OmniVista 3600 Air Manager 8.2.14.0

Alcatel·Lucent Enterprise

Best Practices Guide

Copyright

Open Source Code

Chapter 1 Overview

This document provides best practices for leveraging OmniVista 3600 Air Manager to monitor and manage your Alcatel-Lucent infrastructure, which provides a wealth of functionality such as firewall, VPN, remote AP, IDS, IPS, and ARM, as well as an abundance of statistical information.

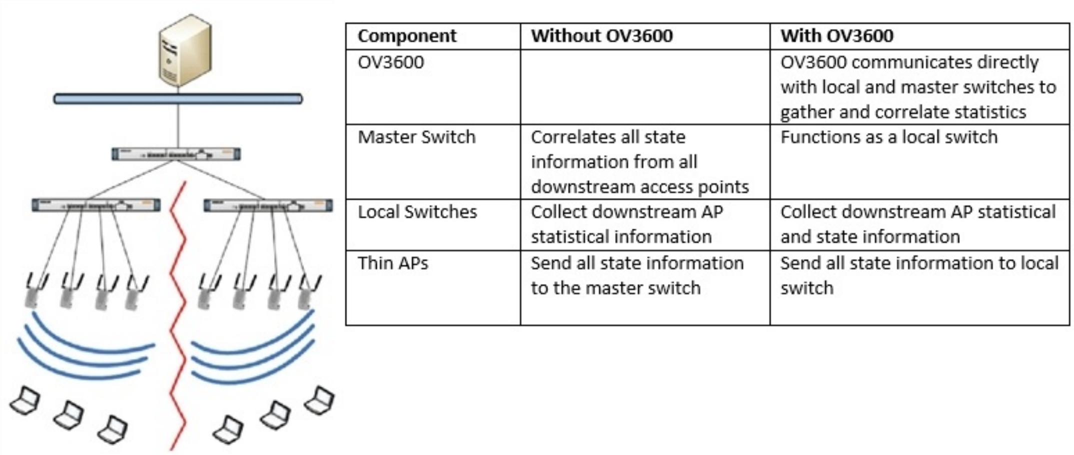
Follow the simple guidelines in this document to garner the full benefit of your Alcatel-Lucent infrastructure.

This overview chapter contains the following topics:

- Understanding Alcatel-Lucent Topology
- Prerequisites for Integrating Alcatel-Lucent Infrastructure

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

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
Thin APs	Send all state information to the master switch	Send all state information to local switch

NOTE

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

In order to integrate your Alcatel-Lucent infrastructure, you need the following information:

- SNMP community string for monitoring and discovery
- Telnet/SSH credentials for configuration
- **Enable** password for configuration

NOTE

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

Chapter 2
Configuring OV3600 for Global Alcatel-Lucent Infrastructure

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

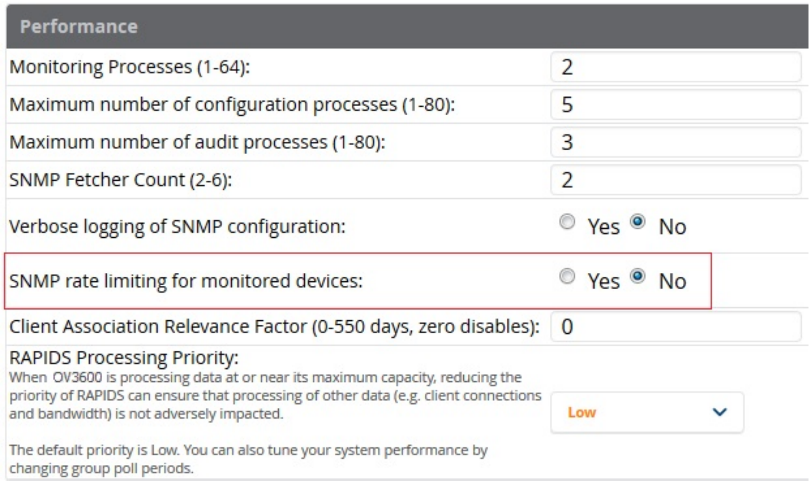
- Disabling Rate Limiting in OV3600 Setup > General
- Entering Credentials in Device Setup > Communication
- Setting Up Recommended SNMP Timeout and Retries
- Setting Up Time Synchronization
- Enabling Support for Channel Utilization And Statistics

The SNMP Rate Limiting for Monitored Devices option adds a small delay between each SNMP GET request, which results in the actual polling intervals that are longer than what is configured. For example, setting a ten-minute polling interval will result in an actual 12-minute polling interval. Disabling rate limiting is recommended in most cases.

To disable rate limiting in OV3600, follow these steps:

1. Navigate to **OV3600 Setup > General**.
2. Locate the **Performance** section.
3. In the **SNMP rate limiting for monitored devices** field, select **No**, as shown in Figure 2.
4. Click **Save**.

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



Performance

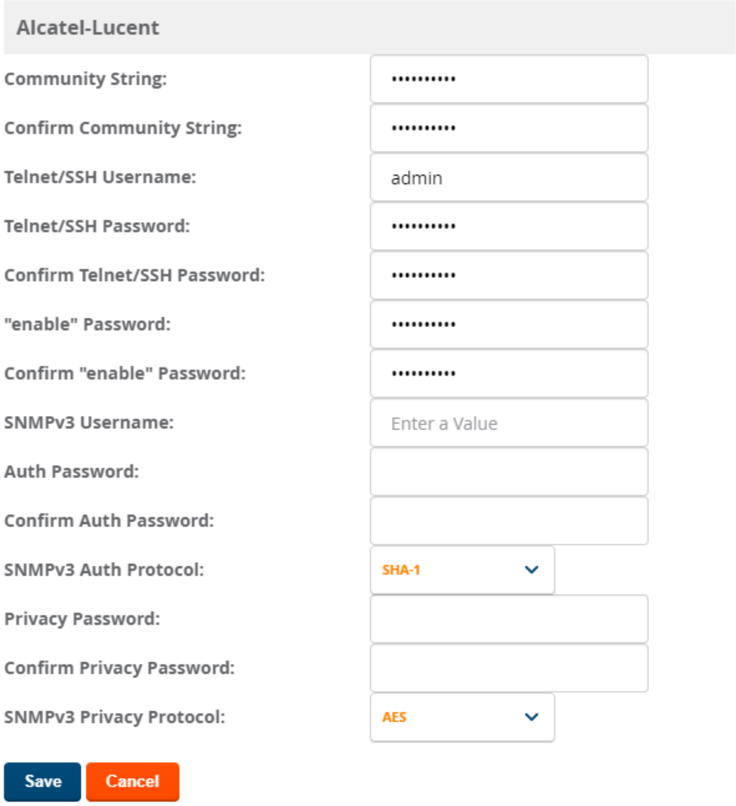
Monitoring Processes (1-64):	2
Maximum number of configuration processes (1-80):	5
Maximum number of audit processes (1-80):	3
SNMP Fetcher Count (2-6):	2
Verbose logging of SNMP configuration:	○ Yes ● No
SNMP rate limiting for monitored devices:	○ Yes ● No
Client Association Relevance Factor (0-550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

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

1. Navigate to **Device Setup > Communication**.
2. In the **Default Credentials** section, click **Edit** link next to **Alcatel-Lucent**. The page illustrated in Figure 3 appears.
3. Enter the **SNMP Community String**.

> NOTE
>
> Be sure to note the community string because it must match the SNMP trap community string. Refer to Define AirWave as a Trap Host Using the ArubaOS CLI.

Figure 3 *Credentials in **Device Setup > Communication***



Alcatel-Lucent

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

a. Enter the required information for configuration and basic monitoring:
   - Telnet/SSH user name
   - Telnet/SSH password
   - Enable mode password

4. Click **Save**.

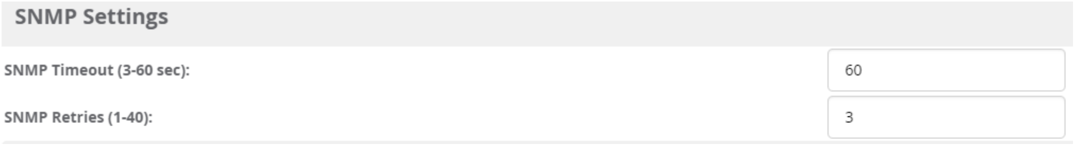
1. In the **Device Setup > Communication** page, locate the **SNMP Settings** section.
2. Change the **SNMP Timeout** setting to a value or either **3**, **4**, or **5**. This is the number of seconds that OV3600 will wait for a response from a device after sending an SNMP request, so a smaller number is more ideal.
3. Change the **SNMP Retries** value to **10**. This value represents the number of times OV3600 tries to poll a device when it does not receive a response within the SNMP Timeout Period or the Group's

Missed SNMP Poll Threshold setting (1-100).

NOTE

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

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



SNMP Settings

SNMP Timeout (3-60 sec): 60

SNMP Retries (1-40): 3

4. Click **Save**.

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

Manually Setting the Clock on a switch

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

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

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

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

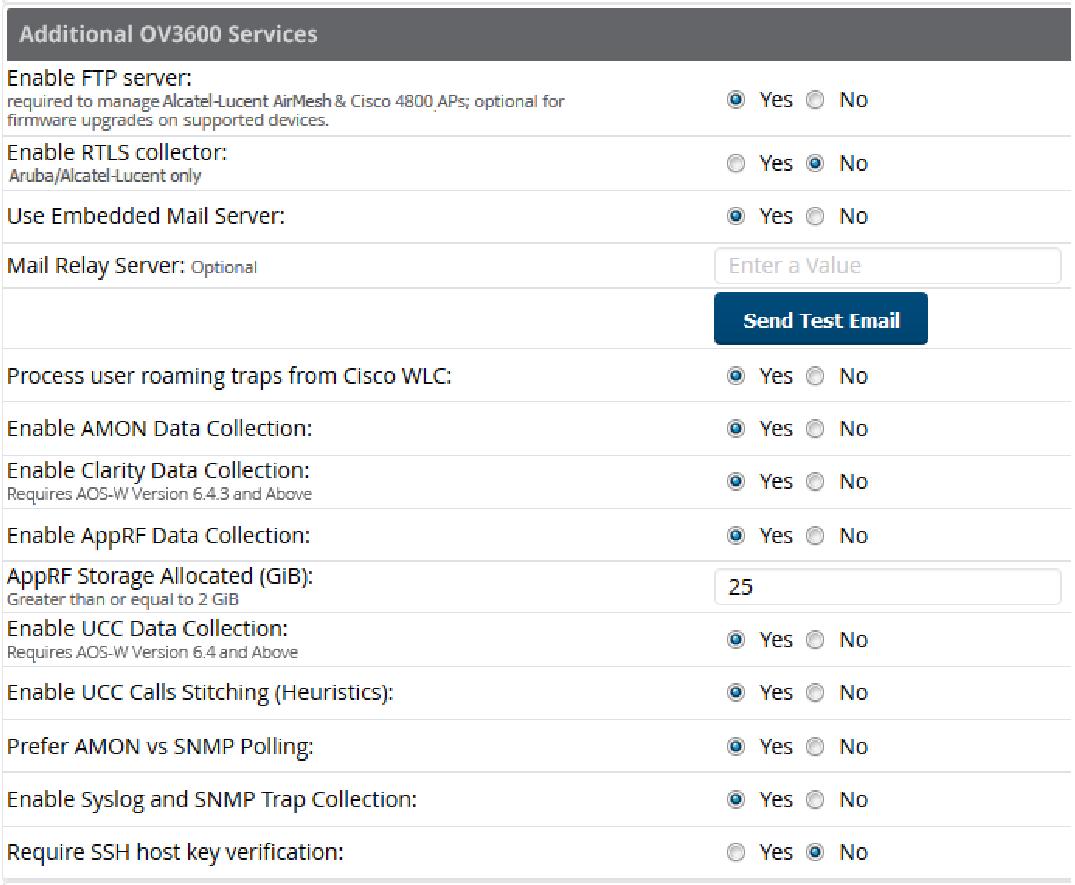
NOTE

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

OV3600 Setup

1. Navigate to **OV3600 Setup > General**.
2. In the **Additional OV3600 Services** section, set **Enable AMON Data Collection** to **Yes**, and set **Prefer AMON vs SNMP Polling** to **Yes**.
3. Click **Save**.

