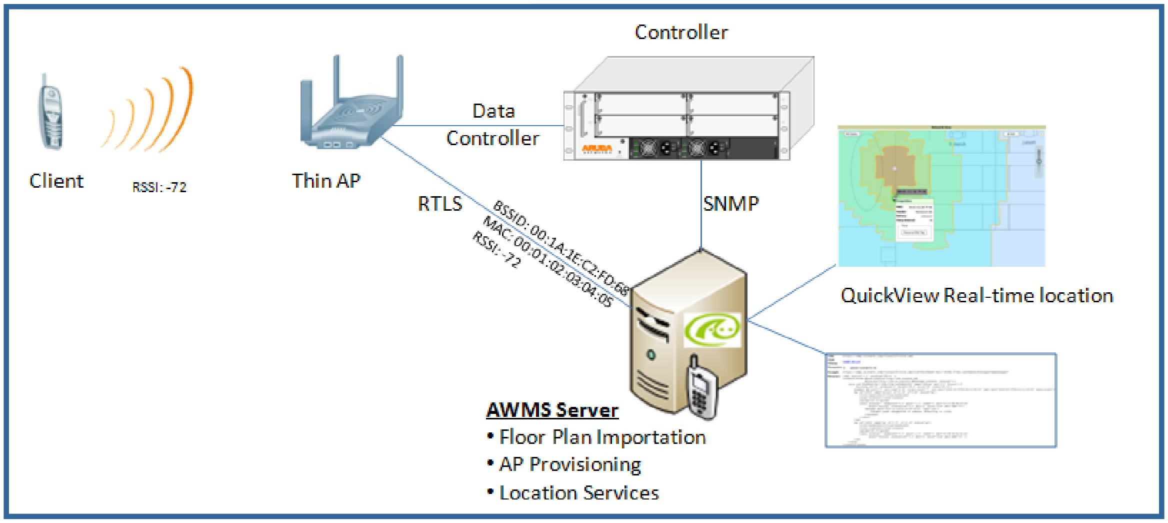
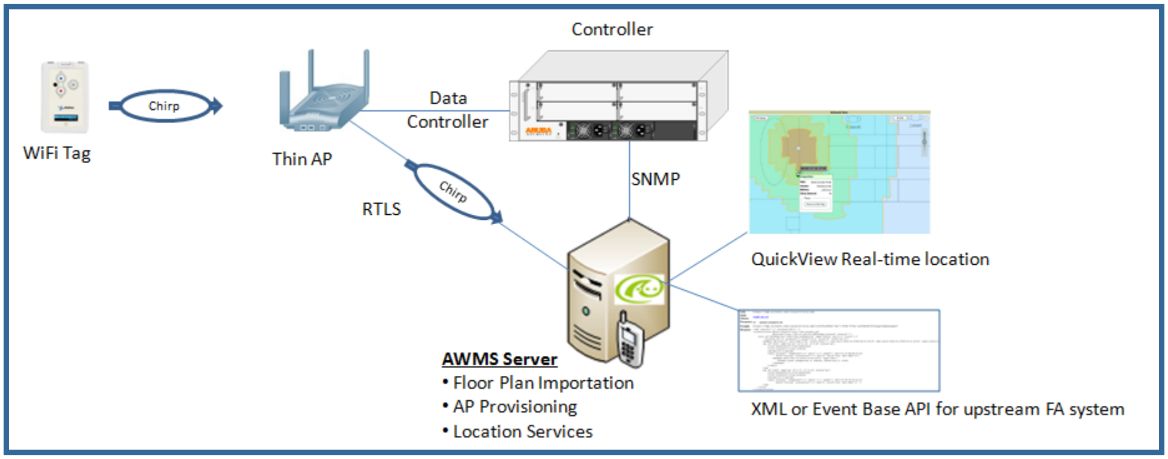


