ALCATEL-LUCENT BEST PRACTICES GUIDE

OV3600, Version 6.2

Document Part Number: 0510595-01

Table of Contents

Overview

This document provides best practices for leveraging the Alcatel-Lucent OmniVista 3600 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.

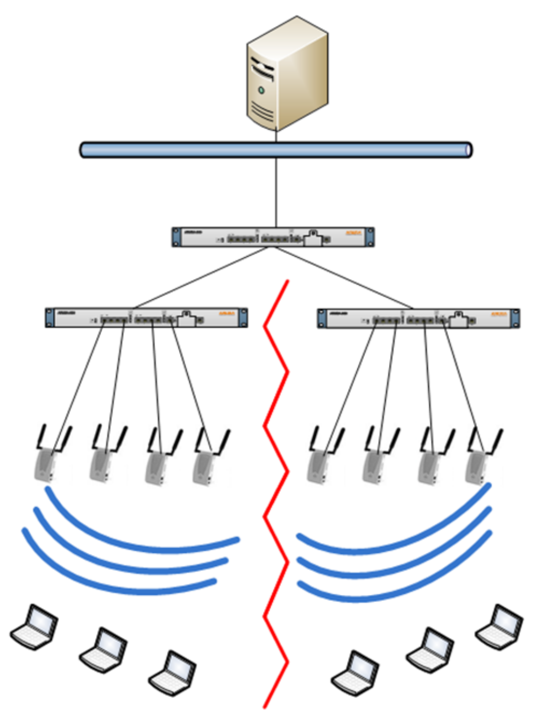
Minimum Requirements

- OV3600 version 6.0 or higher
- AOS-W 2.5.4 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 controllers to gather and correlate statistics
Master Controller	Correlates all state information from all downstream access points	Functions as a local controller
Local Controllers	Collect downstream AP statistical information	Collect downstream AP statistical and state information
Thin APs	Send all state information to the Master Controller	Send all state information to Local Controller

Note: There should never be a Local controller managed by an OV3600 server whose Master controller is also not under management.

Prerequisites for Alcatel-Lucent Infrastructure

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

- SNMP community string
- 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 controllers.
- SNMPv3 requirements (optional in 2.x and mandatory in 3.x)
  - Username
  - Auth password
  - Privacy password
  - Auth protocol

Known and Recently Resolved Issues

AOS-W	OV3600	Description	Resolution
2.5.6		'BW is not reported without issuing 'ems' command	2.5.6.19 (Jan 2009)
3.3.x		11n client BW OIDs resetting very frequently under heavy load. This results in OV3600 reporting inflated BW usage.	Pending
3.3.x		Encryption type is not populated for wireless users.	Pending (Nov-2009)
3.3.1		Ad-hoc SNMP traps do not contain channel information.	AOS-W 3.3.2
3.3.1		Can’t create an SNMPv3 and management user with the same name on a controller.	Patched in AOS-W 3.3.1.5
3.3.x		Reduced accuracy when locating clients, because of improper neighbor and client SNR values.	Upgrade to OV3600 6.0.9 3.3.2.6
	5.3 – 6.x	When two wireless users appear on the controller’s UI with the same MAC (VMware, Parallels, or VPN) OV3600 displays only one user, but flip flops between IP addresses.	ETA OV3600 6.3
3.3.2.x	6.1 – 6.2	Controller MIB indicates radio down when the radios are actually up.	Pending (May-2009)
	All	Local controllers never come up after discovery from Master controller which disables downstream thin APs discovery.	Pending – use the `Poll Now` button on the Controller’s management page.
3.3.x	All	AOS-W improperly initializes engine_id in SNMPv3 informs.	Pending AOS-W fix
3.3.x	All	AP's and Radios disappear when device is in Air Monitor Mode	Pending AOS-W fix
3.3.x	All	MIB reports incorrect switch port for APs	Pending AOS-W fix

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	6.1
Mesh monitoring and visualization support	6.1
Ability to import floor plans from Alcatel-Lucent WLAN Switches	6.1
Support remote AP provisioning	6.2
Support device coordination amongst controllers for WIPS/WIDS	6.2
Support device coordination amongst controllers for ARM	6.2
Ability to provision AMs	6.2
Ability to send ARM/WIPS/WIDS classification to controllers	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 controllers	6.3
Support for AP-65-WB	6.3
AOS-W GUI configuration support for Profiles and AP Groups	6.3
Support for dot11counters	6.3
Support controller based RTLS and WiFi Tag history in OV3600	6.4

Process Detailed in Document

1. Configure Alcatel-Lucent WLAN Switches for Optimal OV3600 Monitoring
   - Disable debugging
   - Ensure OV3600 server is a trap receiver host
   - Ensure proper traps are enabled

2. Configure OV3600 to Optimally Monitor Alcatel-Lucent Infrastructure
   - WMS offload
   - Configure SNMP communication
   - Create a proper policy for monitoring Alcatel-Lucent infrastructure
   - Discover infrastructure

3. Device Classification
   - Rogue classification setup
   - Rogue classification override
   - User classification override devices

4. Alcatel-Lucent Specific Monitoring Features
   - Remote AP and wired network monitoring
   - Viewing controller license information

5. Convert Existing Floor Plans to VisualRF
   - MMS
   - AOS-W
   - RF Plan
6. Utilize RTLS for Increasing Location Accuracy (optional)
   - Enable RTLS service on the OV3600 server
   - Enable RTLS on Alcatel-Lucent Infrastructure

Configuring Alcatel-Lucent WLAN Switches for Optimal OV3600 Monitoring

Alcatel-Lucent designed real-time monitoring and comprehensive configuration capability into their master controller. Customers that require historical trending and reporting functionality will need to make the following changes on the OV3600.

Disable Debugging

Ensure that debugging is disabled; it should be disabled by default. Debugging coupled with gathering the enhanced statistics can put a strain on the controller's CPU, so it is highly recommended to disable debugging.

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

For 2.x and 3.x installations

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

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

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

(Controller-Name) (config) # no logging level debugging <MODULE FROM ABOVE>
(Controller-Name) (config) # write mem

Saving Configuration...

Saved Configuration
```

Ensure the OV3600 Server is defined as a Trap Receiver Host

In order for OV3600 to properly diagnose authentication problems and IDS attacks you must configure the OV3600 server as a trap receiver host on each of the controllers. This will allow Alcatel-Lucent WLAN Switches to send client diagnostic and IDS traps to OV3600.

> Note: For SNMPv2, the Global community string and SNMP trap host community string must be the same for traps to trigger correctly on the controller.

To ensure OV3600 server is a trap receiver host, SSH into each controller, enter “enable” mode, and issue the following commands:

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

(Controller-Name) (config) # snmp-server host <OV3600 IP ADDR> version 2c public

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

(Controller-Name) (config) # write mem

Saving Configuration...

Saved Configuration
```

Warning: Do not configure the SNMP version to v3. OV3600 does not support SNMPv3 traps/informs because of an outstanding issue on AOS-W firmware with the initialization of engine id. This will be fixed in an upcoming AOS-W iteration.