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



Additional OV3600 Services

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

- Avoid running nightly maintenance and scheduled reports in overlapping time intervals.
- Always set a host name for your OV3600.
- If you manage the devices with IPv6, IPv4 addresses as dual-stack, add the devices with IPv6 address in OV3600 **Device setup > Add** or **Import Devices via CSV** file and add the IPv6 address of OV3600 as an mgmt-server on the controller.

switch Setup (Conductor And Local)

NOTE

Enabling these commands on AOS-W versions prior to 6.0.1.0 can result in performance issues on the switch. If you are running previous firmware versions such as AOS-W 6.0.0.0, you should upgrade to AOS-W 6.0.1 (to obtain RF utilization metrics) or 6.1 (to obtain RF utilization *and* classified interferer information) before you enter this command.

Using Alcatel-Lucent AOS-W 6.x

The following commands are for AOS-W versions 6.3.1 and later 6.x releases. To get the commands for other versions of AOS-W 6.x, refer to the *Command-Line Interface Reference Guide* for that version.

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

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

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

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

You can add up to four <OV3600-IP> addresses in a Mobility Conductor setup.

You can add up to three <OV3600-IP> addresses in a managed devices setup.

Using Alcatel-Lucent AOS-W 8.x

The following commands are for AOS-W versions 8.4 and earlier 8.x releases. To get the commands for other versions of AOS-W 8.x, refer to the *Command-Line Interface Reference Guide* for that version.

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

```
(host) [mynode] # configure terminal
```

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

```
(host) [mynode] (config) #mgmt-server primary-server <OV3600-IP>
(host) [mynode] (config) #profile default-amp
(host) [mynode] (config) #write memory
```

You can add up to four <OV3600-IP> addresses in a Mobility Conductor setup.

You can add up to three <OV3600-IP> addresses in a managed devices setup.

- To reduce AMON messages from the controller, disable the unnecessary management profiles on the Alcatel-Lucent controller.
- To reduce **AMON_STATION_RSSI_INFO_V2_MESSAGE** incoming from the controller, reduce the RSSI interval to 60/120 seconds from the default 5 seconds on the controller.

Chapter 3
Configuring an Alcatel-Lucent Group

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

This section contains the following topics:

- Basic Monitoring Configuration
- Advanced Configuration

1. Navigate to **Groups > List**.
2. Click **Add**.
3. Enter a **Name** that represents the Alcatel-Lucent device infrastructure from a security, geographical, or departmental perspective and Click **Add**.
4. You will be redirected to the **Groups > Basic** page for the Group you just created. On this page you will need to verify and/or change the following Alcatel-Lucent-specific settings.

a. Find the **SNMP Polling Periods** section of the page, as illustrated in Figure 6.

b. Verify that the **Override Polling Period for Other Services** option is set to **Yes.**

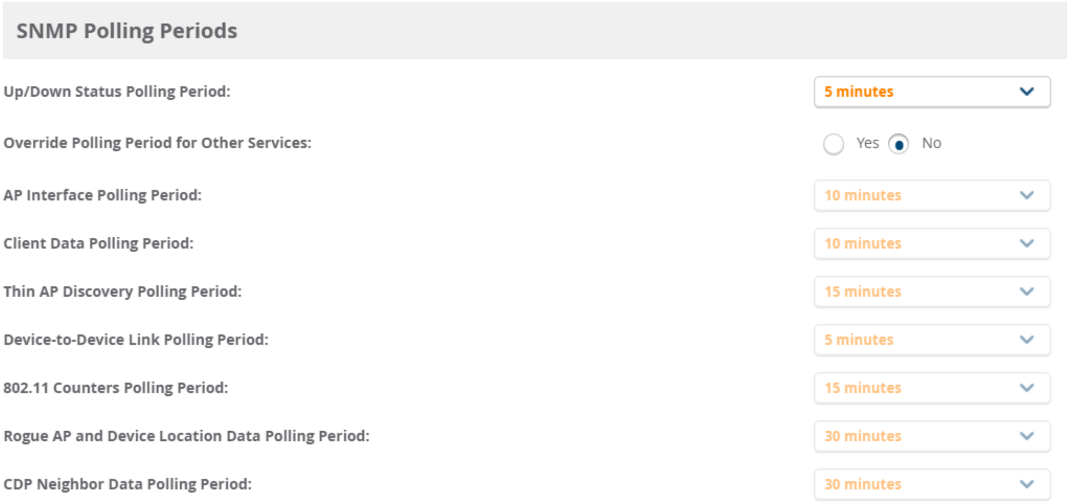
c. Verify that **Client Data Polling Period** is set to 10 minutes. Do not configure this interval lower than 5 minutes.

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

d. Verify that the **Device-to-Device Link Polling Period** option is set to **30 minutes**.

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

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

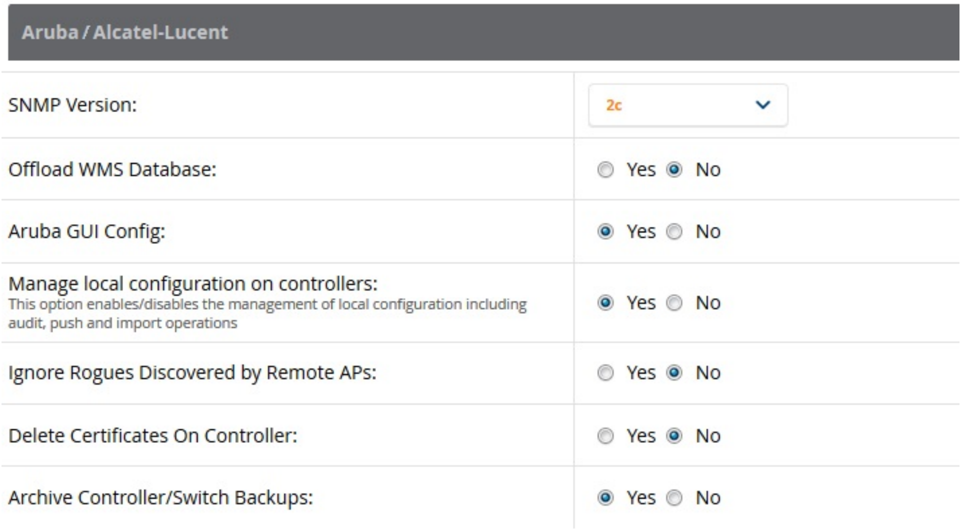


SNMP Polling Periods

Up/Down Status Polling Period:	5 minutes
Override Polling Period for Other Services:	○ Yes ● No
AP Interface Polling Period:	10 minutes
Client Data Polling Period:	10 minutes
Thin AP Discovery Polling Period:	15 minutes
Device-to-Device Link Polling Period:	5 minutes
802.11 Counters Polling Period:	15 minutes
Rogue AP and Device Location Data Polling Period:	30 minutes
CDP Neighbor Data Polling Period:	30 minutes

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

Figure 7 *Group SNMP Version for Monitoring*



Aruba / Alcatel-Lucent

SNMP Version:	2c
Offload WMS Database:	○ Yes ● No
Aruba GUI Config:	● Yes ○ No
Manage local configuration on controllers: This option enables/disables the management of local configuration including audit, push and import operations	● Yes ○ No
Ignore Rogues Discovered by Remote APs:	○ Yes ● No
Delete Certificates On Controller:	○ Yes ● No
Archive Controller/Switch Backups:	● Yes ○ No

7. Click **Save and Apply**.

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

Chapter 4

Discovering Alcatel-Lucent Infrastructure

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

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

- Configuring OV3600 for Global Alcatel-Lucent Infrastructure
- Configuring an Alcatel-Lucent Group

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

- Discovering or Adding Conductor switches
- Local switch/Managed Devices Discovery
- Thin AP Discovery

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.

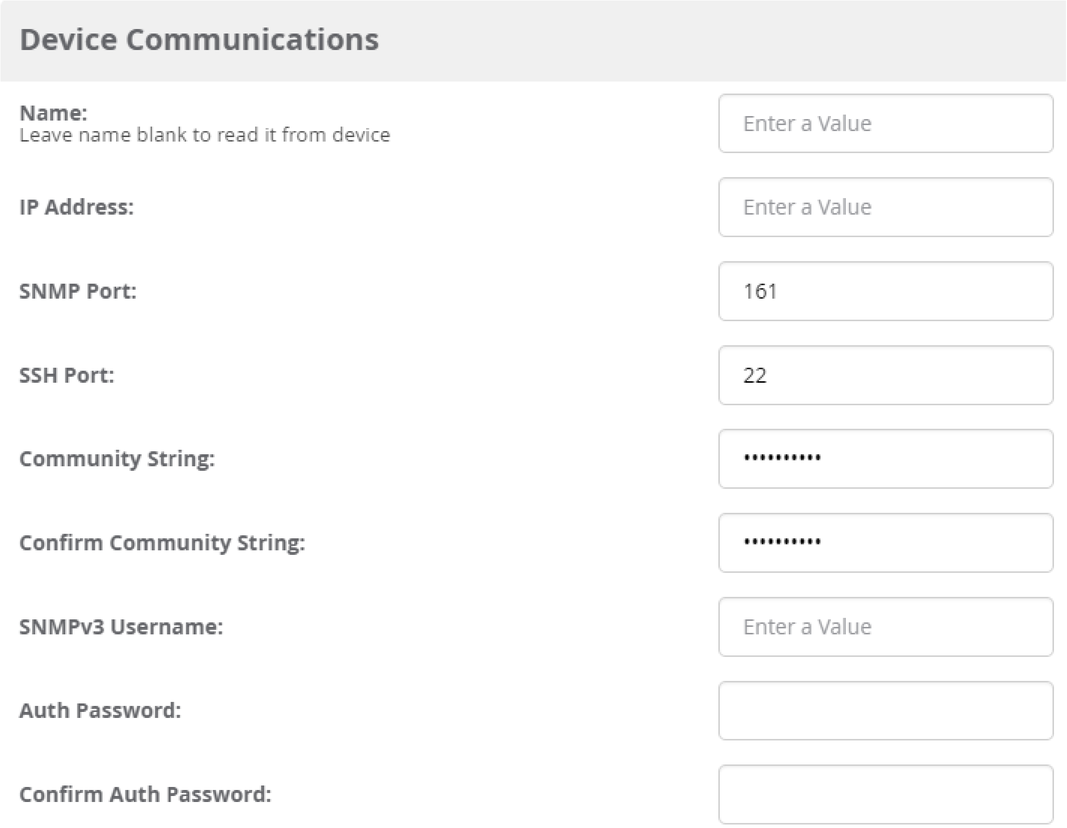
Scan networks containing Alcatel-Lucent conductor switches from the **Device Setup > Discover** page, or manually enter the conductor switch by following these steps in the **Device Setup > Add** page:

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

NOTE

Be sure to note the community string because it must match the SNMP trap community string. Refer to Define OV3600 as a Trap Host Using the AOS-W CLI.

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



Device Communications

Name: Leave name blank to read it from device	Enter a Value
IP Address:	Enter a Value
SNMP Port:	161
SSH Port:	22
Community String:	••••••••••
Confirm Community String:	••••••••••
SNMPv3 Username:	Enter a Value
Auth Password:	
Confirm Auth Password:	

4. Enter the required fields for configuration and basic monitoring:
   - Telnet/SSH user name
   - Telnet/SSH password
   - Enable password

NOTE

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

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

NOTE

If you select Manage read/write, OV3600 will push the group setting configuration, and existing device configurations will be deleted/overwritten.