Figure 27 – Typical Tag Deployment



Prerequisites

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

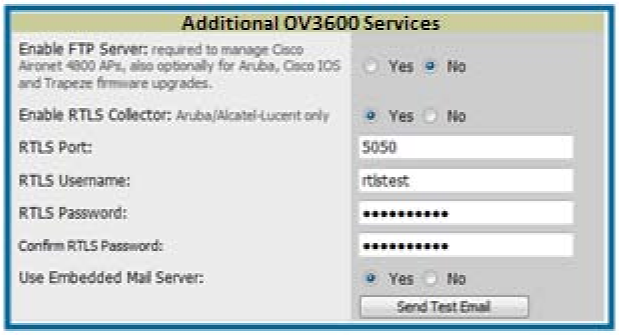
Known Issues

AOS-W	OV3600	Description	Resolution
3.x	6.x	Wi-Fi Tags will only display in VisualRF. Wi-Fi Tags will not display within OV3600' UI or the switch's UI.	OV3600 7.1

Enable RTLS service on the OV3600 server

- Navigate to **OV3600 Setup → General** page

Figure 28 – RTLS Setup



Additional OV3600 Services

Enable FTP Server: required to manage Cisco Aironet 4800 APs, also optionally for Aruba, Cisco IOS and Trapeze firmware upgrades.	○ Yes ● No
Enable RTLS Collector: Aruba/Alcatel-Lucent only	● Yes ○ No
RTLS Port:	5050
RTLS Username:	rtlstest
RTLS Password:	•••••••••••
Confirm RTLS Password:	•••••••••••
Use Embedded Mail Server:	● Yes ○ No

- Locate the **OV3600 Additional Services** section
- Select “Yes” to Enable RTLS Collector
- 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
- Click on the “Save” button at the bottom of the page.

Enable RTLS on Switch

Note: 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:

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

(Switch-Name) (config) # ap system-profile <PROFILE USED BY THIN
APs>
(Switch-Name) (AP system profile "default") # rtls-server ip-addr
<IP OF OV3600 SERVER> port 5050 key <SNMPv3 "MMS" PASSWORD
CONFIGURED ON SWITCH>
(Switch-Name) (AP system profile "default") # write mem
Saving Configuration...

Saved Configuration
```

- To validate exit configuration mode

```
(Switch-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         *
```

Trouble Shooting RTLS

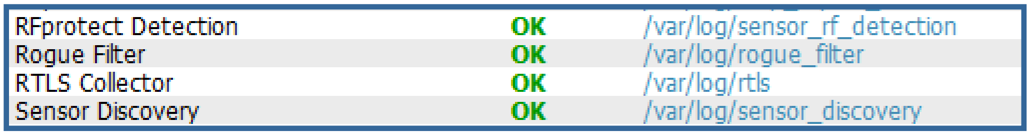
- Ensure the RTLS service is running on your OV3600 server. SSH into your OV3600 server.

```
[root@OV3600Server]# daemons | grep RTLS
root     17859 12809  0 10:35 ?        00:00:00 Daemon::RTLS
```

or

Navigate to System → Status page and look for the RTLS service

Figure 29 – RTLS Service 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@OV3600Server]# logs
[root@OV3600Server]# tail rtls

payload:
00147aaf01000020001a1ec02b3200000001000000137aae0100000c001a1ec02b3
20000001a1e82b322590006ddff02

1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050

Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from
10.51.1.39 on port 5050

payload:
0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec0507
80000000d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb
8ae9a9000006c4ff02

1224534900.588245 - got 96 bytes from 10.51.1.39 on port 5050

Mon Oct 20 13:35:00 2008: 1224534900.588338 - got 96 bytes from
10.51.1.39 on port 5050

payload:
0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec0507
80000000d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb
8ae9a9000006c4ff02
```

- 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 tags can be heard by at least 3 access points from any given location. The recommended is 4 for best results.
- Ensure tags chirp on all regulatory channels.