> Note: Alcatel-Lucent WLAN Switches have many virtual and physical interfaces. You must ensure the source IP of the traps match the IP that OV3600 utilizes to manage the controller.
>
> `Sample: snmp-server trap source 10.2.32.1`

Check to see if the following traps are enabled, exit 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

Saving Configuration...

Saved Configuration
```

Auth Traps Utilized by OV3600

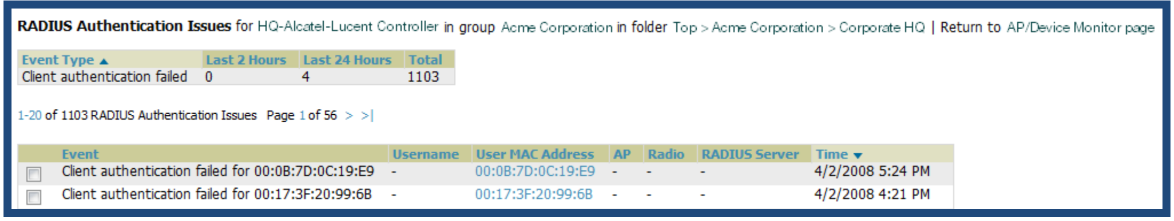
- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimedOut

IDS Traps Utilized by OV3600

- wlsxSignatureMatchAP
- wlsxSignatureMatchSta
- wlsxSignAPNetstumbler
- wlsxSignStaNetstumbler
- wlsxSignAPAsleap
- wlsxSignStaAsleap
- wlsxSignAPAirjack
- wlsxSignStaAirjack
- wlsxSignAPNullProbeResp
- wlsxSignStaNullProbeResp
- wlsxSignAPDeauthBcast
- wlsxSignStaDeauthBcast

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

Figure 2 – RADIUS Authentication Traps as Seen in OV3600



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

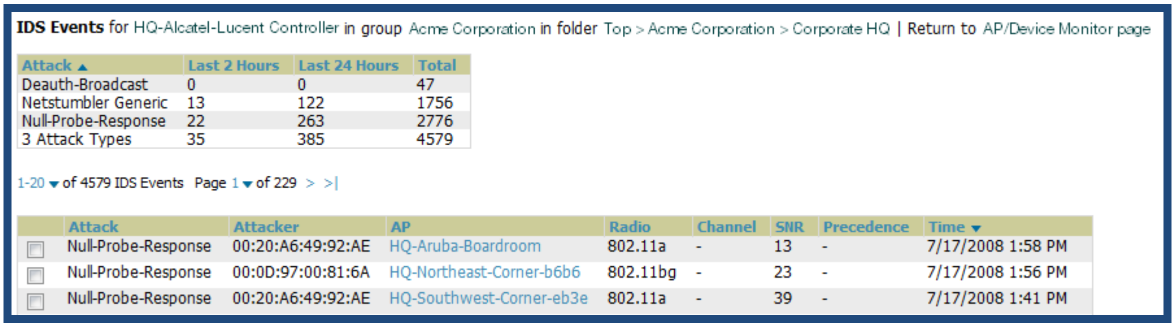
Event Type ▲	Last 2 Hours	Last 24 Hours	Total
Client authentication failed	0	4	1103

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 controller, AP, and user. See Figure below showing all IDS traps related to a controller.

Figure 3 – IDS Traps as Seen in OV3600



IDS Events for HQ-Alcatel-Lucent 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 > >|

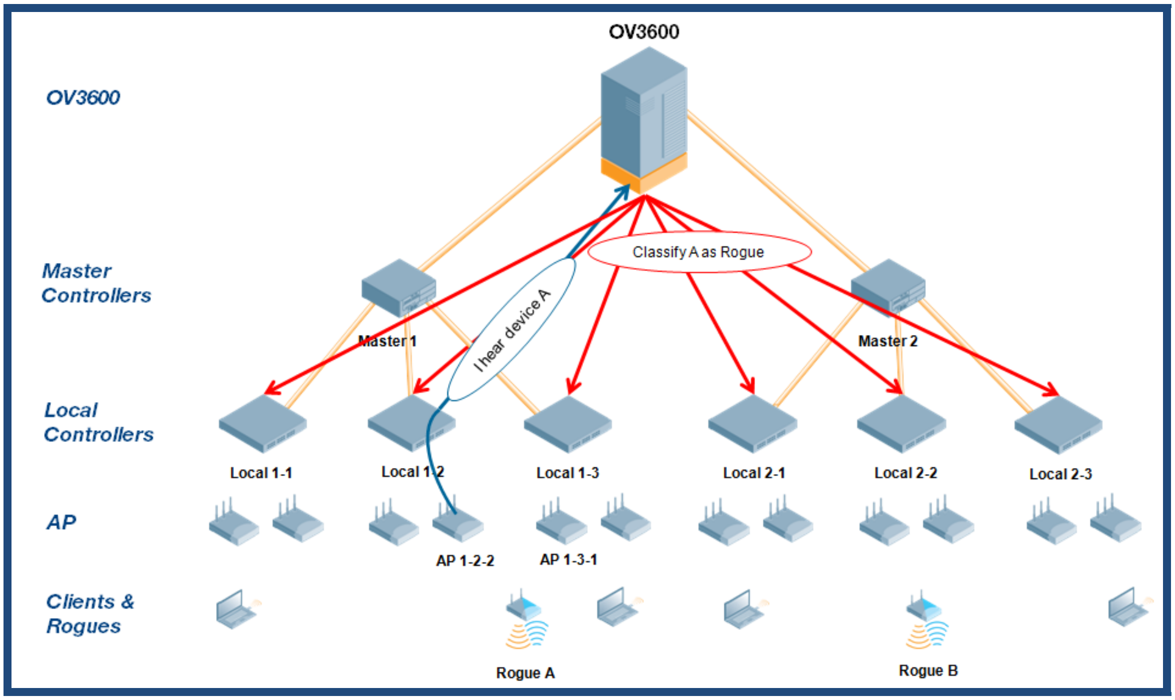
	Attack	Attacker	AP	Radio	Channel	SNR	Precedence	Time ▼
□	Null-Probe-Response	00:20:A6:49:92:AE	HQ-Aruba-Boardroom	802.11a	-	13	-	7/17/2008 1:58 PM
□	Null-Probe-Response	00:0D:97:00:81:6A	HQ-Northeast-Corner-b6b6	802.11bg	-	23	-	7/17/2008 1:56 PM
□	Null-Probe-Response	00:20:A6:49:92:AE	HQ-Southwest-Corner-eb3e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

Configuring OV3600 to Optimally Monitor Alcatel-Lucent Infrastructure

WMS Offload

WMS offload instructs the Master controller to stop correlating ARM, WIPS, and WIDS state information amongst its Local controllers, because OV3600 will assume this responsibility. Figure 4 below depicts how OV3600 communicates state information with Local controllers.

Figure 4 – ARM/WIPS/WIDS Classification Message Workflow



State Correlation Process

1. AP-1-3-1 hears rogue device A.
2. Local controller 1-3 evaluates devices and does initial classification and sends a classification request to the 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 controllers managed by Master controller 1, (1-1, 1-2, and 1-3) .
5. OV3600 sends a classification message back to all additional Local controllers managed by the OV3600 server. In this example all Local controllers under Master controller 2, (2-1, 2-2, and 2-3) would receive the classification messages.
6. If an administrative OV3600 user manually overrides the classification, then OV3600 will send a re-classification message to all applicable local controllers.
7. OV3600 periodically polls each Local controller's MIB to ensure state parity with OV3600' database. If the Local controller'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 OV36006.2 will have all their rogue devices set to a default classification of “unclassified”. Customers will need to classify these devices manually from the OV3600 UI. OV3600 updates the classification of a rogue based on SNMP polling only if the classification on the OV3600 is “unclassified”.
- The rogue detail page displays a BSSID table for each rogue that displays the desired classification and the classification on the device.

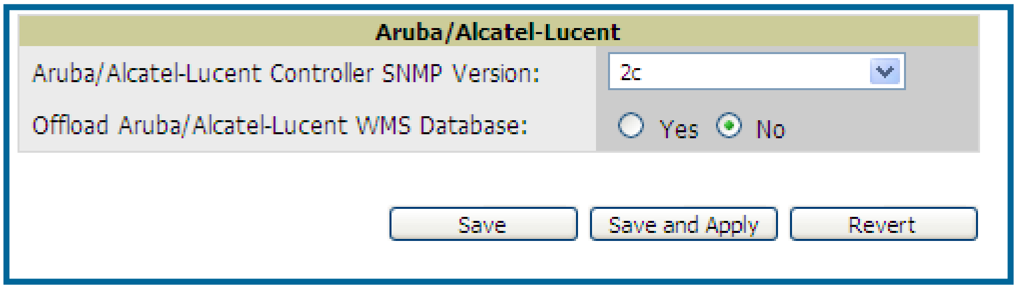
Benefits of Using OV3600 as Master Device State Manager

- Ability to correlate state amongst multiple Master controllers. 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 auto-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.

To offload WMS on the Alcatel-Lucent WLAN Switches:

- Navigate to **Groups→Basic** page.
- Locate the Aruba/Alcatel Lucent section.
- Enable “Offload Aruba/Alcatel-Lucent WMS Database”.
- Click “Save and Apply” button.

Figure 5 – Enable WMS Offload



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 Controllers in management mode to offload WMS. OV3600 will create a new SNMPv3 user on the controllers. OV3600 must have read/write access to the controllers in order to push these commands.

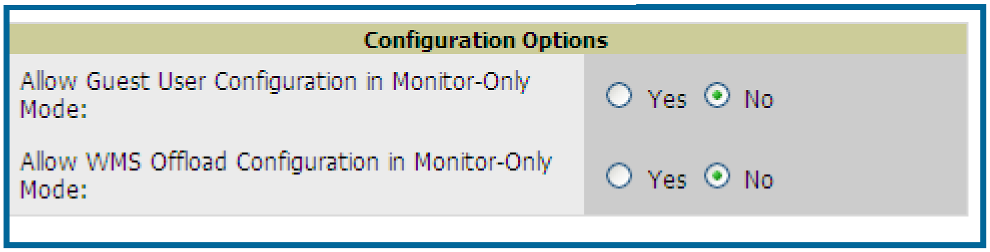
Note: This process will not reboot your controllers.

OV3600 can be configured to push WMS offload commands even when controllers are in monitor-only mode.

To enable this feature:

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