7. Click **Add**.
8. Navigate to the **Devices > New** page.
9. Select the Alcatel-Lucent conductor switch you just added from the list of new devices.
10. Ensure **Monitor Only** option is selected.
11. Click **Add**.

In AOS-W 6.x, the controllers can be deployed as Conductor or Local. In a Conductor-Local deployment, Conductor holds the responsibility of all policy configurations. This include services such as WIPS, Initial AP configurations, user roles, and authentication-related configurations, etc. The local controller/managed devices terminates AP tunnels, processes and forwards user traffic (including authentication), manages ARM (Adaptive Radio Management), mobility features, and QoS.

In AOS-W 8.x, Alcatel-Lucent also offers a Mobility Conductor Appliance which provides additional features which are not available in the other controller models. In AOS-W 8.x deployment, we can have MM-MD deployment where there is a Mobility Conductor and managed devices (MD) forming a cluster. It provides controller clustering capability that allows better user experience via features like Hitless failover, Automatic user load balancing, Automatic AP load balancing, and seamless roaming across the cluster. This type of deployment could perhaps be considered for sensitive environments where high wireless performance and reliability are a requirement for critical services.

NOTE

AOS-W 8.X is necessary with Mobility Conductor Appliance. APs cannot terminate on any Conductor or Mobility Conductor controllers, APs can only terminate on controllers deployed in local mode. ArubaOS 6.X allows AP termination on either Conductor or local controllers/managed devices.

Local switches/managed devices are added to OV3600 via the Conductor switch by a discovery scan, or manually added in **Device Setup > Add**. After waiting for the Thin AP Polling Period interval or executing a **Poll Controller Now** command from the **Devices > Monitor** page, the local switches/managed devices will appear on the **Devices > New** page.

Add the local switch/managed device to the Group defined previously. Within OV3600, local switches/managed devices can be split away from the Conductor switch's Group.

NOTE

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

Thin APs are discovered via the local switch/managed device. After waiting for the Thin AP Polling Period or executing a **Poll Controller Now** command from the **Devices > Monitor** page, thin APs will appear on the **Devices > New** page.

Add the thin APs to the Group defined previously. Within OV3600, thin APs can be split away from the switch's Group. You can split thin APs into multiple Groups if required.

Chapter 5
OV3600 and Alcatel-Lucent Integration Strategies

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

- Integration Goals
- Example Use Cases
- Prerequisites for Integration
- Define OV3600 as a Trap Host Using the AOS-W CLI

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

Table 1: *Integration Goals in All Conductors or Conductor/Local Architectures*

Integration Goals	All Conductors Architecture	Conductor/Local Architecture
Rogue And Client Info	—	enable stats
Rogue containment only	ssh access to switches	ssh access to switches
IDS And Auth Tracking	Define OV3600 as a trap host	Define OV3600 as a trap host
Channel Utilization	enable Application Monitoring (AMON)	enable AMON
Spectrum	enable AMON	enable AMON
Traffic Analysis Visibility	enable AMON	enable AMON
UCC Visability	enable AMON	enable AMON
Health Information	enable Adaptive Radio Management (ARM)	enable ARM

Following are the key integration points:

- IDS Tracking does require enable stats in a conductor/local environment.
- Unless you enable stats on the local switches in a conductor/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 conductor switch.

The following are example use cases of integration strategies:

- When to Use Enable Stats
- When to Use RTLS
- When to Define OV3600 as a Trap Host

When to Use Enable Stats

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

NOTE

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

When to Use RTLS

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

  NOTE

  > RTLS can negatively impact your OV3600 server's performance.

- See Leveraging RTLS to Increase Accuracy.

When to Define OV3600 as a Trap Host

- You want to track IDS events within the OV3600 UI.
- You are in the process of converting their older third-party WLAN devices to Alcatel-Lucent devices and want a unified IDS dashboard for all WLAN infrastructure.
- You want to relate Auth failures to a client device, AP, Group of APs, and switch. OV3600 provides this unique correlation capability.

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

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

- Configuring OV3600 for Global Alcatel-Lucent Infrastructure
- Configuring an Alcatel-Lucent Group
- Discovering Alcatel-Lucent Infrastructure

To ensure the OV3600 server is defined as a trap host, access the command line interface of each switch (conductor 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 those that were configured in Configuring OV3600 for Global Alcatel-Lucent Infrastructure.

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

NOTE

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

Ensuring That IDS and Auth Traps Display in OV3600

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

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

If any of the traps in the output of this command do not appear to be enabled, enter `configure terminal` mode and issue the following command:

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

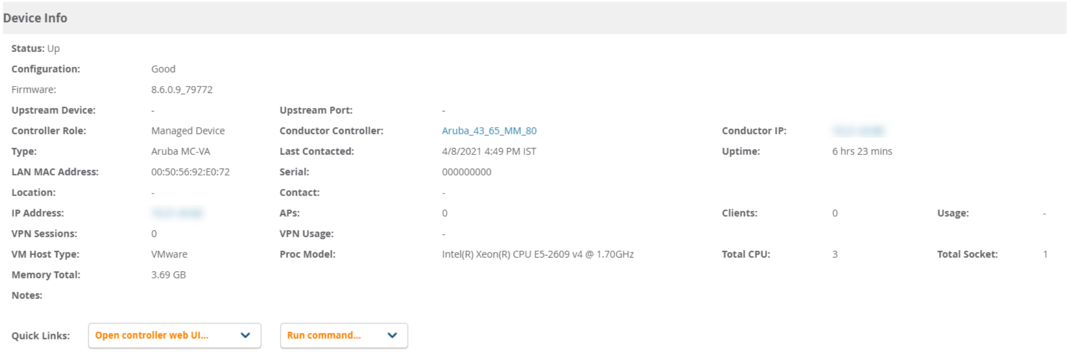
NOTE

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

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

Ensure the source IP of the traps match the IP that OV3600 uses to manage the switch, see Figure 9. Navigate to **Devices > Monitor** to validate the IP address in the **Device Info** section.

Figure 9 *Verify IP Address on **Devices > Monitor** Page*



Device Info

Status: Up

Configuration:	Good						
Firmware:	8.6.0.9_79772						
Upstream Device:	-	Upstream Port:	-				
Controller Role:	Managed Device	Conductor Controller:	Aruba_43_65_MM_80	Conductor IP:	[redacted]		
Type:	Aruba MC-VA	Last Contacted:	4/8/2021 4:49 PM IST	Uptime:	6 hrs 23 mins		
LAN MAC Address:	00:50:56:92:E0:72	Serial:	000000000				
Location:	-	Contact:	-				
IP Address:	[redacted]	APs:	0	Clients:	0	Usage:	-
VPN Sessions:	0	VPN Usage:	-				
VM Host Type:	VMware	Proc Model:	Intel(R) Xeon(R) CPU E5-2609 v4 @ 1.70GHz	Total CPU:	3	Total Socket:	1
Memory Total:	3.69 GB						
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
```

Chapter 6
Alcatel-Lucent Specific Capabilities

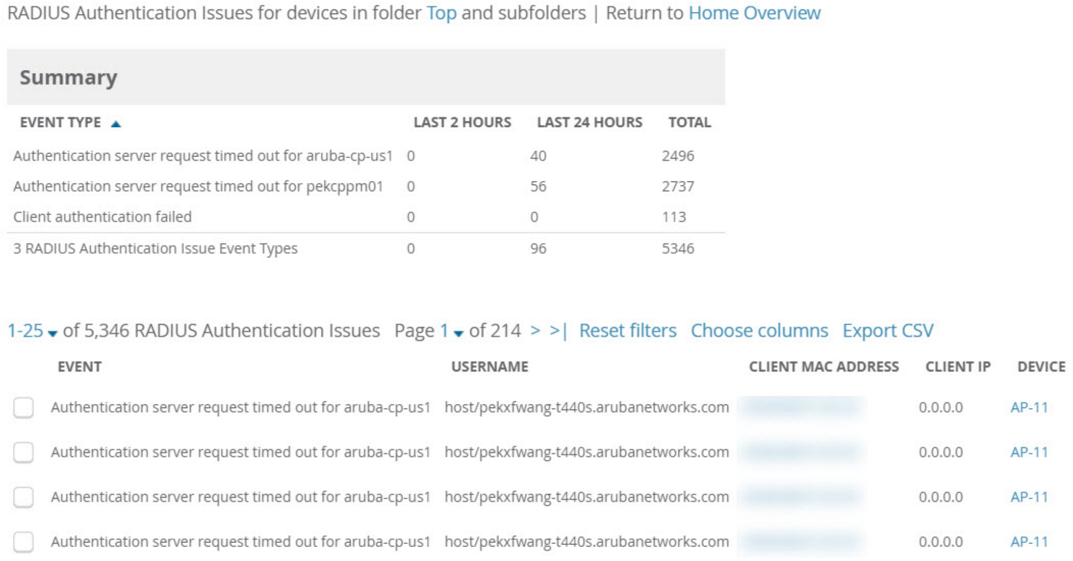
This section discusses Alcatel-Lucent specific capabilities in OV3600 and contains the following topics:

- Alcatel-Lucent Traps for RADIUS Auth and IDS Tracking
- Remote AP Monitoring
- ARM and Channel Utilization Information
- Viewing switch License Information
- Rules-Based Controller Classification
- Best Practices for Switch Setup
- Instant AP and Instant GUI Config
- Best Practices while Using VisualRF

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

View a list of recent RADIUS authentication issues by navigating to the **Home >Overview** page, and selecting the **RADIUS Issues** link in the **Alert Summary** table at the bottom of the page.Figure 10 shows all authentication failures related to RADIUS data.

Figure 10 *RADIUS Issues Summary*



RADIUS Authentication Issues for devices in folder Top and subfolders | Return to Home Overview

Summary

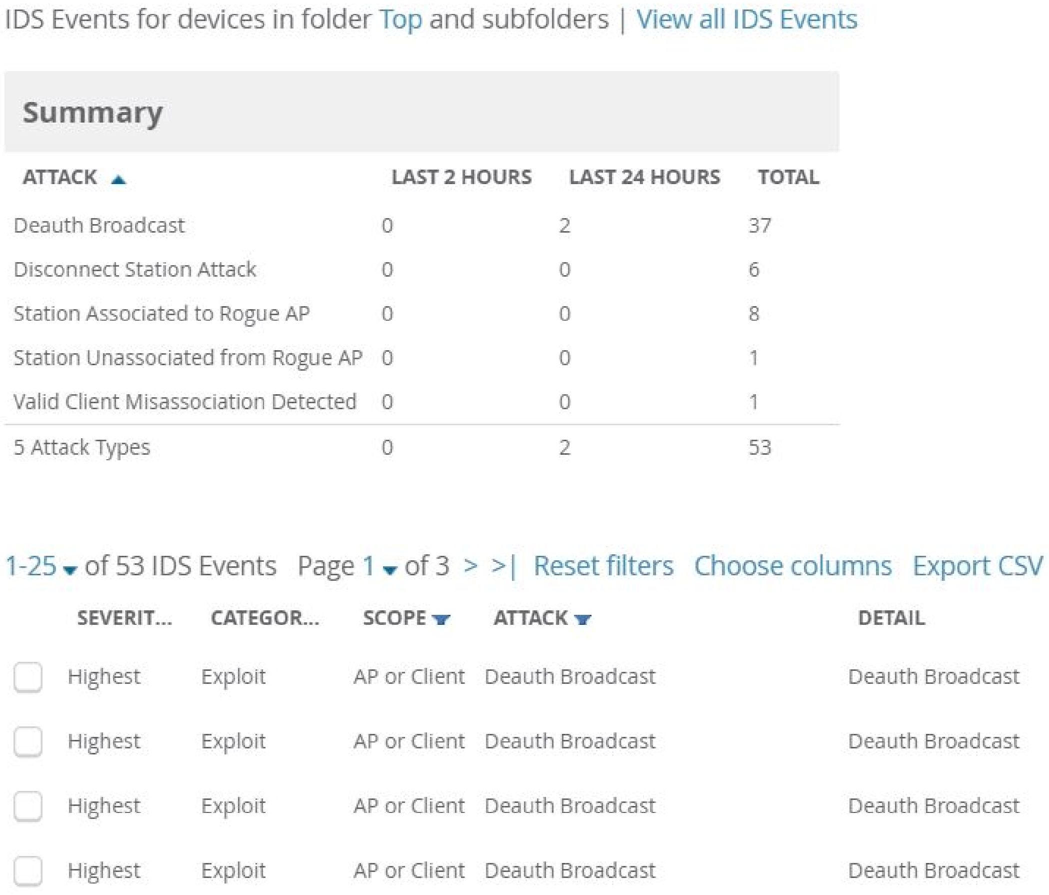
EVENT TYPE ▲	LAST 2 HOURS	LAST 24 HOURS	TOTAL
Authentication server request timed out for aruba-cp-us1	0	40	2496
Authentication server request timed out for pekcppm01	0	56	2737
Client authentication failed	0	0	113
3 RADIUS Authentication Issue Event Types	0	96	5346

1-25 ▾ of 5,346 RADIUS Authentication Issues Page 1 ▾ of 214 > >| Reset filters Choose columns Export CSV

	EVENT	USERNAME	CLIENT MAC ADDRESS	CLIENT IP	DEVICE
□	Authentication server request timed out for aruba-cp-us1	host/pekxfwang-t440s.arubanetworks.com	[redacted]	0.0.0.0	AP-11
□	Authentication server request timed out for aruba-cp-us1	host/pekxfwang-t440s.arubanetworks.com	[redacted]	0.0.0.0	AP-11
□	Authentication server request timed out for aruba-cp-us1	host/pekxfwang-t440s.arubanetworks.com	[redacted]	0.0.0.0	AP-11
□	Authentication server request timed out for aruba-cp-us1	host/pekxfwang-t440s.arubanetworks.com	[redacted]	0.0.0.0	AP-11

There are two ways to navigate to the list of recent IDS events. You can go to the **Home >Overview** page and select the **IDS Events** link in the **Alert Summary** table at the bottom of the page, or go directly to **RAPIDS > IDS Events**. The IDS Events Summary page includes a table that shows the numbers of events in each IDS category, as well as a sortable table of each event. (See Figure 11.)

Figure 11 *IDS Events in OV3600*



IDS Events for devices in folder Top and subfolders | View all IDS Events

Summary

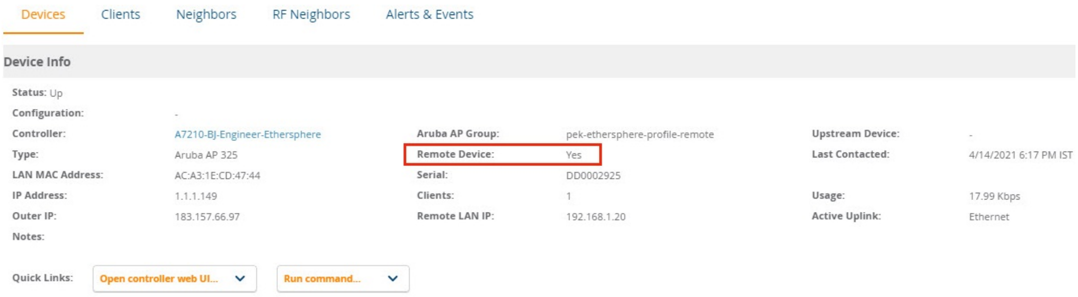
ATTACK ▲	LAST 2 HOURS	LAST 24 HOURS	TOTAL
Deauth Broadcast	0	2	37
Disconnect Station Attack	0	0	6
Station Associated to Rogue AP	0	0	8
Station Unassociated from Rogue AP	0	0	1
Valid Client Misassociation Detected	0	0	1
5 Attack Types	0	2	53

1-25 ▾ of 53 IDS Events Page 1 ▾ of 3 > >| Reset filters Choose columns Export CSV

	SEVERIT...	CATEGOR...	SCOPE ▾	ATTACK ▾	DETAIL
□	Highest	Exploit	AP or Client	Deauth Broadcast	Deauth Broadcast
□	Highest	Exploit	AP or Client	Deauth Broadcast	Deauth Broadcast
□	Highest	Exploit	AP or Client	Deauth Broadcast	Deauth Broadcast
□	Highest	Exploit	AP or Client	Deauth Broadcast	Deauth Broadcast

To monitor remote APs, follow these steps:

1. From the **Devices > List** page, filter on the **Remote Device** column to find remote devices.
2. To view detailed information about the remote device, select the device name. The page illustrated in Figure 12 appears.
3. **Figure 12** *Remote AP Detail Page*



Device Info

Status: Up

Configuration:	-				
Controller:	A7210-BJ-Engineer-Ethersphere	Aruba AP Group:	pek-ethersphere-profile-remote	Upstream Device:	-
Type:	Aruba AP 325	Remote Device:	Yes	Last Contacted:	4/14/2021 6:17 PM IST
LAN MAC Address:	AC:A3:1E:CD:47:44	Serial:	DD0002925		
IP Address:	1.1.1.149	Clients:	1	Usage:	17.99 Kbps
Outer IP:	183.157.66.97	Remote LAN IP:	192.168.1.20	Active Uplink:	Ethernet
Notes:					

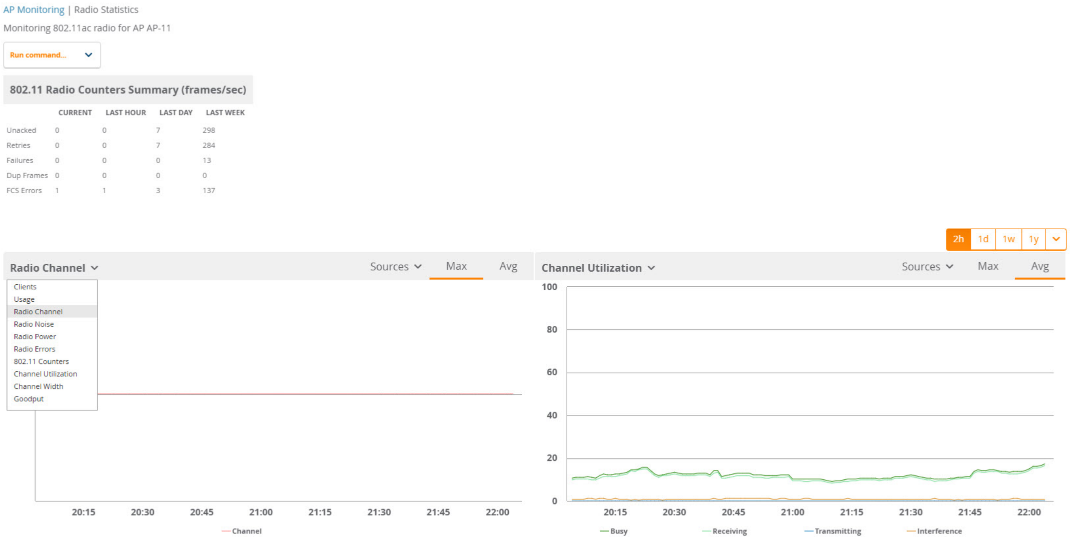
You can also see if there are users plugged into the wired interfaces in the **Connected Clients** list below the **Clients** and **Usage** graphs at the bottom of this page.

NOTE

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

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

1. Navigate to an **Devices > Monitor** page for any AP that supports ARM and channel utilization.
2. In the **Radios** table, select a radio link under the **Name** column for a radio.
3. The graphs default to Client and Usage. Select an icon for each to change the graphs to display Radio Channel and Channel Utilization.
4. **Figure 13** *ARM and Channel Utilization Graphs*



AP Monitoring | Radio Statistics

Monitoring 802.11ac radio for AP AP-11

Run command...

802.11 Radio Counters Summary (frames/sec)

	CURRENT	LAST HOUR	LAST DAY	LAST WEEK
Unacked	0	0	7	298
Retries	0	0	7	284
Failures	0	0	0	13
Dup Frames	0	0	0	0
FCS Errors	1	1	3	137

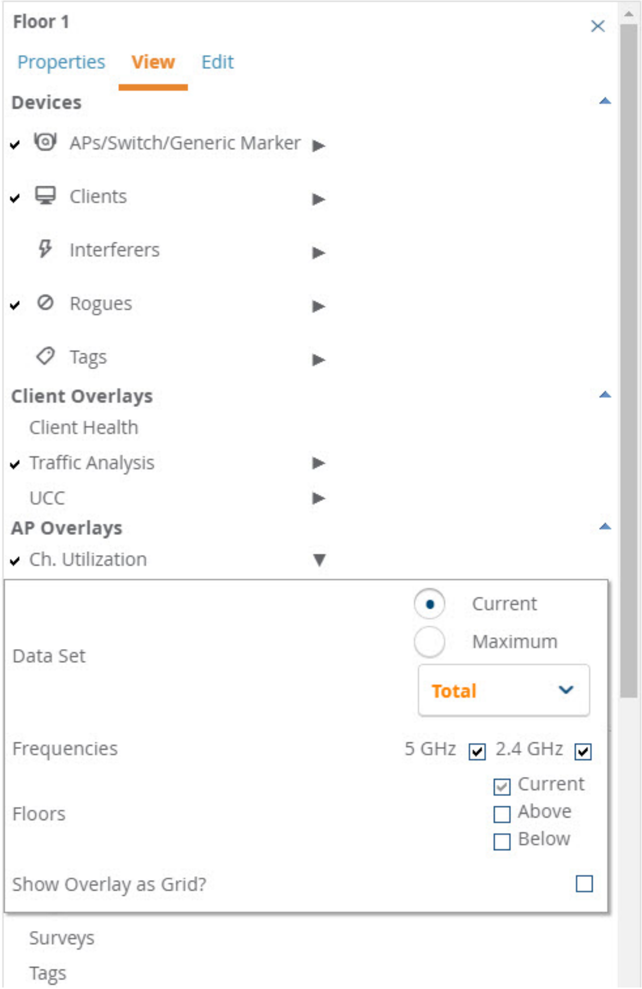
For more information about the data that displays in the **Radio Statistics** page for the devices, refer to the latest *AirWave User Guide*.

VisualRF and Channel Utilization

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

9. Select a frequency **(5 GHz** and/or **2.4 GHz**).

Figure 14 *Overlays*



Floor 1

Properties | View | Edit

Devices

- ✓ APs/Switch/Generic Marker ▶
- ✓ Clients ▶
- Interferers ▶
- ✓ Rogues ▶
- Tags ▶

Client Overlays

- Client Health
- ✓ Traffic Analysis ▶
- UCC ▶

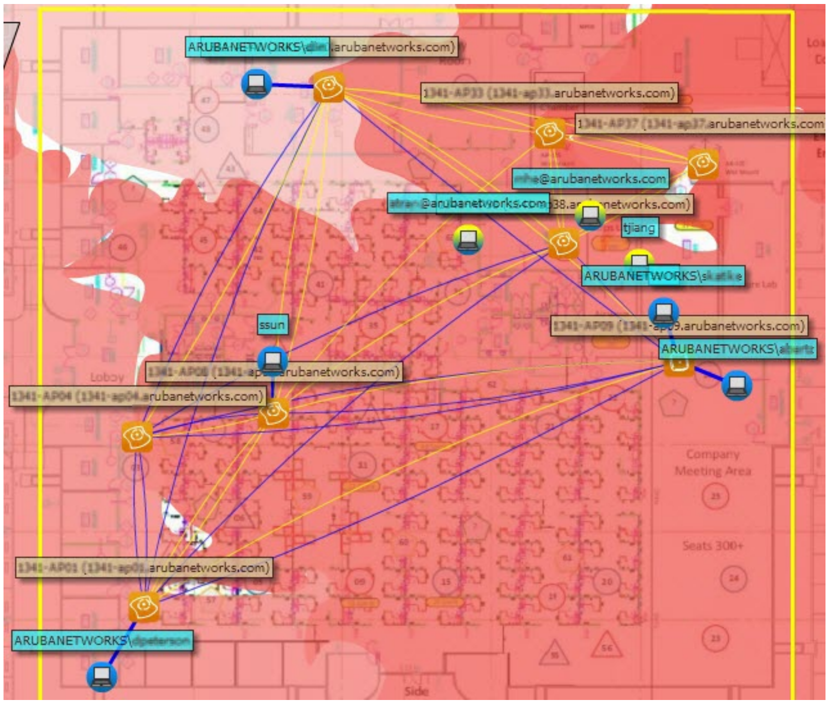
AP Overlays

- ✓ Ch. Utilization ▼

Data Set	● Current ○ Maximum Total
Frequencies	5 GHz ☑ 2.4 GHz ☑
Floors	☑ Current □ Above □ Below
Show Overlay as Grid?	□

- Surveys
- Tags

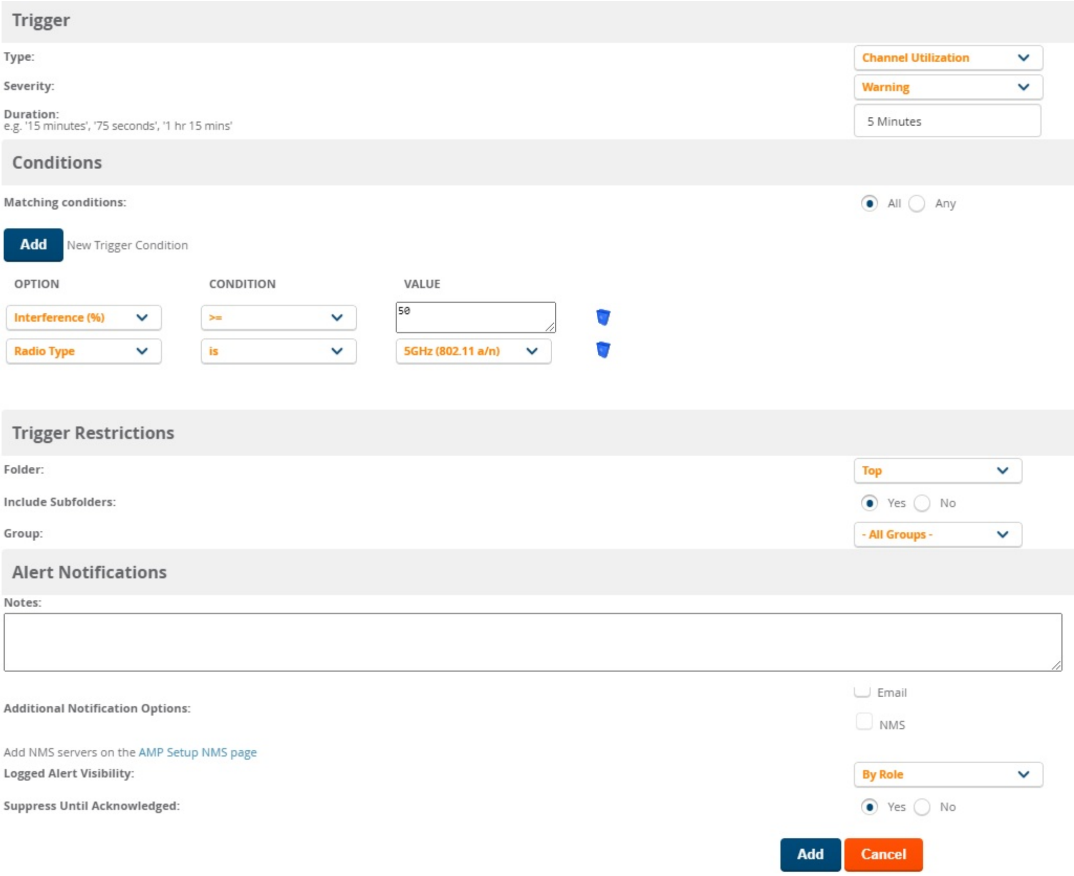
Figure 15 *Channel Utilization in VisualRF (Interference/2.4 GHz)*


ARUBANETWORKS\[redacted].arubanetworks.com)
1341-AP33 (1341-ap33.arubanetworks.com)
1341-AP37 (1341-ap37.arubanetworks.com
[redacted]@arubanetworks.com
[redacted]@arubanetworks.com
38.ar[redacted]networks.com)
tjiang
ARUBANETWORKS\[redacted]
ssun
1341-AP09 (1341-ap09.arubanetworks.com)
ARUBANETWORKS\[redacted]
1341-AP08 (1341-ap[redacted]rubanetworks.com)
1341-AP04 (1341-ap04.arubanetworks.com)
Lobby
Company
Meeting Area
Seats 300+
1341-AP01 (1341-ap01.arubanetworks.com)