Figure 6 – WMS Offload Configuration Options



Configuration Options

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

Warning: *If you don't enable Offload WMS Database and don't enable Allow WMS Offload Configuration in Monitor-Only Mode, local controllers will not populate signal information for client and rogue devices. This decreases OV3600' capability to trend client signal information and to properly locate devices.*

For 2.5.6 and earlier installations

For 2.5.x installation, we recommend upgrading to AOS-W 2.5.7 or higher. *For Alcatel-Lucent WLAN Switches running 2.5.6 and earlier versions you will need to offload WMS in order to see stats on the local controllers. Enabling WMS will hide some tabs on the Alcatel-Lucent WLAN Switche UI running 2.5.6 and earlier.*

The table represents corresponding tabs within OV3600 to those hidden in AOS-W in 2.5.6 and earlier versions.

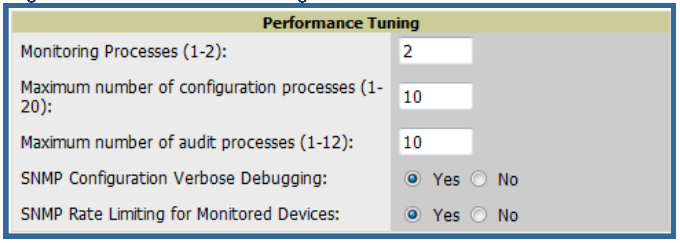
Alcatel-Lucent WLAN Switch UI	OV3600 Equivalent Tabs
Plan	VisualRF
Reports	Reports
Events	System → Events (monitor) System → Triggers (configure)

Configuring SNMP Communication

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

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

Figure 7 – SNMP Rate Limiting



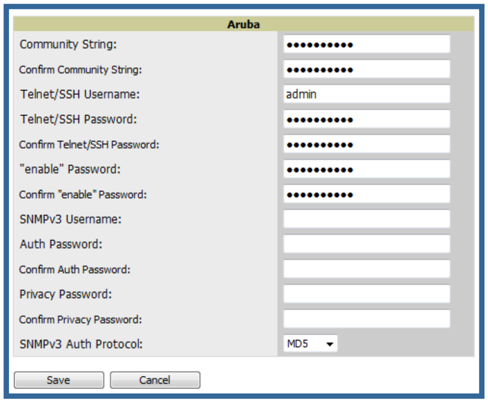
Performance Tuning	
Monitoring Processes (1-2):	2
Maximum number of configuration processes (1-20):	10
Maximum number of audit processes (1-12):	10
SNMP Configuration Verbose Debugging:	● Yes ○ No
SNMP Rate Limiting for Monitored Devices:	● Yes ○ No

Note: This feature could impact OV3600 server’s scalability performance for non-Alcatel-Lucent infrastructure.

OV3600 requires several credentials to properly interface with Alcatel-Lucent infrastructure.

- Navigate to **Device → Setup Communication** page
- Locate the **Default Credentials** section
- Click the Alcatel-Lucent link
  - Enter SNMP Community String
  - Optionally enter Telnet SSH, “enable” Password, and SNMPv3 information.

Figure 8 – Credential Setup



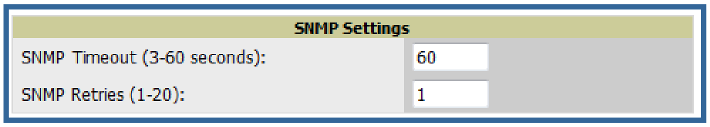
Aruba	
Community String:	••••••••••
Confirm Community String:	••••••••••
Telnet/SSH Username:	admin
Telnet/SSH Password:	••••••••••
Confirm Telnet/SSH Password:	••••••••••
"enable" Password:	••••••••••
Confirm "enable" Password:	••••••••••
SNMPv3 Username:	
Auth Password:	
Confirm Auth Password:	
Privacy Password:	
Confirm Privacy Password:	
SNMPv3 Auth Protocol:	MD5

Note: You don’t have to monitor Alcatel-Lucent WLAN Switches via SNMPv3, but if you do and are running AOS-W 3.x it would be a good idea to match the SNMPv3 Username, Auth Password, and Privacy Password entered via mobility manager command above. SNMPv3 users must be configured to use SHA.

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

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

Figure 9 – SNMP Time & Retries



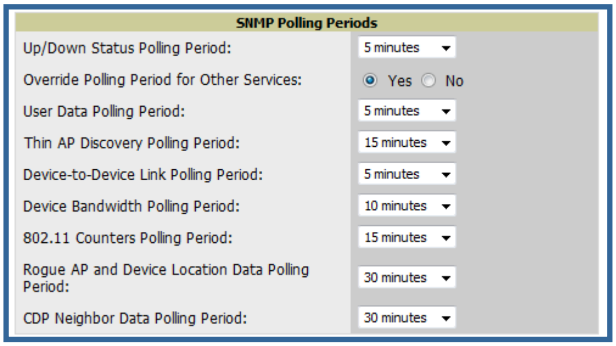
SNMP Settings	
SNMP Timeout (3-60 seconds):	60
SNMP Retries (1-20):	1

Creating a Policy (Group) for Monitoring Alcatel-Lucent Infrastructure

It is prudent to establish an Alcatel-Lucent Group within OV3600.

- 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

Figure 10 – Group Setup



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

- 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 to be lower than "5 minutes".

    Note: Enabling the SNMP Rate Limiting for Monitored Devices option above adds a small delay between each SNMP Get request, thus the actual polling interval is 12 minutes for 10 minute polling interval.
  - Change Device-to-Device Link Polling Period to "30 minutes"
  - Change Rogue AP and Device Location Data Polling Period to "30 minutes".
- Find the Alcatel-Lucent section of page
  - Configure the proper SNMP version
- Click the "Save and Apply" button

Alcatel-Lucent Infrastructure Discovery

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

Summarized procedure for discovery and managing Alcatel-Lucent Infrastructure:

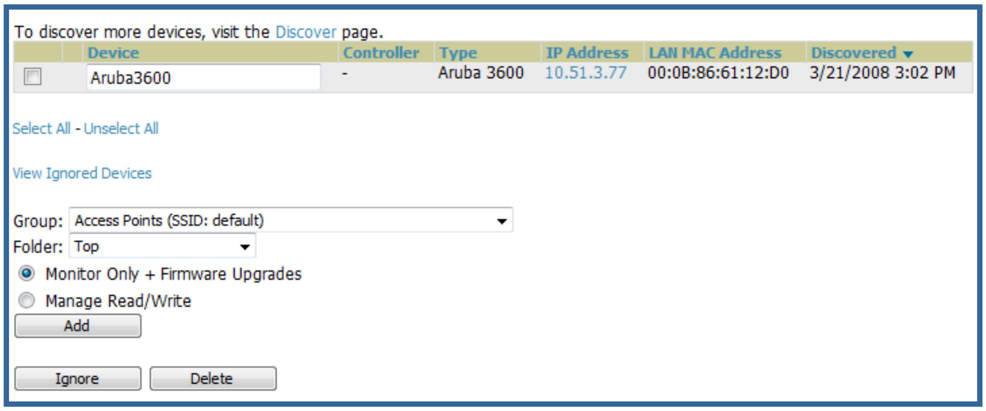
- Discover Master controllers
- Manage Master controllers which automatically discovers Local controllers
- Manage Local controllers which automatically discovers Thin APs affiliated to the controller
- Manage Thin APs

Note: Always add one Controller and its affiliated Thin APs into management or monitoring mode in a serial fashion, one at a time. Adding new devices is a very CPU intensive process for 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.

Master Controller Discovery