ARUBANETWORKS\[redacted]
Side

For more information about the **AP Overlays**, refer to the latest *AirWave User Guide*.

1. Navigate to **System > Triggers** and select **Add**.
2. Select **Channel Utilization** from the **Type** drop-down menu as seen on Figure 16:

   Figure 16 *Channel Utilization Trigger*



Trigger

Type: Channel Utilization

Severity: Warning

Duration: 5 Minutes
e.g. '15 minutes', '75 seconds', '1 hr 15 mins'

Conditions

Matching conditions: ● All ○ Any

Add New Trigger Condition

OPTION	CONDITION	VALUE
Interference (%)	>=	50
Radio Type	is	5GHz (802.11 a/n)

Trigger Restrictions

Folder: Top

Include Subfolders: ● Yes ○ No

Group: - All Groups -

Alert Notifications

Notes:

Additional Notification Options: □ Email □ NMS

Add NMS servers on the AMP Setup NMS page

Logged Alert Visibility: By Role

Suppress Until Acknowledged: ● Yes ○ No

3. Enter the duration evaluation period.
4. Click the **Add New Trigger Condition** button.
5. Create a trigger condition for **Radio Type** and select the frequency to evaluate.
6. Select **Interference(%), Radio Type, Time busy (%), Time Receiving (%), or Time Transmitting (%)** trigger condition.
7. Set up any restrictions or notifications. (Refer to the *OmniVista 3600 Air Manager 8.2.14.0 User Guide* for more details.)
8. When you are finished, click **Add**.

For more information about the **Trigger** page, refer to the latest *AirWave User Guide*.

Viewing Channel Utilization Alerts

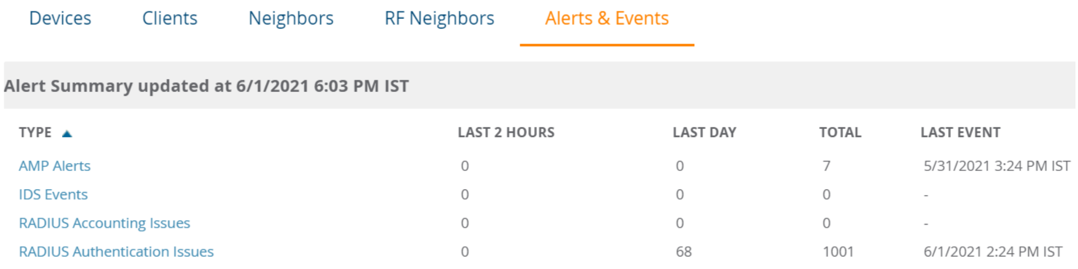
You can view Channel Utilization alerts from the **Devices > Monitor** page and on the **System > Alerts** page.

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

1. Navigate to the **Devices > list** page and select a device.
2. Navigate to the **Monitor** page for that device.

3. Go to the **Alerts & Events** tab and Click **AMP Alerts** to check the Alert summary for the selected device.

Figure 17 *AMP Alerts*

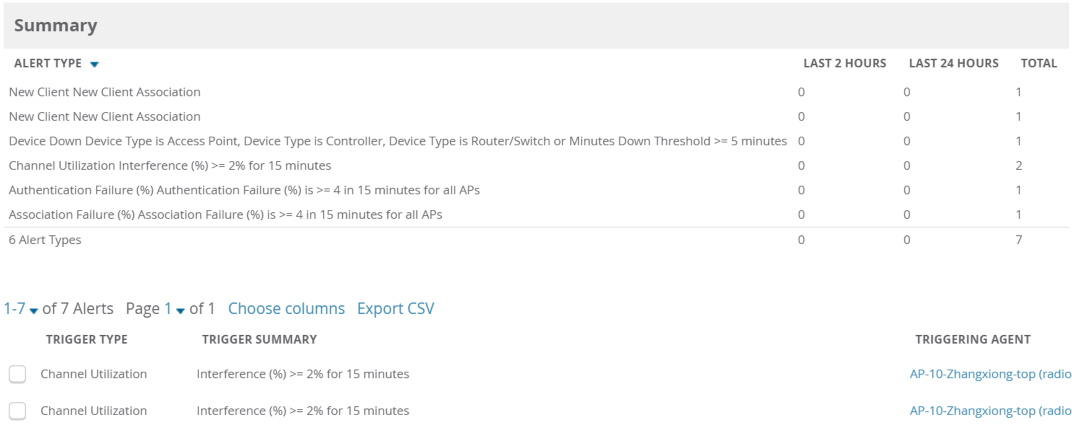


Devices Clients Neighbors RF Neighbors Alerts & Events

Alert Summary updated at 6/1/2021 6:03 PM IST

TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	0	0	7	5/31/2021 3:24 PM IST
IDS Events	0	0	0	-
RADIUS Accounting Issues	0	0	0	-
RADIUS Authentication Issues	0	68	1001	6/1/2021 2:24 PM IST

Figure 18 *Channel Utilization alerts*



Summary

ALERT TYPE ▼	LAST 2 HOURS	LAST 24 HOURS	TOTAL
New Client New Client Association	0	0	1
New Client New Client Association	0	0	1
Device Down Device Type is Access Point, Device Type is Controller, Device Type is Router/Switch or Minutes Down Threshold >= 5 minutes	0	0	1
Channel Utilization Interference (%) >= 2% for 15 minutes	0	0	2
Authentication Failure (%) Authentication Failure (%) is >= 4 in 15 minutes for all APs	0	0	1
Association Failure (%) Association Failure (%) is >= 4 in 15 minutes for all APs	0	0	1
6 Alert Types	0	0	7

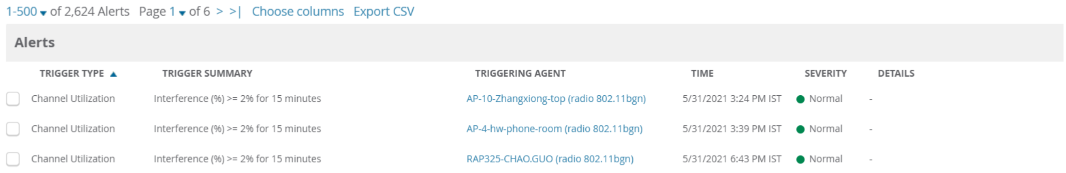
1-7 ▾ of 7 Alerts Page 1 ▾ of 1 Choose columns Export CSV

	TRIGGER TYPE	TRIGGER SUMMARY	TRIGGERING AGENT
□	Channel Utilization	Interference (%) >= 2% for 15 minutes	AP-10-Zhangxiong-top (radio
□	Channel Utilization	Interference (%) >= 2% for 15 minutes	AP-10-Zhangxiong-top (radio

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

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

Figure 19 *Channel Utilization alerts on the System > Alerts page*



1-500 ▾ of 2,624 Alerts Page 1 ▾ of 6 > >| Choose columns Export CSV

Alerts

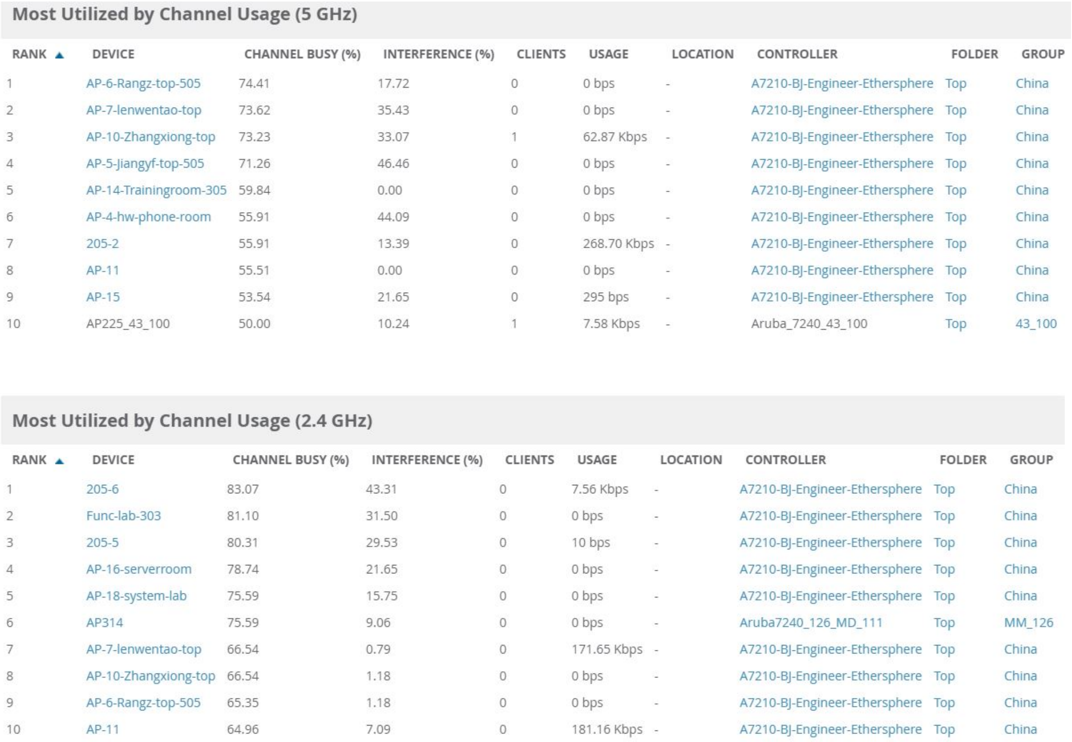
	TRIGGER TYPE ▲	TRIGGER SUMMARY	TRIGGERING AGENT	TIME	SEVERITY	DETAILS
□	Channel Utilization	Interference (%) >= 2% for 15 minutes	AP-10-Zhangxiong-top (radio 802.11bgn)	5/31/2021 3:24 PM IST	● Normal	-
□	Channel Utilization	Interference (%) >= 2% for 15 minutes	AP-4-hw-phone-room (radio 802.11bgn)	5/31/2021 3:39 PM IST	● Normal	-
□	Channel Utilization	Interference (%) >= 2% for 15 minutes	RAP325-CHAO.GUO (radio 802.11bgn)	5/31/2021 6:43 PM IST	● Normal	-

For more information about the **Alerts** page, refer to the latest *AirWave User Guide*.

View Channel Utilization in RF Health Reports

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

Figure 20 *Channel Utilization in an RF Health Report (partial view)*



Most Utilized by Channel Usage (5 GHz)

RANK ▲	DEVICE	CHANNEL BUSY (%)	INTERFERENCE (%)	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
1	AP-6-Rangz-top-505	74.41	17.72	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
2	AP-7-lenwentao-top	73.62	35.43	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
3	AP-10-Zhangxiong-top	73.23	33.07	1	62.87 Kbps	-	A7210-BJ-Engineer-Ethersphere	Top	China
4	AP-5-Jiangyf-top-505	71.26	46.46	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
5	AP-14-Trainingroom-305	59.84	0.00	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
6	AP-4-hw-phone-room	55.91	44.09	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
7	205-2	55.91	13.39	0	268.70 Kbps	-	A7210-BJ-Engineer-Ethersphere	Top	China
8	AP-11	55.51	0.00	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
9	AP-15	53.54	21.65	0	295 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
10	AP225_43_100	50.00	10.24	1	7.58 Kbps	-	Aruba_7240_43_100	Top	43_100

Most Utilized by Channel Usage (2.4 GHz)

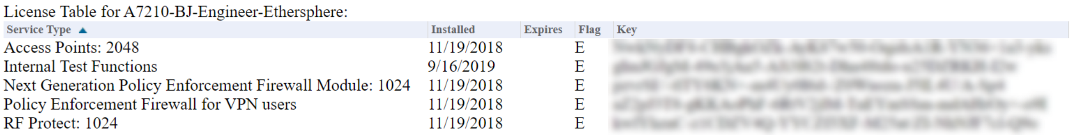
RANK ▲	DEVICE	CHANNEL BUSY (%)	INTERFERENCE (%)	CLIENTS	USAGE	LOCATION	CONTROLLER	FOLDER	GROUP
1	205-6	83.07	43.31	0	7.56 Kbps	-	A7210-BJ-Engineer-Ethersphere	Top	China
2	Func-lab-303	81.10	31.50	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
3	205-5	80.31	29.53	0	10 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
4	AP-16-serverroom	78.74	21.65	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
5	AP-18-system-lab	75.59	15.75	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
6	AP314	75.59	9.06	0	0 bps	-	Aruba7240_126_MD_111	Top	MM_126
7	AP-7-lenwentao-top	66.54	0.79	0	171.65 Kbps	-	A7210-BJ-Engineer-Ethersphere	Top	China
8	AP-10-Zhangxiong-top	66.54	1.18	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
9	AP-6-Rangz-top-505	65.35	1.18	0	0 bps	-	A7210-BJ-Engineer-Ethersphere	Top	China
10	AP-11	64.96	7.09	0	181.16 Kbps	-	A7210-BJ-Engineer-Ethersphere	Top	China

For more information about the **Reports** page, refer to the latest *AirWave User Guide*.

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

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

Figure 21 *switch License Popup from the **Devices > Monitor** page*



License Table for A7210-BJ-Engineer-Ethersphere:

Service Type ▲	Installed	Expires	Flag	Key
Access Points: 2048	11/19/2018		E	[redacted]
Internal Test Functions	9/16/2019		E	[redacted]
Next Generation Policy Enforcement Firewall Module: 1024	11/19/2018		E	[redacted]
Policy Enforcement Firewall for VPN users	11/19/2018		E	[redacted]
RF Protect: 1024	11/19/2018		E	[redacted]

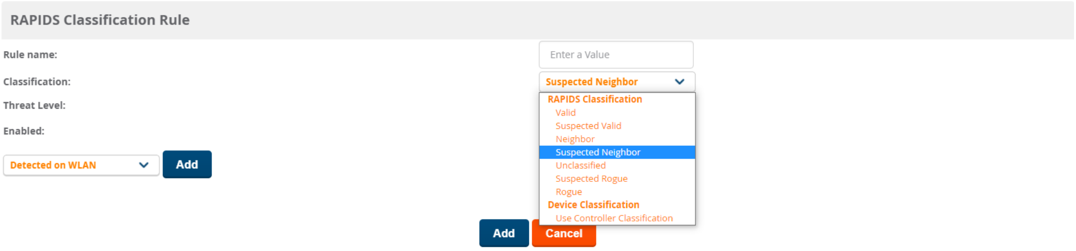
This section contains the following topics:

- Using RAPIDS Defaults for Controller Classification
- Changing RAPIDS Based on switch Classification

Using RAPIDS Defaults for Controller Classification

1. Navigate to the **RAPIDS > Rules** page and select the pencil icon beside the rule that you want to change.
2. In the **Classification** drop-down list, select **Use Controller Classification** (see Figure 22 below).
3. Click **Save**.

Figure 22 *Using Controller Classification*



RAPIDS Classification Rule

Rule name: Enter a Value

Classification: Suspected Neighbor

Threat Level:

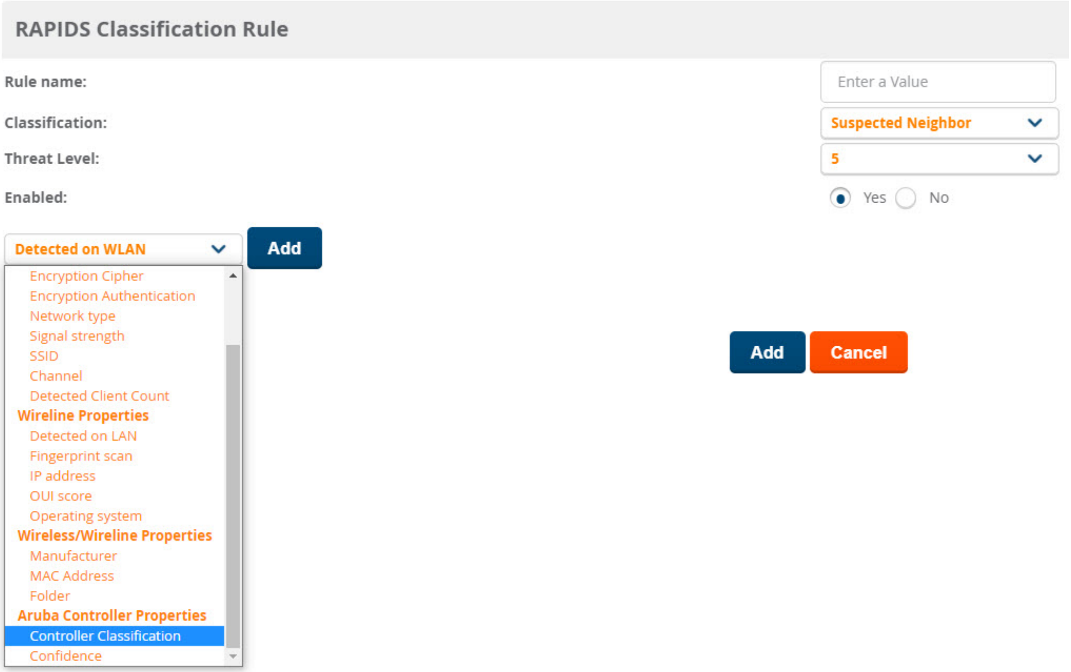
Enabled:

NOTE

OV3600 does not send its classification to the controller when the RAPIDS device classification rule is defined as **Use Controller Classification**, and the containment is enabled.

Changing RAPIDS Based on switch Classification

1. Navigate to **RAPIDS > Rules** and select the desired rule.
2. In the **Classification** menu, select the RAPIDS classification.
3. Select **Controller Classification** (see below).



RAPIDS Classification Rule

Rule name: Enter a Value

Classification: Suspected Neighbor

Threat Level: 5

Enabled: ● Yes ○ No

4. Click **Add**. A new Controller Classification field displays.

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

During network discovery for switches and ZTP on a non-factory device, the best practice is to add credentials in **Device Setup > Communication** page. For Alcatel-Lucent PVOS switches, navigate to AOS-W switch, and for Aruba-CX switches, navigate to ArubaOS-CX switch in OV3600 WebUI.

Changes to Zero-Touch Provisioning for Switches

Security enhancements in OV3600 8.2.11.1 allow OV3600 to reset the credentials of a factory-default Alcatel-Lucent switch running firmware version 16.10.008 or later during the Zero-Touch Provisioning (ZTP) process.

- If you have configured a Telnet/SSH username and password in the switch template on the **Groups > Templates** page, OV3600 will continue to push those settings to the switch.
- If you have not configured a Telnet/SSH username and password in the switch template for the switch running on the 16.10.008 firmware version or later, the OV3600 server creating an SSH connection to the switch will reset the credentials as username: **manager** and password: **<device-serial-number>**.

NOTE

For the switches running firmware earlier than 16.10.008, OV3600 takes the credential as username: **admin** and no password.

Using Templates

- If you set the credentials through a template, OV3600 applies the credentials from the template and not the default factory setting credentials.
- Make sure the device is in manage/read-write mode before pushing the configuration through a template.
- After pushing the template, the switch must be in a non-factory setting. If the switch remains in a factory setting credential, then you must add a dummy VLAN in the template to make the switch to a non-factory setting.
- Make sure the SNMPv3 password is in plain text while importing the template.

NOTE

The switch configuration logs are available in **SSH Command Log**.

- In the template variable name, do not add any special characters. Only alphabets, numerical, and underscore are allowed. Define the template variables as in the example: **%xxxxx%**.

NOTE

If both template variable and dynamic variable are present, OV3600 will consider the dynamic variable.

Commands for Switch Setup

Table 2: *Commands for AOS-W Switches*

Description	Command
Switch configuration commands for ZTP.	`amp-server ip “server ip ” group “group” folder “folder” secret  “secret”`
Switch configuration commands for enabling syslog.	`Syslog x.x.x.x`

Switch configuration command for enabling traps.	`Command=snmp-server enable traps startup-config-change`
	`Command=snmp-server enable traps running-config-change`
	`Command=snmp-server contact "name"`
	`Command=snmp-server host "ip address" trap-level all`

Run this command to see the trap-list supported on switch.	`Command=show snmp-server traps`

Table 3: *Commands for ArubaOS-CX Switches*

Description	Command

Switch default configuration.	`snmp-server vrf mgmt`
	`snmp-server vrf default`
	`snmp-server community public`

Switch VSF configuration.	`sh vsf`

Best practice for using Instant AP and Instant GUI Config are as follows:

- Always verify that the Instant AP devices in a group are either in Monitor-only mode or deleted successfully from the group in the current OV3600 before adding the Instant AP to a New OV3600.
- Always use the IGC policy corresponding to the Instant AP firmware version in the group.
- It is recommended, not to use the same certificate with multiple names. For example: **Cert.pfx** should not be replicated as **Cert1.pfx**, **Cert2.pfx** and so on.
- It is advised to remove the pending or failed firmware upgrade jobs related to Instant AP devices, and group. Retaining the pending or failed jobs may show the Instant AP in a downstate.

- If the source image is a CAD drawing, the CAD files must be generated from Autodesk's AutoCAD® software.
- Before exporting the CAD drawing, make sure that the drawing is set as fit to the view and saved. If not, the last saved view will be shown in VisualRF after importing.
- After importing the drawings, the VisualRF backup exported from an older version of OV3600 may result in a loss of image quality. To improve the image quality, export the original DWG/DXF file and create a new floor plan.
- If there are scaling, cropping, or dimension issues with a specific version of AutoCAD images, it is recommended to use SVG coordinates for rendering the image in VisualRF. The configuration parameter can be set to 1 to use SVG coordinates over DWG coordinates. Remember to reset it back to 0 after uploading the problematic image.

NOTE

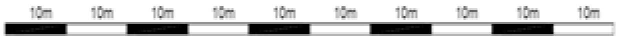
Create a new file if it does not exist. VisualRF restart is necessary after changing the parameters.

Configuration File	Parameter
/usr/local/airwave/lib/java/svg.properties	**svg.dwgtosvg.use.svg.dimension=1**

Drawing Dimension in VisualRF

- The maximum supported floor plan size is 800x800 meters (2624.67x2624.67 in feet). Always use this recommended source image dimension.
- VisualRF detects the dimension from the drawing when a CAD or SVG drawing is uploaded. If the auto-detected dimensions are not the same as the original dimensions in AutoCAD, the measuring scale in the drawings can be used.
- Using the VisualRF measure, you can measure the scale and get the correct dimension. If there is no measuring scale available in the drawing, you need to measure any door to 3 feet and save the floorplan.
- Use the same unit of measurement in all the layouts when an exported drawing file from AutoCAD has many layouts.
- The DWG file should be viewable from any commonly used DWG viewer software. It should match the dimension given in AutoCAD.