- Scan networks containing Alcatel-Lucent Master controllers from Device → Discover page or manually enter the Master controller on the Device → Add page.
- Navigate to APs/Devices → New page
  - Select the Alcatel-Lucent Master controller
  - Ensure “Monitor Only” option is selected
  - Click the “Add” button

Figure 11 – Add New Controller



To discover more devices, visit the Discover page.

	Device	Controller	Type	IP Address	LAN MAC Address	Discovered ▾
☐	Aruba3600	-	Aruba 3600	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

Local Controller Discovery

- Local controllers are discovered via the Master controller. After waiting for the Thin AP Polling Period defined in the Group policy above, the Local controllers will appear on the APs//Devices → New page. Thin APs are discovered via the controller.
- Add the Local controller to a new Group. Within OV3600 Local controllers can be split away from the Master controller’s Group.

Thin AP Discovery

- Thin APs are discovered via the Local controller. After waiting for the Thin AP Polling Period defined in the Group policy above, thin APs will appear on the APs/Devices → New page.
- Add the Thin APs to a new Group. Within OV3600 thin APs can be split away from the controller’s Group. You can split thin APs into multiple Groups if required.

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.

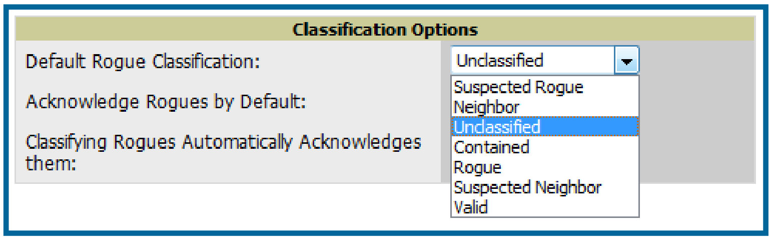
WIPS/WIDS to OV3600 Classification Matrix

OV3600	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 setup default rogue classification

- Navigate to the **Rogue → Setup** page.
- Locate the Classification Options section.
  - Ensure the default rogue classification is set to "Unclassified"

Figure 12 – Rogue Classification Setup



Classification Options

Default Rogue Classification: Unclassified

Acknowledge Rogues by Default:

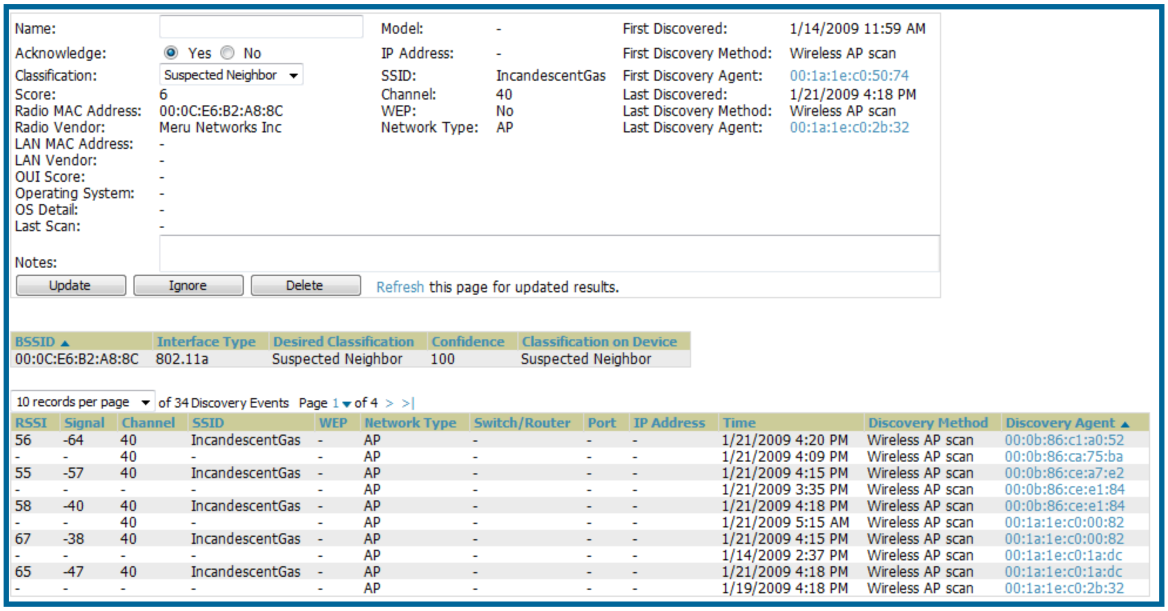
Classifying Rogues Automatically Acknowledges them:

Warning: Changing the default classification can impact the ARM module as well as potentially mitigating devices that might not be true rogues.

To check and reclassify rogue devices

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

Figure 13 – Rogue Detail



Name:		Model:	-	First Discovered:	1/14/2009 11:59 AM
Acknowledge:	● Yes ○ No	IP Address:	-	First Discovery Method:	Wireless AP scan
Classification:	Suspected Neighbor ▾	SSID:	IncandescentGas	First Discovery Agent:	00:1a:1e:c0:50:74
Score:	6	Channel:	40	Last Discovered:	1/21/2009 4:18 PM
Radio MAC Address:	00:0C:E6:B2:A8:8C	WEP:	No	Last Discovery Method:	Wireless AP scan
Radio Vendor:	Meru Networks Inc	Network Type:	AP	Last Discovery Agent:	00:1a:1e:c0:2b:32
LAN MAC Address:	-				
LAN Vendor:	-				
OUI Score:	-				
Operating System:	-				
OS Detail:	-				
Last Scan:	-				
Notes:					

Refresh this page for updated results.

BSSID ▲	Interface Type	Desired Classification	Confidence	Classification on Device
00:0C:E6:B2:A8:8C	802.11a	Suspected Neighbor	100	Suspected Neighbor

10 records per page ▾ of 34 Discovery Events Page 1 ▾ of 4 > >|

RSSI	Signal	Channel	SSID	WEP	Network Type	Switch/Router	Port	IP Address	Time	Discovery Method	Discovery Agent ▲
56	-64	40	IncandescentGas	-	AP	-	-	-	1/21/2009 4:20 PM	Wireless AP scan	00:0b:86:c1:a0:52
-	-	40	-	-	AP	-	-	-	1/21/2009 4:09 PM	Wireless AP scan	00:0b:86:ca:75:ba
55	-57	40	IncandescentGas	-	AP	-	-	-	1/21/2009 4:15 PM	Wireless AP scan	00:0b:86:ce:a7:e2
-	-	-	-	-	AP	-	-	-	1/21/2009 3:35 PM	Wireless AP scan	00:0b:86:ce:e1:84
58	-40	40	IncandescentGas	-	AP	-	-	-	1/21/2009 4:18 PM	Wireless AP scan	00:0b:86:ce:e1:84
-	-	40	-	-	AP	-	-	-	1/21/2009 5:15 AM	Wireless AP scan	00:1a:1e:c0:00:82
67	-38	40	IncandescentGas	-	AP	-	-	-	1/21/2009 4:15 PM	Wireless AP scan	00:1a:1e:c0:00:82
-	-	-	-	-	AP	-	-	-	1/14/2009 2:37 PM	Wireless AP scan	00:1a:1e:c0:1a:dc
65	-47	40	IncandescentGas	-	AP	-	-	-	1/21/2009 4:18 PM	Wireless AP scan	00:1a:1e:c0:1a:dc
-	-	-	-	-	AP	-	-	-	1/19/2009 4:18 PM	Wireless AP scan	00:1a:1e:c0:2b:32

Warning: Changing the rogue classification within the OV3600 UI will push a rogue reclassification message to all controllers managed by the OV3600 server that are in Groups with "Offloading the WMS database" set to "Yes". To reset the classification of a rogue device on OV3600, change the classification on the OV3600 UI to "unclassified".

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

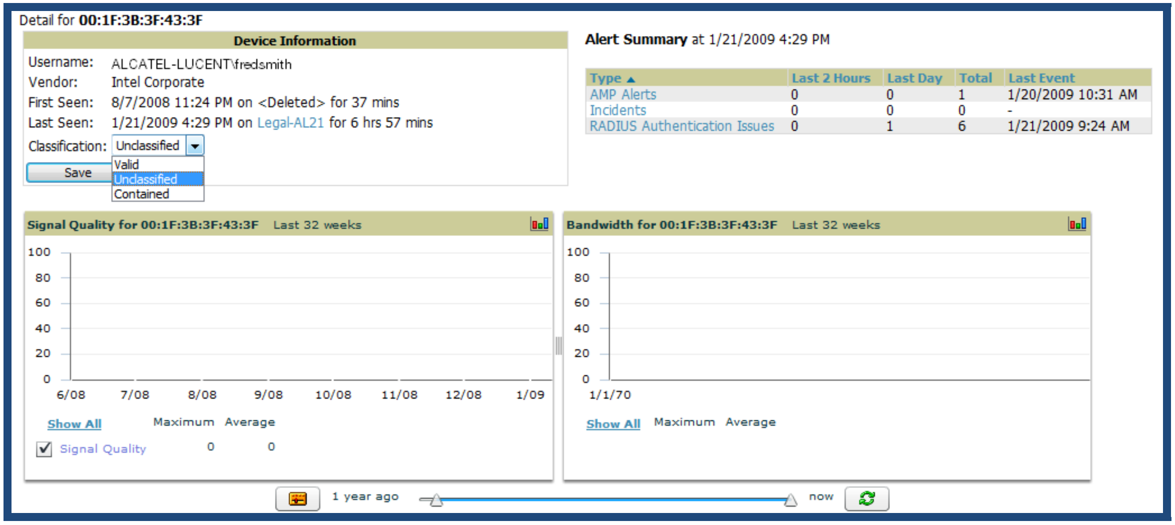
To check and reclassify user devices

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 14 – User Classification



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

Device Information

```
Username:        ALCATEL-LUCENT\fredsmith
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 ▾
                 Valid
                 Unclassified
                 Contained
[Save]
```

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

Signal Quality for 00:1F:3B:3F:43:3F Last 32 weeks

	Maximum	Average
☑ Signal Quality	0	0

Bandwidth for 00:1F:3B:3F:43:3F Last 32 weeks

<span style="color:red">Warning:</span> Changing User Classification within the OV3600 UI will push a user reclassification message to all controllers managed by the OV3600 server that are in Groups with “Offloading the WMS database” set to “Yes”.

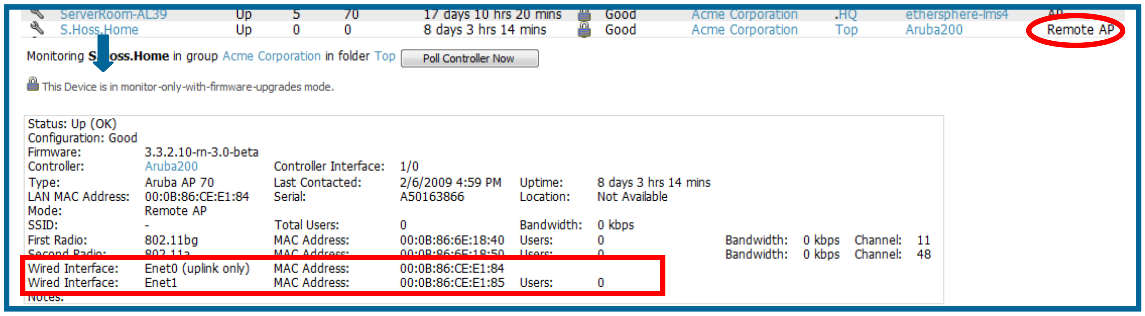
All users will be set to a default classification of “unclassified” on upgrade to OV3600 6.2.\

Alcatel-Lucent-Specific Monitoring Features

OV3600 provides support for many of the Alcatel-Lucent’s unique WLAN capabilities.

Remote AP & Wired Network Monitoring

- From the Device → List page you can distinguish and sort on Mode “Remote”