- It is recommended to add a measuring scale while saving the DWG file from AutoCAD as in Figure 23.

Figure 23 *Measuring Scale*



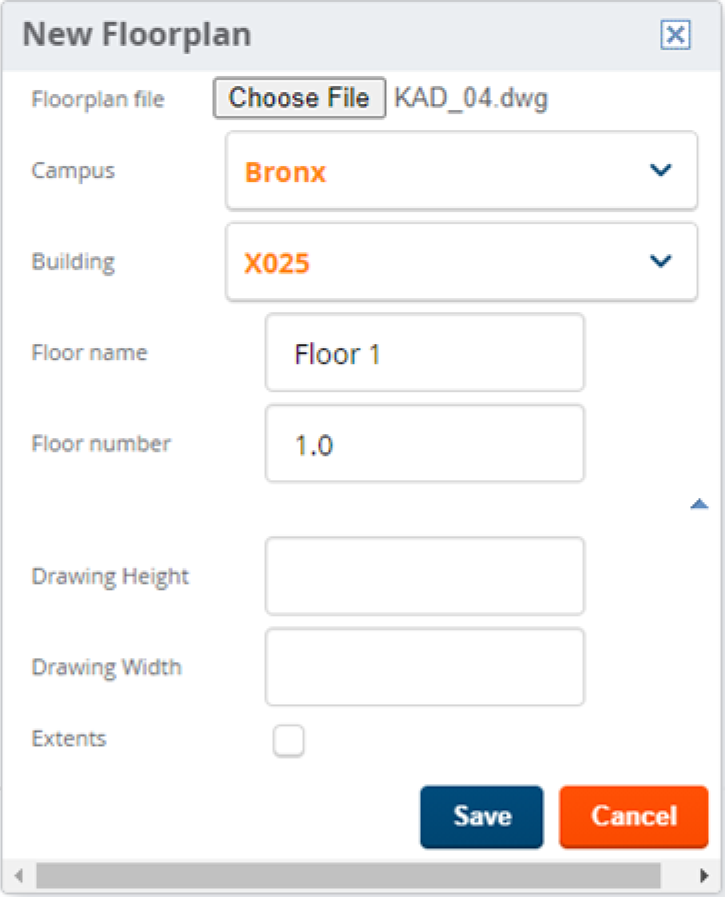
Adding the Drawing Dimension in New Floorplan

OV3600 WebUI allows you to manually specify the height and width of the drawing if the VisualRF fails to read the correct dimension from the AutoCAD drawing.

To add the drawing height and width:

1. Navigate to **VisualRF > Floorplans** page.
2. Click **Edit > New Floorplan**.
3. Choose the drawing in the **Floorplan file**. A drop-down icon appears on the bottom right corner of the **New Floorplan** window. Figure 24
4. Specify the **Drawing Height** and **Drawing Width**.
5. Check the box next to **Extents** for DWG and DXF drawings.
6. Click **Save**.

Figure 24 *New Floorplan*



Floorplan file: KAD_04.dwg

Campus: Bronx

Building: X025

Floor name: Floor 1

Floor number: 1.0

Drawing Height

Drawing Width

Extents □

Wall Attenuation

VisualRF performance degrades if there are more than 200 walls in Ekahau backup. VisualRF supports a maximum of 200 walls from CAD images while creating the floor plan. While importing Ekahau backup to VisualRF the wall types are mapped automatically with Alcatel-Lucent-OV3600 standard and do not match the wall type defined in Ekahau.

Wall Type	Parameter
Glass wall	0-2 db
Cubicle wall	3-5 db

Wall Type	Parameter
Dry wall	6-14 db
Concrete wall	15-29 db
Elevator Shaft	30 db and above

Configuration Parameters to lower the Security Checks

FromOmniVista 3600 Air Manager 8.2.14.0, it blocks XSS and XXE vulnerabilities. VisualRF will validate the XML payload before processing the request. If any of the floor plan image sources **(.svg)** files have a vulnerable tag, then the OV3600 blocks the images. If the images are from trusted sources, you can lower the security checks using the below configuration parameters in the **svg.properties** configuration file and then upload.

- Set the configuration parameter values to 0 to accept the risk and the default parameter is 1.

Configuration File	Parameter
/usr/local/airwave/lib/java/svg.properties	**svg.set.xml.parser.feature.disallow-doctype-decl=0** **svg.set.xml.parser.feature.load-external-dtd=0** **svg.set.xml.parser.feature.external-parameter-entities=0** **svg.set.xml.parser.feature.external-general-entities=0** **svg.set.xml.parser.feature.secure-processing=0**

NOTE

Create a new file if it does not exist. VisualRF restart is necessary after changing the parameters.

Appendix A
OV3600 Data Acquisition Methods

The tables below describe the different methods through which OV3600 acquires data from Alcatel-Lucent devices on the network.

The tables use the following symbols:

- ← Initiated by OV3600
- → Initiated by Controller, or Instant Virtual Controller
- ↑ Initiated by OV3600 to a separate device

Table 4: *Data Flow between Controllers and OV3600*

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
802.11 Counters	←											
AppRF				→								
AP Up/Down Status	←	→										
ARM Events				→								
Channel Utilization				→								
Clarity				→								
Client Hostname											↑	
Client Match Events				→								
Client Monitoring	←			→								If Prefer AMON enabled it's done by AMON.

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
												Requires Alcatel-Lucent AOS-W 6.3 or later and OV3600 7.7.7 or later.
Configuration Audit			←									
Configuration Push			←									
Controller Up/Down Status	←							←				
Device CPU/Memory	←											
Exec UI							→					When AMON is used for client monitoring, OV3600 uses this at startup time to get current user status.
Firewall Stats				→								
Firmware Images							↑			←		Images are sent to controller over FTP/TFTP. They can be transferred to

Data Type	SNMP	Traps	SSH	AMON	PAPI	Syslog	HTTPS	ICMP	NMAP	FTP/TFTP	DNS	Notes
												OV3600 via HTTPS.
IDS Events		→										
Interface Monitoring	←											
Lync/UCC/Voice				→								Available in OV3600 8.0 and later.
Neighbor Clients	←			→								
Network Derivations			←									
RADIUS Auth Issues		→										
RAPIDS	←											
RF Capacity				→								
RF Health				→								
Rogue AP OS									↑			
Rogue Classification	←				←							
Rogue Clients	←											
Syslog						→						
VisualRF	←			→								VisualRF's client data comes from OV3600, which gets its data from SNMP + AMON.

Table 5: *Data Flow between Instant Devices and OV3600*

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

Appendix A
Increasing Location Accuracy

This appendix describes the impact that band steering can have on location accuracy. It also explains how RTLS can be used to increase location accuracy.

Band steering can negatively impact location accuracy when testing in a highly mobile environment. The biggest hurdles to overcome are scanning times in 5 GHz frequency.

Table 6: *Location accuracy impact*

Operating Frequency	Total Channels	Scanning Frequency	Scanning Time	Total Time One Pass
2.4 GHz	11 (US)	10 seconds	110 milliseconds	121.21 seconds
5 GHz	24 (US)	10 seconds	110 milliseconds	242.64 seconds

This section provides instructions for integrating the OV3600 and Alcatel-Lucent WLAN infrastructure with Alcatel-Lucent's RTLS feed to more accurately locate wireless clients and Wi-Fi Tags.

Deployment Topology

Figure 25 *Typical Client Location*

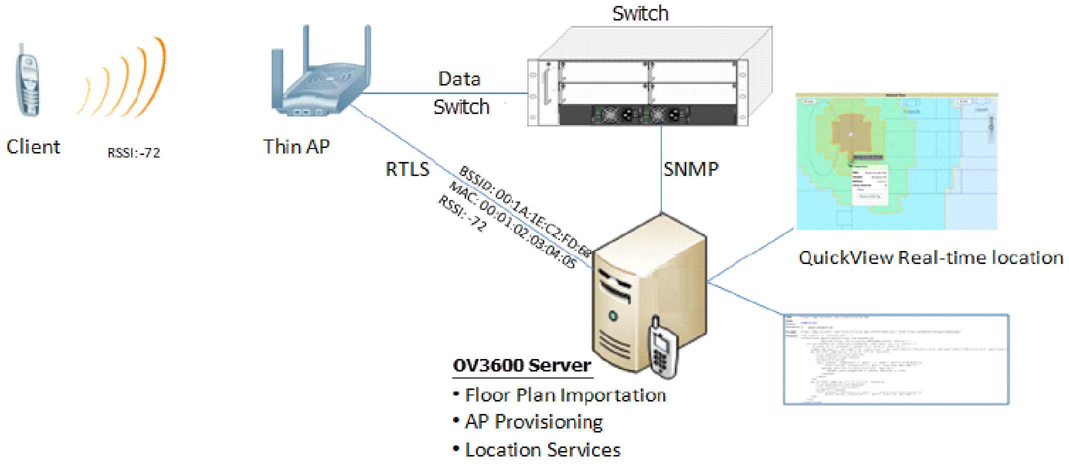
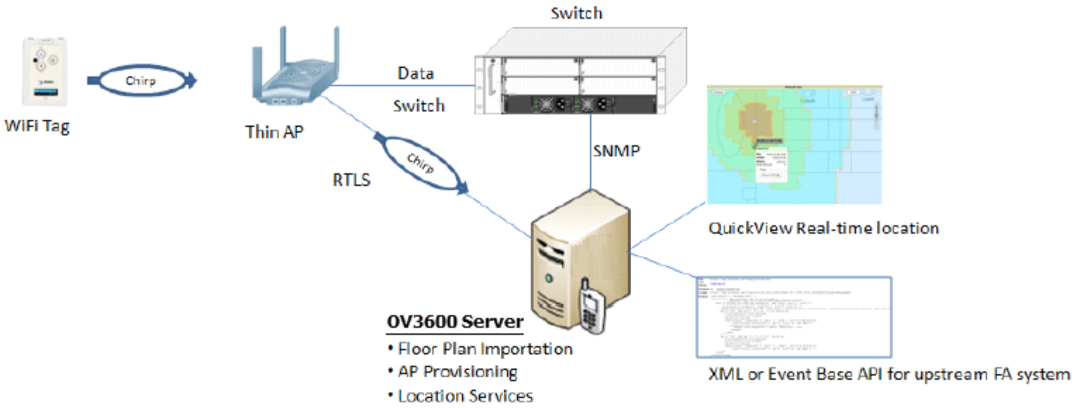


Figure 26 *Typical Tag Deployment*



Prerequisites

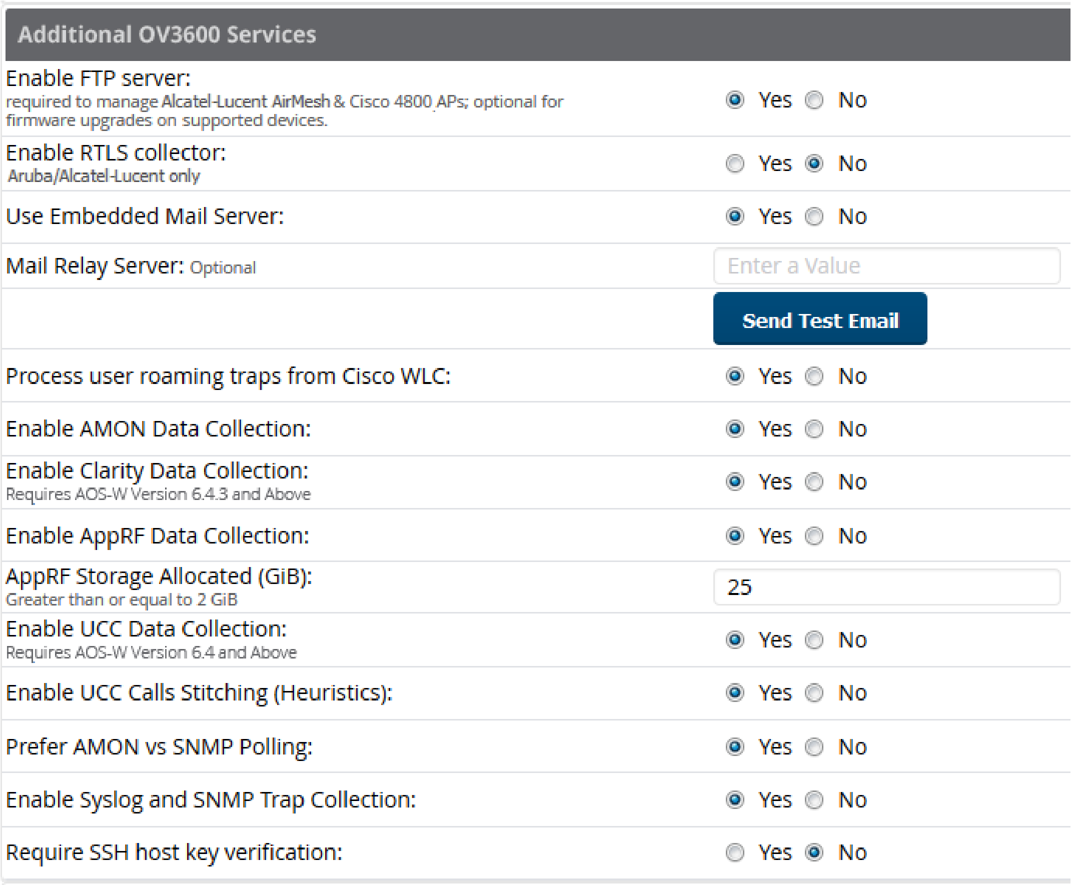
You will need the following information to monitor and manage your Alcatel-Lucent infrastructure.

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

Enable RTLS Service on the OV3600 Server

1. Navigate to **OV3600 Setup > General** and locate the **Additional OV3600 Services** section.
2. Select **Yes** for the **Enable RTLS Collector** option (see Figure 27 below).
3. A new section will automatically appear with the following settings:
    - **RTLS Port**—The match switch default is 5050.
    - **RTLS Username—**This must match the SNMPv3 MMS user name configured on the switch.
    - **RTLS Password—**This must match the SNMPv3 MMS password configured on the switch.
4. Click **Save**.

Figure 27 *RTLS Fields in* ***OV3600 Setup> General> Additional OV3600 Services***



Additional OV3600 Services

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

Enable RTLS on the switch

> **NOTE**
>
> RTLS can only be enabled on the conductor switch and it will automatically be propagated to all local switches.

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

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

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

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

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

To validate exit configuration mode:

```
(switch-Name) # show ap monitor debug status ip-addr <AP-IP-Address>
...
RTLS configuration
-------------------
Type       Server IP   Port Frequency Active
----       ---------   ---- --------- ------
MMS        10.51.2.45  5070  120
Aeroscout  N/A         N/A   N/A
```

```
RTLS        10.51.2.45   5050   60          *
```

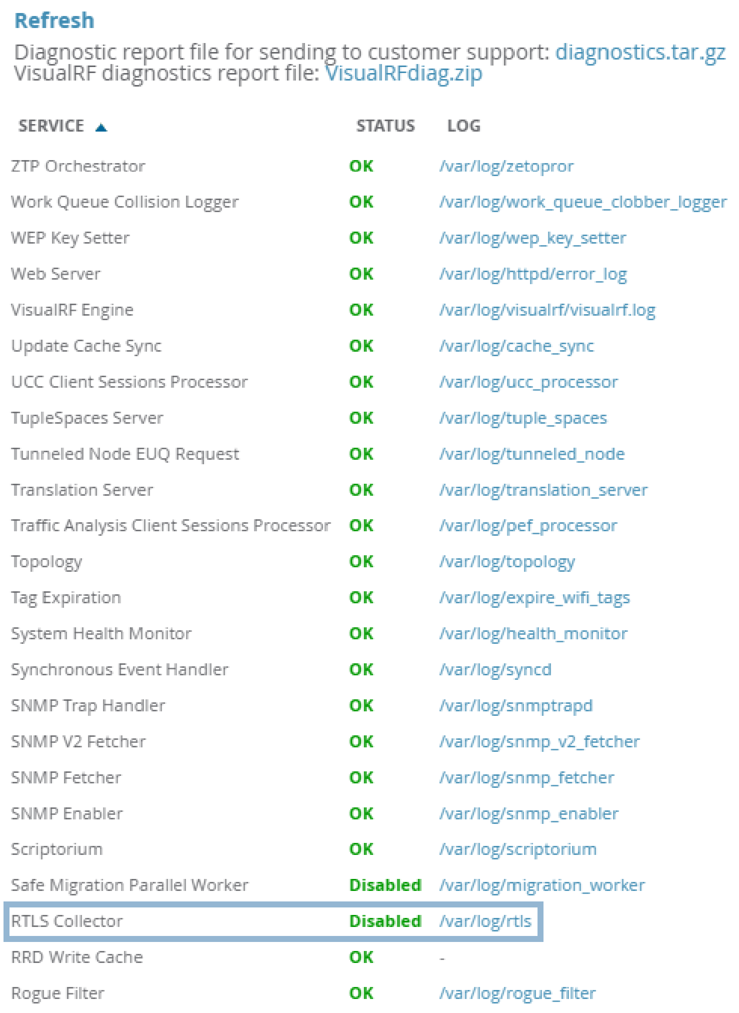
Troubleshooting RTLS

You can use either the WebUI or CLI to ensure the RTLS service is running on your OV3600 server.

Using the WebUI to See Status

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

Figure 28 *RTLS System Status*



Refresh

Diagnostic report file for sending to customer support: diagnostics.tar.gz
VisualRF diagnostics report file: VisualRFdiag.zip

SERVICE ▲	STATUS	LOG
ZTP Orchestrator	OK	/var/log/zetopror
Work Queue Collision Logger	OK	/var/log/work_queue_clobber_logger
WEP Key Setter	OK	/var/log/wep_key_setter
Web Server	OK	/var/log/httpd/error_log
VisualRF Engine	OK	/var/log/visualrf/visualrf.log
Update Cache Sync	OK	/var/log/cache_sync
UCC Client Sessions Processor	OK	/var/log/ucc_processor
TupleSpaces Server	OK	/var/log/tuple_spaces
Tunneled Node EUQ Request	OK	/var/log/tunneled_node
Translation Server	OK	/var/log/translation_server
Traffic Analysis Client Sessions Processor	OK	/var/log/pef_processor
Topology	OK	/var/log/topology
Tag Expiration	OK	/var/log/expire_wifi_tags
System Health Monitor	OK	/var/log/health_monitor
Synchronous Event Handler	OK	/var/log/syncd
SNMP Trap Handler	OK	/var/log/snmptrapd
SNMP V2 Fetcher	OK	/var/log/snmp_v2_fetcher
SNMP Fetcher	OK	/var/log/snmp_fetcher
SNMP Enabler	OK	/var/log/snmp_enabler
Scriptorium	OK	/var/log/scriptorium
Safe Migration Parallel Worker	Disabled	/var/log/migration_worker
RTLS Collector	Disabled	/var/log/rtls
RRD Write Cache	OK	-
Rogue Filter	OK	/var/log/rogue_filter

Wi-Fi Tag Setup Guidelines

- Ensure that the tags can be heard by at least three access points from any given location. The recommended value is four APs.
- Ensure that the tags chirp on all regulatory channels.