```
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:
```

- To view detailed information on the remote device click on the device name.

Figure 15 – Remote AP Detail Page

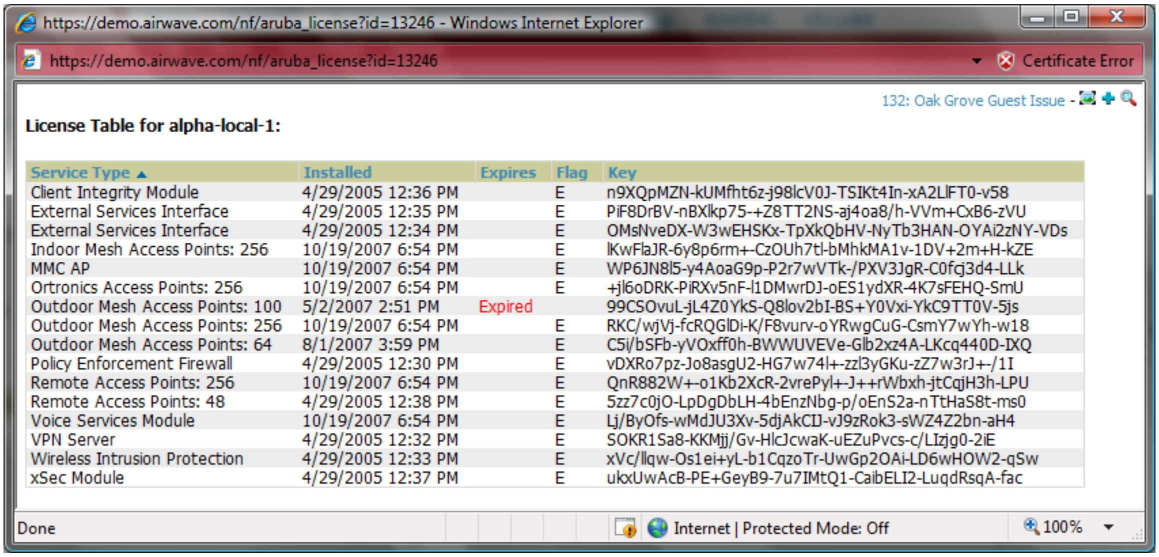
  - You can see if there are users plugged into the wired interfaces.

Note: This feature is only available in OV3600 version 6.2 or greater and AOS-W 3.3.2.10rn2.0 or greater when the remote APs are in split tunnel and tunnel modes.

Controller License Information

- Navigate to the Device → Detail page of a controller 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 -

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

Converting Floor Plans from MMS, AOS-W, and RF Plan 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

Migrating floor plans from MMS to OV3600

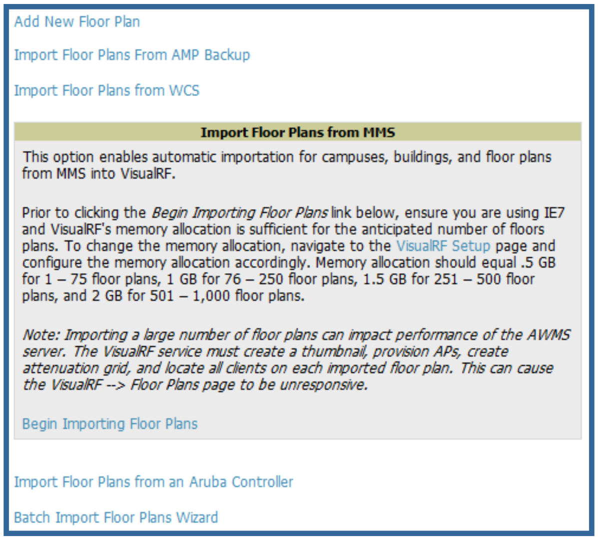
Process

- 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.

Figure 17 – MMS Export Instructions


Add New Floor Plan
Import Floor Plans From AMP Backup
Import Floor Plans from WCS
Begin Importing Floor Plans
Import Floor Plans from an Aruba Controller
Batch Import Floor Plans Wizard

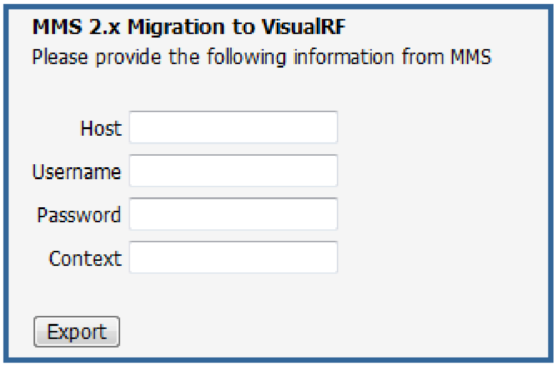
Import Floor Plans from MMS

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.

Figure 18 – MMS Export to OV3600 window

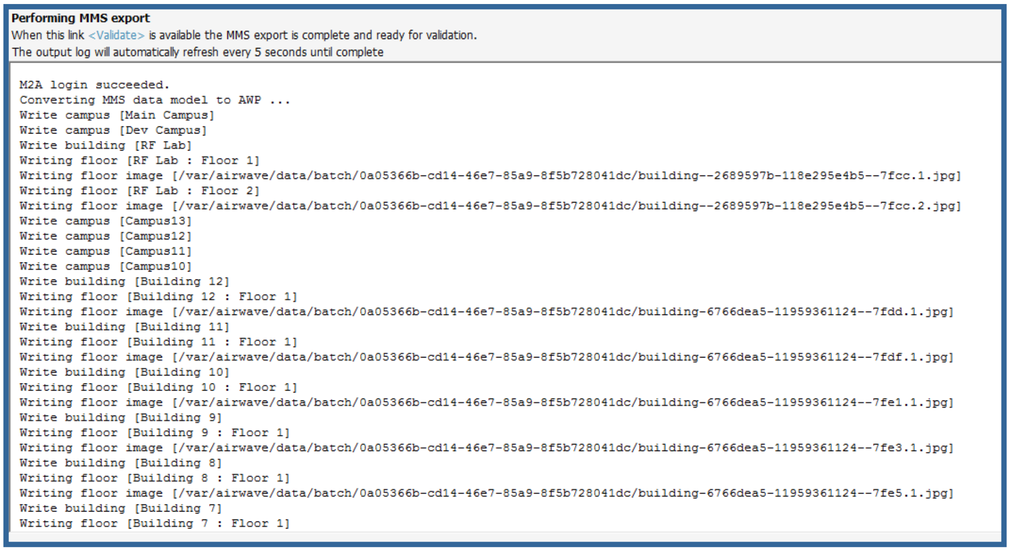


MMS 2.x Migration to VisualRF

Please provide the following information from MMS

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

Figure 19 – MMS export

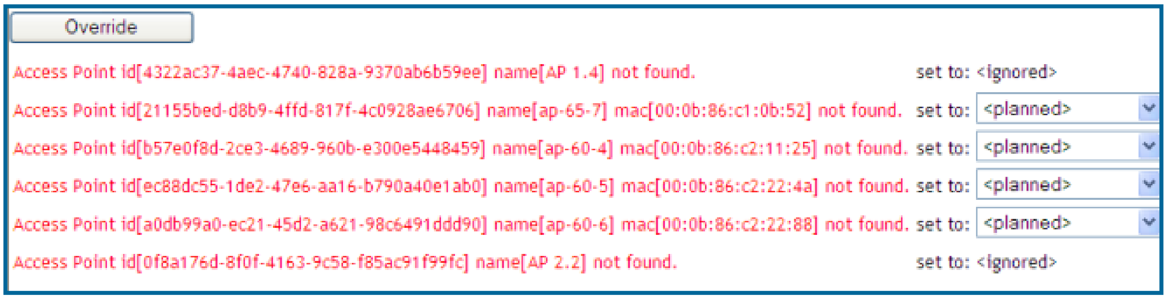


Performing MMS export
When this link <Validate> is available the MMS export is complete and ready for validation.
The output log will automatically refresh every 5 seconds until complete

```
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 20 – Override options



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 OV3600 server; once the batch process is initiated, it can take up to 30 minutes to complete the import process. The VisualRF service must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. The can cause the ***VisualRF → Floor Plans*** *page to be unresponsive.*

Migrating floor plans from an Alcatel-Lucent WLAN Switch to OV3600

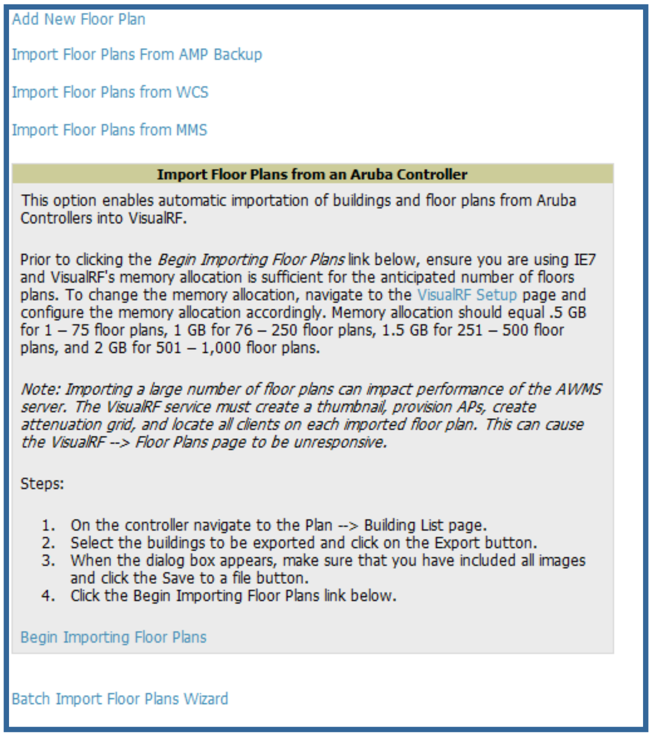
Process on Alcatel-Lucent WLAN Switch

- Login into the Alcatel-Lucent WLAN 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 WLAN 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 controller export process above.
- Click the "Upload" button to validate the XML exported from the controller.
- If there are errors in the XML you will see errors on screen.

Figure 21 – Import Floor Plans from an Alcatel-Lucent WLAN Switch



Add New Floor Plan

Import Floor Plans From AMP Backup

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.

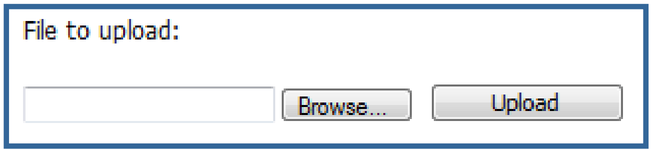
Steps:

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.

Begin Importing Floor Plans

Batch Import Floor Plans Wizard

Figure 22 – File Upload Explorer



File to upload:

Note: Importing a large number of floor plans can impact performance on the OV3600 server. The VisualRF service must create a thumbnail, provision APs, create attenuation grid, and locate all clients on each imported floor plan. The can cause the VisualRF → Floor Plans page to be unresponsive.

Migrating floor plans from an RF Plan to OV3600

Process with RF Plan

- Navigate to the File → Export page.
- From Export drop down select "Controller WebUI Format 3.0"
- 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 Alcatel-Lucent WLAN 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 RF Plan export process above.
- Click the "Upload" button to validate the XML exported from the controller.
- If there are errors in the XML you will see errors on screen.

Utilizing RTLS for Increasing Location 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.

Minimum Requirements

- OV3600 version 6.1 with special RTLS VisualRF build
- AOS-W 3.1.x or higher

Deployment Topology

Figure 23 – Typical Client Location Deployment

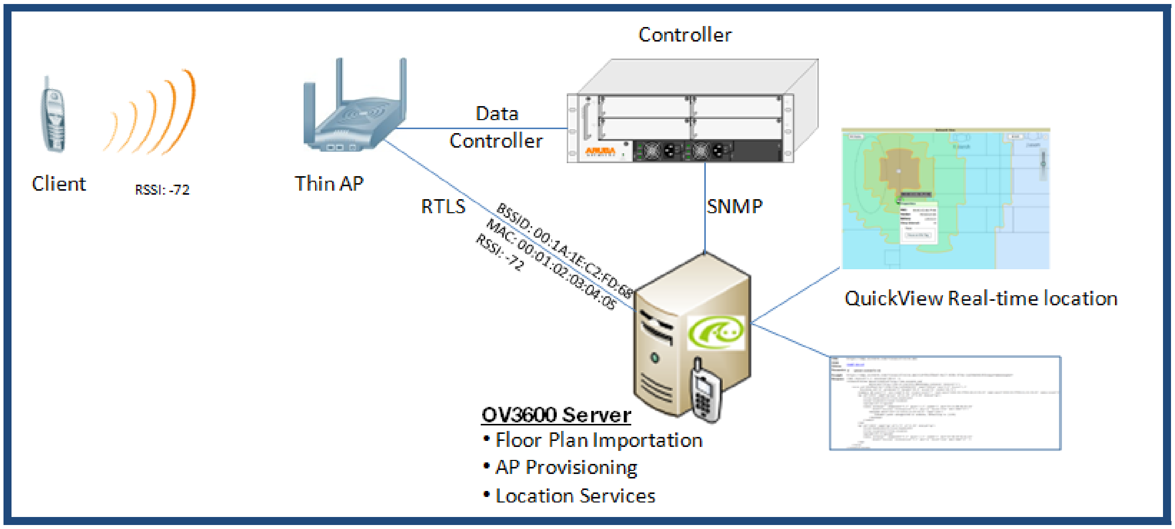
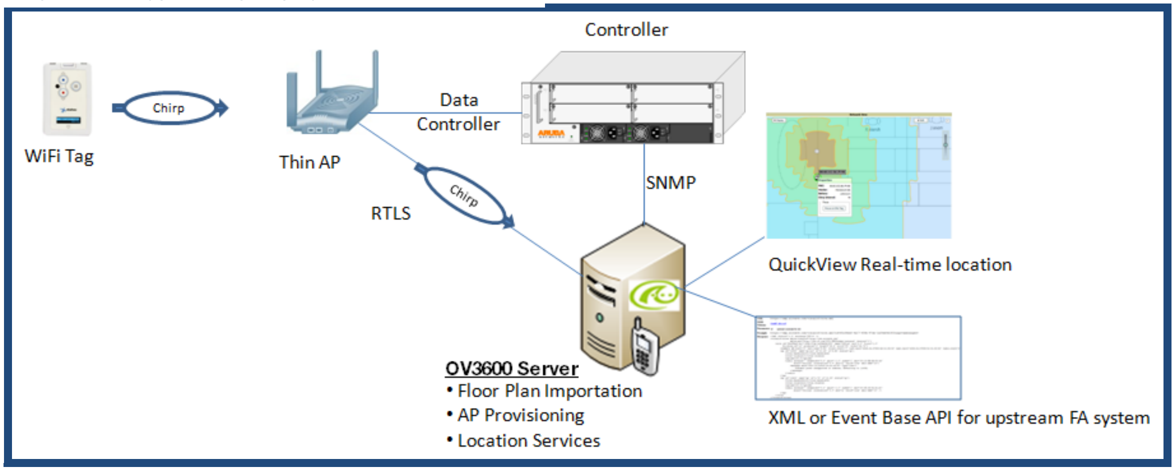


Figure 24 – Typical Tag Deployment



Prerequisites for RTLS

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.

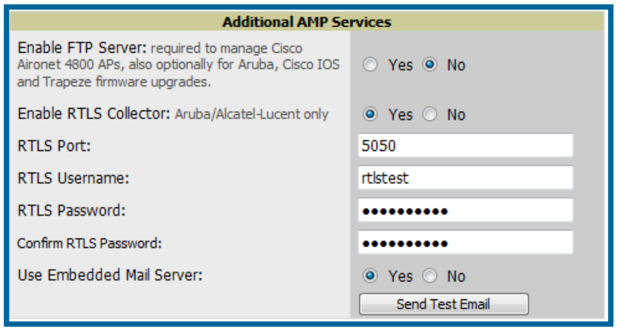
Known Issues

AOS-W	OV3600	Description	Resolution
3.1	6.1	Wi-Fi Tags will only display in VisualRF. Wi-Fi Tags will not display within OV3600' UI or the controller's UI.	No ETA

Enabling RTLS service on the OV3600 server

- Navigate to OV3600 **Setup** → **General** page
- 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 controller default is 5050
  - RTLS Username – match the SNMPv3 "MMS" username configured on controller
  - RTLS Password – match the SNMPv3 "MMS" password configured on controller
- Click on the "Save" button at the bottom of the page.

Figure 25 – RTLS Setup



Additional AMP 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

Enabling RTLS on Alcatel-Lucent Infrastructure

Note: RTLS can only be enabled on the master controller and it will automatically propagate to all local controllers.

- SSH into master controller, enter "enable" mode, and issue the following commands:

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

(Controller-Name) (config) # ap system-profile <PROFILE USED BY THIN APs>
```

```
(Controller-Name) (AP system profile "default") # rtls-server ip-addr <IP
OF OV3600 SERVER> port 5050 key <SNMPv3 "MMS" PASSWORD CONFIGURED ON
CONTROLLER>
(Controller-Name) (AP system profile "default") # write mem
Saving Configuration...

Saved Configuration
```

- To validate exit configuration mode

```
(Controller-Name) # show ap monitor debug status ip-addr <IP ADDRESS OF ANY
THIN ACCESS POINTS>
...
RTLS configuration
-------------------
Type        Server IP    Port  Frequency  Active
----        ---------    ----  ---------  ------
MMS         10.51.2.45   5070  120
Aeroscout   N/A          N/A   N/A
RTLS        10.51.2.45   5050  60         *
```

Troubleshooting RTLS

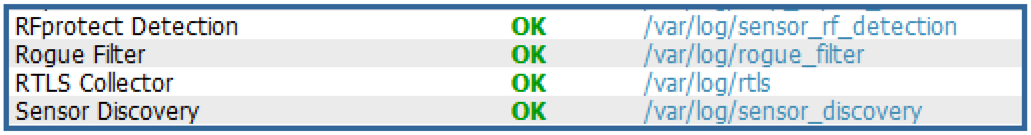
- Ensure the RTLS service is running on your OV3600 server. SSH into your OV3600 server.

```
[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 26 – 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:
00147aaf01000020001a1ec02b3200000001000000137aae0100000c001a1ec02b3200000
01a1e82b322590006ddff02
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:
0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec0507800000
00d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006
c4ff02

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:
0014c9c90100003c001a1ec050780000000200000013c9c70100000c001a1ec0507800000
00d54a7a280540001ddff020013c9c80100000c001a1ec050780000000cdb8ae9a9000006
c4ff02
```

- 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.